ETF – ELEKTROTEHNIČKI FAKULTET
UNIVERZITET U BEOGRADU
Bulevar kralja Aleksandra 73, PF 3554, 11120 Beograd, Srbija
+381 (0) 11 - Tel 3248464, Fax 3248681, Račun 840-1438666-48

Katedra za telekomunikacije
+381 (0) 11 - Tel 3218422, Fax 3218399, e-mail: radio_lab@etf.rs

STUDIJA IZVODLJIVOSTI IZGRADNJE NACIONALNOG CERT-A

Odgovorni projektant:

Prof. dr Aleksandar Nešković, dipl.ing.

Александар М. Нешковић дипл. инж. ел. 353 4448 03 — Инжењерска комора Србије — Одговорни пројектант

Projektanti:

Dr Nenad Krajnović, dipl.ing.

Ненад Д. Крајновић дипл. инж. ел. 353 1041 03 — Инжењерска комора Србије — Одговорни пројектант

Prof. dr Nataša Nešković, dipl.ing.

Наташа Ј. Нешковић дипл. инж. ел. 353 4449 03 — Инжењерска комора Србије — Одговорни пројектант

BEOGRAD, 2016.

SADRŽAJ

I ZAKONSKA DOKUMENTACIJA

OSNOVNI PODACI O INVESTITORU

Poslovno ime:

REGULATORNA AGENCIJA ZA ELEKTRONSKE KOMUNIKACIJE I POŠTANSKE USLUGE

Skraćeno poslovno ime:

RATEL

Pravna forma: Nezavisna regulatrona organizacija sa svojstvom pravnog lica

Matični broj: 17606590

Sedište:

Opština: Beograd (grad)
Mesto: Beograd (grad)
Ulica i broj: Palmotićeva 2
PAK 106306

Datum osnivanja: maj 2005.

Početak rada: 19.05.2005

Šifra delatnosti: 83.14

Ostali identifikacioni podaci:

Poreski identifikacioni broj PIB: 103986571

Žiro-račun: 840-963627-41

Kontakt centar: 011/32 42 673

Faks: 011/32 32 537

Internet stranica: www.ratel.rs

E-mail: ratel@ratel.rs

Посл. бр.	I Fi 90/07

TRGOVINSKI суд у BEOGRADU судија Tatjana Vlaisavljević

као судија појединац у судскорегистарској правној ствари предлагача Elektrotehnički fakultet Univerziteta u Beogradu, Beograd, Ul. Bulevar revolucije br.73

ради уписа proširenja delatnosti, promene naziva, promene podataka od značaja za pravni promet koje se odnose na sedište.

дана 16.03.2007.god., донео је

РЕШЕЊЕ

Усваја се захтев предлагача за упис у судски регистар и одређује се упис у судски регистар, у регистарски уложак

бр. 5-11-00, података садржаних у прилозима уз пријаву бр. 1,3.

који су саставни део овог решења.

Судија,

Tatjana Vlaisavljević, s.r.

За тачност отправка overava:

Поука о правном леку: Против овог решења може се изјавити жалба, преко овог суда, Višem trgovinskom суду у BEOGRADU, у року од 8 дана од дана достављања преписа решења.

САВРЕМЕНА • Београд
образац бр.: 950140

4. ПРЕПИС РЕШЕЊА

Фирма и седиште субјекта уписа	**Elektrotehnički fakultet Univerziteta u Beogradu** **B e o g r a d**	Прилог уз решење број	**1**

Број регистарског улошка регистарског суда и његово седиште	**5-11-00 Trgovinski sud, Beograd**

Датум уписа	Ознака и број решења	Број уписа	Назив суда
16.03.2007.god.	I Fi 90/07	6	T.S.Beograd

1. Фирма и седиште субјекта уписа и његов матични број

Univerzitet u Beogradu - Elektrotehnički fakultet
Skraćeni naziv: Elektrotehnički fakultet u Beogradu
Sedište: Beograd, Bulevar kralja Aleksandra br. 73
Matični broj: 7032498
Broj računa: 840-1438660
PIB: 100206130

2. Овлашћење субјекта уписа у правном промету

Fakultet je pravno lice i ima pravo da u prometu zaključuje ugovore i preduzima druge pravne poslove i pravne radnje u okviru svoje pravne i poslovne sposobnosti.

3. Врста и обим одговорности за обавезе субјекта уписа у правном промету и врста и обим одговорности за обавезе других субјеката

Fakultet odgovara za svoje obaveze u pravnom prometu celokupnom svojom imovinom.

4. Одговорност оснивача за обавезе субјекта уписа

Osnivač odgovara za obaveze u skladu sa Zakonom.

Судија,
Tatjana Vlaisavljević ,s.r.
за тачност отправка оверава:

Следи наставак број:	4. Прилог уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.

ОБРАЗАЦ: Прилог уз решење број 1

Издавач: ЈП Службени лист СРЈ, Београд

Прилог уз решење број	2

Број регистарског улошка регистарског суда и његово седиште	X-Fi.738/03 10.03.2003. god. 5-11-00 TS BEOGRAD

Редни број	Фирма, односно назив и седиште, ознака регистра и број регистарског уписа, матични број и број рачуна оснивача односно име и адреса, лични број и број личне карте оснивача и члана	Број и датум акта о оснивању	Датум приступања
1	2	3	4
1	REPUBLIKA SRBIJA	Uredba Vlade od 21.6.1948.g.	
2			
3			
4			
5			

4. Прилог уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.

ОБРАЗАЦ: **Прилог уз решење број 2**

Прилог уз решење број	2

Редни број	Укупан износ улога оснивача и члана	Врста и обим одговорности за обавезе субјекта уписа	Датум иступања
5	6	7	8
1			
2			
3			
4			
5			

Уписани и уплаћени основни капитал; повећање, односно смањење основног капитала.

Судија,

Liliana Milovanc

за тачност отправка

4. Прилог уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.

ОБРАЗАЦ: **Прилог уз решење број 2**

	Прилог уз решење број	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T.S.Beograd

Датум уписа	Ознака и број решења	Број уписа	Назив суда
16.03.2007.god.	I Fi 90/07	7	T.S.Beograd

1. Делатности, односно послови и послови спољнотрговинског промета субјекта уписа

Delatnosti Fakulteta su:

Podgrupa	Naziv i opis delatnosti
	Visoko obrazovanje
80322	Tehnički fakulteti
80312	Više tehničke škole
80319	Ostale više škole
80420	Obrazovanje odraslih i ostalo obrazovanje na drugom mestu nepomenuto.
22110	Izdavanje knjiga, brošura i drugih publikacija.
22130	Izdavanje časopisa i sličnih periodičnih izdanja.
30020	Proizvodnja računarskih mašina i druge opreme za obradu podataka.
31100	Proizvodnja električnih motora, generatora i transformatora.
31200	Proizvodnja opreme za distribuciju električne energije i upravljačke opreme.
31610	Proizvodnja električne opreme za motore i vozila na drugom mestu nepomenuto.
32100	Proizvodnja elektronskih lampi i cevi i drugih elektronskih komponenata.
32200	Proizvodnja televizijskih i radio predajnika i aparatura za telefoniju i telegrafiju.

Sudija,

Tatjana Vlaisavljević, s.r.

za tačnost otpravka overava:

Следи наставак број: 1	4. Прилог уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.

ОБРАЗАЦ: Прилог уз решење број 3

Издавач: ЈП Службени лист СРЈ, Београд
Ознака за поруџбину: Обр. бр 161541

	ПРИЛОГ УЗ РЕШЕЊЕ БРОЈ	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T.S.Beograd I Fi 90/07 16.03.2007.god.

Датум уписа	Ознака и број решења	Број уписа	Назив суда

1 Делатности, односно послови и послови спољнотрговинског промета субјекта уписа

1.	2.
32300	Proizvodnja televizijskih i radio-prijemnika, aparata za snimanje i reprodukciju zvuka ili slike i proizvodnja pratećeg pribora.
33102	Proizvodnja ortopedskih aparata, ostala medicinska oprema i instrumenata.
33200	Proizvodnja kontrolnih i mernih instrumenata i aparata osim opreme za upravljanje u industrijskim procesima.
33300	Proizvodnja oprema za upravljanje u industrijskim procesima.
33400	Proizvodnja optičkih instrumenata i fotografske opreme.
34300	Proizvodnja delova i pribora za motorna vozila i njihove motore.
45310	Postavljanje električnih instalacija i opreme.
45340	Ostali instalacioni radovi.
52470	Trgovina na malo sa knjigama, novinama i pisaćim materijalom.
52480	Ostala trgovina na malo.
64200	Telekomunikacije.
71330	Iznajmljivanje kancelarijskih mašina i opreme uključujući i kompjutere.
71340	Iznajmljivanje ostalih mašina i opreme, na drugom mestu nepomenuto.
74130	Istraživanje tržišta i ispitivanje javnog mnjenja.
74830	Sekretarske i prevodilačke aktivnosti.

Судија,
Tatjana Vlaisavljević, s.r.
za tačnost otpravka overava:

Следи наставак број: 2	4. ПРИЛОГ УЗ ПРЕПИС РЕШЕЊА

Овлашћено лице потписује само прилог уз пријаву, а судија - прилог уз изворник решења и регистарски лист.
ОБРАЗАЦ: **Прилог уз решење број 3**

• САВРЕМЕНА • Београд
образац бр.: **950133**

	Прилог уз решење број	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T.S.Beograd

Датум уписа	Ознака и број решења	Број уписа	Назив суда
16.03.2007.god.	I Fi 90/07	7	T.S.Beograd

1. Делатности, односно послови и послови спољнотрговинског промета субјекта уписа

Delatnosti Fakulteta su:

Podgrupa	Naziv i opis delatnosti
	Visoko obrazovanje
80322	Tehnički fakulteti
80312	Više tehničke škole
80319	Ostale više škole
80420	Obrazovanje odraslih i ostalo obrazovanje na drugom mestu nepomenuto.
22110	Izdavanje knjiga, brošura i drugih publikacija.
22130	Izdavanje časopisa i sličnih periodičnih izdanja.
30020	Proizvodnja računarskih mašina i druge opreme za obradu podataka.
31100	Proizvodnja električnih motora, generatora i transformatora.
31200	Proizvodnja opreme za distribuciju električne energije i upravljačke opreme.
31610	Proizvodnja električne opreme za motore i vozila na drugom mestu nepomenuto.
32100	Proizvodnja elektronskih lampi i cevi i drugih elektronskih komponenata.
32200	Proizvodnja televizijskih i radio predajnika i aparatura za telefoniju i telegrafiju.

Судија,

Tatjana Vlaisavljević, s.r.

За тачност отправка оверава:

Следи наставак број: 1	4. Прилог уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.

ОБРАЗАЦ: Прилог уз решење број 3

Издавач: ЈП Службени лист СРЈ, Београд
Ознака за поруџбину: Обр. бр. 161541

	Наставак прилога уз решење број	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T .S.Beograd I Fi 90/07 16.03.2007.god.
Наставак: 2	

1.	2.
74840	Ostale poslovne aktivnosti, na drugom mestu nepomenute.
72100	Pružanje saveta u vezi sa kompjuterskom opremom.
72200	Pružanje saveta i izrada kompjuterskih programa.
72300	Obrada podataka.
72400	Izgradnja baze podataka.
72600	Ostale aktivnosti u vezi sa kompjuterima.
73101	Istraživanje i eksperimentalni razvoj u prirodno-matematičkim naukama.
73102	Istraživanje i eksperimentalni razvoj u tehničko-tehnološkim naukama.
73105	Istraživanje i eksperimentalni razvoj u multidisciplinarnim naukama.
73109	Istraživanje i eksperimentalni razvoj u prirodnim naukama.
74140	Konsalting i menadžment poslovi. Holding poslovi.
74150	Arhitektonski i inženjerske aktivnosti i tehnički saveti.
74202	Projektovanje građevinskih i drugih objekata.
74203	Inženjering: inženjering, vođenje projekata i tehničke aktivnosti.

Судија,
Tatjana Vlaisavljević ,s.r.
za tačnost otpravka overava:

Следи наставак број: 3	4. Наставак прилога уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист

ОБРАЗАЦ: Наставак прилога уз решење

Издавач: ЈП Службени лист СРЈ, Београд
Ознака за поруџбину: Обр. бр 161611

	ПРИЛОГ УЗ РЕШЕЊЕ БРОЈ	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T.S.Beograd

Датум уписа	Ознака и број решења	Број уписа	Назив суда
16.03.2007.god.	I Fi 90/07		

1 Делатности, односно послови и послови спољнотрговинског промета субјекта уписа

1.	2.
74204	Ostale arhitektonske i inženjerske aktivnosti i tehnički saveti.
74300	Tehničko ispitivanje i analiza.
74112	Ostali pravni poslovi: veštačenje.
92511	Delatnost biblioteka.
55510	Kantine.
55300	Restorani.

Судија,

Tatjana Vlaisavljević ,s.r.

За тачност отправка оверава:.....

Следи наставак број:	4. ПРИЛОГ УЗ ПРЕПИС РЕШЕЊА

Овлашћено лице потписује само прилог уз пријаву, а судија - прилог уз изворник решења и регистарски лист.
ОБРАЗАЦ: **Прилог уз решење број 3**

• САВРЕМЕНА • Београд
образац бр.: **950133**

	Наставак прилога уз решење број	3

Број регистарског улошка регистарског суда и његово седиште	5-11-00 T .S.Beograd I Fi 90/07 16.03.2007.god.
Наставак: 2	

1.	2.
74840	Ostale poslovne aktivnosti, na drugom mestu nepomenute.
72100	Pružanje saveta u vezi sa kompjuterskom opremom.
72200	Pružanje saveta i izrada kompjuterskih programa.
72300	Obrada podataka.
72400	Izgradnja baze podataka.
72600	Ostale aktivnosti u vezi sa kompjuterima.
73101	Istraživanje i eksperimentalni razvoj u prirodno-matematičkim naukama.
73102	Istraživanje i eksperimentalni razvoj u tehničko-tehnološkim naukama.
73105	Istraživanje i eksperimentalni razvoj u multidisciplinarnim naukama.
73109	Istraživanje i eksperimentalni razvoj u prirodnim naukama.
74140	Konsalting i menadžment poslovi. Holding poslovi.
74150	Arhitektonski i inženjerske aktivnosti i tehnički saveti.
74202	Projektovanje gradjevinskih i drugih objekata.
74203	Inženjering: inženjering, vodjenje projekata i tehničko aktivnosti.

Судија,
Tatjana Vlaisavljević ,s.r.
za tačnost otpravka overava:

Следи наставак број: 3	4. Наставак прилога уз препис решења

Овлашћено лице потписује само прилог уз пријаву, а судија — прилог уз изворник решења и регистарски лист

ОБРАЗАЦ: Наставак прилога уз решење

Издавач: ЈП Службени лист СРЈ, Београд
Ознака за поруџбину: Обр. бр 161611

Посл. бр. 2 Фи 509/2015

Привредни суд у Београду судија Љиљана Вуковић

као судија појединац у судскорегистарској правној ствари предлагача Универзитет у Београду -

Електротехнички факултет, Београд, ул. Булевар краља Александра бр.73

ради уписа Промене лица овлашћеног за заступање

дана 05.10.2015. г., донео је

Р Е Ш Е Њ Е

Усваја се захтев предлагача за упис у судски регистар и одређује се упис у судски регистар, у регистарски уложак

бр. 5-11-00, података садржаних у прилозима уз пријаву бр. 4

који су саставни део овог решења.

Република Србија Привредни суд у Београду II Београд

Судија,

Љиљана Вуковић

Поука о правном леку: Против овог решења може се изјавити жалба, преко овог суда, Привредном апелационом

суду у Београду у року од 8 дана од дана достављања преписа решења.

4. Препис решења

Издавач: ЈП „Службени гласник", Београд
Ознака за поруџбину: Обр. бр. 161451

	ПРИЛОГ УЗ РЕШЕЊЕ БРОЈ	**4**

Број регистарског улошка регистарског суда и његово седиште	5 – 11 – 00 Привредни суд у Београду

Датум уписа	Ознака и број решења	Број уписа	Назив суда
05.10.2015.g.	2 Fi 509/15	18	Privredni sud u Beogradu

1 Имена лица овлашћених за заступање субјекта уписа и границе њихових овлашћења

Уписује се др. ЗОРАН ЈОВАНОВИЋ, редовни професор, за декана Електротехничког факултета Универзитета у Београду, са неограниченим овлашћењима, ЈМБГ 1208953710475

брише се

др Бранко Ковачевић, редовни професор, у својству декана Електротехничког факултета Универзитета у Београду, са неограниченим овлашћењима, ЈМБГ 2906951714026

2 Имена лица овлашћених за заступање субјекта уписа у обављању послова спољнотрговинског промета и границе њихових овлашћења

Судија,

Милош Ђурђевић

Следи наставак број:	4. ПРИЛОГ УЗ ПРЕПИС РЕШЕЊА

Овлашћено лице потписује само прилог уз пријаву, а судија – прилог уз изворник решења и регистарски лист.
ОБРАЗАЦ: **Прилог уз решење број 4**

дм/зм

Р Е П У Б Л И К А С Р Б И Ј А
МИНИСТАРСТВО ЖИВОТНЕ СРЕДИНЕ,
РУДАРСТВА И ПРОСТОРНОГ ПЛАНИРАЊА
Сектор за грађевинарство, инвестиције и
грађевинско земљиште
Број: 351-02-01199/2006-07
Датум: 15.11.2011. године
Немањина 22-26

Решавајући по захтеву Електротехничког факултета Универзитета у Београду - Београд, Краља Александра бр. 73, за издавање лиценце за израду техничке документације за објекте за које грађевинску дозволу издаје министарство надлежно за послове грађевинарства, или надлежни орган аутономне покрајине на основу члана 16. Закона о министарствима ("Службени гласник РС", бр. 16/11), члана 126. став 4. и члана 222. став 2. Закона о планирању и изградњи ("Службени гласник РС", бр. 72/2009, 81/2009, 64/2010 и 24/2011), и члана 192. Закона о општем управном поступку ("Службени лист СРЈ", бр. 33/1997 и 31/2001 и "Службени гласник РС", бр. 30/2010), по овлашћењу министра животне средине, рударства и просторног планирања број: 021-01-10/2011 од 28.03.2011. године, помоћник министра доноси

Р Е Ш Е Њ Е

1. Утврђује се да **Електротехнички факултет Универзитета у Београду - Београд, Краља Александра бр. 73, ИСПУЊАВА УСЛОВЕ** за добијање лиценце за израду техничке документације за објекте за које грађевинску дозволу издаје министарство надлежно за послове грађевинарства, или надлежни орган аутономне покрајине и то:

П050Е4 – пројеката управљања електромоторним погонима – аутоматика, мерења и регулација за хидроелектране са припадајућом браном снаге 10 и више MW
П052Е4 – пројеката управљања електромоторним погонима – аутоматика, мерења и регулација за термоелектране снаге 10 и више MW
П061Е1 – пројеката електроенергетских инсталација високог и средњег напона за далеководе напона 110 и више KV

П062Е1 – пројеката електроенергетских инсталација високог и средњег напона за трафостанице напона 110 и више KV

П150Е3 – пројеката телекомуникационих мрежа и система за телекомуникационе објекте, односно мреже, системе или средства која су међународног и магистралног значаја

П151Е3 – пројеката телекомуникационих мрежа и система за телекомуникационе објекте, односно мреже, системе или средства која се граде на територији две или више општина

О б р а з л о ж е њ е

Електротехнички факултет Универзитета у Београду - Београд, Краља Александра бр. 73, поднело је овом министарству 07.10.2011. године захтев број: 351-02-01199/2006-07 за издавање лиценце за израду техничке документације за објекте за објекте за које грађевинску дозволу издаје министарство надлежно за послове грађевинарства, или надлежни орган аутономне покрајине.

Уз захтев за издавање лиценце достављена је сва потребна документација прописана чланом 126. Закона о планирању и изградњи ("Службени гласник РС", бр. 72/09, 81/09, 64/10 и 24/11) и чланом 4. Правилника о начину, поступку и садржини података за утврђивање испуњености услова за издавање лиценце за израду техничке документације и лиценце за грађење објеката за које одобрење за изградњу издаје министарство, односно аутономна покрајина, као и о условима за одузимање тих лиценци ("Службени гласник РС", бр. 114/04).

На седници стручне комисије образоване од стране министра, одржаној дана 15.11.2011. године утврђено је да подносилац захтева испуњава услове за добијање наведене лиценце, у смислу одредби чл. 126. Закона о планирању и изградњи и чл. 7. и чл. 14. Правилника о начину, поступку и садржини података за утврђивање испуњености услова за издавање лиценце за израду техничке документације и лиценце за грађење објеката за које одобрење за изградњу издаје министарство, односно аутономна покрајина, као и о условима за одузимање тих лиценци.

На основу изнетог, на предлог стручне комисије и члана 192. Закона о општем управном поступку, одлучено је као у диспозитиву решења.

Такса за ово решење наплаћена је у износу од 16.570,00 (шеснаестхиљадапетстотинаседамдесет) динара.

Упутство о правном средству: Ово решење је коначно у управном поступку и против њега се не може изјавити жалба, али се може покренути управни спор тужбом код Управног суда Србије у року од 30 дана од дана достављања.

Решење доставити: **подносиоцу захтева**, надлежној инспекцији и архиви овог министарства.

ПОМОЋНИК МИНИСТРА

Александра Дамњановић-Петровић, дипл.правник

ETF – ELEKTROTEHNIČKI FAKULTET
UNIVERZITET U BEOGRADU
Bulevar kralja Aleksandra 73, PF 3554, 11120 Beograd, Srbija
+381 (0) 11 - Tel 3248464, Fax 3248681, Račun 840-1438666-48, ETF-sopstveni prihodi

Katedra za telekomunikacije
+381 (0) 11 - Tel 3218422, Fax 3218399, e-mail: radio_lab@etf.rs

Na osnovu odredbi člana 126. i 128. Zakona o planiranju i izgradnji ("Službeni glasnik RS" broj 72/2009, 81/2009 - ispr., 64/2010 – odluka US, 24/2011, 121/2012, 42/2013 - odluka US, 50/2013 - odluka US, 98/2013 - odluka US, 132/2014 i 145/2014), kao i shodno Odluci fakulteta, donosim:

REŠENJE O ODREĐIVANJU PROJEKTANATA NA IZRADI

STUDIJE IZVODLJIVOSTI IZGRADNJE NACIONALNOG CERT-A

Ovlašćujem kao odgovornog projektanta

prof. dr Aleksandra Neškovića, dipl.ing.,

projektante

dr. Nenada Krajnovića, dipl. ing.,
prof. dr Natašu Nešković, dipl.ing.,

i saradnike

Slobodana Radovanovića, dipl.ing.,
mr Irenu Marković, dipl. ing, i
Majdu Petrić, dipl.ing.-master

za projektovanje - izradu investiciono-tehničke dokumentacije.

Za Elektrotehnički fakultet

Prof. dr Zoran Jovanović, dekan

ИНЖЕЊЕРСКА КОМОРА СРБИЈЕ

ЛИЦЕНЦА

ОДГОВОРНОГ ПРОЈЕКТАНТА

На основу Закона о планирању и изградњи и
Статута Инжењерске коморе Србије

УПРАВНИ ОДБОР ИНЖЕЊЕРСКЕ КОМОРЕ СРБИЈЕ
утврђује да је

Александар М. Нешковић

дипломирани инжењер електротехнике

ЈМБ 0312968710348

одговорни пројектант

телекомуникационих мрежа и система

Број лиценце

353 4448 03

У Београду,
13. новембра 2003. године

ПРЕДСЕДНИК КОМОРЕ
Милош Лазовић

Проф. др Милош Лазовић
дипл. грађ. инж.

Број: 12-02/196906
Београд, 16.11.2015. године

На основу члана 75. Статута Инжењерске коморе Србије ("СГ РС", бр. 88/05 и 16/09), а на лични захтев члана Коморе, Инжењерска комора Србије издаје

П О Т В Р Д У

Којом се потврђује да је Александар М. Нешковић, дипл.инж.ел.
лиценца број

353 4448 03

за

одговорног пројектанта телекомуникационих мрежа и система

на дан издавања ове потврде члан Инжењерске коморе Србије, да је измирио обавезу плаћања чланарине Комори закључно са 13.11.2016. године, као и да му одлуком Суда части издата лиценца није одузета.

М.П.

Председник Инжењерске коморе Србије

Проф. др Милисав Дамњановић, дипл. инж. арх.

ИНЖЕЊЕРСКА КОМОРА СРБИЈЕ

ЛИЦЕНЦА

ОДГОВОРНОГ ПРОЈЕКТАНТА

На основу Закона о планирању и изградњи и
Статута Инжењерске коморе Србије

УПРАВНИ ОДБОР ИНЖЕЊЕРСКЕ КОМОРЕ СРБИЈЕ
утврђује да је

Ненад Д. Крајновић

дипломирани инжењер електротехнике
ЈМБ 1711968710084

одговорни пројектант

телекомуникационих мрежа и система

Број лиценце
353 1041 03

У Београду,
25. септембра 2003. године

ПРЕДСЕДНИК КОМОРЕ
Милош Лазовић
Проф. др Милош Лазовић
дипл. грађ. инж.

Број: 12-02/237721
Београд, 07.10.2016. године

На основу члана 75. Статута Инжењерске коморе Србије ("СГ РС", бр. 88/05 и 16/09), а на лични захтев члана Коморе, Инжењерска комора Србије издаје

П О Т В Р Д У

Којом се потврђује да је Ненад Д. Крајновић, дипл.инж.ел.
лиценца број

353 1041 03

за

одговорног пројектанта телекомуникационих мрежа и система

на дан издавања ове потврде члан Инжењерске коморе Србије, да је измирио обавезу плаћања чланарине Комори закључно са 25.09.2017. године, као и да му одлуком Суда части издата лиценца није одузета.

М.П.

Председник Инжењерске коморе Србије

Проф. др Милисав Дамњановић, дипл. инж. арх.

ИНЖЕЊЕРСКА КОМОРА СРБИЈЕ

ЛИЦЕНЦА

ОДГОВОРНОГ ПРОЈЕКТАНТА

На основу Закона о планирању и изградњи и
Статута Инжењерске коморе Србије

УПРАВНИ ОДБОР ИНЖЕЊЕРСКЕ КОМОРЕ СРБИЈЕ
утврђује да је

Наташа Ј. Нешковић

дипломирани инжењер електротехнике

ЈМБ 1608969785015

одговорни пројектант

телекомуникационих мрежа и система

Број лиценце

353 4449 03

У Београду,
13. новембра 2003. године

ПРЕДСЕДНИК КОМОРЕ
Милош Лазовић

Проф. др Милош Лазовић
дипл. грађ. инж.

Број: 12-02/196905
Београд, 16.11.2015. године

На основу члана 75. Статута Инжењерске коморе Србије ("СГ РС", бр. 88/05 и 16/09), а на лични захтев члана Коморе, Инжењерска комора Србије издаје

П О Т В Р Д У

Којом се потврђује да је Наташа Ј. Нешковић, дипл.инж.ел.
лиценца број

353 4449 03

за

одговорног пројектанта телекомуникационих мрежа и система

на дан издавања ове потврде члан Инжењерске коморе Србије, да је измирио обавезу плаћања чланарине Комори закључно са 13.11.2016. године, као и да му одлуком Суда части издата лиценца није одузета.

М.П.

Председник Инжењерске коморе Србије

Проф. др Милисав Дамњановић, дипл. инж. арх.

ETF – ELEKTROTEHNIČKI FAKULTET
UNIVERZITET U BEOGRADU
Bulevar kralja Aleksandra 73, PF 3554, 11120 Beograd, Srbija
+381 (0) 11 - Tel 3248464, Fax 3248681, Račun 840-1438666-48, ETF-sopstveni prihodi

Katedra za telekomunikacije
+381 (0) 11 - Tel 3218422, Fax 3218399, e-mail: radio_lab@etf.rs

Na osnovu odredbi člana 126. i 128. Zakona o planiranju i izgradnji ("Službeni glasnik RS" broj 72/2009, 81/2009 - ispr., 64/2010 – odluka US, 24/2011, 121/2012, 42/2013 - odluka US, 50/2013 - odluka US, 98/2013 - odluka US, 132/2014 i 145/2014), kao i shodno Odluci fakulteta, donosim:

POTVRDU

da je

STUDIJA IZVODLJIVOSTI IZGRADNJE NACIONALNOG CERT-A

dalje priložen uz ovaj dokument usaglašen u svim svojim delovima.

Odgovorni projektant

Prof. dr Aleksandar Nešković, dipl.ing.

Инжењерска комора Србије
Александар М. Нешковић
дипл. инж. ел.
353 4448 03
одговорни пројектант

ETF – ELEKTROTEHNIČKI FAKULTET
UNIVERZITET U BEOGRADU
Bulevar kralja Aleksandra 73, PF 3554, 11120 Beograd, Srbija
+381 (0) 11 - Tel 3248464, Fax 3248681, Račun 840-1438666-48, ETF-sopstveni prihodi

Katedra za telekomunikacije
+381 (0) 11 - Tel 3218422, Fax 3218399, e-mail: radio_lab@etf.rs

IZJAVA
O KORIŠĆENJU PROPISA

Prilikom izrade priložene

STUDIJE IZVODLJIVOSTI
IZGRADNJE NACIONALNOG CERT-A

korišćeni su zakonski i podzakonski propisi, kao i međunarodne preporuke i standardi navedeni u prilogu 1 ove izjave.

Prilog:1

Odgovorni projektant

Prof. dr Aleksandar Nešković, dipl.ing.

Prilog 1

Izjave odgovornog projektanta o korišćenju propisa

Prilikom izrade

STUDIJE IZVODLJIVOSTI IZGRADNJE NACIONALNOG CERT-A

korišćeni su sledeći propisi:

Međunarodni propisi:

- NIS (*Network and Information Security*) Direktiva EU – *„DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL", of 6 July 2016, concerning measures for a high common level of security of network and information systems across the Union"*
- IETF (*Internet Engineering Task Force*) RFC (*Request for Comments*) 2350: *Expectations for Computer Security Incident Response*, 1988.
- Strategije informacione bezbednosti zemalja članica EU (Estonija, Finska, Slovačka, Češka, Francuska, Nemačka, Litvanija, Luksemburg, Holandija i Velika Britanija), kao i zemalja van EU (SAD, Kanada, Japan)
- ENISA preporuka – „*Baseline capabilities for national / governmental* CERTs – v1.0", *December* 2009.
- ENISA preporuka – „Definition of Cybersecurity - Gaps and overlaps in standardisation – v1.0", *December* 2015.
- ENISA preporuka – „*Guidelines for national and governmental* CSIRTs – v1.6", *December* 2015.
- Ostali relevantni propisi.

Nacionalni propisi:

- Zakon o informacionoj bezbednosti Republike Srbije ("Službeni glasnik RS" broj 6/2016);
- Zakon o planiranju i izgradnji ("Službeni glasnik RS", br. 72/2009, 81/2009 - ispr., 64/2010 - odluka Ustavnog Suda, 24/2011, 121/2012, 42/2013 - odluka Ustavnog Suda, 50/2013 - odluka Ustavnog Suda, 98/2013 - odluka Ustavnog Suda, 132/2014 i 145/2014);
- Zakon o elektronskoj trgovini ("Službeni glasnik RS", br. 41/2009);
- Zakon o izmenama i dopunama Zakona o elektronskoj trgovini ("Službeni glasnik RS", br. 95/2013);
- Zakon o elektronskom potpisu ("Službeni glasnik RS", br. 135/2004);
- Zakon o elektronskom dokumentu ("Službeni glasnik RS", br. 51/2009);
- Zakon o elektronskim komunikacijama ("Službeni glasnik RS", br. 44/2010);
- Zakon o izmenama i dopunama Zakona o elektronskim komunikacijama ("Službeni glasnik RS", br. 62/2014);
- Pravilnik o univerzalnom servisu ("Službeni glasnik RS", br. 24/12);
- Pravilnik o tehničkim i drugim zahtevima pri izgradnji prateće infrastrukture potrebne za

postavljanje elektronskih komunikacionih mreža, pripadajućih sredstava i elektronske komunikacione opreme prilikom izgradnje poslovnih i stambenih objekata "Službeni glasnik RS", br. 44/2010);

- Pravilnik o bližim uslovima za izdavanje kvalifikovanih elektronskih sertifikata "Službeni glasnik RS", br. 26/2008);
- Pravilnik o tehničko-tehnološkim postupcima za formiranje kvalifikovanog elektronskog potpisa i kriterijumima koje treba da ispune sredstva za formiranje kvalifikovanog elektronskog potpisa ("Službeni glasnik RS", br. 26/2008, 13/2010);
- Pravilnik o Registru sertifikacionih tela za izdavanje kvalifikovanih elektronskih sertifikata u Republici Srbiji ("Službeni glasnik RS", br. 26/2008);
- Pravilnik o evidenciji sertifikacionih tela ("Službeni glasnik RS", br. 48/2005, 82/2005 i 116/2005);
- Pravilnik o izdavanju vremenskog žiga ("Službeni glasnik RS", br. 112/2009);
- Strategija razvoja informacionog društva ("Službeni glasnik RS", br. 51/2010);
- Strategija razvoja elektronske uprave u Republici Srbiji za period od 2009. do 2013. godine ("Službeni glasnik RS", br. 83/2009, 5/2010);
- Strategija razvoja elektronskih komunikacija u periodu od 2010. do 2020. godine ("Službeni glasnik RS", br. 68/2010);
- Akcioni plan za sprovođenje strategije razvoja elektronskih komunikacija u Republici Srbiji od 2010. do 2020.;
- Zakon o potvrđivanju konvencije o visokotehnološkom kriminalu ("Službeni glasnik RS", br. 19/2009);
- Zakon o bezbednosti i zdravlju na radu ("Službeni glasnik RS", br. 101/2005, 91/2015);

II PROJEKTNI ZADATAK

ОДЕЉАК III

На основу члана 61. Закона о јавним набавкама („Службени гласник РС“, бр. 124/12, 14/15 и 68/15), члана 2. Правилника о обавезним елементима конкурсне документације у поступцима јавних набавки и начину испуњености услова („Службени гласник РС“, број 86/15), наручилац је припремио образац:

СПЕЦИФИКАЦИЈЕ И ЗАХТЕВИ ПРЕДМЕТА НАБАВКЕ

Партија I – Студија изводљивости изградње националног CERT-а

1. Увод

Доношењем Закона о информационој безбедности („Сл. гласник РС“, бр. 6/2016) који уређује мере заштите од безбедносних ризика у информационо-комуникационим системима, одговорности правних лица приликом управљања и коришћења информационо-комуникационих система и одређује надлежне органе за спровођење мера заштите, координацију између чинилаца заштите и праћење правилне примене прописаних мера заштите, Регулаторна агенција за електронске комуникације и поштанске услуге је одређена као надлежна за послове Националног ЦЕРТ-а.
Национални центар за превенцију безбедносних ризика у ИКТ обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.

Регулаторна агенција за електронске комуникације и поштанске услуге ће од Понуђача добијену студију користити као један од основних докумената у пројекту успостављања Националног ЦЕРТ-а као ефикасне и сврсисходне институције.

2. Термини и дефиниције

Закон	Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016)
Национални ЦЕРТ	Национални центар за превенцију безбедносних ризика у ИКТ системима, наведен у члану 14. Закона
Надлежни орган	Орган државне управе надлежан за безбедност ИКТ система, наведен у члану 4. Закона
Агенција	Регулаторна агенција за електронске комуникације и поштанске услуге

3. Предмет студије

Агенција, на основу обавезе прописане Законом, креће у пројекат оснивања посебне организационе јединице која ће обављати функцију Националног ЦЕРТ-а. Тражена студија треба да одговори на питања организације, структуре, функције, потребних ресурса, процеса и буџета (процену трошкова) будућег Националног ЦЕРТ-а и да представи Акциони план за успостављање Националног ЦЕРТ-а за период од 5 година.

4. Садржај студије

Студија треба да представи анализу тренутног стања у пословима превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији, у мери у којој је то могуће набавити од ималаца таквих система. Потребно је представити правни оквир у Републици Србији, Европску регулативу и наше обавезе везане за безбедност у ИКТ системима, националне и међународне стандарде и стандарде који се примењују у области ИКТ сигурности. Студија треба да престави тренутно стање и планиране активности у институцијама учесницима у процесима превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији наведеним у Закону, као и другим, у анализи идентификованим, битним институцијама за успешан процес (ИКТ компаније, међународне организације из области ИКТ сигурности, итд.).

Студија треба да наведе актере са којима Национални ЦЕРТ остварује сарадњу и комуникацију, начине и циљеве сарадње, улоге, процесе и остале ресурсе потребне за успешно вршење сарадње у пословима координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу.
Студија треба да предложи предложи стандардизована правила, форме, дефиниције и моделе података за размену информација.

Студија треба детаљно да опише препоручену организациону структуру, улоге и функције Националног ЦЕРТ-а, потребне људске и материјалне ресурсе, буџет за успостављање и функционисање, интерне и екстерне процесе који подржавају, и актере са којима Национални ЦЕРТ сарађује у испуњавању Законом поверених послова и обавеза.
За потребне људске ресурсе потребно је навести пожељне и алтернативне минималне и оптималне квалификације – формално и специјализовано образовање, знања, вештине, потенцијалне специјалне обавезне и пожељне услове, итд. Потребно је дефинисати радна места у Националном ЦЕРТ-у, детаљан опис посла, као и препоручен даљи ток образовања и усавршавања кадра са потребним буџетом за усавршавање, које је усаглашено са Акционим планом.

Опис материјалних ресурса мора да обухвата просторије, опрему, инфраструктуру, потребне информационе системе који подржавају поверене послове и обавезе Националног ЦЕРТ-а, итд. За наведене материјалне ресурсе потребно је навести детаљне описе, буџет и време потребно за њихово набављање, усаглашено са акцијама у акционом плану. Посебно обратити пажњу на дефинисање ИКТ инфраструктуре и система који подржавају поверене послове и обавезе Националног ЦЕРТ-а, са посебним нагласком на аспект ИКТ сигурности система.

Навођење и дефинисање процедура и процеса мора да обухвата интерне и екстерне процедуре које подржавају рад и испуњење поверених послова и обавеза Националног ЦЕРТ-а. Потребно је детаљно дефинисати функцију, улоге, актере и исходе процедура, њихову везу са дефинисаним ИКТ системима Националног ЦЕРТ-а и спољних актера са којима Национални ЦЕРТ непосредно сарађује у смислу Закона, као и било које друге актере са којим би сарадња унапредила функцију Националног ЦЕРТ-а (међународне организације, ИКТ компаније, медији, итд.).

Студија мора детаљно описати референце других Националних ЦЕРТ-ова или других институција у вршењу еквивалентног посла, у мери у којој је то могуће набавити од ималаца таквих система, У Акционом плану дефинисати успостављање и континуално

вршење обавезе. Посебно обратити пажњу на потребне ИКТ системе који подржавају поверени посао и комуникацију са актерима у вршењу посла.

У складу са свим претходно наведеним захтевима, Студија мора посебно детаљно да анализира и дефинише начине испуњавања следећих поверених послова и обавеза Националног ЦЕРТ-а описаних у Закону :

1. Праћење стања о инцидентима на националном нивоу.
2. Пружање раних упозорења, узбуна и најава, и информисање релевантних лица о ризицима и инцидентима.
3. Реаговање по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и преузимање других потребних мера из своје надлежности на основу добијених сазнања.
4. Континуирана израда анализа ризика и инцидената.
5. Подизање свести код грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, о ризицима и мерама заштите, укључујући спровођење кампања у циљу подизања те свести.
6. Вођење евиденције Посебних ЦЕРТ-ова.
7. Непосредна сарадња са Надлежним органом, Посебним ЦЕРТ-овима у Републици Србији, сличним организацијама у другим земљама, са јавним и привредним субјектима, ЦЕРТ-овима самосталних оператора ИКТ система, као и са ЦЕРТ-ом републичких органа.
8. Промоција усвајања и коришћење прописаних и стандардизованих правила за:

a) управљање и санирање ризика и инцидената;
b) класификацију информација о ризицима и инцидентима;
c) класификацију озбиљности инцидената и ризика;
d) дефиницију формата и модела података за размену информација о ризицима и инцидентима и дефиницију правила по којима ће се именовати значајни системи.

Студија мора да садржи Акциони план који треба да представи активности на пројекту успостављања Националног ЦЕРТ-а, временски план, учеснике, ресурсе, буџет и циљеве активности. Временски план треба да успостави баланс, колико је могуће, и да што пре реализује оне активности које успостављају функционалности које се у анализи покажу као најпотребније, а да такав приступ буде и реалан и да не угрожава укупно трајање пројекта.

5. Опште напомене

Студија у својим представљеним решењима мора да се води начелима дефинисаним у члану 3. Закона: начело управљања ризиком, начело свеобухватне заштите, начело стручности и добре праксе, начело свести и оспособљености.

III ELABORAT

0. UVOD

Zakon o informacionoj bezbednosti („Službeni glasnik RS“, br. 6/2016) uređuje mere zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima, uređuje odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, određuje nadležne organe za sprovođenje mera zaštite, definiše koordinaciju između činilaca zaštite i prati pravilne primene propisanih mera zaštite. Prema odredbama ovog Zakona, Regulatorna agencija za elektronske komunikacije i poštanske usluge (skraćeno RATEL) određena je kao nadležna za poslove realizacije Nacionalnog centra za prevenciju bezbednosnih rizika (skraćeno Nacionalni CERT; CERT - *Computer Emergency Response Teams*). Nacionalni centar za prevenciju bezbednosnih rizika treba da obavlja poslove koordinacije prevencije i zaštite od bezbednosnih rizika u informaciono-komunikacionim sistemima u Republici Srbiji na nacionalnom nivou.

Regulatorna agencija za elektronske komunikacije i poštanske usluge, osnovana Zakonom o elektronskim komunikacijama („Službeni glasnik RS”, br. 44/10, 60/13 – US i 62/14), nezavisna je regulatorna organizacija sa svojstvom pravnog lica, koja vrši javna ovlašćenja u cilju efikasnog sprovođenja utvrđene politike u oblasti elektronskih komunikacija, podsticanja konkurencije elektronskih komunikacionih mreža i usluga, unapređivanja njihovog kapaciteta, odnosno kvaliteta, doprinosa razvoju tržišta elektronskih komunikacija i zaštite interesa korisnika elektronskih komunikacija, u skladu sa odredbama Zakona i propisa donetih na osnovu njega, kao i regulatornih i drugih poslova u skladu sa posebnim zakonom kojim se uređuju poštanske usluge.

Agencija RATEL je, u skladu sa članom 8. Zakona o elektronskim komunikacijama, nadležna da:

1) donosi podzakonske akte,
2) odlučuje o pravima i obavezama operatora i korisnika,
3) sarađuje sa organima i organizacijama nadležnim za oblast radiodifuzije, zaštite konkurencije, zaštite potrošača, zaštite podataka o ličnosti i drugim organima i organizacijama po pitanjima značajnim za oblast elektronskih komunikacija,

4) sarađuje sa nadležnim regulatornim i stručnim telima država članica Evropske unije i drugih država radi usaglašavanja prakse primene propisa iz oblasti elektronskih komunikacija i podsticanja razvoja prekograničnih elektronskih komunikacionih mreža i usluga,
5) učestvuje u radu međunarodnih organizacija i institucija u oblasti elektronskih komunikacija u svojstvu nacionalnog regulatornog tela u oblasti elektronskih komunikacija,
5a) obavlja regulatorne i druge poslove iz oblasti poštanskih usluga, a u skladu sa posebnim zakonom kojim se uređuju poštanske usluge, i
6) obavlja druge poslove u skladu sa ovim Zakonom.

Pri tome, prethodno navedene poslove agencija treba da obavlja kao poverene poslove, nepristrasno i javno.

Imajući vidu tipove poslova koje je na osnovu zakona RATEL sprovodio u dosadašnjem radu, ali i postignuti kvalitet u izvršavanju tih poslova, jasno je da RATEL ima veliki potencijal za uspešnu realizaciju Nacionalnog CERT-a.

Regulatorna agencija za elektronske komunikacije i poštanske usluge, na osnovu obaveze propisane Zakonom, pokrenula je projekat osnivanja posebne organizacione jedinice koja će obavljati funkciju Nacionalnog CERT-a. Prvi korak u tom pravcu jeste izrada Studije izvodljivosti izgradnje Nacionalnog CERT-a, što je i tema ovog projekta. Studija izvodljivosti izgradnje Nacionalnog CERT-a treba da odgovori na pitanja organizacije, strukture, funkcije, potrebnih resursa, procesa i budžeta (procene troškova) budućeg Nacionalnog CERT-a i da predstavi Akcioni plan za uspostavljanje Nacionalnog CERT-a za period od 5 godina.

1. ZAKON O INFORMACIONOJ BEZBEDNOSTI

1.1 MESTO I ULOGA NACIONALNOG CERT-A

Zakon o informacionoj bezbednosti (u daljem tekstu Zakon) objavljen je u Službenom glasniku Republike Srbije broj 06/2016. od 28.01.2016. godine. Nastao je kao rezultat potrebe da se na adekvatan način uredi pitanje zaštite informaciono-komunikacione infrastrukture u Republici Srbiji. U okviru Zakona je pojam informaciono-komunikacionog sistema (u daljem tekstu IKT sistem) definisan kao tehnološko-organizaciona celina koja obuhvata:

- elektronske komunikacione mreže u smislu zakona koji uređuje elektronske komunikacije,
- uređaje ili grupe međusobno povezanih uređaja takvih da se u okviru uređaja, odnosno u okviru barem jednog iz grupe uređaja, vrši automatska obrada podataka korišćenjem računarskog programa,
- podatke koji se pohranjuju, obrađuju, pretražuju ili prenose pomoću sredstava iz prethodno navedenih stavki, a u svrhu njihovog rada, upotrebe, zaštite ili održavanja, i
- organizacionu strukturu putem koje se upravlja IKT sistemom.

Predmet Zakona je uređenje:

- mera zaštite od bezbednosnih rizika u IKT sistemima,
- odgovornosti pravnih lica prilikom upravljanja i korišćenja informaciono-komunikacionih sistema, i
- nadležnih organa za sprovođenje mera zaštite, koordinacije između činilaca zaštite i praćenje pravilne primene propisanih mera zaštite.

Pojam „informaciona bezbednost“ definisan je kao skup mera koje omogućavaju da podaci kojima se rukuje korišćenjem IKT sistema budu zaštićeni od neovlašćenog pristupa, kao i da se zaštiti integritet, raspoloživost, autentičnost i neporecivost podataka, da bi taj sistem funkcionisao kako je predviđeno, kada je predviđeno i pod kontrolom ovlašćenih lica.

Član 2 Zakona definiše operatora IKT sistema kao pravno lice, organ javne vlasti ili organizacionu jedinicu organa javne vlasti koja koristi IKT sistem u okviru obavljanja svoje

delatnosti, odnosno poslova iz svoje nadležnosti. Obaveze operatora IKT sistema su definisane kroz:

- preduzimanje adekvatnih tehničkih i organizacionih mera kojima se obezbeđuje prevencija od nastanka incidenata, kao i prevencija i minimizacija štete od incidenata koji ugrožavaju vršenje nadležnosti i obavljanje delatnosti,
- donošenje akta o bezbednosti IKT sistema kojim se određuju mere zaštite IKT sistema, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti ovog sistema, i
- obaveštavanje nadležnog organa, tj. Ministarstva trgovine, turizma i telekomunikacija (u daljem tekstu MTTT), o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti.

Član 4 Zakona uvodi instituciju Nadležnog organa kao organa državne uprave koji je nadležan za bezbednost IKT sistema - Ministarstvo trgovine, turizma i telekomunikacija (MTTT). U članu 6 Zakona, definisani su IKT sistemi od posebnog značaja u formi funkcionalnog opisa. Obaveza Vlade Republike Srbije je da kroz podzakonska akta bliže definiše koji su to IKT sistemi od posebnog značaja, kao i da donese odluku o formiranju Tela za koordinaciju poslova informacione bezbednosti (predviđeno članom 5 Zakona). Do sada je formirano Telo za koordinaciju poslova informacione bezbednosti (Službeni glasnik RS broj 24/2016 od 08.03.2016. godine) i urađeni su nacrti odgovarajućih uredbi koje su predviđene Zakonom. Članom 5 Zakona predviđeno je da Nacionalni CERT delegira jednog člana za Telo za koordinaciju poslova informacione bezbednosti što će biti urađeno kada se formira Nacionalni CERT.

IKT sistemi od posebnog značaja, definisani članom 6 Zakona, dele se u tri kategorije:

- sistemi koji se koriste u obavljanju poslova u organima javne vlasti,
- sistemi koji se koriste za obradu podataka koji se, u skladu sa zakonom koji uređuje zaštitu podataka o ličnosti, smatraju naročito osetljivim podacima o ličnosti, i
- sistemi koji se koriste u obavljanju delatnosti od opšteg interesa.

IKT sistemi od posebnog značaja, koji se koriste u obavljanju delatnosti od opšteg interesa, su IKT sistemi u sledećim oblastima (član 6 Zakona):

1. proizvodnja, prenos i distribucija električne energije,
2. proizvodnja i prerada uglja,
3. istraživanje, proizvodnja, prerada, transport i distribucija nafte i prirodnog i tečnog gasa,
4. promet nafte i naftnih derivata, i železničkog, poštanskog i vazdušnog saobraćaja,
5. elektronska komunikacija,
6. izdavanje službenog glasila Republike Srbije,
7. upravljanje nuklearnim objektima,
8. korišćenje, upravljanje, zaštita i unapređivanje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja),
9. proizvodnja, promet i prevoz naoružanja i vojne opreme,
10. upravljanje otpadom,
11. komunalne delatnosti,
12. poslovi finansijskih institucija,
13. zdravstvena zaštita, i
14. usluge informacionog društva namenjene drugim pružaocima usluga informacionog društva u cilju omogućavanja pružanja njihovih usluga.

Član 7 preciznije definiše mere zaštite IKT sistema od posebnog značaja tako što se ove mere odnose na:

1. uspostavljanje organizacione strukture, sa utvrđenim poslovima i odgovornostima zaposlenih, kojom se ostvaruje upravljanje informacionom bezbednošću u okviru operatora IKT sistema,
2. postizanje bezbednosti rada na daljinu i upotrebe mobilnih uređaja,
3. obezbeđivanje da lica koja koriste IKT sistem, odnosno upravljaju IKT sistemom, budu osposobljena za posao koji rade i razumeju svoju odgovornost,
4. zaštitu od rizika koji nastaju pri promenama poslova ili prestanka radnog angažovanja lica zaposlenih kod operatora IKT sistema,
5. identifikovanje informacionih dobara i određivanje odgovornosti za njihovu zaštitu,
6. klasifikovanje podataka tako da nivo njihove zaštite odgovara značaju podataka u skladu sa načelom upravljanja rizikom iz člana 3. Zakona,
7. zaštitu nosača podataka,
8. ograničenje pristupa podacima i sredstvima za obradu podataka,
9. odobravanje ovlašćenog pristupa i sprečavanje neovlašćenog pristupa IKT sistemu i uslugama koje IKT sistem pruža,
10. utvrđivanje odgovornosti korisnika za zaštitu sopstvenih sredstava za autentikaciju,
11. predviđanje odgovarajuće upotrebe kriptozaštite radi zaštite tajnosti, autentičnosti, odnosno integriteta podataka,
12. fizičku zaštitu objekata, prostora, prostorija, odnosno zona, u kojima se nalaze sredstva i dokumenti IKT sistema i obrađuju podaci u IKT sistemu,
13. zaštitu od gubitka, oštećenja, krađe ili drugog oblika ugrožavanja bezbednosti sredstava koja čine IKT sistem,
14. obezbeđivanje ispravnog i bezbednog funkcionisanja sredstava za obradu podataka,
15. zaštitu podataka i sredstva za obradu podataka od zlonamernog softvera,
16. zaštitu od gubitka podataka,
17. čuvanje podataka o događajima koji mogu biti od značaja za bezbednost IKT sistema,
18. obezbeđivanje integriteta softvera i operativnih sistema,
19. zaštitu od zloupotrebe tehničkih bezbednosnih slabosti IKT sistema,
20. obezbeđivanje da aktivnosti na reviziji IKT sistema imaju što manji uticaj na funkcionisanje sistema,
21. zaštitu podataka u komunikacionim mrežama uključujući uređaje i vodove,
22. bezbednost podataka koji se prenose unutar operatora IKT sistema, kao i između operatora IKT sistema i lica van operatora IKT sistema,
23. pitanja informacione bezbednosti u okviru upravljanja svim fazama životnog ciklusa IKT sistema, odnosno delova sistema,
24. zaštitu podataka koji se koriste za potrebe testiranja IKT sistema, odnosno delova sistema,
25. zaštitu sredstava operatora IKT sistema koja su dostupna pružaocima usluga,
26. održavanje ugovorenog nivoa informacione bezbednosti i pruženih usluga u skladu sa uslovima koji su ugovoreni sa pružaocem usluga,
27. prevenciju i reagovanje na bezbednosne incidente, što podrazumeva adekvatnu razmenu informacija o bezbednosnim slabostima IKT sistema, incidentima i pretnjama, i
28. mere koje obezbeđuju kontinuitet obavljanja posla u vanrednim okolnostima.

Pored samih mera, Zakon u članu 8 propisuje i obavezu operatora IKT sistema od posebnog značaja da donese i Akt o bezbednosti u okviru koga se određuju mere zaštite, a naročito principi, način i procedure postizanja i održavanja adekvatnog nivoa bezbednosti sistema, kao i ovlašćenja i odgovornosti u vezi sa bezbednošću i resursima IKT sistema od posebnog značaja. Članovima 9 i 10 se bliže uređuje pitanje *outsourcing*-a poslova vezanih za informacionu bezbednost.

Za operatore IKT sistema od posebnog značaja uvedena je obaveza obaveštavanja nadležnog organa (MTTT) o incidentima u IKT sistemima koji mogu da imaju značajan uticaj na narušavanje informacione bezbednosti (član 11 Zakona). Izuzetak od tog pravila su:

- finansijske institucije koje svoje incidente prijavljuju Narodnoj banci Srbije,
- telekomunikacioni operatori koji svoje incidente prijavljuju Regulatornom telu za elektronske komunikacije (RATEL), i
- operatori IKT sistema za rad sa tajnim podacima koji postupaju u skladu sa propisima kojima se uređuje oblast zaštite tajnih podataka.

Imajući u vidu da ugrožavanje informacione bezbednosti najčešće nije ograničeno na teritoriju jedne države, Zakon je u članu 12 uveo obavezu Nadležnog organa (MTTT) da ostvari međunarodnu saradnju u oblasti bezbednosti IKT sistema u cilju razmene informacija o ugrožavanju informacione bezbednosti. Ova aktivnost je naročito predviđena za incidente koji:

- brzo rastu i imaju tendenciju da postanu visoki rizici,
- prevazilaze ili mogu da prevaziđu nacionalne kapacitete, i
- mogu da imaju negativan uticaj na više od jedne države.

Izuzetak od prethodno navedenih obaveza su samostalni operatori IKT sistema (član 13 Zakona). Pod pojmom samostalnog operatora IKT sistema Zakon je obuhvatio: Ministarstvo nadležno za poslove odbrane, Ministarstvo nadležno za unutrašnje poslove i Ministarstvo nadležno za spoljne poslove i službe bezbednosti (definisano u okviru člana 2 Zakona).

U cilju prevencije i zaštite od bezbednosnih rizika u IKT sistemima u Republici Srbiji, Zakon je odredio formiranje Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima - Nacionalni CERT (član 14 Zakona). Prema Zakonu, obaveza je RATEL-a da formira Nacionalni CERT. Uloga Nacionalnog CERT-a je da prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema, i u vezi toga obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost, a posebno:

1) prati stanje o incidentima na nacionalnom nivou,
2) pruža rana upozorenja, uzbune i najave i informiše relevantna lica o rizicima i incidentima,
3) reaguje po prijavljenim ili na drugi način otkrivenim incidentima, tako što pruža savete na osnovu raspoloživih informacija licima koja su pogođena incidentom i preduzima druge potrebne mere iz svoje nadležnosti na osnovu dobijenih saznanja,
4) kontinuirano izrađuje analize rizika i incidenata,
5) podiže svest kod građana, privrednih subjekata i organa javne vlasti o značaju informacione bezbednosti, o rizicima i merama zaštite, uključujući sprovođenje kampanja u cilju podizanja te svesti, i
6) vodi evidenciju posebnih CERT-ova.

Nacionalni CERT ima zadatak da neposredno sarađuje sa Nadležnim organom (MTTT), posebnim CERT-ovima u Republici Srbiji, sličnim organizacijama u drugim zemljama, sa javnim i privrednim subjektima, CERT-ovima samostalnih operatora IKT sistema, kao i sa CERT-om republičkih organa. Pored toga, ima zadatak da promoviše usvajanje i korišćenje propisanih i standardizovanih pravila za:

1) upravljanje i saniranje rizika i incidenata,
2) klasifikaciju informacija o rizicima i incidentima,
3) klasifikaciju ozbiljnosti incidenata i rizika, i
4) definiciju formata i modela podataka za razmenu informacija o rizicima i incidentima i definiciju pravila po kojima će se imenovati značajni sistemi.

S druge strane, Nadležni organ (MTTT) vrši nadzor nad radom Nacionalnog CERT-a u vršenju poslova poverenih Zakonom (član 16. Zakona). U tom smislu, Nadležni organ je iznad Nacionalnog CERT-a.

Zakon je u članu 17 uveo pojam posebnog CERT-a kao CERT-a koji obavlja poslove prevencije i zaštite od bezbednosnih rizika u IKT sistemima u okviru određenog pravnog lica, grupe pravnih lica, oblasti poslovanja i slično. U okviru Zakona nije uspostavljena nikakva čvrsta veza između posebnih CERT-ova i Nacionalnog CERT-a, osim obaveze vođenja evidencije posebnih CERT-ova od strane Nacionalnog CERT-a.

U članu 18 Zakona eksplicitno je naveden i Centar za bezbednost IKT sistema u republičkim organima (CERT republičkih organa). Prema Zakonu, CERT republičkih organa je sastavni deo Uprave za zajedničke poslove republičkih organa. Poslovi CERT-a republičkih organa obuhvataju:

1) zaštitu IKT sistema Računarske mreže republičkih organa (u daljem tekstu: RMRO),
2) koordinaciju i saradnju sa operatorima IKT sistema koje povezuje RMRO u prevenciji incidenata, otkrivanju incidenata, prikupljanju informacija o incidentima i otklanjanju posledica incidenata, i
3) izdavanje stručnih preporuka za zaštitu IKT sistema republičkih organa, osim IKT sistema za rad sa tajnim podacima.

Pitanja kriptozaštite i zaštite od kompromitujućeg elektromagnetnog zračenja su regulisana u okviru članova 20 do 27 Zakona. Prema Zakonu (član 20), Ministarstvo nadležno za poslove odbrane je nadležno za poslove informacione bezbednosti koji se odnose na odobravanje kriptografskih proizvoda, distribuciju kriptomaterijala i zaštitu od kompromitujućeg elektromagnetnog zračenja, i poslove i zadatke u skladu sa zakonom i propisima donetim na osnovu zakona.

Članom 28 uvedena je Inspekcija za informacionu bezbednost koja vrši inspekcijski nadzor nad primenom Zakona i radom operatora IKT sistema od posebnog značaja, osim samostalnih operatora IKT sistema i IKT sistema za rad sa tajnim podacima, a u skladu sa zakonom kojim se uređuje inspekcijski nadzor. Poslovi inspekcije za informacionu bezbednost su dati u nadležnost ministarstva nadležnog za poslove informacione bezbednosti (MTTT).

1.2 ZAKLJUČAK

Prema Zakonu, operatori IKT sistema od posebnog značaja imaju obavezu obaveštavanja Nadležnog organa (MTTT) što implicitno znači da će Nadležni organ morati da formira interni CERT koji će se baviti ovim poslovima. S druge strane, pošto je Nacionalni CERT podređen Nadležnom organu, ne postoji obaveza obaveštavanja Nacionalnog CERT-a od strane Nadležnog organa o bilo kakvim bezbednosnim incidentima. Ostavljeno je Nadležnom organu da proceni u kojoj meri će o bezbednosnim incidentima obaveštavati Nacionalni CERT. Sa druge strane, Zakonom je predviđena saradnja Nacionalnog CERT-a i posebnih CERT-ova u zemlji, ali nivo ove saradnje nije preciznije definisan Zakonom. S obzirom na činjenicu da će se Nacionalni CERT nalaziti u okviru RATEL-a koji treba da vodi evidenciju o bezbednosnim incidentima telekomunikacionih operatora, otvoreno je pitanje integracije ove dve funkcije. Zakon ih tretira odvojeno, ali nigde nije isključena mogućnost i njihove integracije, što bi svakako bilo i najracionalnije rešenje.

2. ANALIZA TRENUTNOG STANJA U POSLOVIMA PREVENCIJE I ZAŠTITE OD BEZBEDNOSNIH RIZIKA U IKT SISTEMIMA OD POSEBNOG ZNAČAJA U REPUBLICI SRBIJI

2.1 PREGLED IKT SISTEMA I KOMPANIJA OD POSEBNOG ZNAČAJA U REPUBLICI SRBIJI

Zakon je u članu 6 definisao, polazeći od njihove namene, koji IKT sistemi se, u opštem smislu, smatraju sistemima od posebnog značaja. Polazeći od te definicije, IKT sistemi od posebnog značaja su sistemi koji se koriste:

- u obavljanju poslova u organima javne vlasti,
- za obradu naročito osetljivih podataka o ličnosti u smislu zakona kojim se uređuje zaštita podataka o ličnosti, i
- u obavljanju delatnosti od opšteg interesa (energetika, saobraćaj, elektronske komunikacije, nuklearni objekti, finansijske institucije, zdravstvena zaštita...).

IKT sistemi od posebnog značaja u obavljanju delatnosti od opšteg interesa su sistemi koji se koriste u sledećim oblastima:

1. proizvodnja, prenos i distribucija električne energije,
2. proizvodnja i prerada uglja,
3. istraživanje, proizvodnja, prerada, transport i distribucija nafte i prirodnog i tečnog gasa,
4. promet nafte i naftnih derivata, i železničkog, poštanskog i vazdušnog saobraćaja,
5. elektronska komunikacija,
6. izdavanje službenog glasila Republike Srbije,
7. upravljanje nuklearnim objektima,
8. korišćenje, upravljanje, zaštita i unapređenje dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja),

9. proizvodnja, promet i prevoz naoružanja i vojne opreme,
10. upravljanje otpadom,
11. komunalne delatnosti,
12. poslovi finansijskih institucija,
13. zdravstvena zaštita,
14. usluge informacionog društva namenjene drugim pružaocima usluga i informacionog društva u cilju omogućavanja pružanja njihovih usluga.

IKT sistemi od posebnog značaja u oblasti proizvodnje, prenosa i distribucije električne energije, u smislu zakona kojim se uređuje energetika, su sistemi kod:

1. proizvođača električne energije,
2. snabdevača električnom energijom, uključujući i snabdevače na veliko,
3. operatora prenosnog sistema električne energije,
4. operatora distributivnog sistema električne energije, i
5. operatora tržišta.

ITK sistemi od posebnog značaja u oblasti proizvodnje i prerade uglja, u smislu zakona kojim se uređuje rudarstvo, su sistemi kod nosioca eksploatacije uglja.

IKT sistemi od posebnog značaja u oblasti proizvodnje, prerade, transporta i distribucije nafte i prirodnog i tečnog gasa, kao i prometa nafte i naftnih derivata, u smislu zakona kojim se uređuje energetika, su sistemi kod:

1. proizvođača prirodnog gasa,
2. snabdevača prirodnim gasom,
3. javnih snabdevača prirodnim gasom,
4. operatora transportnog sistema prirodnog gasa,
5. operatora distributivnog sistema prirodnog gasa,
6. operatora skladišta prirodnog gasa,
7. energetskih subjekata koji obavljaju delatnosti:
   - proizvodnje derivata nafte,
   - transporta nafte naftovodima,
   - transporta derivata nafte produktovodima,
   - transporta nafte i derivata nafte drugim oblicima transporta,
8. trgovine naftom i derivatima nafte nosioca eksploatacije nafte i prirodnog gasa, u smislu zakona kojim se uređuje rudarstvo.

IKT sistemi od posebnog značaja u oblasti železničkog, poštanskog i vazdušnog saobraćaja su sistemi kod:

1. upravljača javne železničke infrastrukture, u smislu zakona kojim se uređuje železnica,
2. železničkog prevoznika, u smislu zakona kojim se uređuje poštanski saobraćaj,
3. javnog poštanskog operatora, u smislu zakona kojim se uređuje poštanski saobraćaj,
4. operatora aerodroma, u smislu zakona o vazdušnom saobraćaju,
5. jedinica kontrole letenja, u smislu zakona o vazdušnom saobraćaju, i
6. avio-prevoznika, u smislu zakona o vazdušnom saobraćaju.

IKT sistemi od posebnog značaja u oblasti elektronskih komunikacija su sistemi kod operatora javnih komunikacionih mreža i operatora javno dostupnih elektronskih komunikacionih usluga, u smislu zakona kojim se uređuju elektronske komunikacije.

IKT sistem od posebnog značaja u oblasti izdavanja službenog glasila Republike Srbije je sistem kod republičkog službenog glasila, u smislu zakona kojim se uređuje objavljivanje zakona i drugih propisa i akata.

IKT sistem od posebnog značaja u oblasti upravljanja nuklearnim objektima je sistem kod javnog preduzeća osnovanog za obavljanje delatnosti upravljanja nuklearnim objektima, u skladu sa zakonom kojim se uređuje zaštita od jonizujućeg zračenja i nuklearna sigurnost.

IKT sistemi od posebnog značaja u oblasti korišćenja, upravljanja, zaštite i unapređenja dobara od opšteg interesa (vode, putevi, mineralne sirovine, šume, plovne reke, jezera, obale, banje, divljač, zaštićena područja) su IKT sistemi kod:

1. javnih vodoprivrednih preduzeća u smislu zakona kojim se uređuju vode,
2. upravljača javnog puta u smislu zakona kojim se uređuju javni putevi,
3. nosioca eksploatacije mineralnih sirovina u smislu zakona kojim se uređuje rudarstvo,
4. pravnih lica za gazdovanje šumama u državnoj svojini, u smislu zakona kojim se uređuju šume,
5. ovlašćenih pravnih lica za tehničko održavanje državnih vodnih puteva, u smislu zakona kojim se uređuje plovidba i luke na unutrašnjim vodama,
6. javnih preduzeća za upravljanje nacionalnim parkovima, u smislu zakona kojim se uređuju nacionalni parkovi,
7. javnih preduzeća za obavljanje delatnosti korišćenja, upravljanja, zaštite i unapređivanja populacije divljači i njihovih staništa, u smislu zakona kojim se uređuje divljač i lovstvo.

IKT sistemi od posebnog značaja u oblasti proizvodnje, prometa i prevoza naoružanja i vojne opreme su IKT sistemi kod:

1. preduzeća koja proizvode naoružanje i vojnu opremu,
2. preduzeća koja vrše promet naoružanja i vojne opreme, i
3. preduzeća koja vrše prevoz naoružanja i vojne opreme.

IKT sistem od posebnog značaja u oblasti upravljanja otpadom je sistem kod operatora za upravljanje otpadom.

IKT sistemi od posebnog značaja u oblasti komunalne delatnosti su sistemi kod javnih preduzeća i privrednih društava koje vrše komunalne delatnosti.

IKT sistemi od posebnog značaja u oblasti poslova finansijskih institucija su sistemi kod finansijskih institucija u smislu zakona kojim se uređuje Narodna banka.

IKT sistemi od posebnog značaja u oblasti zdravstvene zaštite su sistemi kod ustanova koje obavljaju zdravstvenu delatnost.

IKT sistemi od posebnog značaja u oblasti usluga informacionog društva namenjenih drugim pružaocima usluga informacionog društva u cilju omogućavanja pružanja njihovih usluga su sistemi kod:

1. pružaoca usluga platformi za elektronsku trgovinu,
2. pružaoca usluga u oblaku (*cloud*),
3. usluga „*Internet exchange point*-a”, i
4. pravnog lica koje upravlja registrom nacionalnog Internet domena.

2.2 ANALIZA STANJA INFORMACIONE BEZBEDNOSTI U IKT SISTEMIMA I KOMPANIJAMA OD POSEBNOG ZNAČAJA

Sva pitanja vezana za bezbednost kritične infrastrukture jedne države su uvek bila obavijena velom tajne. U skladu sa tim, ista je situacija i sa pitanjem informacione bezbednosti. Ni jedan subjekat, čija je informaciona bezbednost bila kompromitovana, ne želi da te podatke javno objavi. Zbog toga je veoma teško napraviti realan prikaz stanja informacione bezbednosti u IKT sistemima i kompanijama od posebnog značaja u Republici Srbiji. Činjenica da se informacije o kompromitovanju informacione bezbednosti veoma retko pojavljuju u sredstvima javnog informisanja ne znači da je situacija dobra i da su domaći IKT sistemi kvalitetno administrirani i zaštićeni. U nedostatku zvaničnih izvora informacija, za potrebe ove studije, biće predstavljeni podaci objavljeni na alternativnim izvorima informacija, kao što su hakerski sajtovi. Zahvaljujući činjenici da hakeri vole da se hvale svojim uspesima u kompromitovanju IKT sistema, deo informacija o kompromitovanju informacione bezbednosti dospeva u javnost.

Jedan od poznatijih sajtova sa informacijama i kompromitovanju *web* sajtova je www.zone-h.org. Na ovom sajtu hakeri ostavljaju izglede *web* stranica koje su uspeli da hakuju. Ako se pogleda septembar mesec 2016. godine i kompromitovane *web* stranice samo državne uprave, dobija se lista data u tabeli 2.1. Zbirni podaci po mesecima za kompletan .RS *web* prostor na Internetu i za sve *web* stranice, a ne samo one koje pripadaju državnoj upravi, predstavljeni su u tabeli 2.2.

Tabela 2.1: Lista hakovanih *web* stranica državne uprave u 2016. godini (izvor: www.zone-h.org)

Datum	***Web* stranica**	**Operativni sistem servera**
19.09.2016.	uzb.minpolj.gov.rs	Linux
19.09.2016.	itcm.minpolj.gov.rs	Linux
02.08.2016.	juznobanatski.okrug.gov.rs	Linux
16.06.2016.	digitalnaagenda.gov.rs	Linux
13.06.2016.	raski.okrug.gov.rs	Linux

Tabela 2.2: Ukupan broj hakovanih *web* stranica u .RS domenskom prostoru po mesecima za 2016. godinu (izvor: www.zone-h.org)

Mesec i godina	**Broj hakovanih *web* stranica**
01.2016.	115
02.2016.	73
03.2016.	95
04.2016.	39
05.2016.	43
06.2016.	105
07.2016.	50
08.2016.	106
09.2016.	36

Podaci navedeni u tabelama 2.1 i 2.2 su samo mali deo sigurnosnih incidenata koji su se dogodili na Internetu. Navedeni izvor informacija sigurno nema informacije o svim

kompromitacijama *web* stranica u .RS domenskom prostoru. S obzirom da je kompromitacija *web* stranice samo jedan od velikog broja mogućih incidenata u oblasti informacione bezbednosti, jasne su razmere problema. Prilikom analize ovih podataka treba imati u vidu da se ne radi o zvaničnom sajtu neke državne institucije tako da podaci nisu zvanično verifikovani. S druge strane, provere su pokazale da su ovi podaci, po pravilu, tačni. Takođe je bitno navesti da veliki broj incidenata ne dospeva u javnost, počevši od trivijalnih incidenata koji se tiču zaraze kompjuterskim virusima, preko kriptovanja kompletnih hard diskova zbog *ransomware* virusa, pa zaključno sa upadima u sisteme koji za direktnu posledicu imaju gubitak informacija, novca i ugleda kompanija. Posebno treba naglasiti da u ovom trenutku ne postoji institucija na nivou države koja se na organizovani način bavi pitanjem informacione bezbednosti IKT sistema od posebnog značaja i skupljanjem i obradom informacija iz ove oblasti. Upravo zbog toga je i problem dati kompletnu analizu stanja informacione bezbednosti IKT sistema od posebnog značaja.

Donošenjem Zakona o informacionoj bezbednosti započet je proces unapređenja situacije u ovoj oblasti. Veliki broj institucija i kompanija ubrzano radi na formiranju svojih stručnih timova koji će se isključivo baviti pitanjima informacione bezbednosti IKT sistema.

3. PRAVNA REGULATIVA, STRATEGIJE INFORMACIONE BEZBEDNOSTI I RAZVOJ CERT ORGANIZACIJA

3.1 NIS DIREKTIVA I NACIONALNE CERT ORGANIZACIJE

Tokom decembra 2015. godine, Evropska Komisija, Parlament EU i Savet ministara su postigli dogovor o Direktivi za bezbednost mreža i informacija (*Network and Information Security Directive* – NIS). Finalni dokument objavljen je u julu 2016. godine.

Ova direktiva propisuje mere sa ciljem postizanja visokog zajedničkog stepena bezbednosti mreža i informacionih sistema unutar zemalja članica EU. U tom smislu ova direktiva:

- propisuje obavezu za sve zemlje članice da usvoje nacionalnu strategiju o bezbednosti mreža i informacionih sistema,
- uspostavlja Grupu za međunarodnu saradnju kako bi se omogućila i olakšala strateška saradnja i razmena informacija među zemljama članicama EU, i izgradilo međusobno poverenje,
- uspostavlja Mrežu CERT organizacija, sa ciljem da doprinese razvoju poverenja i efikasne operativne saradnje među ovim organizacijama,
- postavlja zahteve za bezbednošću i deljenje informacija sa operatorima ključne infrastrukture i servisa, i operatorima digitalnih servisa, i
- propisuje obvezu za sve zemlje članice da definišu nadležne organe, jedinstvene tačke kontakta, i CERT organizacije čiji će zadatak biti očuvanje bezbednosti mreža i informacionih sistema.

Kada je u pitanju Republika Srbija, još uvek nije usvojena nacionalna strategija o bezbednosti mreža i informacionih sistema, ali Zakonom o informacionoj bezbednosti, o kojem je bilo više reči u glavi 1 ove Studije, definišu se osnovni pojmovi i činioci, kao i okviri razvoja informacione bezbednosti, koji su u potpunosti u skladu sa odredbama i ciljevima NIS direktive. To, između ostalog, uključuje i obavezu uspostavljanja nacionalne CERT organizacije, koja bi se bavila koordinacijom i operativnim poslovima na očuvanju informacione bezbednosti na teritoriji Republike Srbije, ali i uzela učešće u ovim poslovima na planu međunarodne saradnje, u skladu sa ovlašćenjima koja iz Zakona proističu, tj. zadacima koje u tom smislu dobije od nadležnih organa za pitanja informacione bezbednosti.

U narednim poglavljima objašnjena je struktura direktive, sa posebnim osvrtom na delove koji su relevantni za nacionalne CERT organizacije.

3.1.1 Struktura direktive

Direktiva je strukturirana po sekcijama, pri čemu su specifične odredbe koje se direktno odnose na nacionalne CERT organizacije nalaze uglavnom u Poglavlju 3 i Aneksu 1.

Uvodni deo definiše kontekst u kojem se direktiva kreće. Naglašava se važnost i specifičnosti bezbednosti mreža i informacija, i opisuju akteri koji u tome imaju svoju bitnu ulogu.

Poglavlje 1 – opšte odredbe. U ovom poglavlju opisuju se ciljevi direktive, kao i njen pravni okvir. Takođe, dati su opisi osnovnih pojmova koji se koriste u daljem tekstu.

Poglavlje 2 – nacionalni okviri za NIS. Ovo poglavlje definiše listu različitih entiteta i pravne okvire koje svaka zemlja članica EU treba da uspostavi i koji bi bili usklađeni sa direktivom. Svaka zemlja članica EU treba da usvoji nacionalnu NIS strategiju, da odredi jednu ili više ovlašćenih nacionalnih organizacija sa kompetencijama za informacionu bezbednost, tj. nadležne organe, (kao i jedinstvenu tačku kontakta za slučajeve međunarodne saradnje), i da uspostavi barem jedan CERT tim. Sve ove organizacije moraju da pokriju određene pravce aktivnosti i servisa.

Poglavlje 3 – saradnja između kompetentnih organizacija. Ovo poglavlje definiše dve grupe za koje je predviđeno da treba da rade na poboljšanju saradnje između zemalja članica EU, na poslovima koji su u vezi sa NIS direktivom. Prva grupa je mreža za saradnju, koja se sastoji od predstavnika zemalja članica EU, Evropske Komisije i organizacije ENISA (*European Network and Information Security Agency*). Zadatak ove grupe treba da budu strateška pitanja. Druga grupa je mreža CERT organizacija, koja se sastoji od predstavnika nacionalnih CERT organizacija zemalja EU (kao i organizacije CERT-EU), sa predstavnicima Evropske Komisije u ulozi posmatrača, i ENISA-e za potrebe koordinacije i aktivne podrške.

Poglavlje 4 – bezbednost operatora ključnih servisa. Ovo poglavlje definiše bezbednosne zahteve i obaveze koje se postavljaju pred operatore i nosioce ključnih servisa. Ovi servisi su opisani u Aneksu 2 direktive.

Poglavlje 5 – bezbednost provajdera digitalnih servisa. Ovo poglavlje definiše bezbednosne zahteve i obaveze koje se postavljaju pred provajdere digitalnih servisa. Ovi provajderi su opisani u Aneksu 3 direktive.

Poglavlje 6 – standardizacija. Ovim poglavljem se ohrabruje i poziva na primenu standarda EU.

Poglavlje 7 – završne odredbe. Ovo poglavlje pokriva sve druge aspekte, kao što su detalji o vremenskim okvirima za implementaciju direktive, ili kaznene mere.

Aneks 1 – zahtevi i zadaci za CERT organizacije. Ovaj aneks navodi listu zadataka koje CERT organizacije zemalja EU treba da ispune.

Aneks 2 – pravci aktivnosti i entiteti. Ovaj aneks navodi sektore i podsektore koji treba da budu pokriveni strategijama informacione bezbednosti i aktivnostima CERT organizacija svake zemlje članice EU.

Aneks 3 – tipovi digitalnih servisa. Ovaj aneks navodi listu digitalnih servisa na koje se odnose odredbe direktive.

U narednim poglavljima biće detaljnije opisan sadržaj poglavlja direktive koji se odnose na delovanje nacionalnih CERT organizacija i njihovu međusobnu saradnju.

3.1.2 Poglavlje 2 – Nacionalni okviri za NIS

3.1.2.1 Član 7 – Nacionalna strategija za NIS

Svaka zemlja članica EU treba da usvoji nacionalnu strategiju za NIS, kojom se definišu strateški ciljevi i odgovarajuće politike i regulatorne mere sa ciljem postizanja i održavanja visokog nivoa bezbednosti mreža i informacionih sistema, koji se odnose barem

na sektore definisane u Aneksu 2 (poglavlje 3.1.4.2) i servise definisane u Aneksu 3 (poglavlje 3.1.4.3). U svojim pojedinostima nacionalna strategija za NIS se odnosi na:

- ciljeve i strategije na planu bezbednosti mreža i informacionih sistema,
- organizacione okvire za postizanje ciljeva i prioriteta nacionalne strategije za NIS, uključujući i uloge i odgovornosti organa uprave i drugih relevantnih entiteta,
- identifikacija mera za odgovor i oporavak od posledica incidenata, uključujući i saradnju javnog i privatnog sektora,
- ukazatelje na edukaciju, podizanje svesti i programe obuka koje se odnose na nacionalnu strategiju za NIS,
- ukazatelje na planove razvoja i istraživanja koji se odnose na nacionalnu strategiju za NIS,
- plan procene rizika, radi identifikacije rizika, i
- listu različitih činilaca i subjekata uključenih u implementaciju nacionalne strategije za NIS.

Države članice EU mogu tražiti pomoć od ENISA-e u razvoju nacionalne strategije za NIS.

Države članice EU treba da obaveste Evropsku Komisiju o svojim nacionalnim strategijama za NIS, u roku od tri meseca od dana usvajanja strategije. Tom prilikom mogu se izuzeti elementi straegije koji su u vezi sa pitanjima nacionalne bezbednosti.

3.1.2.2 Član 8 – Nadležni organi za informacionu bezbednost i jedinstvena tačka kontakta

Svaka zemlja članica EU treba da odredi jednu ili više ovlašćenih nacionalnih organizacija sa kompetencijama za informacionu bezbednost („nadležni organ“), koji svojim aktivnostima pokrivaju barem sektore opisane u Aneksu 2, i servise opisane u Aneksu 3. Pri tome, ove uloge mogu se dodeliti već postojećim ovlašćenim organizacijama.

Nadležni organi treba da nadgledaju primenu direktive na nacionalnom nivou.

Svaka zemlja članica EU treba da odredi jedinstvenu tačku kontakta na nacionalnom nivou za pitanja bezbednosti mreža i informacionih sistema. Pri tome, ova uloga se može dodeliti nekoj od već postojećih organizacija. U slučaju da se u nekoj zemlji odredi samo jedna organizacija kao nadležni organ za NIS, ta organizacija preuzima i ulogu jedinstvene tačke kontakta.

Jedinstvena tačka kontakta treba da preuzme funkciju veze kako bi se omogućila prekogranična saradnja sa sličnim organizacijama u drugim zemljama EU, i grupom za saradnju koja je opisana u članu 11 direktive, kao i mrežom CERT organizacija koja je opisana u članu 12 direktive.

Zemlje članice EU treba da obezbede da nadležni organi i jedinstvene tačke kontakta imaju na raspolaganju adekvatne resurse da na efikasan način sprovode zadatke i na taj način ispunjavaju ciljeve definisane direktivom. Zemlje članice EU će obezbediti efikasnu i bezbednu saradnju svojih ovlašćenih predstavnika sa predstavnicima grupe za saradnju.

Nadležni organ i jedinstvena tačka će, kada god je to moguće i u skladu sa nacionalnim zakonodavstvom, učestvovati u saradnji sa relevantnim nacionalnim istražnim i pravosudnim organima i agencijama za zaštitu podataka.

Svaka zemlja članica EU će bez odlaganja obavestiti Evropsku Komisiju o izboru nadležnog organa i jedinstvene tačke kontakta, njihovim ciljevima i zadacima, i svim izmenama koje se u tom smislu dogode. Takođe, informacije o nadležnom organu i jedinstvenoj tački kontakta moraju biti javno objavljene u svakoj zemlji. Pri tome, Evropska Komisija objavljuje listu nadležnim organa i jedinstvenih tačaka kontakta u EU.

3.1.2.3 Član 9 – CERT organizacije

Svaka zemlja članica EU će odrediti jednu ili više CERT organizacija koje će u skladu sa zahtevima iz tačke 1 Aneksa 1, pokrivati barem sektore definisane u Aneksu 2 i servise definisane u Aneksu 3, i biti odgovorne za upravljanje bezbednosnim rizicima i incidentima u skladu sa prethodno kvalitetno definisanim procedurama. CERT organizacije mogu biti osnovane u okviru organizacija prethodno definisanih nadležnih organa.

Zemlje članice EU će osigurati da CERT organizacije imaju na raspolaganju adekvatne resurse da efikasno izvršavaju svoje zadatke, kao što je to opisano u tački 2 Aneksa 1. Takođe, zemlje članice će osigurati efikasnu i bezbednu saradnju svojih CERT organizacija sa mrežom CERT organizacija, kao što je opisano u članu 12.

Zemlje članice će osigurati da njihove CERT organizacije imati pristup odgovarajućoj bezbednoj i pouzdanoj komunikacionoj i informacionoj infrastrukturi na nacionalnom nivou.

Zemlje članice će obavestiti Evropsku Komisiju o delokrugu, kao i glavnim elementima procesa upravljanja incidentima njihovih CERT organizacija.

Zemlje članice mogu zahtevati pomoć ENISA-e u uspostavljanju nacionalnih CERT organizacija.

3.1.2.4 Član 10 – Saradnja na nacionalnom nivou

U slučaju kada su u pitanju razdvojene organizacije u okviru iste države, nadležni organ, jedinstvena tačka kontakta i CERT organizacije će međusobno sarađivati radi ispunjenja obaveza u vezi sa direktivom.

Zemlje članice EU će osigurati da ili nadležni organi, ili nacionalne CERT organizacije, primaju obaveštenja o incidentima prijavljenim u skladu sa ovom direktivom. Čak i ukoliko zemlje članice odluče da CERT organizacije ne treba da primaju obaveštenja o incidentima, ovim organizacijama, u meri u kojoj je to neophodno za ispunjenje njihovih zadataka, potrebno je omogućiti pristup podacima o incidentima koje prijavljuju operatori ključnih servisa, ili provajderi digitalnih servisa.

Zemlje članice će osigurati da nadležni organi, ili nacionalne CERT organizacije, informišu jedinstvenu tačku kontakta o incidentima prijavljenim u skladu sa ovom direktivom. Do 9. avgusta 2018. godine, i svake godine nakon toga, jedinstvena tačka kontakta će grupi za međunarodnu saradnju podneti sumarni izveštaj o prijavljenim incidentima, uključujući i broj prijava i prirodu prijavljenih incidenata, kao i akcije koje su preduzete u skladu sa ovom direktivom.

3.1.3 Poglavlje 3 – Međunarodna saradnja

3.1.3.1 Član 11 – Grupa za međunarodnu saradnju

Kako bi se omogućila i olakšala strateška saradnja i razmena informacija među zemljama članicama EU, i kako bi se izgradilo neophodno poverenje, a sa ciljem postizanja visokog i ujednačenog nivoa bezbednosti komunikacionih i informacionih sistema širom EU, ustanovljava se Grupa za međunarodnu saradnju na polju informacione bezbednosti. Grupa za međunarodnu saradnju će sprovoditi svoje aktivnosti u skladu sa ovom direktivom, kako je u daljem tekstu navedeno.

Grupa za međunarodnu saradnju će biti sastavljena od predstavnika zemalja članica EU, Evropske Komisije i organizacije ENISA. Ukoliko je moguće i potrebno, grupa može pozvati i predstavnike drugih organizacija da učestvuju u njenom radu.

Evropska Komisija će obezbediti i funkciju sekretarijata.

Grupa za međunarodnu saradnju će sprovoditi sledeće aktivnosti:

- obezbediti strateške smernice za aktivnosti mreže CERT organizacija formirane po odredbama ove direktive (član 12),
- razmenjivati primere dobre prakse i informacije u vezi sa incidentima prijavljenim u skladu sa ovom direktivom,
- razmenjivati primere dobre prakse među zemljama članicama EU, u saradnji sa ENISA-om, pomažući zemljama članicama u izgradnji kapaciteta za osiguranje bezbednosti informacionih sistema i mreža,
- razmatranje kapaciteta i sposobnosti zemalja članica EU da osiguraju informacionu bezbednost, kao i (na doborovoljnoj bazi) evaluacija nacionalnih strategija o informacionoj bezbednosti i efikasnosti CERT organizacija, uz identifikaciju dobre prakse,
- razmena informacija i dobre prakse na polju podizanja svesti i obuka na temu informacione bezbednosti,
- razmena informacija i dobre prakse na polju razvoja i istraživanja na temu informacione bezbednosti,
- u situacijama gde je to relevantno, razmena iskustava na polju informacione bezbednosti sa relevantnim institucijama, kancelarijama i agencijama EU,
- razmatranje standarda i specifikacija koje donose relevantne evropske organizacije za standardizaciju,
- prikupljanje informacija o dobroj praksi na temu bezbednosnih rizika i incidenata,
- analiza sumarnih godišnjih izveštaja dobijenih od nadležnih organa zemalja EU u skladu sa ovom direktivom,
- razmatranje obavljenog posla na temu preduzetih bezbednosnih testova informacionih i komunikacionih sistema, programa edukacija i obuka, uključujući i posao koji obavlja ENISA,
- razmena dobre prakse, u saradnji sa ENISA-om, na polju identifikacije operatora ključnih servisa u zemljama članicama EU, uključujući i veze i međuzavisnoti koje se odnose na bezbednosne rizike i incidente koji pogađaju ove operatore,
- razmatranje modaliteta za izveštavanje o prijavama incidenata u skladu sa ovom direktivom.

Do 9. februara 2018. godine, i svake druge godine nakon toga, grupa za međunarodnu saradnju će izraditi plan rada u pogledu akcija koje treba sprovesti radi postizanja svojih ciljeva i sprovođenja zadataka koji će biti konzistentni sa ciljevima ove direktive.

Za potrebe revizija u skladu sa ovom direktivom, do 9. avgusta 2018, i na svakih godinu i po nakon toga, grupa za međunarodnu saradnju će pripremiti izveštaj o proceni stečenog iskustva na temu strateške saradnje koja je opisana u ovom članu.

Evropska Komisija će usvojiti osnivačka akta zajedno sa procedurama neophodnim za implementaciju i funkcionisanje Grupe za međunarodnu saradnju. Prva radna verzija osnivačkog akta biće spremna do 9. februara 2017. godine.

3.1.3.2 Član 12 – Mreža CERT organizacija

Mreža nacionalnih CERT organizacija se uspostavlja sa ciljem da se obezbedi poverenje između zemalja članica EU i promoviše brza i efikasna operativna saradnja.

Mreža CERT organizacija sastojaće se od predstavnika nacionalnih CERT organizacija država članica EU i organizacije CERT-EU. Takođe, predstavnici Evropske Komisije će uzeti učešće kao posmatrači. ENISA će obezbediti funkciju sekretarijata i aktivno podržavati saradnju CERT organizacija.

Mreža CERT organizacija će sprovoditi sledeće aktivnosti:

- razmenu informacija o servisima CERT organizacija, i kapacitetima za operativno delovanje i saradnju,
- na zahtev predstavnika nacionalne CERT organizacije države članice EU, koja je potencijalno pogođena nekim bezbednosnim incidentom, sprovodiće se razmena i analiza poverljivih informacija u vezi sa tim bezbednosnim incidentom i pridruženim rizicima. Međutim, CERT organizacija može odbiti da učestvuje u ovoj diskusiji ukoliko postoji rizik da se na taj način negativno utiče na istragu incidenta,
- razmenu nepoverljivih informacija koje se tiču individualnih incidenata na dobrovoljnoj bazi,
- na zahtev predstavnika nacionalne CERT organizacije države članice EU sprovodiće se analiza, i ukoliko je to moguće, izvođenje koordinisanog odgovora na incident koji je identifikovan pod jurisdikcijom te države,
- obezbeđenje podrške za zemlje članice EU u razrešavanju prekograničnih incidenata na bazi dobrovoljne uzajamne pomoći,
- razmatranje, istraživanje i identifikovanje budućih formi operativne saradnje koja se tiče:
    - kategorija rizika i incidenata,
    - ranog upozoravanja,
    - uzajamne pomoći,
    - principa i modaliteta za saradnju u slučaju potrebe za odgovorom na prekogranične rizike i incidente,
- informisanje međunarodne grupe za saradnju o svojim aktivnostima i budućim okvirima operativne saradnje, kao i traženje smernica u tom smislu,
- analizu iskustava stečenih tokom testova bezbednosti informacionih sistema i mreža, uključujući i testove koje organizuje ENISA,
- analizu kapaciteta i sposobnosti pojedinačnih CERT organizacija na njihov zahtev, i
- izdavanje smernica kako bi se olakšalo usaglašavanje operativnih procedura, koje se tiču primene odredbi ovog člana po pitanjima operativne saradnje.

Za potrebe revizija u skladu sa ovom direktivom, do 9. avgusta 2018. godine, i na svakih godinu i po dana nakon toga, Mreža CERT organizacija će pripremiti izveštaj o proceni stečenog iskustva na polju operativne saradnje, uključujući i zaključke i preporuke koji proističu iz ove direktive. Taj izveštaj će biti podnet grupi za međunarodnu saradnju.

3.1.3.3 Član 13 – Međunarodna saradnja van EU

Evropska Unija može zaključiti međunarodne ugovore sa zemljama koje nisu njene članice, ili međunarodnim organizacijama, kojima se stvaraju uslovi da se organizuje njihovo

učešće u nekim aktivnostima grupe za međunarodnu saradnju. Takvi ugovori će uzeti u obzir potrebu da se obezbedi odgovarajući nivo zaštite podataka i informacija.

3.1.4 Aneksi NIS direktive

3.1.4.1 Aneks 1 – Zahtevi i zadaci za CERT organizacije

Zahtevi i zadaci koji se postavljaju pred CERT organizacije biće adekvatno i jasno definisani i podržani nacionalnim politikama i/ili regulativom. Oni obuhvataju sledeće:

- Zahtevi za CERT organizacije:
  - CERT organizacije će obezbediti visok nivo dostupnosti svojih komunikacionih servisa izbegavanjem jedinstvenih tačaka ispada, i postojaće nekoliko načina na koje mogu biti kontaktirane, i preko kojih oni mogu kontaktirati druge organizacije, u bilo kom trenutku. Takođe, kanali komunikacije biće jasno specificirani i javno dostupni svim konstituentima i spoljnjim partnerima.
  - Prostorije CERT tima i pripadajući informacioni sistemi biće smešteni na bezbednim lokacijama.
  - Kontinuitet poslovanja:
    - CERT organizacije biće opremljene odgovarajućim sistemom za upravljanje incidentima, kako bi se olakšalo svakodnevno obavljanje tog posla,
    - CERT organizacije imaće odgovarajući broj zaposlenih kako bi osigurali svoju dostupnost u bilo kom trentuku, i
    - CERT organizacije će se oslanjati na infrastrukturu sa garantovanom visokom dostupnošću. U tom smilsu biće obezbeđeni redundantni sistemi i rezervna lokacija za rad.
  - CERT organizacije imaće mogućnost da, prema svojim željama i potrebama, učestvuju u mreži za međunarodnu saradnju.

- Zadaci za CERT organizacije:
  - Zadaci CERT organizacija obuhvataće u najmanjem sledeće:
    - upravljanje incidentima na nacionalnom nivou,
    - izdavanje ranih upozorenja, alarma, najava, i razmena informacija sa relevantnim entitetima o bezbednosnim rizicima i incidentima,
    - razrešavanje incidenata,
    - izvođenje dinamične analize i podizanje svesti o bezbednosnim rizicima i incidentima, i
    - učestvovanje u radu mreže za saradnju CERT organizacija.
  - CERT organizacije će uspostaviti kontakte za saradnju sa privatnim sektorom.
  - Radi olakšanja saradnje CERT organizacije će promovisati usvajanje i korišćenje zajedničke i standardizovane prakse za:
    - procedure za upravljanje bezbednosnim rizicima i incidentima, i
    - šeme klasifikacije informacija o bezbednosnim rizicima i incidentima.

3.1.4.2 Aneks 2 – Tipovi nosilaca ključne informacione infrastrukture

SEKTOR	PODSEKTOR	TIP ENTITETA
Energetika	Električna energija	Proizvođači električne energije
		Operatori distributivnih sistema
		Operatori transmisionih sistema
	Nafta	Operatori cevovoda za prenos nafte
		Operatori proizvodnje nafte, rafinisanja, skladištenja i transporta nafte
	Gas	Proizvođači gasa
		Operatori distributivnih sistema
		Operatori transmisionih sistema
		Operatori skladišnih sistema
		Operatori LNG (*Liquid Natural Gas*) sistema
		Preduzeća za istraživanje prirodnog gasa
		Operatori za rafinisanje i tretman prirodnog gasa
Saobraćaj	Vazdušni saobraćaj	Vazduhoplovne kompanije
		Aerodromi, organizacije koje rukovode aerodromima, i organizacije koje izvode pomoćne radove na održavanju aerodromskih sistema i instalacija
		Organizacije za upravljanje vazdušnim saobraćajem (kontrola leta)
	Železnički saobraćaj	Organizacije za upravljanje železničkom infrastrukturom
		Preduzeća za železnički saobraćaj i usluge
	Vodeni saobraćaj	Preduzeća za pružanje usluga putničkog i teretnog saobraćaja na vodi, ne uključujući pojedinačna plovila koja te organizacije poseduju
		Organizacije za upravljanje lukama i lučkim postrojenjima i organizacije koje izvode pomoćne radove na održavanju lučkih sistema i instalacija
	Drumski saobraćaj	Organizacije za upravljanje drumskim saobraćajem
		Preduzeća za pružanje usluga u drumskom saobraćaju
Banke		Kreditne institucije

SEKTOR	PODSEKTOR	TIP ENTITETA
Infrastruktura finansijskih tržišta		Operatori trgovačkih prostora (berze)
		Organizacije za trgovinu hartijama od vrednosti
Zdravstvo	Istitucije zdravstvene zaštite, uključujući bolnice i privatne klinike	Institucije za brigu o zdravlju i pružanje medicinske pomoći
Proizvodnja i distribucija vode za piće		Preduzeća za proizvodnju i distribuciju pijaće vode za ljudsku upotrebu, izuzev preduzeća kojima je ova delatnost samo deo aktivnosti koje se odnose i na distribuciju i prodaju drugih roba koje nisu od ključnog značaja
Digitalna infrastruktura		Provajderi telekomunikacionih i internet servisa
		Provajderi DNS (*Domain Name System*) servisa
		Registratori domena (TLD – *Top-Level Domain*)

3.1.4.3 Aneks 3 – Tipovi digitalnih servisa

- Platforme za online trgovinu,
- Platforme za pretraživanje na Internetu,
- *Cloud computing* servisi.

3.2 NACIONALNE STRATEGIJE INFORMACIONE BEZBEDNOSTI

Pouzdane komunikacione mreže i servisi su već dugo vremena kritični element u obezbeđivanju dobrobiti društva i napredovanju i stabilnosti ekonomije. Na kvalitetno funkcionisanje važnih javnih servisa, koji se oslanjaju na javne telekomunikacione mreže, utiču maliciozni napadi preko interneta, smetnje usled prirodnih fenomena, softverski i hardverski ispadi sistema, ali i ljudske greške. Sve ove smetnje otkrivaju povećanu zavisnost društava od korišćenja komunikacionih mreža i odgovarajućih servisa. Sve se ovo reflektuje kroz jednu od odredaba nemačke strategije za informacionu bezbednost: „Dostupnost mreža i servisa, kao i integritet, autentičnost i poverljivost podataka postali su pitanja od vitalnog značaja u 21. veku. Stoga se osiguranje informacione bezbednosti pretvorilo u glavni izazov za države, ekonomije i društvo, kako na nacionalnom, tako i na međunarodnom nivou.“

Nekoliko publikacija Evropske Komisije podvlači važnost mrežne i informacione bezbednosti i pouzdanosti sistema, sa težnjom da se formira jedinstveni evropski informacioni prostor. Razna dokumenta, koja se stalno dopunjuju, kao što su regulatorne direktive i dokumenta o zaštiti kritične informacione infrastrukture, predlažu konkretne politike i

regulatorne odredbe sa ciljem da se poboljša bezbednost i pouzdanost javnih telekomunikacionih mreža i servisa.

Informaciona bezbednost se sve više posmatra kao strateški nacionalni zadatak, koji se proteže horizontalno kroz sve slojeve društva. Nacionalna strategija informacione bezbednosti je alat kojim se poboljšava bezbednost i pouzdanost nacionalne infrastrukture i servisa. To je opšti temeljni dokument koji se tiče informacione bezbednosti kojim se definiše skup nacionalnih prioriteta i ciljeva koje treba postići u zadatom vremenskom okviru. Kao takav, on predstavlja strateški okvir u nacionalnom pristupu informacionoj bezbednosti.

Kako bi se pomoglo zemljama članicama EU u definisanju uspešne nacionalne strategije informacione bezbednosti ENISA je razvila priručnik sa preporukama i primerima dobre prakse u izradi dokumenta strategije. U narednim poglavljima data je kratka analiza trenutnog statusa razvoja strategija informacione bezbednosti u zemljama EU i šire, identifikovane su zajedničke teme i razlike u pristupima, i navedene primedbe i odgovarajuće preporuke.

3.2.1 Evolucija strategija informacione bezbednosti u zemljama članicama EU

Prve nacionalne strategije informacione bezbednosti počele su da se pojavljuju pre 15-tak godina. Jedna od prvih zemalja koja je prepoznala informacionu bezbednost kao temu od strateškog nacionalnog značaja je SAD. Tokom 2003. godine oni su objavili dokument „*National Strategy to Secure Cyberspace*“. Taj dokument je bio deo sveobuhvatne nacionalne strategije državne bezbednosti, koja je bila razvijena kao odgovor na terorističke napade 11. septembra 2001. godine.

U narednim godinama, a iz sličnih razloga kao u SAD, počeli su da se pojavljuju slični akcioni planovi i strategije i u zemljama Evrope. Nemačka je 2005. godine usvojila „Nacionalni plan za zaštitu informacione infrastrukture“. Sledeće godine Švedska je usvojila dokument „Strategije za poboljšanje bezbednosti na Internet mreži u Švedksoj“. Posle ozbiljnog bezbednosnog incidenta u Estoniji 2007. godine, ta zemlja je bila prva zemlja članica EU koja je objavila opšti dokument nacionalne strategije informacione bezbednosti 2008. godine. S obzirom da je do tada već obavljeno puno posla po ovom pitanju na nacionalnim nivoima, u naredne četiri godine još 10 zemalja EU je objavilo nacionalne strategije informacione bezbednosti. Ovi dokumenti su ukratko opisani u narednom tekstu:

- *Estonija (2008)*: Estonija podvlači potrebu za opštom informacionom bezbednošću, i fokusira se na informacione sisteme. Sve preporučene mere zaštite su civilnog karaktera i koncentrišu se na regulativu, edukaciju i saradnju na poslovima informacione bezbednosti.
- *Finska (2008)*: osnova njihove strategije je stanovište da se informaciona bezbednost odnosi na problem bezbednosti podataka, i da je to stvar od značaja za ekonomiju, i u bliskoj vezi sa razvojem finskog informatičkog društva.
- *Slovačka (2008)*: osiguranje informacione bezbednosti se posmatra kao ključna potreba za funkcionisanje i razvoj društva. Stoga je svrha strategije da se razvije sveobuhvatan okvir za razvoj informacione bezbednosti. Ciljevi njihove strategije uglavnom se fokusiraju na prevenciju, i spremnost na reagovanje i održivost bezbednosti.
- *Češka (2011)*: ključne teme strategije informacione bezbednosti uključuju zaštitu od pretnji kojima su informacioni i komunikacioni sistemi i tehnologije izloženi, kao i saniranje eventualnih posledica u slučaju napada na ove sisteme. Strategija se uglavnom fokusira na neometani pristup servisima, integritet i poverljivost podataka

unutar češkog informatičkog prostora, i koordinisana je sa drugim povezanim strategijama i konceptima.

- *Francuska (2011)*: njihova strategija se fokusira na omogućavanje da informacioni sistemi budu otporni u slučaju događaja koji bi mogli kompromitovati dostupnost, integritet i poverljivost podataka. Francuska daje naglasak na tehnička sredstva koja su u vezi sa bezbednošću informacionih sistema, ali i borbu protiv informatičkog kriminala i uspostavljane sistema odbrane informacionih sistema.
- *Nemačka (2011)*: Nemačka se fokusira na prevenciju incidenata i procesuiranje napadača na informacione sisteme, a naročito na zaštitu ključne informacione infrastrukture. Strategijom se postavlja osnova kritičnih informacionih i komunikacionih sistema. Njome se analizira postojeća regulativa da bi se otkrilo da li je, i u kom segmentu, potrebno uložiti dodatne napore da bi se obezbedili informacioni sistemi u Nemačkoj, kako bi se postojeće funkcije sertifikovale od strane države, i kako bi se formirale radne grupe za pomoć privrednim društvima i drugim subjektima u poslovima informacione bezbednosti.
- *Litvanija (2011)*: Litvanija ima za cilj da utvrdi ciljeve i zadatke za razvoj informatičkog društva, sa ciljem da se osigura poverljivost, integritet i dostupnost informacija i servisa. Dodatno, cilj je i zaštita mreža elektronskih komunikacija, informacionih sistema i ključne informacione infrastrukture od bezbednosnih incidenata i napada, kao i zaštita privatnosti podataka o ličnosti. Strategija, takođe, definiše zadatke, koji kada budu islunjeni treba da garantuju potpunu bezbednost informacionog okruženja i svih entiteta koji u njemu sprovode svoje aktivnosti.
- *Luksemburg (2011)*: prepoznajući sveprisutnost informacionih tehnologija i servisa, strategija navodi da je njen prioritet zaštita od štetnih efekata po javnu bezbednost i ekonomiju države. Takođe se podvlači i važnost informacionih i komunikacionih tehnologija za građane, društvo, i napredak ekonomije u celini. Strategija se bazira na pet linija aktivnosti, koje se ukratko mogu sumirati kao zaštita ključne informacione infrastrukture i upravljanje incidentima, modernizacija zakonodavstva, saradnja na nacionalnom i međunarodnom nivou, edukacija i podizanje svesti, i promovisanje standarda bezbednosti.
- *Holandija (2011)*: Holandija ima za cilj očuvanje bezbednosti i pouzdanosti informacionih i komunikacionih tehnologija, istovremeno potvrđujući potrebu da se zaštiti otvorenost i slobode na Internetu. Holandija u svoju strategiju uključuje i definiciju informacione bezbednosti: „informaciona bezbednost znači biti oslobođen od opasnosti i pretnji koje mogu biti posledica smetnji, napada ili ispada u funkcionisanju informacionih i komunikacionih sistema. Opasnosti i pretnje koje mogu biti posledica smetnji, napada ili ispada u funkcionisanju informacionih i komunikacionih sistema, sastoje se od ograničenja u dostupnosti ili pouzdanosti informacionih i komunikacionih sistema, narušavanje poverljivosti informacija koje se čuvaju u informacionim sistemima, ili narušavanje integriteta podataka.“
- *Velika Britanija (2011)*: pristup Velike Britanije je koncentrisati se na nacionalne ciljeve, koji su u vezi sa sve većom potrebom za informacionom bezbednošću: učiniti Veliku Britaniju glavnom ekonomskom silom u inovacijama, investicijama i kvalitetu na polju informacionih i komunikacionih tehnologija, i na taj način biti kadar da se iskoriste svi potencijali i prednosti informacionih tehnologija. Cilj strategije je sprečiti rizike od napada kriminalnih organizacija, terorističkih organizacija, ili drugih država, kako bi se informaciono okruženje učinilo bezbednim za potrebe svojih građana i ekonomije.

3.2.2 Strategije informacione bezbednosti van zemalja članica EU

U ovom poglavlju biće reči o strategijama tri države koje nisu članice EU. I mnoge druge zemlje, koje ovde nisu navedene, usvojile su strategije informacione bezbednosti, što je znak da je važnost informacione bezbednosti prepoznata na globalnom nivou:

- *SAD* – u SAD je maja 2011. godine usvojen dokument „*International Strategy for Cyber-space*“, koji opisuje skup aktivnosti u sedam različitih oblasti, koje se baziraju na modelu saradnje koji uključuje državni sektor, međunarodne partnere i privatni sektor:
  - ekonomija: promovisanje međunarodnih standarda, inovacija i otvorenog tržišta,
  - zaštita komunikacionih mreža: poboljšanje bezbednosti i pouzdanosti,
  - sprovođenje zakona: proširivanje saradnje i vladavina zakona,
  - vojska: priprema za izazove 21. veka,
  - upravljanje Internet mrežom: promovisanje efikasnih i inkluzivnih struktura,
  - međunarodni razvoj: uspostavljanje mogućnosti za napredak, bezbednost i prosperitet, i
  - slobode na Internet mreži: podrška osnovnim vrednostima slobode i privatnosti.

- *Kanada* – strategija informacione bezbednosti u Kanadi je objavljena 2010. godine, i bazira se na tri stuba:
  - obezbeđenje državnih sistema,
  - partnerstvo u obezbeđivanju sigurnosti informacionih sistema izvan državnih ustanova, i
  - pomoć građanima da budu bezbedni na Internetu.

  Cilj prve stavke je da se ustanove jasne uloge i odgovornosti, kako bi se ojačala bezbednost državnih informacionih sistema i kako bi se podigla svest o važnosti informacione bezbednosti u njenim institucijama.
  Druga stavka pokriva veliki broj partnerskih inicijativa sa lokalnim samoupravama i uključuje i privatni sektor, kao i sektor kritične informacione infrastrukture.
  I na kraju, treća stavka pokriva borbu protiv informatičkog kriminala, i zaštitu građana na Internetu, sa posebnim osvrtom na privatnost podataka.

- *Japan* – i japanska strategija informacione bezbednosti može biti razložena na odgovarajući broj ključnih oblasti delovanja:
  - ojačavanje bezbednosnih politika i uspostavljanje organizacija za suprotstavljanje napadima na informacionu bezbednost,
  - uspostavljanje bezbednosnih politika usklađenih sa promenama u bezbednosnom okruženju informacionih sistema, i
  - uspostavljanje aktivnih, umesto pasivnih, mera bezbednosti.

  Glavne aktivnosti koje strategija pokriva su sledeće:
  - prevazilaženje rizika kako bi se postigla bezbednost i pozdanost sistema,
  - implementacija bezbednosnih politika kojima se ojačava nacionalna bezbednost i informatička ekspertiza u upravljanju kriznim situacijama,

- uspostavljanje trojne bezbednosne politike koja obuhvata sve aspekte nacionalne bezbednosti, upravljanja kriznim situacijama, i zaštitu krajnjih korisnika. Aspekt informacione bezbednosti koji se fokusira na zaštitu krajnjih korisnika je od posebne važnosti,
- uspostavljanje politike informacione bezbednosti koja doprinosi strategiji ekonomskog razvoja,i
- izgradnja međunarodne saradnje na poslovima informacione bezbednosti.

3.2.3 Zajedničke teme

Jasna i usaglašena definicija informacione bezbednosti je nešto što nedostaje i u evropskim i u svetskim okvirima. Razumevanje ovog i drugih ključnih termina varira od zemlje do zemlje. To utiče na različite pristupe strategijama informacione bezbednosti u raznim zemljama. Nedostatak zajedničkog razumevanja i pristupa među državama može otežati međunarodnu saradnju, što je potreba koje su svesne sve države.

Glavne tačke koje nacionalne strategije informacione bezbednosti obično pokrivaju su:

- Definisati okvire upravljanja informacionom bezbednošću.
- Definisati odgovarajući mehanizam (obično je u pitanju javno-privatno partnerstvo) kojim se omogućava svim subjektima da razmotre i dogovore se o različitim politikama i problemima koji se tiču informacione bezbednosti.
- Otkriti i definisati potrebne političke i regulatorne mere, i jasno definisane uloge, odgovornosti i prava na strani javnog i privatnog sektora (tj. uspostavljanje nove pravne regulative za borbu protiv informatičkog kriminala, obavezno prijavljivanje bezbednosnih incidenata, definisanje minimuma bezbednosnih mera i smernica, nova pravila nabavke i slično).
- Uspostavljanje ciljeva i načina razvoja nacionalnih kapaciteta i potrebnih pravnih akata radi angažovanja u međunarodnim naporima u neutralisanju efekata informatičkog kriminala.
- Identifikovanje kritične informacione infrastrukture, uključujući ključne sisteme, servise, i njihove međuzavisnosti.
- Razvoj i unapređenje spremnosti za odbranu i priprema planova oporavka te ključne informacione infrastrukture u slučaju napada. To uključuje i integraciju organizacionih struktura koje razvijaju, implementiraju i testiraju spremnost za odbranu i planove i mere oporavka. Ovo se može odnositi i na integraciju postojećih nacionalnih i državnih CERT organizacija.
- Definisanje sistematskog i integrisanog pristupa upravljanju rizicima na nacionalnom nivou (tj. razmena poverljivih informacija i kreiranje nacionalnih registara rizika).
- Definisanje skupa ciljeva radi sprovođenja kampanja za podizanje svesti o informacionoj bezbednosti, koje bi uticale na navike i ponašanje krajnjih korisnika informacionih sistema.
- Definisanje potreba za edukacijom profesionalaca koji se bave informacionim sistemima i bezbednošću, kao i kreiranje programa obuke kojima bi se poboljšale veštine krajnjih korisnika informacionih sistema i servisa.
- Međunarodna saradnja među državama članicama EU, kao i šire.
- Sveobuhvatna istraživanja i razvoj programa koji se fokusiraju na narastajuće bezbednosne probleme postojećih i budućih sistema i servisa.

3.2.4 Zaključci i preporuke

U okruženju u kojem pretnje po informacionu bezbednost stalno narastaju i evoluiraju, zemlje članice EU će imati velike koristi od fleksibilne i dinamične strategije informacione bezbednosti, kako bi se suočile sa novim globalnim pretnjama. S obzirom na prirodu ovih pretnji koje ne poznaju granice, od ključnog značaja je fokusirati se na snažnu međunarodnu saradnju. Saradnja na nivou čitave Evrope je neophodna kako bi se efikasno pripremili, ali i odgovorili na napade na informacione sisteme i mreže. Sveobuhvatne nacionalne strategije informacione bezbednosti su prvi neophodan korak u tom smeru.

Zemljama članicama EU daju se sledeće preporuke:

- Kratkoročno:
  - Razvijati, procenjivati i održavati nacionalne strategije informacione bezbednosti, kao i akcione planove definisane ovim strategijama.
  - Jasno naznačiti delokrug i ciljeve strategije, kao i definiciju informacione bezbednosti koja se koristi u strategiji.
  - Obezbediti da se prime i ispoštuju primedbe i sugestije koje dolaze od državne uprave, nacionalnih regulatornih agencija i drugih javnih institucija.
  - Sarađivati sa drugim evropskim zemljama i Evropskom Komisijom kako bi se obezbedio koherentan pristup problemima bezbednosti koji su globalne prirode, tj. pristuni u raznim državama.
  - Biti svestan da konstantni razvoj informacionih sistema i servisa podrazumeva i evoluciju bezbednosnih pretnji, pa je dokument strategije stalno podložan promenama.
  - Prethodna napomena ne odnosi se samo na narastajuće pretnje i rizike, već je i prilika za napredak i poboljšanje načina na koji se informacione i komunikacione tehnologije koriste za državne uprave, ili dobrobit privrede i građana.
  - Osigurati da strategije uzimaju u obzir posao koji je već obavljen na poboljšanju bezbednosti informacionih sistema i nacionalne i međunarodne ključne informacione infrastrukture, izbegavajući na taj način bespotrebno trošenje resursa umesto da se oni koriste za rešavanje novih izazova.
  - Podržati Evropsku Komisiju u definisanju bezbednosne strategije na Internetu.

- Dugoročno:
  - Dogovoriti se o opšte prihvatljivoj radnoj definiciji informacione bezbednosti, koja je dovoljno precizna da bi bila osnova za definisanje zajedničkih ciljeva širom EU.
  - Obezbediti da se strategije informacione bezbednosti EU i njenih članica ne kose sa ciljevima u okviru šire međunarodne zajednice, već da budu podrška globalnim naporima na polju informacione bezbednosti.

Potrebno je da javni i privatni sektor blisko sarađuju na implementaciji strategija informacione bezbednosti. Ovo se može postići razmenom informacija, primenom dobrih praksi u upravljanju incidentima, i učestovovanjem u sveobuhvatnim testovima bezbednosti na nacionalnom i međunarodnom nivou.

3.3 RAZVOJ CERT ORGANIZACIJA

Nacionalne i državne CERT organizacije imaju ključnu ulogu u zaštiti bezbednosti informacionih i komunikacionih sistema u svojim zemljama. Njihova uloga može biti veoma široka, od upravljanja razrešenjem bezbednosnih incidenata, do podizanja svesti o informacionoj bezbednosti i poslova edukacije.

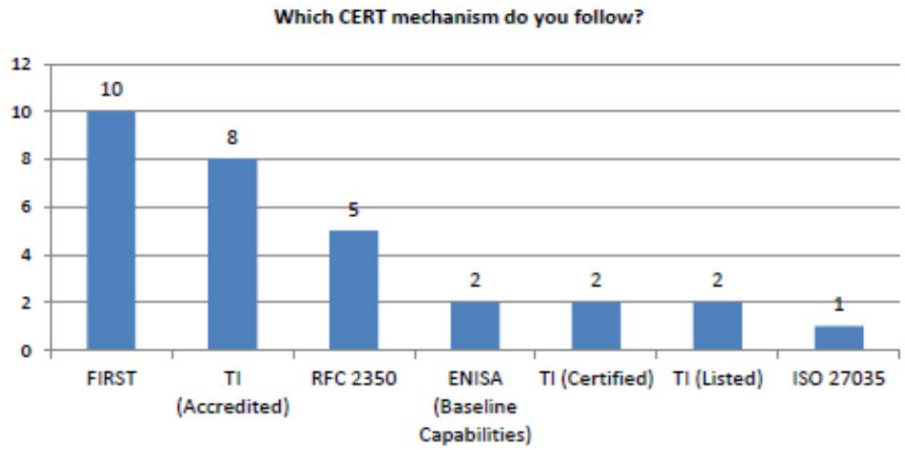
Trenutna situacija u evropskim zemljama je da se državne CERT organizacije tipično bave zaštitom državnih institucija i ključne informacione infrastrukture svoje države. Sa druge strane, nacionalne CERT organizacije mogu imati različite uloge u različitim zemljama. U nekim zemljama su odgovorne za ceo IP adresni prostor svoje zemlje, a u nekim imaju i dodatnu ulogu poslednjeg odredišta, kada ne postoji drugi kontakt koji bi mogao da preduzme neophodne akcije u razrešenju nekog incidenta. U svakom slučaju, kada u procesu razrešenja nekog incidenta, koji prevazilazi granice jedne države, treba uspostaviti kontakt sa drugom državom, to se obično čini preko kontakta nacionalne CERT organizacije druge države. Pri tome, sve je češći slučaj da CERT organizacije očekuju da i timovi u drugim zemljama, koji se bave istim poslom, budu u stanju da reaguju na zahteve za saradnju u kratkom vremenskom roku, i da se prema informacijama koje se tom prilikom razmenjuju odnose na profesionalan način.

U skladu sa prethodno navedenim, od izuzetne je važnosti da nacionalne CERT organizacije budu članice međunarodnih organizacija i tela za saradnju, kao i da nivo svojih sposobnosti i ekspertize potvrde kroz odgovarajući proces sertifikacije, što je i tema izlaganja u narednim poglavljima.

3.3.1 Međunarodne organizacije za informacionu bezbednost

Postoje brojne organizacije, kako na tlu Evrope tako i šire, koje definišu različite mehanizme za razvoj sposobnosti CERT organizacija, i samim tim njihovog iskustva i zrelosti. Ove organizacije obezbeđuju korisne informacije o poslovanju CERT organizacija koje su njihove članice, kao što su njihove politike, procedure, mogućnosti za saradnju, ili alati koje koriste u svakodnevnom radu. Sve CERT organizacije se trude da konstantno razvijaju svoje sposobnosti i budu dobro prihvaćene među svojim konstituentima, ali i da više i češće sarađuju i da budu priznate među drugim CERT organizacijama, u svojoj zemlji i na međunarodnom nivou.

Zajednice CERT organizacija prema opsegu svog delovanja mogu biti različitih tipova, od globalnih (kao što je *Forum of Incident and Response Security Teams* – FIRST), preko regionalnih (kao što je *Asia Pacific Computer Emergency Response Team* – APCERT), do onih koje su više servisno orijentisane (ISO 27035). Zajednica CERT organizacija na tlu Evrope (ENISA) je sprovela istraživanje među svojim članicama o tome čije mehanizme razvoja najčešće koriste i prate, i većina je odgovorila da se koriste mehanizmima više međunarodnih organizacija (kao što je prikazano na slici 3.1, na bazi odgovora od 16 CERT timova iz Evrope), ali najčešće su u pitanju FIRST i TI (*Trusted Introducer*).



Slika 3.1: Mehanizmi razvoja koje prate CERT organizacije u Evropi

3.3.1.1 ENISA

ENISA je osnovana 2004. godine sa ciljem da se poboljša mrežna i informaciona bezbednost u Evropskoj Uniji (EU), i odgovori na značajne bezbednosne izazove sa kojima se suočavaju zemlje članice EU i njihove privrede. ENISA opslužuje institucije EU, kao i države članice, uključujući i javna i privatna preduzeća.

U junu 2013. godine EU je ENISA-i dodelila novih sedam godina mandata, sa proširenim skupom dužnosti. Kao dodatak na postojeće poslove pomoći državama članicama da uspostave državne i nacionalne CERT organizacije, ili sprovođenja bezbednosnih kampanja i testova, novi mandat podrazumeva i:

- omogućava se ENISA-i korišćenje instrumenata kojima se podržava borba protiv informatičkog kriminala, i to na bazi detekcije i prevencije, u saradnji sa evropskim centrom za informacionu bezbednost Europol-a,
- daju se ENISA-i ovlašćenja i odgovornosti za podršku razvoju politika informacione bezbednosti i prateće pravne regulative,
- zahteva se od ENISA-e da učestvuje u poslovima istraživanja, razvoja i standardizacije na polju informacione bezbednosti,
- zadužuje se ENISA da podrži prevenciju, detekciju i borbu protiv međunarodnih incidenata,
- delovanje ENISA-e se više usklađuje sa zakonodavnim procesima u okvirima EU, kako bi se zemljama članicama i institucijama EU pomoglo u poslovima informacione bezbednosti, u operativnom i savetodavnom smislu.

ENISA svoju ulogu među CERT organizacijama u zemljama EU vidi više kao savetodavnu, i u smislu olakšavanja razmene informacija, nego što teži da ima operativnu ulogu. Kao ekspertsko telo EU za poslove informacione bezbednosti, ENISA je uvek u toku sa problemima sa kojima se suočavaju CERT organizacije, i ona uspostavlja i održava kontakte sa svim ključnim igračima u oblasti CERT organizacija, uključujući i one o kojima će biti reči u narednim poglavljima. ENISA redovno distribuira informacije koje se tiču dobre prakse u delovanju CERT organizacija, i pomaže u organizaciji, ili je domaćin radionica, konferencija i drugih događaja na temu informacione bezbednosti.

Jedan od prioriteta u delovanju ENISA-e je pomoć državama članicama EU u uspostavljanju državnih i nacionalnih CERT organizacija, i podrška njihovim timovima u razvoju svojih sposobnosti i servisa, kao i dostizanju odgovarajućeg nivoa zrelosti. Kao dodatak na osnovne mehanizme kojima se podržava razvoj CERT organizacija, ENISA pruža i dodatne programe podrške, kao što su na primer namenski pripremljene obuke iz oblasti koje su CERT timovima od posebnog interesa.

ENISA je izvorno objavila dokument o osnovnim kapacitetima CERT organizacija 2009. godine. Tehnički aspekti ovog dokumenta dopunjeni su preporukama na temu bezbednosnih politika i procedura državnih i nacionalnih CERT organizacija, u dokumentu iz 2010. godine. Poslednja verzija dokumenta sa preporukama o osnovnim kapacittima nacionalnih i državnih CERT organizacija kompletirana je 2012. godine.

ENISA, takođe, redovno objavljuje spisak i mapu poznatih CERT organizacija u Evropi (*CERT Inventory map*) kao i dokument sa listingom njihovih aktivnosti (*CERT Activities in Europe*). Oba dokumenta se ažuriraju dva puta godišnje, i u velikoj meri se oslanjaju na bazu podataka o CERT timovima organizacije *Trusted Introducer* (TI).

Od 2013. godine ENISA je uspostavila programe obuke za CERT timove država članica EU. Ovo je nova inicijativa kojom se promoviše i podržava razvoj i sazrevanje CERT timova u država članicama, kroz tehničke treninge i vežbe na temu različitih servisa, operativnih procedura i procedura za saradnju i razmenu informacija u uslovima svakodnevnog poslovanja.

3.3.1.2 TF-CSIRT Trusted Introducer (TI)

TF-CSIRT *Trusted Introducer* (TF-CSIRT/TI) je novo ime za integrisane aktivnosti organizacija TF-CSIRT i TI, u okviru asocijacije TERENA (*Trans-European Research and Education Netowrking Associationi*). To je primer organizacije u kojoj se članstvo CERT organizacija bazira na određenom geografskom regionu. Organizacija TF-CSIRT (*Task Force for Computer Security Incident Response Teams*) je osnovana 2000. godine, i tokom godina je evoluirala u forum koje različite CERT organizacije rado i često koriste za razmenu iskustava i znanja. *Trusted Introducer* (TI) servis je proistekao iz TF-CSIRT organizacije 2001. godine, i ustanovio se kao opšte poznati servis za akreditaciju i listing servisa koje pružaju različiti CERT timovi, u okviru zajednice CERT organizacija.

TF-CSIRT je u prošlosti bila otvorena za sve CERT organizacije na teritoriji Evrope, ali se u poslednje vreme prilagodila strukturi članstva koju poseduje TI, iz razloga formalnog jedinstva ove dve organizacije. TF-CSIRT sebe opisuje kao „organizaciju koja promoviše saradnju i koordinaciju među CERT timovima u Evropi i susednim regionima, sarađujući pri tome sa relevantnim organizacijama na globalnom nivou, tj. u drugim regionima“.

TI sebe opisuje kao „okosnicu zajednice CERT organizacija na tlu Evrope“, koja služi kao servis za „listing, akreditaciju i sertifikaciju CERT timova“, u okviru TF-CSIRT organizacije. Dva glavna servisa koje pruža TI su: održavanje liste svih poznatih CERT timova na tlu Evrope, i servisi akreditacije i sertifikacije CERT timova. Osnovna ideja u pozadini servisa listinga, tj. akreditacije i sertifikacije, jeste da se njima pomogne u izgradnji poverenja u okvirima zajednice CERT organizacija u Evropi. U osnovi, „pečat“ TI organizacije potvrđuje drugim stranama da je neka CERT organizacija dostigla određeni nivo zrelosti i funkcionalnosti, što je važno za izgradnju međusobnog poverenja unutar zajednice CERT organizacija. U skladu sa ovim servisima, svaki CERT tim može da se registruje kod TF-CSIRT/TI organizacije (što je uslov da se pojavi u njihovom listingu), i to je relativno jednostavan proces, za razliku od akreditacije ili sertifikacije koje su mnogo komplikovaniji i dugotrajniji procesi. Sertifikacija podrazumeva da CERT tim mora da ispuni brojne zahteve

koji su predstavljeni SIM³ (*Security Incident Management Maturity Model*) modelom sertifikacije koji je uspostavila TI organizacija.

3.3.1.3 FIRST

Forum of Incident and Response Security Teams (FIRST) je organizacija koja je osnovana 1990. godine, kao zajednica CERT timova na globalnom nivou, koji sarađuju na dobrovoljnoj osnovi kako bi poboljšali svoje sposobnosti i mogućnosti da se bore protiv bezbednosnih incidenata u komunikacionim i informacionim sistemima.

Postoje dva tipa članstva u FIRST organizaciji:

- punopravni članovi – to su CERT organizacije koje pomažu određenim konstituentima u sprečavanju u upravljanju razrešenjem bezbednosnih incidenata, i
- pridruženi članovi – to su pojedinci, ili predstavnici organizacija koje nisu CERT organizacije, ali koje imaju legitimne interese od članstva u FIRST organizaciji, kao i ona od njih.

3.3.1.4 IETF (Internet Engineering Task Force)

IETF je otvorena zajednica mrežnih inženjera i dizajnera, operatora, proizvođača opreme i istraživača, koji su fokusirani na evoluciju Internet arhitekture. IETF je podeljena u radne grupe, u zavisnosti od tema kojima se pojedine grupacije bave. IETF je objavio dokument RFC 2350, koji predstavlja detaljan pregled politika i procedura koje svaka CERT organizacija treba da sprovodi, kao i servisa koje bi trebalo da nudi svojim konstituentima. Iako je objavljen 1998. i poslednji put ažuriran 2003. godine, RFC 2350 se i dalje jako često koristi kao dokument kojim CERT organizacije opisuju svoje kapacitete i aktivnosti. RFC 2350 je važan dokument u okvirima zajednice CERT organizacija jer ga veliki broj CERT timova koristi kao „obrazac“ za samo-procenjivanje. CERT timovi koji su akreditovani i sertifikovani kod TI organizacije prihvatili su RFC 2350 kao skup osnovnih preporuka koje moraju da ispune.

3.3.1.5 CERT/CC

CERT *Coordination Center* (CERT/CC) nije organizacija koja se bazira na članstvu, na način na koji je to navedeno za FIRST ili TI, ali je ipak uticajna organizacija u okvirima zajednica CERT timova. CERT/CC je osnovana 1998. u okviru Instituta za softverski inženjering *Carnegie Mellon* univerziteta, kao odgovor na bezbednosni incident poznat pod imenom „Morisov crv“. Ova institucija je zapravo osnovala prvu CERT organizaciju na svetu. U okvirima svoga delovanja CERT/CC sarađuje sa Internet zajednicom na otkrivanju i rešavanju bezbednosnih incidenata, i to:

- obezbeđuje pouzdanu i poverljivu, 24 časa dostupnu tačku kontakta, u slučajevima kada je nekom potrebna pomoć u borbi sa bezbednosnim napadima i incidentima,
- olakšava komunikaciju između eksperata za informacionu bezbednost,
- služi kao centralna tačka za identifikovanje i eliminisanje ranjivosti sistema,
- održavanje bliskih veza sa istraživačkim aktivnostima i zajednicama, i
- proaktivno deluje na podizanju svesti o važnosti informacione bezbednosti.

Takođe, ova organizacija je uključena u poslove standardizacije na polju delovanja CERT organizacija, i razvila je i objavila brojne otvorene alate za testiranje ranjivosti sistema, analizu mrežnog saobraćaja, kao i digitalnu forenziku.

3.3.1.6 APCERT

Asia Pacific Computer Emergency Response Team (APCERT) je još jedan primer regionalne organizacije CERT timova. Ona sebe opisuje kao organizaciju koja „ohrabruje i podržava koordinaciju“ između CERT organizacija na području regiona Azije i Pacifika. Ova organizacija je otvorena za sve timove iz svog regiona koji ispunjavaju njene kriterijume za članstvo. Članovi APCERT organizacije moraju podržavati njene ciljeve, poštovati procedure za upravljanje informacijama, i u najvećoj mogućoj meri pružati pomoć drugim članovima organizacije.

3.3.1.7 International Organization for Standardization (ISO)

ISO je nevladina organizacija koju sačinjavaju članovi nacionalnih tela za standardizaciju 163 države sveta. ISO objavljuje standarde koji se razvijaju na okruglim stolovima eksperata, u okviru tehničkih odbora. 2011. godine ISO je objavio dokument sa svojim smernicama za upravljanje bezbednosnim incidentima za velike i srednje organizacije. Ova publikacija, koja je poznata i kao ISO 27035, ima svrhu da obezbedi strukturirani i planski pristup problemima kao što su:

- otkrivanje, izveštavanje i razrešavanje bezbednosnih incidenata,
- upravljanje bezbednosnim incidentima,
- otkrivanje, izveštavanje i razrešavanje uočenih ranjivosti sistema, i
- kontinuirano poboljšavanje informacione bezbednosti i procesa upravljanja incidentima.

Takođe, ISO 27035 obezbeđuje smernice za delovanje eksternih organizacija koje se bave pružanjem servisa za upravljanje incidetnima.

3.3.1.8 Druge organizacije

Osim pomenutih organizacija postoje i druge organizacije koje promovišu mehanizme za razvoj sposobnosti CERT timova. Primera radi, mnoge korporacije imaju interne CERT timove koji su u stanju da odgovore na bezbednosne incidente koji su u vezi sa njihovim proizvodima ili servisima.

Još jedan primer ovakvih organizacija je *European Government CERT Group* (EGC Group), koja je neformalna asocijacija kvalitetnijih državnih CERT timova zemalja Evrope. Članovi ove organizacije efikasno sarađuju na poslovima upravljanja incidentima, izgrađujući pri tome međusobno poverenje i razumevanje, baveći se sličnim problemima sličnih grupa konstituenata. Ova organizacija je fokusirana na tehničke aspekte problema kojima se zajednički bave, i obično su ovi timovi istovremeno i članovi drugih organizacija, kao što su FIRST, ili TF-CSIRT/TI.

3.3.2 Sertifikacija

Proces sticanja iskustva, tj. sazrevanja i sertifikacije CERT organizacija, pomaže u tome da se ispune očekivanja koje se postavljaju pred CERT organizacije u domenu međunarodne saradnje. Poželjan je visok nivo zrelosti CERT organizacije (oličen kroz proces

sertifikacije, ili slične aktivnosti) kako bi se ona uključila u mrežu evropskih CERT organizacija i uspešno učestvovala u aktivnostima međunarodne saradnje. Mnoge državne i nacionalne CERT organizacije su takođe odgovorne za upravljanje kriznim situacijama i procese zaštite ključne informacione infrastrukture u svojim zemljama. Imajući u vidu važnost i kompleksnost tih procesa, nivo iskustva i zrelosti ovih organizacija je jedan od ključnih faktora koji obezebeđuje uspeh u ovim poslovima.

Faktori motivacije za državne i nacionalne CERT organizacije da uđu u proces sertifikacije su obično sledeći:

- odnosi sa javnošću i dobra slika o organizaciji, na nacionalnom i međunarodnom nivou,
- poređenje kvaliteta CERT organizacije sa međunarodnim kriterijumima i standardima,
- potreba da se razumeju, dokumetuju i urede procedure i procesi funkcionisanja CERT tima,
- potreba da se urede odgovornosti, proces nadgledanja poslovanja, i šeme izveštavanja,
- kontinuirano implementiranje poboljšanja u upravljanju kvalitetom servisa.

CERT organizacije koje stupaju u proces sertifikacije mogu se klasifikovati u sledeće tri kategorije:

- organizacije koje žele da demonstriraju zrelost, kao dokaz iskustva i statusa CERT tima (u tom slučaju proces sertifikacije može da im pomogne da identifikuju aspekte delovanja na koje se nisu fokusirali u dovoljnoj meri),
- organizacije koje žele da mogućnosti njihovog tima budu prepoznate od spoljnjih entiteta, tj. drugih CERT organizacija ili konstituenata (na primer novi CERT timovi),
- organizacije kojima je potrebno usaglašavanje sa standardima, radi ispunjenja zahteva svojih osnivača (na primer države). Ovo je naročito izazovno kada su u pitanju novi timovi, a pritisak i zahtevi osnivača su veliki, kada je potrebno angažovati puno resursa na implementaciji raznih promena u organizaciji u kratkom vremenskom roku.

U današnje vreme uloga i funkcije državnih i nacionalnih CERT organizacija se stalno šire i povećavaju, tako da timovi moraju biti u stanju da se izbore sa novim zahtevima i očekivanjima, uz stalni rad na sticanju iskustva i poboljšanjima u organizaciji i sposobnostima.

Jedan od alata za procenu sposobnosti i zrelosti CERT organizacija je SIM³ model (*Security Incident Management Maturity Model*), koji je prihvatila i adaptirala TF-CSIRT/TI organizacija za potrebe svoje šeme za sertifikaciju. U ranije objavljenim i pomenutim dokumentima ENISA-e, koji se tiču osnovnih kapaciteta CERT organizacija, pominje se da su ti kapaciteti podeljeni u četiri osnovne kategorije: mandat, servisi, operativno delovanje i saradnja. Ove kategorije nisu u direktnoj vezi sa SIM³ modelom ali s obzirom da je TI model sertifikacije jedan od najčešće primenjivanih modela kod nacionalnih i državnih CERT organizacija zemalja članica EU, u nastavku će fokus biti na svim parametrima koji se odnose na ovu klasifikaciju.

Generalno, TI model sertifikacije je pogodan za bilo koji tip CERT organizacije, ali postoje specifičnosti koje treba uzeti u obzir kada su u pitanju nacionalne i državne CERT organizacije. Imajući u vidu činjenicu da su glavne članice ENISA-e nacionalne i državne CERT organizacije, pomoć i iskustvo eksperata ENISA-e i TI su jako važni u procesu sazrevanja CERT timova i njihove sertifikacije.

3.3.2.1 Razvojni put CERT organizacija

Razvojni put nacionalnih i državnih CERT organizacija obično je različit u različitim zemljama. Neke države kreću od definisanja nacionalne strategije za informacionu bezbednost, da bi zatim usledilo uspostavljanje odgovarajućeg zakonodavstva i formiranje CERT organizacija. U drugim država se kreće od uspostavljanja zakonodavstva i formiranja CERT organizacija kao osnove delovanja, a kasnije se ide na formulisanje strategije o informacionoj bezbednosti. U svakom slučaju, neophodno je da nacionalne i državne CERT organizacije u toku ovih procesa, što je pre moguće, imaju jasan mandat, i jasno definisanu zajednicu konstituenata. Pri tome, pod vremenom uspostavljanja CERT organizacije smatra se trenutak kada ona počne da pruža svoje osnovne servise (najčešće je to servis za upravljanje incidentima).

Prvi korak u uspostavljanju prisustva CERT organizacije na međunarodnoj sceni počinje onda kada se pojavi potreba za međunarodnom saradnjom i razmenom informacija sa sličnim organizacijama u drugim zemljama. TI organizacija je razvila šemu kategorizacije i sertifikacije koja podrazumeva tri nivoa zrelosti CERT orgnaizacija:

- listing – CERT tim je operativan i njegove kontakt informacije su dostupne drugim timovima,
- akreditacija – CERT tim je u potpunosti funkcionalan, servisi su definisani prema RFC 2350 preporukama, i slično. Informacije o CERT timu moraju biti ažurirane na svaka četiri meseca, što je u nadležnosti same CERT organizacije,
- sertifikacija – tim je dostigao odgovarajući nivo zrelosti. Sam proces sertifikacije je opisan u narednim poglavljima.

3.3.2.2 Modeli razvoja CERT organizacija

Zrelost jedne CERT organizacije definiše se kao mera njenih sposobnosti u aspektima organizacije, ljudskih resursa, procesa i tehnologija. Ona odslikava određeni nivo sigurnosti da organizacija može da obavlja svoje aktivnosti na konzistentan način, da zavređuje poverenje drugih organizacija, kao i da je sposobna da se fokusira na svoj kontinuirani razvoj.

U slučaju nacionalnih i državnih CERT organizacija, pod zrelošću se podrazumeva sposobnost da se efikasno upravlja kapacitetima organizacije u cilju pružanja deklarisanih servisa, koji treba da budu na odgovarajući način dokumentovani, isporučeni, i čiji učinak je merljiv.

Tokom vremena, mnoge nacionalne i državne CERT organizacije su se razvile iz veoma neformalnih, ponekad čak i ad hoc grupa, motivisanih ljudi sa velikom tehničkom i tehnološkom ekspertizom. S obzirom na porast obaveza i odgovornosti stvorila se potreba za odgovarajućim nivoom organizacije u upravljanja ovakvim timovima. Potrebno je da postoji temeljno razumevanje internih procesa unutar CERT organizacija kako bi se obezbedila konzistentnost u pružanju servisa, kao i jasan put razvoja i poboljšanja sposobnosti i kapaciteta CERT tima.

Postoji nekoliko modela razvoja CERT organizacija, i kao što je već pomenuto, u narednom izlaganju fokus će biti na SIM³ modelu, koji je osnova za proces sertifikacije kod TI organizacije.

Postoje i druge šeme sertifikacije, koje nisu fokusirane na CERT organizacije. Najpoznatije od njih se odnose na međunarodne standarde, kao što je na primer ISO 27001. Ovakve šeme sertifikacije su jako dobro definisane, ali više odgovaraju velikim organizacijama, nego relativno malim timovima koji se bave specifičnim delatnostima u vezi

sa informacionom bezbednošću, kao što su CERT timovi. Nekoliko CERT timova je dobilo sertifikate na bazi ISO 27001, ali većina CERT timova u Evropi smatra da ovakva šema sertifikacije ne odgovara njihovoj oblasti delovanja.

Dodatno, postoje i organizacije kao što su COBIT (*Control Objectives for Information and Related Technology*), ili ITIL (*Information Technology Infrastructure Library*), koje su fokusirane na IT okruženja i servise. Iako se njihovi principi mogu primeniti na organizacije bilo koje veličine, često se smatraju previše kompleksnim za implementaciju u većini nacionalnih i državnih CERT organizacija.

3.3.2.3 TI sertifikacija

Proces sertifikacije prema šemi organizacije *Trusted Introducer* (TI) podrazumeva da CERT tim koji želi da pristupi sertifikaciji mora prethodno biti na listi „akreditovanih" timova. Sticanje statusa sertifikovane organizacije je cilj onih akreditovanih CERT timova koji imaju interne ili eksterne razloge da verifikuju nivo svojih sposobnosti i zrelosti organizacije preko nezavisne eksterne organizacije.

Kandidat za TI sertifikaciju može biti CERT tim koji je već TI akreditovan, tj. ispunjava sve obaveze i uslove akreditacije, u periodu od najmanje poslednjih osam meseci pre pristupa procesu sertifikacije, i pri tome nije predmet posebne revizije Upravnog odbora TF-CSIRT organizacije. Dodatno, potrebno je da je prisustvovao bar jednom od skupova TI organizacije, koji se održavaju u okviru skupova TF-CSIRT organizacije tri puta godišnje.

Šema koja se koristi za merenje parametara sposobnosti i zrelosti CERT organizacije je SIM³ model, koji opisuje 45 parametara podeljenih u 4 kategorije:

- organizacija,
- ljudski resursi,
- alati, i
- procesi.

Ocenjivanje u svakoj kategoriji se vrši u pet nivoa, počev od „0", što znači da se taj parametar ne uzima u obzir, do „4", što znači da je parametar podložan procesima interne i eksterne revizije. Proces sertifikacije podrazumeva merenje specifičnih i tačno određenih minimalnih nivoa za svaki od parametara.

Svaki nivo ocene određenog parametra ima sledeće značenje:

- 0 – parametar nije prisutan ni u kom obliku,
- 1 – tim se svestan nekog specifičnog problema, i ima način na koji ga razrešava, ali taj proces nije dokumentovan,
- 2 – parametar je dokumentovan u nekoj internoj bazi znanja ili priručniku,
- 3 – parametar je dokumentovan i odobren od rukovodstva CERT organizacije, u formi odobrenog priručnika, ili potpisanog dokumenta,
- 4 – parametar je prošao reviziju i postoji povratna informacija od revizora, ili rukovodstva CERT organizacije, u formi izveštaja sa revizije, ili u vidu potvrđenih kvartalnih ili godišnjih izveštaja, i slično.

Jednom kada dostigne nivo potreban za sertifikaciju, CERT organizacija ostaje deo zajednice TI akreditovanih timova, a sam sertifikat je dodatno „brendiranje" organizacije, koje može biti korisno za mnoge različite svrhe u budućem delovanju CERT organizacije.

Proces TI sertifikacije može da traje od tri do dvanaest meseci, u zavisnosti od količine posla koji CERT organizacija treba da obavi da bi ispunila sve potrebne zahteve, i u zavisnosti

od nivoa prioriteta koji pridaje tom procesu. Sertifikat je validan tokom tri godine, nakon čega CERT organizacija treba da sprovede proces re-sertifikacije, kako bi dokazala da je nivo kvaliteta organizacije zadržan, ili čak i povećan.

Do septembra 2015. godine, 15 CERT timova je uspešno prošlo proces sertifikacije, 5 timova je već prošlo proces re-sertifikacije, i još nekoliko timova je bilo u procesu sertifikacije, ili re-sertifikacije.

3.3.2.3.1 Proces sertifikacije

Prvi korak u procesu sertifikacije je da se razume motivacija CERT tima da pristupi tom procesu. Motivacija može imati uticaja na prioritetizaciju tog procesa i dodeljivanje resursa, u cliju poboljšanja operativnih procedura CERT tima i njihovog dokumentovanja.

Sledeći korak bi bio da CERT organizacija izvrši reviziju svog poslovanja koristeći se SIM³ modelom. Rezultat toga je prva indikacija u kojoj meri su zahtevi sertifikacije već ispunjeni, tj. u kojim segmentima je potrebno uložiti dodatne napore. Radi dobijanja korektnih rezultata sopstvene revizije važno je dobro razumeti skalu ocena iz SIM³ modela. U tom smislu treba se konsultovati sa ekspertima TI organizacije svaki put kada postoji neka nedoumica.

Još jedan korak ka sertifikaciji je da se prikupe referentni materijali i dokumentacija, koji se tiču npr. zakonske regulative, mandata CERT organizacije, njenih konstituenata, i slično.

Neke nacionalne i državne CERT organizacije imaju uglavnom ulogu koordinatora u poslovima informacione bezbednosti. Za takve organizacije, neki od parametara sertifikacije nisu primenljivi, i takvi parametri se isključuju iz evaluacije, tj. dobijaju ocenu „-1“. Ciljevi organizacija koje se bave samo poslovima koordinacije su drugačiji od onih koje se bave i operativnim delovanjem, i ta činjenica se uzima u obzir u procesu ocenjivanja, tj. sertifikacije.

3.3.2.3.2 Upotreba jezika

CERT timovi koji su članovi TI organizacije pripadaju različitim govornim područjima (engleski, nemački, poljski, holandski, ruski, francuski ...), ali može se desiti da određena CERT organizacija koristi jezik koji nije poznat ekspertima TI organizacije.

Uobičajeno, ukoliko je neki CERT tim član organizacije FIRST, i akreditovani član organizacije TI, onda on poseduje i neku dokumentaciju na engleskom jeziku (barem RFC 2350 dokument). Eksperti TI organizacije ne očekuju da imaju na rasplaganju zvanični prevod dokumentacije CERT organizacije, jer bi to bilo skupo i oduzelo previše vremena. Umesto toga, TI se trudi da angažuje pomoćnika koji razume jezik CERT organizacije (a da pri tome nije zaposlen u toj organizaciji), kako bi se utvrdilo da li je dokumentacija CERT organizacije u skladu sa TI parametrima.

Neki od internih dokumenata CERT organizacije mogu se relativno lako prevesti (na primer opisi tokova poslovanja), uz pomoć alata za prevođenje, ukoliko ta dokumentacija nije poverljive prirode. Prevođenje kompleksnih i dugačkih dokumenata, kao i dokumenata koji sadrže poverljive informacije obično nije neophodno. Naravno, podrazumeva se da CERT timovi moraju obezbediti dovoljnu količinu informacija ekspertima TI organizacije, kako bi oni mogli da razumeju i verifikuju procese i procedure poslovanja posmatrane CERT organizacije.

Proces sertifikacije obično podrazumeva održavanje radionice, gde se može diskutovati o otvorenim pitanjima. Protokol sa tog skupa mora da potpiše rukovodilac tima za

sertifikaciju, potvrđujući na taj način da su sve stavke koje su bile problematične, kao posledica jezičke barijere, razjašnjene i verifikovane.

3.3.2.3.3 Radionica za sertifikaciju

Radionica za sertifikaciju je obično celodnevni događaj koji se organizuje u prostorijama CERT tima. Preporuka je da barem tri člana CERT tima uzmu učešće u radionici za sertifikaciju. Tom prilikom se diskutuje o procesima, procedurama i alatima koje CERT tim koristi. Takođe, različiti članovi CERT tima se intervjuišu radi davanja svoga mišljenja o funkcionisanju svoje CERT organizacije, kako bi se utvrdilo da među članovima tima ne postoje značajne razlike u razumevanju uloge i načina funkcionisanja CERT organizacije.

Jedan od važnih ciljeva radionice je da CERT tim identifikuje oblasti u kojima mu nedostaje dokumentacija ili razvijene procedure, kao i poboljšanja koja treba uvesti. Iskustvo pokazuje da svaki tim ima nešto na čemu mora dodatno da radi, i šta treba da poboljša kako bi uspešno prošao kroz proces sertifikacije.

3.3.2.3.4 Proces re-sertifikacije

Prema pravilima TI organizacije, sertifikacija je validna na period od tri godine, nakon čega CERT tim mora da prođe proces re-sertifikacije, kako bi sačuvao svoj status TI sertifikovane organizacije.

Glavni cilj procesa re-sertifikacije je da se diskutuje o tome koliko je CERT tim napredovao u svojim sposobnostima i zrelosti tokom poslednje tri godine. Ukoliko nije evidentan nikakav napredak to može da ugrozi proces re-sertifikacije, jer to znači da je tim statičan, i ne ulaže napore u razvijanje svojih sposobnosti i mogućnosti tima.

Naravno, postoje i situacije u kojima se ne može očekivati od CERT tima da napreduje. Na primer, ukoliko se promenila krovna organizacija u okviru koje tim funkcioniše, ili je proširen mandat delovanja CERT tima, u takvim slučajevima tim će morati da angažuje većinu svojih resursa da se prilagodi takvim promenama, i novim očekivanjima koja su sa njima u vezi. U takvim slučajevima proces re-sertifikacije se ne fokusira na nedostatak napretka, već se pažnja posvećuje tome da li su na adekvatan način implementirane sve neophodne promene kako bi se CERT tim prilagodio novonastaloj situaciji.

U procesu re-sertifikacije se takođe organizuje radionica na kojoj se diskutuje o izveštaju sa prethodne radionice (koja je održana radi sertifikacije), i upoređuje se stanje CERT organizacije, tada i sada, kako bi se ustanovilo da li je CERT organizacija i dalje u stanju koje je neophodno da bi se zadržao status TI sertifikovane organizacije.

3.3.2.4 Ocenjivanje zrelosti organizacionih parametara CERT organizacije

U narednim poglavljima razmatraju se parametri SIM³ modela koji se koriste u šemi TI sertifikacije, spram osnovnih kapaciteta i karakteristika CERT organizacija, i za svaki parametar navodi se minimalan nivo ocene, neophodan za uspešnu sertifikaciju CERT organizacije, zajedno sa odgovarajućim objašnjenjima i sugestijama.

3.3.2.4.1 Mandat

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Kada je reč o nacionalnim i državnim CERT organizacijama postoji izražena potreba za postojanjem pravnog akta, ili drugog mehanizma, kojim se jasno definiše mandat CERT organizacije. Ovo nije neophodno radi sertifikacije kao takve, već se smatra dobrom praksom koje se treba pridržavati. I u drugim studijama, kao što su dokumenti organizacije ENISA, koja je fokusirana na nacionalne i državne CERT organizacije, navodi se da mandat, a naročito definicija uloge i odgovornosti CERT organizacija, moraju biti dovoljno jasni i nedvosmisleni, kako bi se podržale sve relevantne aktivnosti ovih organizacija. Mandat nacionalnih i državnih CERT organizacija mora biti javno objavljen i svima dostupan, na maternjem jeziku organizacije, ali i na engleskom jeziku. Za sve navedene uloge i funkcije nacionalne ili državne CERT organizacije u okviru mandata moraju biti navedeni i odgovarajući izvori finansiranja.

Postojanje mandata je osnovni zahtev za svaki tip CERT organizacije, ali kada su u pitanju nacionalne i državne CERT organizacije, ENISA poziva na unapred definisane i jake pravne osnove njihovih operacija.

Mandat treba da sadrži i odredbu o tome kome nacionalna ili državna CERT organizacija odgovara za svoje delovanje (državnom regulatornom organu, ili ministarstvu, i slično).

Za sve do sada sertifikovane nacionalne i državne CERT organizacije, organizacioni parametri su uglavnom jednostavni za razmatranje. Mandat je u većini slučajeva jasno definisan u odgovarajućim zakonima. Samo je jedan CERT tim tokom sertifikacije naveo da njihove funkcije obuhvataju i oblasti mimo dodeljenog mandata, tako da je bila potrebna izmena u zakonodavstvu kako bi se razrešila ova situacija, i neometano završio proces re-sertifikacije te organizacije.

3.3.2.4.2 Konstituenti

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Nacionalne i državne CERT organizacije imaju različite grupe konstituenata, a ponekad su i obe uloge kombinovane u jednoj organizaciji. Konstituenti državnih CERT organizacija su obično vladine i druge javne institucije. Sa druge strane, nacionalne CERT organizacije su obično odgovorne za ekonomske subjekte u zemlji, ali isto tako one imaju ulogu nacionalne tačke kontakta za razmenu informacija, tokom razrešavanja bezbednosnih incidetata, sa nacionalnim CERT organizacijama u drugim državama članicama EU, ili širom sveta. Ponekad je nacionalni CERT poslednje odredište za prijavu bezbednosnih incidenata za sve subjekte u jednoj državi, naročito u manjim državama, gde su konstituenti ovih organizacija i privatni i javni sektor, pa čak i krajni korisnici telekomunikacionih ili informacionih usluga i servisa.

Kada su u pitanju nacionalne ili državne CERT organizacije, njihovi konstituenti moraju biti definisani odgovarajućim zakonodavstvom, ili drugim ekvivalentnim mehanizmima. Ni ovo nije neophodno za sam proces sertifikacije, ali se smatra dobrom praksom. Dokument o konstituentima CERT organizacije mora da bude javno dostupan, na maternjem jeziku organizacije, kao i na engleskom jeziku.

Svaka CERT organizacija mora da ima definisan skup svojih konstituenata, ali kada su u pitanju nacionalne i državne CERT organizacije, ENISA poziva na jake pravne osnove u tom smislu.

Za sve do sada sertifikovane nacionalne i državne CERT organizacije, konstituenti su u većini slučajevima bili definisani u odgovarajućim zakonima. Samo dva CERT tima su imala dodatne ugovore sa još nekim organizacijama, koje nisu obuhvaćene zakonodavstvom.

3.3.2.4.3 Ovlašćenja

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Ovlašćenja nacionalnih i državnih CERT organizacija moraju biti jasno definisana, tj. šta je to što mogu da sprovedu prema svojim konstituentima kako bi postigli ciljeve svoga delovanja. U tom smislu, jako je dobro ako su ovlašćenja CERT organizacije definisana u odgovarajućim zakonskim aktima (što nije neophodno za sertifikaciju, ali je dobra praksa). Opis ovlašćenja CERT organizacije mora biti javno dostupan, na maternjem jeziku organizacije, i engleskom jeziku. I kada su u pitanju ovlašćenja nacionalnih i državnih CERT organizacija, ENISA poziva na jake pravne osnove za njihovo delovanje.

Da bi CERT organizacije mogle na kvalitetan i efikasan način da sprovode svoje aktivnosti potrebno je da imaju odgovarajući nivo prava i ovlašćenja. Pri tome, treba uzeti u obzir sledeće aspekte:

- obrada privatnih podataka (naročito kada se to odnosi na poverljive podatke o bezbednosnim incidentima),
- pravo da zahtevaju saradnju i informacije od telekom operatora i provajdera internet servisa,
- pravo da zahtevaju saradnju i informacije od državnih institucija,
- prava i ovlašćenja u odnosu na nosioce kritične informacione i telekomunikacione infrastrukture.

Sve do sada sertifikovane nacionalne ili državne CERT organizacije navele su da su njihova ovlašćena opisana, ili će biti opisana u odgovarajućim zakonskim aktima, a dva tima su svoja ovlašćenja dodatno definisala kroz ugovore sa svojim konstituentima.

3.3.2.4.4 Odgovornosti

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Minimalni zahtevi za sertifikaciju ne zahtevaju da se odgovornosti definišu mimo dokumentacije koju odobrava rukovodstvo CERT organizacije, ali u slučaju nacionalnih i državnih CERT organizacija je dobro da u zakonodavtsvu postoje jasno definisane odgovornosti, kako bi se olakšalo svakodnevno funkcionisanje organizacije. Bez obzira na pravne definicije, jasan opis odgovornosti CERT organizacije treba da bude javno dostupan, na maternjem jeziku organizacije, kao i na engleskom jeziku.

Dok nacionalne i državne CERT organizacije sprovode svoje aktivnosti mogu postojati tendencije da im se dodaju nove funkcije i zadaci koji se mogu razlikovati od osnovnih funkcija CERT organizacije (na primer kada se mora dodati nova funkcija zbog izmene u zakonodavstvu). Sprovođenje novih aktivnosti može biti izazovno, osim ukoliko nisu obezbeđeni i dodatni izvori finansiranja. Takođe, potrebno je pažljivo proveriti i da li su novi zadaci u konfliktu sa osnovnim delatnostima koje CERT organizacija već sprovodi. Primera radi, CERT organizacija ne može biti zadužena za sprovođenje novih aktivnosti u kojima već ima ulogu nadzornog organa.

Potreban je i jasan opis odgovornosti i jasno razumevanje obaveza koje se tiču zaštite ključne informacione i komunikacione infrastrukture. Saradnja sa istražnim i pravosudnim organima je često jednosmerna, u slučajevima kada te institucije nisu u prilici da razmenjuju informacije kojima raspolažu, naročito tokom trajanja istražnih radnji. Iako je neophodno poštovati određena zakonska ograničenja, postoje načini da nacionalne i državne CERT organizacije drže otvorene kanale komunikacije, i sarađuju sa ovim institucijama onda kada za to postoji zajednički interes.

Kada su u pitanju nacionalne i državne organizacije koje su već prošle proces TI sertifikacije, njihove odgovornosti su u najboljem slučaju definisane u odgovarajućim zakonima. U slučajevima kada to nije dovoljno jasno, postoje posebni ugovori sa konstituentima. U jednom slučaju CERT organizacija je navela da su njihove ugovorne obaveze definisane na uopšten način, kako bi mogli brzo da se adaptiraju na promenljive situacije i iznenadne pretnje po informacionu bezbednost.

3.3.2.4.5 Opis servisa

Minimalni zahtevani nivo ocene	Opis
4	Eksplicitan i podložan reviziji na nivoima van CERT organizacije, od strane spoljnjih subjekata zaduženih za kontrolu i nadzor

Opisi servisa imaju najstrožije zahteve za sertifikaciju, i oni moraju biti revidirani i pod nadzorom od subjekata koji nisu deo CERT organizacije. Potrebno je da postoje javno dostupne kontakt informacije i opisi servisa, kao i politike koje se odnose na upravljanje informacijama, na maternjem jeziku organizacije i na engleskom jeziku. U slučaju nacionalnih i državnih CERT organizacija jasan opis servisa mora postojati i u zakonskim aktima.

Ukoliko postoji opis servisa u zakonskim aktima, onda može biti slučaj da su navedeni samo osnovni servisi, i CERT organizacija ne nudi servise izvan uobičajenog portofolija, koji bi mogli imati dodatnu vrednost za njihove konstituente. Postoje naravno i slučjevni kada nacionalne i državne CERT organizacije nude servise koji bi za konstituente mogli imati dodatnu vrednost, ali ih isto tako nude i druge CERT organizacije na komercijalnoj osnovi.

Primera radi, servisi kao što su ispitivanje ranjivosti sistema, ili analiza artefakata koji ostaju kao trag iza bezbednosnih incidenata, nisu uobičajeno u portfoliju nacionalnih i državnih CERT organizacija, a većina njih se ne bavi ni planiranjem zaštite od katastrofa ili osiguranjem kontinuiteta poslovanja.

Organizacije koje su već prošle proces TI sertifikacije navode da su njihovi servisi opisani u odgovarajućim zakonskim aktima, ili kroz ugovore sa njihovim konstituetnima, ili u okviru RFC 2350 dokumenta.

3.3.2.4.6 Opis nivoa servisa

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Minimalni zahtevi za TI sertifikaciju podrazumevaju da postoji opis nivoa servisa koji se odnosi na vreme reakcije CERT tima po primljenoj prijavi incidenta, kao i minimalno vreme odziva u slučaju da stigne zahtev za pomoć od neke druge CERT organizacije (preporučeno vreme u ovom slučaju je najviše dva dana). Generalni princip za nacionalne i državne CERT organizacije je da one moraju biti dostupne u režimu 24/7. Naravno, ova ključna činjenica da su nacionalne i državne CERT organizacije stalno dostupne svojim konstituentima mora biti jasno naznačena, tj. javno objavljena i poznata konstituentima.

S obzirom da nije uvek lako, a ni jeftino, sprovesti rad organizacije u režimu tj. njenog stručnog osoblja u režimu 24/7, postoje i druge opcije koje se mogu uzeti u obzir:

- delegiranje funkcije kontakt centra spoljnjim entitetima, sa jasnim instrukcijama kako da postupaju u određenim situacijama (koji tip incidenata može da sačeka sledeći radni dan, a koji mora hitno da se eskalira radi što ranijeg razrešenja),
- prosleđivanje kontakata (brojevi mobilnih telefona) ključnih članova CERT tima, svim najvažnijim konstituentima i partnerskim CERT organizacijama (na primer kroz bazu podataka o kontakt informacijama TI organizacije),
- uspostavljanje dežurstva, gde se agentima kontakt centra ostavlaju na raspolaganje kontakt podaci dežurnog člana CERT tima, za slučaj da je potrebe u hitnim situacijama).

Kada su u pitanju nacionalni i državni CERT timovi koji su prošli proces TI sertifikacije, opis nivoa njihovih servisa je definisan zakonodavstvom, ili posebnim ugovorima sa njihovim konstituentima, ili u okviru RFC 2350 dokumenta. Nivoi servisa mogu biti različiti za različite tipove konstituenata.

3.3.2.4.7 Klasifikacija incidenata

Minimalni zahtevani nivo ocene	Opis
1	Implicitno, na bazi lične procene, prethodnih znanja ili iskustava

Sa stanovišta TI sertifikacije, minimalno je da postoji svest o potrebi klasifikacije incidenata. Naravno, s obzirom da je proces klasifikacije incidenata u onsnovi servisa za upravljanje incidentima, potrebno je i da postoji neka vrsta opisa ovog procesa. Ne postoji unificirana šema klasifikacije incidenata za sve CERT organizacije, što znači da postoje razlike u terminologiji i šemama koje primenjuju nacionalne i državne CERT organizacije. Dodatno, ni sami incidenti ponekad nisu jasno definisani, tj. mogu postojati kombinovani tipovi incidenata, ili novi tipovi incidenata koji se ne uklapaju u postojeće šeme klasifikacije.

Svaka CERT organizacija treba da odluči koja šema klasifikacije incidenata najviše odgovara njihovim potrebama, uzimajući u obzir incidente sa kojima se najčešće sreću, statističke analize incidenata, zahteve od strane konstituenata, zakonske obaveze prema konstituentima, i slično.

CERT organizacije koje su već prošle proces TI sertifikacije, u opštem slučaju nisu navodile nikakve probleme u vezi sa klasifikacijom incidenata. Većina timova je svoju šemu klasifikacije incidenata primenila i u svojim alatima za prijavu incidenata i vođenje evidencije o incidentima. Jedan tim je prijavio da se posvetio razradi novog modela klasifikacije incidenata zbog promena u zakonodavtsvu koje podrazumevaju uvođenje opšte obaveze prijavljivanja bezbednosnih incidenata za sve subjekte u državi.

3.3.2.4.8 Učešće u zajednicama CERT organizacija

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Nacionalne i državne CERT organizacije obično nemaju ”nadređenu” CERT organizaciju. U slučajevima kada u jednoj zemlji postoji više od jedne nacionalne ili državne CERT organizacije, a da bi se sprečili problemi u njihovoj saradnji, mora se jasno definisati ko je nacionalna tačka kontakta za druge CERT organizacije, u zemlji ili van nje.

Ukoliko CERT tim razmatra sertifikaciju to znači da je član barem TI organizacije, gde je obavezan i da prisustvuje skupovima organizacije koji se organizuju tokom godine. Mnogi timovi se suočavaju sa problemima, i u smislu ljudskih resursa i u smislu finansija, kada žele da učestvuju u radu više različitih foruma. Bez obzira na sve, za nacionalne i državne CERT timove je važno da reprezentuju svoju zemlju, izgrađuju veze sa drugim CERT organizacijama i razmenjuju informacije. Međunarodna organizacija Mreža CERT organizacija Evropske Unije je predviđena kao pogodan mehanizama da se prevaziđu problemi sa resursima.

Takođe, potrebno je da nacionalne i državne CERT organizacije razvijaju odnose sa sličnim organizacijama u susednim državama. To može uključivati različite tipove saradnje, od neformalnih ličnih kontakata, do potpisivanja memoranduma o saradnji, deljenju tehničkih informacija, korišćenju raznih alata za bezbednu komunikaciju u realnom vremenu, i slično. Za svaki tip partnerskih odnosa važna je izgradnja poverenja, i kao i svuda to je težak i dugotrajan proces.

Za uspešnu saradnju i poverenje važno je i da organizacije budu na približno istom nivou kvaliteta i zrelosti, a to na žalost nije uvek slučaj. Dešava se i da u slučaju međunarodnih incidenata sve organizacije ne sprovode potrebne aktivnosti na zadovoljavajući način, spram informacija koje dobiju. Za to postoje brojni razlozi, a jedan od njih može biti nedostatak standardizacije u odnosu na informacije koje se razmenjuju, što nacionalnim i državnim CERT organizacijama može da oteža analizu dobijenih informacija, i utvrđivanje njihove relevantnosti. Postoje i drugi faktori, kao što su u nekim slučajevima pravne barijere u smislu poverljivosti informacija, ili ograničenja u delovanju zbog nedostatka ovlašćenja u nekim oblastima.

CERT timovi koji su već prošli proces TI sertifikacije aktivno učestvuju u različitim forumima CERT organizacija, kao što su FIRST, ili TF-CSIRT/TI. Svaki od tih timova ima bar jednu kontakt osobu, koja je zadužena za komunikaciju sa ovim organizacijama. Sa stanovišta sertifikacije, ovaj parametar se lako može potvrditi uvidom u baze podataka

članova pomenutih organizacija. Genralno, svi timovi ulažu velike napore za aktivno učešće u ovim organizacijama.

3.3.2.4.9 Organizacioni parametri

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Dokument koji opisuje organizaciju poslovanja nije potreban samo za proces TI sertifikacije, već treba da bude dostupan i svim članovima CERT tima. Taj dokument ne treba da sadrži samo opis ranije pomenutih organizacionih parametara, već i opis organizacione strukture CERT-a, kao i njegovo mesto i ulogu u široj bezbednosnoj zajednici na nivou države. U tom smislu mogu postojati različiti dokumenti i reference, koji treba da budu dostupni svim članovima tima, u skladu sa nivoom tajnosti pojednih dokumenata, i politikom zaštite podataka.

Opis organizacije poslovanja može biti objedinjen u jednom dokumentu, u formi priručnika, ili se inforamcije mogu prikupljati i deliti preko internog informativnog portala, ili na neki drugi način.

Kada su u pitanju CERT organizacije koje su prošle proces serifikacije, ovo je jedan od parametara prema kojem organizacije imaju različit pristup. Sve ove organizacije imaju izrađen dokument RFC 2350, ali neki od timova su iskoristili proces sertifikacije da razviju još formalniji i sveobuhvatniji dokument ili priručnik, i ulažu napore da se ova dokumentacija koristi i redovno ažurira.

3.3.2.4.10 Bezbednosna politika

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Iz opisa poslova CERT organizacija je očigledno da je potrebno da imaju razvijene bezbednosne politike iz svojih sopstvenih razloga. Ta politika može biti deo bezbednosne politike krovne organizacije u okviru koje CERT ostvaruje svoje aktivnosti, ili može biti posebno razvijena politika. Sa stanovišta CERT organizacije politika bezbednosti se primarno fokusira na zaštitu poverljivih informacija, tj. poverljivost podataka. Kada se formuliše bezbednosna politika u obzir treba uzeti i lokalno zakonodavstvo, naročito u delu koji se odnosi na zaštitu podataka o ličnosti, i klasifikaciju i zaštitu informacija. Takođe, CERT organizacije mogu uzeti u obzir i politike koje su u skladu sa međunarodnim standardima, kao što je ISO 27001.

Svi CERT timovi koji su prošli proces TI sertifikacije implementirali su bezbednosnu politiku krovne organizacije koja je njihov osnivač (u jednom slučaju krovna organizacija je sertifikovana po standardu ISO 27001, pa je i bezbednosna politika sertifikovana u tom smislu). Neki od timova su imali aktivno učešće u formulisanju bezbednosne politike svoje krovne organizacije. Međutim, većina CERT organizacija ima i neke dodatne odredbe i smernice koje se tiču njihovih specifičnih aktivnosti.

3.3.2.4.11 Opšta zapažanja u pogledu organizacionih parametara

Na osnovu povratnih informacija iz procesa sertifikacije, koje potiču od eksperata TI organizacije, organizacioni parametri za nacionalne i državne CERT organizacije su u dobrom stanju, potpuno dokumentovani, sa redom pojavom nekih ozbiljnijih problema.

Iako sertifikovane nacionalne i državne CERT organizacije nisu pominjale nikakve probleme u vezi sa klasifikacijom incidenata, eksperti TI su naveli da takvi problemi ipak povremeno postoje, na primer kada klasifikacija nije usaglašena između različitih organizacija, kada se ne objasni konstituentima na valjan način, ili ako nije podržana alatima za automatizaciju. Ipak, glavno pitanje koje se postavlja tokom sertifikacije jeste da li je postojeća šema klasifikacije odgovarajuća, tj. da li je timu pogodna za korišćenje.

Tokom procesa sertifikacije eksperti TI organizacije ne daju ocenu o razlikama koje uočavaju u klasifikacionim šemama različitih CERT timova, jer iako je uobičajeno da postoje određene sličnosti među timovima, one se u nekim delovima ipak razlikuju. Primera radi, klasifikacija incidenata može biti određena karakteristikama alata za evidenciju incidenata koje neki tim koristi, ili može biti diktirana od strane zakonodavca u nekoj zemlji. Na tlu Evrope ne postoji konzistentan način za klasifikaciju incidenata, i ovo je jedna od oblasti na kojoj je potrebno dodatno raditi u budućnosti.

3.3.2.5 Ocenjivanje zrelosti parametara ljudskih resursa

3.3.2.5.1 Kodeks poslovanja i etika

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Proces sertifikacije zahteva da postoji određeni skup pravila i smernica za profesionalno ponašanje članova CERT tima, unutar CERT organizacije i van nje. Jedan od primera kodeksa poslovanja u CERT organizaciji je dokument organizacije TF-CSIRT *The CSIRT Code of Practice* – CCoP. Ovaj dokument porkiva pravne aspekte (uključujući i slučajeve međunarodnih incidenata), odgovornosti u pogledu razmene informacija, kao i neke specifične zahteve u pogledu istraživanja ranjivosti sistema. Kada su u pitanju nacionalne i državne CERT organizacije, od njihovih zaposlenih se očekuje adekvatan način ponašanja, naročito kada ostvaruju kontakt sa partnerskim organizacijama. Naravno, kodeks poslovanja i etike mora biti formulisan tako da ne ometa, ili ne ograničava normalne radne procese u okviru tima.

Nacionalne i državne CERT organizacije mogu primenjivati i kodeks poslovanja svoje krovne organizacije. U slučaju da su ta pravila previše uopštena za potrebe CERT organizacije, njih treba nadograditi stavkama iz CCoP. Svi zaposleni treba da budu upoznati sa kodeksom poslovanja i etike, i treba ih ohrabrivati da o tok dokumentu diskutuju, kako bi se on stalno poboljšavao.

Većina do sada sertifikovanih CERT timova ima kodeks poslovanja u nekom obliku, bilo kao deo politika svoje krovne organizacije, ili u vidu pravila koje nameće zakonodavac (kao što su pravila za zaposlene u javnim ustanovama, ili politike bezbednosti državnih organizacija). Jedan od timova je pomenuo da je kodeks poslovanja jedna od prvih tema za razgovor sa novim zaposlenima. Sa druge strane, jedan od timova je naveo da se prilikom

zapošljavanja više oslanja na nečiju reputaciju u okvirima odrgovarajuće zajednice, nego na način njegovog budućeg ophođenja unutar organizacije ili ka spoljnjim entitetima.

3.3.2.5.2 Popunjenost osoblja

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Nedostatak kvalifikovanog osoblja je jedan od najvećih problema nacionalnih i državnih CERT organizacija. Uslov za sertifikaciju je da CERT tim ima najmanje tri člana (stalno zapooslena, ili honorarno angažovana). Dosta je uobičajeno da CERT timovi imaju honorarno angažovano osoblje, mada u ugovorima sa njima treba jasno definisati da u hitnim situacijama njihovo angažovanje u CERT-u mora imati prioritet u odnosu na bilo koji drugi njihov angažman.

Kao dodatak na stalne članove tima, dobra ideja je i da se formira skup dobrovoljaca koji bi se stavio na raspologanje CERT timu u slučajevima ekstremnih kriznih situacija. Njih treba uključivati u aktivnosti CERT organizacije, kako bi stekli osnovno razumevanje njenog načina rada. Takođe, treba im obezbediti i odgovarajuća ovlašćenja po pitanju delovanja u okviru CERT organizacije.

CERT timovi obično imaju mali broj članova, i organizacija mora da usvoji procedure kojima bi se obezbedilo da svaka kritična funkcija bude pokrivena sa jednim zaposelnim kome je to primarni posao, i još jednim zaposlenim koji može da ga preuzme u slučaju nužde.

Do sada sertifikovani CERT timovi nisu pominjali probleme sa popunjenošću osoblja, mada neki od njih ne nude servise u režimu radnog vremena 24/7. Većina timova ima na raspolaganju dodatno ljudstvo (na primer zaposleni iz krovne organizacije) koje mogu angažovati u kriznim situacijama. U zavisnosti od funkcija i veličine zajednice konstituenata, nacionalni i državni CERT tiovi teže da imaju više od tri zaposlena. Broj zaposlenih u nacionalnim i državnim CERT timovima koji su do sada sertifikovani kreće se od 8 do 35 ljudi u jezgru tima, pa čak i do 100 zaposlenih u okviru njihove krovne organizacije, koji mogu biti angažovani kao podrška na poslovima CERT tima u slučaju krizne situacije.

3.3.2.5.3 Opis stručne osposobljenosti

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Zaposleni u okviru CERT timova imaju različite nivoe obrazovanja, i potiču iz raznih okruženja. Postoje brojni materijali i dokumenta koji opisuju veštine i znanja kojima članovi CERT tima moraju raspolagati radi uspešnog obavljanja posla.

Zadatak pronalaženja i angažovanja iskusnih profesionalaca može biti izuzetno težak, naročito za nacionalne i državne CERT organizacije (s obzirom na njihove finansijske resurse), tako da tokom razgovora za posao CERT organizacije treba da se fokusiraju na nalaženje osoba koje imaju odgovarajući pristup poslu i način razmišljanja, pre nego da pokušavaju da pronađu potpuno kvalifikovane profesionalce. Još jedan aspekt u sastavljanju

CERT tima, tj. angažovanja dodatnih zaposlenih, je da treba biti svestan svih mogućnosti svakog zaposlenog u okviru tima (uzimajući u obzir i mogućnosti njihovog budućeg razvoja).

Skup potrebnih znanja i veština treba da bude interno definisan, na primer u vidu kolekcije opisa poslova i radnih mesta, i dostupan zaposlenima preko internih portala.

Kada su u pitanju do sada sertifikovane CERT organizacije, skup znanja i veština za svaku specifičnu poziciju daje se u oglasu za zapošljavanje, a postoji i u formalnom opisu svake funkcije ili radnog mesta.

3.3.2.5.4 Interne obuke

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Interne obuke su usmerene na poboljšavanje radnih sposobnosti novih članova CERT tima, ali i za poboljšanje znanja i veština starih zaposlenih.

Kada su u pitanju novi zaposleni pogodno je da postoji neki interni priručnik koji mogu da iskoriste za sticanje znanja i razumevanje trenutne pozicije i poslova CERT organizacije čiji su član. Ukoliko je to moguće, novim zaposlenima treba dodeliti jenog (ili više) mentora, tj. starijih zaposlenih koji će svojim iskustvom uvesti nove ljude u posao u što kraćem roku. Takođe, poželjno se da se svaki novi član tima upozna sa svim zaposlenima, tj. njihovim funkcijama i svakodnevnim poslovima koje obavljaju.

CERT organizacije treba da podstiču internu razmenu znanja i informacija među zaposlenima, kao i prilika za stručni razvoj i napredovanje u okviru organizacije.

U svakom slučaju, procedure za mentorstvo i internu obuku moraju biti dokumentovane, kako bi CERT organizacija mogla da se posveti ovom važnom i zahtevnom poslu na ispravan način.

Kada su u pitanju do sada sertifikovane CERT organizacije, one uglavnom primenjuju proces mentorstva, kao i internih treninga i korišćenje priručnika, za obuku novih i starih zaposlenih. Neke od njih imaju i više formalan program obuke koji pokriva sve osnovne aspekte poslovanja (interne alate za evidenciju incidenata, alate za testiranje bezbednosti sistema, mandat i funkcije organizacije, opise servisa, bezbednosne procedure, i slično). Još jedan mogući pristup je da se proces interne obuke sprovodi kroz programe krovne organizacije u okviru koje je CERT tim formiran.

3.3.2.5.5 Eksterne tehničke obuke

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Mogućnosti za pohađanje eksternih tehničkih obuka su jako brojne, i u tom smislu glavni izazov je naći balans između postojećih potreba i raspoloživih resursa, kako bi CERT organizacija normalno funkcionisala i u periodima kada su zaposleni odsutni sa posla zbog obuka. Preporuka je da za nove zaposlene postoji obavezan eksterni trening (na primer TRANSITS I (*Technology Review Assistance Notification Standards Integration and Testing*). Dobra ideja za održavanje nivoa znanja i sposobnosti je i korišćenje kurseva i seminara koji

su dostupni preko interneta. Kao deo kontinualne napredne tehničke edukacije zaposlenih može se koristiti i trening TRANSITS II.

S obzirom da se nacionalne i državne CERT organizacije u svom poslovanju oslanjanju na fiksne budžete, veoma je važno da se troškovi obuka zaposlenih uključe u godišnje budžete.

CERT timovi mogu da razmotre i korišćenje besplatnih obuka organizacije ENISA, pri čemu nacionalne i državne CERT organizacije mogu zahtevati od ENISA-e da pripremi obuke koje su skrojene prema specifičnim potrebama tima.

Većina do sada sertifikovanih CERT organizacija navodi TRANSITS I kao osnovnu eksternu obuku koja je potrebna novim zaposlenima. Uobičajeno je da postoje dobro dokumentovani procesi i budžet za eksterne obuke.

3.3.2.5.6 Eksterne obuke za komunikaciju

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Većina članova nacionalnih i državnih CERT timova svakodnevno komuniciraju sa svojim konstituentima, ili drugim eksternim organizacijama. Iskusnije CERT organizacije trebalo bi da budu osposobljene i za efikasnu komunikaciju novinarima ,tj. medijima, i generalno širom javnošću. Poželjno je da bar neki članovi tima pohađaju eksterne obuke naprednih tehnika komunikacije, a neke osnovne vidove obuke (koje se mogu organizovati interno, ili u okviru krovne organizacije) treba da imaju i ostali članovi tima.

U okviru TRANSIT II obuke postoji odličan trening na temu komunikacije, koji je dostupan CERT organizacijama.

Dodatno, ukoliko to dozvoljavaju finansijski uslovi, nacionalne i državne CERT organizacije treba da razmotre i angažovanje eksperata koji bi u kriznim situacijama preuzeli na sebe komunikaciju sa medijima i širom javnošću.

Timovi koji su do sada prošli kroz proces sertifikacije imaju različite pristupe u tome kome je dozvoljeno da komunicira sa medijima. U nekim CERT timovima je svima dozvoljeno da komuniciraju sa medijima, i stoga svi moraju da imaju obuke na temu komunikacije. U nekim drugim timovima komunikacija sa medijima je ograničena na određene članove tima koji su za to obučeni. Međutim, svi timovi navode da razmatraju mogućnost da obezbede odgovarajuće treninge iz oblasti komunikacija sa javnošću za sve članove tima.

3.3.2.5.7 Saradnja sa eksternim organizacijama

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Saradnja sa eksternim organizacijama ima dve komponente: sastanci sa predstavnicima drugih CERT organizacija, i aktivno učestvovanje u zajednicama CERT organizacija. Postoji određeni broj ključnih organizacija koje omogućavaju CERT organizacijama da se susreću i komuniciraju između sebe (kao što su FIRST, ili ENISA). Skupovi ovih organizacija se

održavaju nekoliko puta godišnje na različitim lokacijama, i nacionalne i državne CERT organizacije bi trebalo da ulože napore da prisustvuju barem nekim od tih skupova.

Nacionalne i državne CERT organizacije trebalo bi da budu aktivne u međunarodnim forumima, ali još važnije, trebalo bi da učestvuju u forumima koji se organizuju posebno za njihove potrebe, kao što su:

- radionica u organizaciji ENISA-e, pod nazivom „*CERT Workshop*“, koja se organizuje jednom godišnje i posvećena je evropskim nacionalnim i državnim CERT organizacijama,
- skup u organizaciji FIRST-a, pod nazivom „*Annual FIRST Conference*“, koji se organizuje jednom godišnje za potrebe CERT organizacija.

Učešće u međunarodnim formima je izuzetno važno, i nacionalne i državne CERT organizacije bi trebalo da planiraju budžetska sredstva za učešće na ovakvim skupovima.

Svi do sada sertifikovani CERT timovi podvukli su važnost učešća na međunarodnim skupovima. U većini slučajeva, za svaku od međunarodnih organizacija (FIRST, TF-CSIRT, EGC ...) postoji kontakt osoba iz CERT tima koja sarađuje sa ovim organizacijama. Sastancima ovih grupa najčešće prisustvuju osoba koja je zadužena za kontakt sa konkrentom organizacijom, i još jedan dodatni član tima, po principu rotacije među članovima tima.

3.3.2.5.8 Opšta zapažanja o parametrima ljudskih resursa

Na osnovu povratnih informacija iz procesa sertifikacije, koje potiču od eksperata TI organizacije, parametri ljudskih resursa za nacionalne i državne CERT organizacije pod uticajem su nedostatka resursa, veština i iskustva.

Najveći izazovi vezani su za parametre koji se tiču mentorstva i obuke za postojeće i nove članove CERT timova. Svi timovi su tokom sertifikacije prijavili da je ova praksa u njihovim organizacijama dokumentovana, ali dešava se da je obuka za nove članove tima neredovna, i u mnogim slučajevima je sprovode različiti članovi tima, tako da se nekad čini da se ceo proces „izmišlja“ svaki put iznova. Preporuka je da se ovim procesima dobro promisli, i da se oni dokumentuju u skladu sa potrebama CERT organizacije.

Još jedan izazov pred organizacijama je da se opravdaju finansijska sredstva koja su neophodna za eksterne tehničke obuke. Smanjenje dostupnosti finansijskih sredstava utiče na mogućnost CERT timova da ulažu u obuku i sertifikaciju članova svojih timova, dovodeći time u pitanje i proces re-sertifikacije svojih organizacija. Neki timovi navode da je programe obuke moguće izvoditi i na bazi materijala koji su dostupni preko interneta, ali nedostatak međuljudske interakcije dovodi do toga da timovi nisu u prilici da se međusobno upoznaju i izgrađuju neophodno poverenje.

3.3.2.6 Ocenjivanje zrelosti tehničkih parametara

3.3.2.6.1 Lista resursa

Minimalni zahtevani nivo ocene	Opis
1	Implicitno, na bazi lične procene, prethodnih znanja ili iskustava

Zajednica konstituenata nacionalnih i državnih CERT organizacija u opštem slučaju je jako široka, pa je takav i skup softverskih i hardverskih resursa koje CERT tim treba da podrži. Međutim, da bi se ispunili kriterijumi za sertifikaciju CERT tim bi morao biti u stanju

da prepozna koji servisi su njima potrebni, ili tačnije, koji tip pomoći i informacija konstituenti očekuju od svoje CERT organizacije.

Kada su u pitanju državne CERT organizacije postoji mogućnost da one dobiju dodatne informacije od određenih institucija (kao što su npr. nosioci kritične informacione infrastrukture, ili državne institucije). To se može postići obilaskom lokacija i intervjiusanjem konstituenata, radi dobijanja informacija o njihovim informatičkim resrsima. Resultate ovih istraživanja treba čuvati u nekoj organizovanoj formi, npr. u odgovarajućoj bazi podataka.

Kada su u pitanju nacionalne CERT organizacije, u nekim slučajevima nije moguće da one imaju na raspolaganju kompletne liste resursa svojih konstituenata, što otežava situaciju kada im treba distribuirati informacije ili savete o novootkrivenim ranjivostima sistema. Nacionalne i državne CERT organizacije treba da budu obučene da opslužе bilo koji zahtev svojih konstituenata.

Mnogi već sertifikovani CERT timovi održavaju liste resursa svojih konstituenata, mada ti podaci u nekim slučajevima nisu kompletni. Obično je slučaj da se poseduje veća količina informacija o nosiocima ključne informacione infrastrukture i državnim institucijama. Neki timovi navode da je održavanje liste resursa u ažurnom stanju izazovan zadatak, a ove informacije zahtevaju i adekvatan nivo zaštite, s obzirom da se često radi o poverljivim podacima. Nacionalne CERT organizacije često imaju samo grubu predstavu o resursima svojih konstituenata, ali se u najvećem broju slučajeva oslanjaju na svoje iskustvo i mogućnost da rešavaju probleme na svim tipovima hardvera ili softvera.

3.3.2.6.2 Lista izvora informacija

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Nacionalne i državne CERT organizacije treba da imaju barem jednu pisanu proceduru o tome kako dobijaju informacije o ranjivostima sistema i pretnjama po bezbednost, uključujući i listu izvora informacija. O svakom izvoru mogu postojati i dodatne informacije (o nivou poverenja u taj izvor, ili o korisnosti informacija koje odatle stižu). Postoji i široka lepeza izvora informacija koje se mogu integrisati sa sistemom za evidenciju incidenata CERT organizacije, i koji se mogu koristiti za potrebe edukacije.

Sve sertifikovane nacionalne i državne CERT organizacije pominju da poseduju liste izvora informacija u različitim formama, u vidu internih baza znanja ili specijalnih sistema (kao što su TARANIS, ili OTRS – *Open-source Ticket Request System*). Liste izvora informacija obično obuhvataju medijske, ili javne izvore informacija, ali i neke poverljive izvore informacija.

3.3.2.6.3 Konsolidovani sistem elektronske pošte

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Sva elektronska pošta CERT organizacije treba da bude čuvana na jednom repozitorijumu, koji je dostupan svim članovima CERT tima po potrebi. Preporučuje se i da

sistem za prijavu incidenata bude integrisan sa sistemom elektronske pošte (kako bi se prijave incidenata putem elektronske pošte automatski evidentirale), što treba da bude dokumentovano i odobreno od strane rukovodstva CERT organizacije.

Svi sertifikovani timovi potvrdili su da koriste RTIR (*Request Tracker for Incident Response*) sistem, koji omogućava konsolidaciju sistema elektronske pošte, i omogućava određeni nivo automatizacije pri obradi dolazećih prijava incidenata (u slučaju nekih timova 80% prijava incidenata putem elektronske pošte se obrađuje automatski).

3.3.2.6.4 Sistem za evidenciju o incidentima

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Potrebno je da postoji dokument koji opisuje kako se upravlja incidentima korišćenjem alata za evidenciju incidenata. Postoji veliki broj ovakvih alata (RTIR, AIRT ...). Takođe, za nove zaposlene mora da postoji program obuke u korišćenju ovih alata. Svaki od ovih alata su dizajnirani za potrebe CERT organizacija, ali je često potrebna i neka izmena u njima zbog specifičnosti svake od organizacija, i čest je slučaj da CERT timovi imaju interno zaposlene programere koji se bave ovakvim adaptacijama sistema. U tom smislu, jako su važne sve primedbe i sugestije zaposlenih koji koriste ove sisteme u svakodnevnom radu.

Svi sertifikovani timovi navode da koriste RTIR sistem za evidenciju incidenata, ali i da ulažu dodatne napore za prilagođavanje ovog sistema svojim specifičnim potrebama.

3.3.2.6.5 Pouzdanost telefonsog sistema

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

CERT organizacije moraju biti svesne svojih potreba u pogledu telefonskih servisa. Iako formalni dokument nije uslov za potrebe sertifikacije, potrebno je da u ugovoru sa isporučiocem telefonskog servisa budu definisani parametri garancije kvaliteta servisa, tj. maksimalnog mogućeg trajanja prekida u isporuci ovog servisa. Rezervno rešenje u ovakvim situacijama je korišćenje servisa mobilne telefonije.

Sertifikovane nacionalne i državne CERT organizacije koriste telefonsku infrastrukturu krovne organizacije, i u većini slučajeva imaju ugovor o garantovanom nivou kvaliteta i dostupnosti ovog servisa.

3.3.2.6.6 Pouzdanost sistema elektronske pošte

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Kada su u pitanju sistemi elektronske pošte, najbolja praksa je da CERT organizacije imaju svoje sopstvene sisteme. Pri tome je obavezna enkripcija konekcija i za odlazni i za dolazni saobraćaj, a treba razmotriti i maskiranje IP adrese pošiljaoca.

U slučaju da je sistem elektronske pošte poveren spoljnjim entitetima, mora biti definisan nivo garancije kvaliteta servisa, sa definisanim maksimalnim mogućim vremenom prekida u isporuci servisa. Takođe, treba jako voditi računa i o poverljivosti podataka, tj. bezbednosnoj zaštiti ovog sistema.

Sve sertifikovane nacionalne i državne CERT organizacije imaju svoje sopstvene sisteme elektronske pošte, ili koriste sisteme svoje krovne organizacije.

3.3.2.6.7 Pouzdanost internet pristupa

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

CERT timovi treba da budu svesni svojih potreba u pogledu pristupa internetu. Nacionalne i državne CERT organizacije treba da imaju pristup internetu preko više od jednog provajdera internet servisa, ili barem redundantne fizičke konekcije ka svom provajderu. I u ovom slučaju mora biti definisan nivo garancije kvaliteta servisa, sa definisanim maksimalnim mogućim vremenom prekida u isporuci servisa.

Svi sertifikovani timovi koriste internet infrastrukturu svoje krovne organizacije, a neki timovi navode da postoje i posebne garancije za nivo kvaliteta servisa. Svi CERT timovi imaju konektivnost preko više provajdera internet servisa, a neki imaju pristup i nacionalnoj mreži za krizne situacije.

3.3.2.6.8 Skup alata za prevenciju incidenata

Minimalni zahtevani nivo ocene	Opis
1	Implicitno, na bazi lične procene, prethodnih znanja ili iskustava

Nacionalne CERT organizacije u većini slučajeva imaju ulogu koordinatora u poslovima informacione bezbednosti, pa se u tom smislu ovaj parametar ne mora ocenjivati. U slučaju da CERT ne igra samo ulogu koordinatora, proces sertifikacije podrazumeva da tim mora biti svestan da postoje alati za prevenciju bezbednosnih incidenata.

Državne CERT organizacije mogu imati potencijala da bliže sarađuju sa svojim konstituentima, uključujući i opciju da predlažu korišćenje nekih alata za prevenciju incidenata, kao i mogućnost da prikupljaju informacije iz takvih alata (na primer SPAM (*Self Propelled Automatic Mail*) filtera, virus skenera, i slično).

Za nacionalne i državne CERT organizacije koje nemaju direktan pristup sistemima svojih konstituenata preporučuje se upotreba ovih alata kako bi bili svesni određenih aktivnosti u mreži i opasnosti koje vrebaju.

Većina do sada sertifikovanih CERT organizacija navodi da poseduje odgovarajuće alate, koji su opisani u internoj dokumentaciji timova, osim jednog tima koji na ovom parametru ima ocenu „-1“. Neki timovi omogućavaju svojim konstituentima da koriste ove alate kao servis, npr. za skeniranje otvorenih komunikacionih portova. Neke od informacija u

vezi sa prevencijom incidenata objavljuju se i na internet stranicama CERT organizacija. Tokom sertifikacije najbitnije je dokazati da zaposleni umeju na odgovarajući način da koriste skup navedenih alata koje CERT organizacija koristi.

3.3.2.6.9 Skup alata za detekciju incidenata

Minimalni zahtevani nivo ocene	Opis
1	Implicitno, na bazi lične procene, prethodnih znanja ili iskustava

Izuzetno je važno, naročito za državne CERT organizacije, da dobijaju informacije o incidentima kada se oni dogode, ili postoji opasnost da će se dogoditi. Najdragoceniji su podaci koji bi se dobili direktno od konstituenata (sa sistema za detekciju incidenata, ili alata za analizu mrežnog saobraćaja). Državne CERT organizacije bi trebalo da budu u mogućnosti da postignu takve dogovore sa svojim konstituentima. Druga opcija za CERT organizacije, ukoliko bi to bilo zakonski moguće, je da kreiraju namensku mrežu senzora za otkrivanje bezbednosnih incidenata kod konstituenata.

Za nacionalne i državne CERT organizacije postoji i opcija da dobijaju informacije iz eksternih izvora (kao što su *Spamhaus*, *Team Cymru*, *Shadowserver*, i slične) o incidentima koji su detektovani kod njihovih konstituenata. Ukoliko se procesiraju na odgovarajući način, iz takvih informacija može da proistekne vrlo konkretan i ciljani savet za zaštitu svojih konstituenata.

Većina sertifikovanih timova ima alate za detekciju bezbednosnih incidenata, koji su dobro dokumentovani i opisani u internim procedurama CERT organizacija. Tokom sertifikacije neki timovi su izveli i demonstraciju učinka svojih alata.

3.3.2.6.10 Skup alata za razrešavanje incidenata

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Jedan od uslova za sertifikaciju je da postoji alat za razrešenje incidenata koji je barem interno opisan i dokumentovan. Opseg ovih alata može biti širok, od jako bazičnih (*Whois*, *Traceroute*, ...), do naprednih laboratorija i alata. Nacionalne i državne CERT organizacije trebalo bi da budu u stanju da se izbore sa bilo kojom vrstom bezbednosnih incidenata, tako da bi trebalo da poseduju i odgovarajući skup alata, tj. trebalo bi da im budu dostupni barem alati za digitalnu forenziku, reverzni inženjering i analizu *web* aplikacija.

Zajednica CERT organizacija je otvorena za razmenu informacija, i koristi različite tipove alata. U većini slučajeva postoje *open source* alati, koji omogućavaju CERT organizacijama da obavljaju svoje funkcije bez dodatnih troškova. U slučaju komercijalnih proizvoda, nacionalne i državne CERT organizacije najčešće mogu da računaju na niže cene ovih alata, od uobičajenih za druge korisnike.

Sve sertifikovane nacionalne i državne CERT organizacije imaju alate za razrešenje incidenata, koji su jako dobro dokumentovani unutar organizacije. Jedan od timova ima i javnu prezentaciju o alatima koje koristi za razrešenje incidenata.

3.3.2.6.11 Opšta zapažanja o tehničkim parametrima

Na osnovu povratnih informacija iz procesa sertifikacije, koje potiču od eksperata TI organizacije, samo nove CERT organizacije imaju problema sa korišćenjem različitih alata. Iskusne organizacije imaju sve neophodne alate i sisteme za svoje uspešno poslovanje.

Ukoliko tim ima dobar balas u ljudima koji su angažovani na tehničkim, odnosno proceduralnim i procesnim pitanjima, onda su tehničke mogućnosti i sposobnosti tima kao celine izuzetno velike, ali i na pravi način dokumentovane.

3.3.2.7 Ocenjivanje zrelosti procesnih parametara

3.3.2.7.1 Eskalacija na nivo upravljanja

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Proces eskalacije, u cilju bržeg razrešavanja incidenata, ka rukovodstvima nacionalnih i državnih CERT organizacija, kao i upravljačkim nivoima konstituentskih organizacija, mora biti formalizovan i odobren minimalno od strane rukovodstva CERT organizacija. Formalizovani proces mora da uzme u obzir različite scenarije, dok proces eskalacije mora u sebi da sadrži i opis nivoa ozbiljnosti incidenta i hitnosti situacije. Ukoliko nacionalne i državne CERT organizacije imaju ulogu entiteta za koordinaciju, mora postojati mehanizam za definisanje rokova i osoba odgovornih za razrešavanje incidenata, i davanje povratnih informacija CERT organizaciji. Ukoliko se ovi rokovi ne ispoštuju treba da postoji mogućnost da se kontaktira rukovodstvo organizacije koja nije dovršila posao u predviđenom vremenu.

Rukovodstvo nacionalnih i državnih CERT organizacija treba da ima potpuno razmevanje mehanizama i načina na koji može da kontaktira rukovodioce odgovarajućih organizacija onda kada je to neophodno.

Kod već sertifikovanih CERT organizacija proces eskalacije je implementiran na veoma kvalitetan način. On je dokumentovan u internim procedurama i priručnicima za poslovanje, i procedurama sa krovnom organizacijom, ili može imati formu ugovora sa drugim organizacijama. Takođe, važno je povremeno izvoditi vežbe kojima se testira funkcionisanje ovih procedura i mehanizama.

3.3.2.7.2 Eskalacija ka medijima

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Proces eskalacije ka medijima trebalo bi da opiše kako nacionalne i državne CERT organizacije ostvaruju kontakt sa odeljenjem za odnose sa medijima svoje krovne organizacije. Potrebno je da postoje jasne granice šta je to što CERT organizacija može javno da objavi bez koordinacije sa svojom krovnom organizacijom, a koje su to poruke koje je potrebno usaglasiti. Primer objava koje je potrebno koordinisati sa rukovodstvom organizacije

mogu biti napadi velikih razmera na državne institucije, ili kritičnu informacionu infrastrukturu.

Sertifikovani CERT timovi imaju dobro dokumentovane procese eskalacije ka medijima. U većini slučajeva ti procesi su dokumentovani u procedurama sa krovnom organizacijom, kao i u internim priručnicima za poslovanje. CERT organizacije se trude da imaju odeljenja za komunikacije koja su tako dimenzionisana da mogu se uključe u aktivnosti CERT organizacija, ukoliko se za to ukaže potreba usled bezbednosnih incidenata velikih razmera.

3.3.2.7.3 Pravne eskalacije

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Do potrebe za eskalacijama pravne prirode može da dođe u različitim situacijama – koordinacija i pravna podrška u kriznim situacijama razrešavanja bezbednosih incidenata (naročito međunarodnih bezbednosnih incidenata), ili administrativni poslovi kao što je odobravanje ugovora ili memoranduma o saradnji. I ovi procesi i procedure treba da budu redovno testirani i proveravani, a moraju da postoje i ažurne kontakt informacije za slučaj da je potrebno obratiti se za pomoć službi pravnih poslova.

Sertifikovani CERT timovi imaju uspostavljene procedure saradnje sa pravnim službama svojih krovnih organizacija, koje su interno dokumentovane u priručnicima za poslovanje.

3.3.2.7.4 Proces prevencije incidenata

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Nacionalne CERT organizacije utiču na prevenciju bezbednosnih incidenata kroz aktivnosti podizanja svesti o informacionoj bezbednosti, programe obuka svojih konstituenata i savetodavne aktivnosti. Kada su u pitanju državne CERT organizacije taj uticaj može biti i direktniji, u zavisnosti od saradnje sa različitim institucijama. Potrebno je da postoje pisane procedure za korišćenje alata pomenutih u ranijim poglavljima, koje su svima dostupne po potrebi, i koje se redovno ažuriraju.

Sve sertifikovane nacionalne i državne CERT organizacije imaju dokumentovane procese za prevenciju incidenata, koji su usaglašeni sa alatima koji im stoje na raspolaganju za te svrhe (o kojima je bilo reči u poglavlju 3.2.6.8).

3.3.2.7.5 Proces detekcije incidenata

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Procedura za korišćenje alata pomenutih u poglavlju 3.2.6.9 trebalo bi da postoji u pisanoj formi, dostupna svima kojima je potrebna, i redovno ažurirana. Kada se informacije dobijaju direktno od konstituenata, može postojati i potreba za posebnim ugovorima koji se tiču poverljivosti podataka.

Sve sertifikovane nacionalne i državne CERT organizacije imaju dokumentovane procese za detekciju incidenata, koji su usaglašeni sa alatima koji im stoje na raspolaganju za te svrhe (o kojima je bilo reči u poglavlju 3.2.6.9).

3.3.2.7.6 Procesi za razrešavanje incidenata

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Procedura za korišćenje alata pomenutih u poglavlju 3.2.6.10 trebalo bi da postoji u pisanoj formi, dostupna svima kojima je potrebna, i redovno ažurirana.

Sve sertifikovane nacionalne i državne CERT organizacije imaju dokumentovane procese za razrešavanje incidenata, koji su usaglašeni sa alatima koji im stoje na raspolaganju za te svrhe (o kojima je bilo reči u poglavlju 3.2.6.10). Jedna CERT organizacija je objavila proces upravljanja incidentima na svojoj *web* stranici, objašnjavajući kako njihov tim može da učestvuje u razrešenju bezbednosnih incidenata.

3.3.2.7.7 Specifični procesi u vezi sa incidentima

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

CERT organizacije moraju doneti odluku o tome da li različiti tipovi incidenata podrazumevaju različite načine njihove obrade. U tom smislu, potrebno je razviti odgovarajuće procedure (ili jedan proces rada u koji se uklapaju svi tipovi incidenata, ili različite procese za svaki od tipova incidenata).

Tri sertifikovane nacionalne i državne CERT organizacije imaju različite procese rada za različite vrste incidenata. Ovi procesi su interno dokumentovani, redovno se ažuriraju i obavezno primenjuju. Primeri različitih tipova incidenata koji podrazumevaju različite načine obrade su DDoS (*Distributed Denial-of-Service*) incidenti, incidenti u vezi sa PKI (*Public Key Infrastructure*) ključevima, *phishing* napadi, IP adrese i URL-ovi (adrese na Internetu) sa malicioznim kodom, kao i druge vrste pretnji. Različiti procesi obrade podrazumevaju i korišćenje različitih alata.

3.3.2.7.8 Proces revizije

Minimalni zahtevani nivo ocene	Opis
4	Eksplicitan i podložan reviziji na nivoima van CERT organizacije, od strane spoljnjih subjekata zaduženih za kontrolu i nadzor

Ovo je jedan od najstriktinijih uslova za sertifikaciju, gde je potrebno da postoji eksplicitan i aktivan proces revizije, sa nivoa iznad nacionalne i državne CERT organizacije. Revizija mora da uključuje povratne informacije od rokuvodstva ili klijenata, kao i sprovođenje dodatnih aktivnosti koje su u skladu sa rezultatima revizije, kako bi se obezbedilo da dođe do poboljšanja u odgovarajućim oblastima. Kao deo procesa, potrebno je da se izrade i izveštaji za institucije koje se bave upravljanjem ili nadzorom CERT organizacija. Takođe, kada su u pitanju nacionalne i državne CERT organizacije, potrebno je izraditi i izveštaje koji bi bili dostupni široj javnosti.

Sertifikovani timovi imaju različite pristupe procesu revizije. U nekim slučajevima eksterni revizori izvode testove bezbednosti sistema CERT organizacije.

3.3.2.7.9 Dostupnost u hitnim situacijama

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Jedan od zahteva sertifikacije je da postoji formalni dokument koji opisuje dostupnost CERT organizacije u hitnim slučajevima van redovnog radnog vremena. Kada su u pitanju nacionalne i državne CERT organizacije potrebno je obezbediti dostupnost u režimu 24/7, za hitne slučajeve koji uključuju međunarodnu tačku kontakta. Organizacije kao što su TI, ili FIRST, mogu pomoći u deljenju kontakt informacija između CERT organizacija na međunarodnom nivou (obe organizacije čuvaju kontakt informacije u bazama podataka koje su dostupne akreditovanim i/ili sertifikovanim članicama). Nacionalne i državne CERT organizacije zemalja EU trebalo bi da budu deo mreže za saradnju, gde je predviđeno da ENISA daje podršku i deluje kao nezavisno telo u čuvanju i deljenju neophodnih informacija.

Sve sertifikovane nacionalne i državne CERT organizacije imaju na kvalitetan način organizovanu dostupnost organizacije u hitnim slučajevima. Načini dostupnosti u režimu 24/7, kao i druge kontakt informacije dostupne su na *web* stranicama organizacija, u ugovorima sa konstituentima, u bazama podataka organizacija TI i FIRST, kao i u RFC 2350 dokumentima organizacija.

3.3.2.7.10 Preporuke u vezi internet prezentacija i sistema elektronske pošte

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Nacionalne i državne CERT organizacije trebalo bi da imaju generičke alijase za elekotronsku poštu, koji se tiču informacione bezbednosti (kao što su „security@”, ili „abuse@”). Naravno, nisu svi generički alijasi relevantni za ove organizacije, na primer „hostmaster“, „webmaster“ i „postmaster“ su više relevantni za neke CERT organizacije koje imaju specifične konstituente.

Takođe, nacionalne i državne CERT organizacije moraju imati svoju internet stranicu, a potrebno je da postoji i sekcija sa informacijama na engleskom jeziku. Internet stranica treba da sadrži jasan opis konstituenata, servise i kontakte CERT organizacije. Timovi mogu da

razmotre da li će objaviti kontakt informacije svih članova tima, ili samo dela koji se bavi saradnjom sa spoljnjim entitetima.

Ovi parametri se testiraju tokom procesa sertifikacije. Testiranje može biti teško ukoliko domen delovanja CERT organizacije nije jasno definisan. Sertifikovane nacionalne i državne CERT organizacije imaju različita iskustva, neki od timova su kreirali neophodne alijase za elektronsku poštu tokom sertifikacije, dok su drugi bili uporni u tome da nedostajući alijasi nisu ni potrebni. Ukoliko CERT tima ima svoj sopstveni sistem elektronske pošte onda je dodavanje potrebnih alijasa relativno jednostavno.

3.3.2.7.11 Proces upravljanja poverljivim informacijama

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Nacionalne i državne CERT organizacije svkodnevno imaju kontakt sa poverljivim informacijama. Potrebno je da postoji procedura za korišćenje i razmenu informacija različitih nivoa poverljivosti. U te procedure moraju biti uključene i odredbe lokalnog zakonodavstva na temu upravljanja poverljivim podacima. Sve informacije moraju biti klasifikovane na odgovarajući način.

Međunarodni *de facto* standard za saradnju između CERT organizacija je ISTLP (*Information Sharing Traffic Light Protocol*). Njegovom primenom obezbeđuje se uspešna međunarodna saradnja, pri čemu je jako praktičan i jednostavan za implementaciju.

Dodatno, potrebno je da postoje tehnička sredstva za zaštitu informacija, kojima se osigurava bezbednost elektronske pošte, ili govorne komunikacije, omogućava čuvanje podataka i pravljenje rezervnih kopija (u i van lokacija organizacija), kao i bezbedno uništavanje diskova ili drugih medijuma za čuvanje podataka.

Svi zaposleni moraju biti obučeni o tome kako se potupa sa poverljivim informacijama.

Proces bezbednog upravljanja informacijama je deo bezbednosne politike većine timova. U većini slučajeva postoje odvojeni procesi za korišćenje PGP (*Pretty Good Privacy*) ili TLP (*Traffic Light Protocol*), koji su dokumentovani u internoj dokumentaciji i priručnicima za poslovanje. Nacionalne, a naročito državne CERT organizacije moraju vršiti klasifikaciju poverljivih informacija u skladu sa nacionalnim i međunarodnim propisima, i u tom smislu su zakonima definisane odgovarajuće procedure.

3.3.2.7.12 Izvori informacija

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Procedure za korišćenje izvora informacija opisanih u poglavlju 3.2.6.2 moraju biti definisane u pisanoj formi, dostupne svima po potrebi, i redovno ažurirane.

Sve sertifikovane nacionalne i državne CERT organizacije imaju ustanovljene procese kako da se odnose prema izvorima informacija, a najčešće korišćeni sistem za ove potrebe je TARANIS.

3.3.2.7.13 Prisustvo u javnosti

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Ovaj parametar se odnosi na komunikaciju sa konstituentima van regularnih procesa upravljanja incidentima. Ovo se odosni i na javne i medijske objave, kao i razne aktivnosti na podizanju svesti o informacionoj bezbednosti. Uslov za sertifikaciju je da unutar organizacije postoji formalni dokument na ovu temu. Za nacionalne i državne CERT organizacije je važno da prenose informacije o informacionoj bezbednosti, ali i o sebi kao organizaciji. Ovo doprinosi sposobnosti CERT timova da se nose sa bezbednosnim incidentima na dva načina: podizanje svesti o informacionoj bezbednosti doprinosi smanjenju rizika od pojave incidenata, i povećavaju se vidljivost i poverenje konstituenata u svoju CERT organizaciju.

Prisustvo u javnosti može obuhvatati razne aktivnosti kao što su:

- događaji kao što su seminari ili radionice koji su namnjeni određenim ciljnim grupama (od školske dece, preko IT stručnjaka, do rukovodilaca raznih organizacija),
- različiti tipovi edukativnih materijala,
- učestvovanje na nacionalnim i međunarodnim skupovima partnerskih organizacija,
- podrška ekspertskim grupama i forumima,
- učešće u televizijskim i radijskim emisijama koje se tiču informacione bezbednosti,
- deljenje određenih informacija sa novinarima, medijima i novinskim agencijama.

Zaposleni u CERT organizacijama treba da budu svesni ovih aktivnosti i da im daju svoj puni doprinos.

U većini sertifikovanih CERT organizacija ovaj proces je uspostavljen na kvalitetan način, i opisan je u internim dokumentima i priručnicima. Jedna od organizacija je razradila i politiku korišćenja društvenih mreža u komunikaciji sa konstituentima, a postoje i inicijative da se izvode testovi i vežbe kako bi se utvrdilo da li postoje delovi javnosti do kojih poruke CERT organizacija ne dopiru na odgovarajući način.

3.3.2.7.14 Proces izveštavanja

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Nacionalne i državne CERT organizacije moraju biti odgovorne za svoje aktivnosti, ne samo organizacijama koje su zadužene za nadzor njihovog rada, već i široj javnosti. Proces izveštavanja trebalo bi da bude na odgovarajući način dokumentovan u internim dokumentima i priručnicima za poslovanje. Zaposleni unutar CERT organizacija moraju biti svesni ovih procesa i moraju dati svoj adekvatan doprinos u njihovom sprovođenju.

Sve sertifikovane nacionalne i državne CERT organizacije imaju dobro dokumentovane procedure izrade izveštaja za potrebe rukovodstva, kao i alate koji im u tom

smislu pomažu. Tipovi izveštaja su različiti, od godišnjih ili kvartalnih izveštaja o incidentima, preko finansijskih izveštaja, pa do izveštaja koji su namenjeni široj javnosti.

3.3.2.7.15 Statistike o incidentima

Minimalni zahtevani nivo ocene	Opis
3	Eksplicitan i formalizovan – formalni dokument je verifikovan od rukovodstva CERT organizacije

Kada se govori o klasifikaciji incidenata, potrebno je da postoji i formalni dokument koji opisuje kako se kreiraju i objavljuju statistički izveštaji o incidentima. Izrada statistika o incidentima može biti deo sveobuhvatog procesa izveštavanja.

Kada su u pitanju do sada sertifikovani timovi, postoje primeri da se statistički izveštaji izrađuju samo za interne potrebe CERT organizacije, i ne šalju se konstituentima (ocena ovog parametra u tom slučaju bi bila „-1“). Većina timova barem jednom godišnje, a i češće, objavljuje statističke izveštaje na svojim internet stranicama. Takođe, većina timova je primetila da bi bilo korisno da postoji neka unificirana metrika, kako bi izveštaji i rezultati različitih timova mogli da se porede.

3.3.2.7.16 Interni sastanci

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

Interni sastanci u CERT organizacijama treba da se održavaju barem jednom mesečno kako bi svi članovi tima bili upućeni u svakodnevne aktivnosti. Ovi sastanci ne moraju biti naročito formalni, ali treba praviti neku vrstu zapisnika na koji je moguće kasnije se referencirati. Takođe, ohrabruje se i održavanje redovnim sastanaka u manjim grupama u okviru CERT tima. Radi bolje razmene informacija o operativnim problemima treba održavati i redovne operativne sastanke pri predaji poslova u okviru smenskog rada.

Svi sertifikovani timovi imaju redovne sastanke i ovaj proces je dokumentovan u internoj dokumentaciji i priručnicima za poslovanje. Učestanost ovih sastanaka varira – operativni sastanci se obično održavaju češće, čak i na dnevnoj bazi, dok se organizacioni sastanci održavaju ređe, najčešće jednom nedeljno ili u dve nedelje.

3.3.2.7.17 Saradnja sa partnerskim organizacijama

Minimalni zahtevani nivo ocene	Opis
2	Eksplicitan, interni – interna neformalna dokumenta i procedure u pisanoj formi

CERT organizacije moraju biti svesne važnosti saradnje sa sličnim partnerskim organizacijama. Razmena informacija sa drugim organizacijama može pomoći CERT timovima u njihovom svakodnevnom operativnom delovanju, a podrška međunarodnih organizacija je u tom smislu jako važna.

Kod sertifikovanih nacionalnih i državnih CERT organizacija proces saradnje sa partnerskim organizacijama je jako dobro prepoznat i dokumentovan u internoj dokumentaciji i priručnicima za poslovanje. Većina timova definiše i kontakt osobe zadužene za odgovarajuću vrstu saradnje sa spoljnjim entitetima.

3.3.2.7.18 Opšta zapažanja o procesnim parametrima

Ispunjavanje zahteva za potrebe sertifikacije u pogledu procesnih parametara može biti izazov za neke CERT timove. Ukoliko se tim sastoji od osoblja koje je više operativno i tehnički orijentisano, onda se može uočiti nedostatak odgovarajućih procedura. Ukoliko se tim više fokusira na procedure i politike, onda može biti u zaostatku sa tehničkim iskustvom i alatima. Kroz proces sertifikacije najlakše prolaze dobro izbalansirani timovi, koji imaju kvalitetno tehničko osoblje, ali i nekoga ko je dovoljno iskusan da se na kvalitetan način bavi procedurama poslovanja.

3.3.2.8 Zaključak

U opštem slučaju, nacionalne i državne CERT organizacije moraju da postignu viši nivo zrelosti i sposobnosti kako bi mogle da se nose sa poslovima informacione bezbednosti, u uslovima gde pretnje bezbednosti i ranjivosti sistema stalno evoluiraju. SIM³ model može da se koristi kao alat koji će im pomoći u tom procesu, ali i kao sredtsvo za nezavisnu procenu mogućnosti timova.

Kako bi osigurali napredak u svojim sposobnostima, timovi moraju da načine korak unazad, i objektivno sagledaju stanje svojih internih i eksternih procesa i procedura poslovanja. Pitanja na koja treba odgovoriti su da li je tim konzistentan u obavljanju svojih aktivnosti, i da li su njihove sposobnosti dovoljne za ispunjvanje ciljeva njihovih funkcija. Proces sertifikacije je pogodan alat za ove namene, jer se bavi procenom da li su mogućnosti organizacije u skladu sa njenom deklarisanom misijom, više nego što se bavi nekim opštim kriterijumima.

Potrebno je da CERT timovi razumeju da to nije samo revizija kojom se proverava njihov trenutni status, već je to proces u kojem se utvrđuju i oblasti u kojima je potrebno uložiti dodatne napore radi napretka organizacije. Čak i kada se prolazi kroz proces re-sertifikacije, tim mora da pruži dokaze o svom napretku tokom protekle tri godine, od kada je stekao status sertifikovane organizacije.

Važno je da svaki CERT tim samostalno uradi veći deo posla, pre nego što se prijavi za proces sertifikacije, uglavnom kroz proces samoocenjivanja, iako su mnogi od parametara uglavom već na zadovoljavajućem nivou, ili se relativno lako mogu ispuniti. Tim mora da bude spreman da bude iskren prema svojoj organizaciji, ali i ekspertima koji vrše ocenjivanje, jer je to jedini pristup koji donosi dobre rezultate.

Eksperti koji vrše ocenjivanje pokušavaju da sagledaju sve procese tima, i procene da li su suviše komplikovani, ili je moguće uvesti neka poboljšanja. Radionice za sertifikaciju daju priliku da se razgovara o procesima, i da se neki od njih osmisle na bolji način. Korisno je kada tim pokuša da sagleda svoje procese iz nekog drugačijeg ugla.

Na osnovu informacija koje potiču od već sertifikovanih timova formirane su sledeće praktične preporuke:

- podrška rukovodstva – u proces sertifikacije treba uključiti rukovodstvo organizacije od samog početka, kako bi se obezbedili odgovarajući resursi i odobrenja,
- resursi – treba osigurati da postoje dovoljni resursi za potrebe sertifikacije, i u pogledu ljudskih resursa i u pogledu finansijskih sredstava,

- odgovorno lice – ukoliko postoji osoba koja je zadužena da prati proces sertifikacije ceo proces će biti produktivniji, i teći će lakše i brže,
- uputstvo za rad – postojanje kvalitetnog dokumenta radnog uputstva olakšava proces sertifikacije,
- procedure – potrebno je razviti procedure koje su konzistentne sa deklarisanom misijom CERT tima, i njihovim svakodnevnim aktivnostima. Procedure je potrebno redovno ažurirati,
- RFC 2350 – CERT organizacija treba da ima kvalitetan dokuement RFC 2350 i da ga redovno ažurira,
- internet prezentacija – CERT organizacija treba da ima svoju internet stranicu, sa adekvatnim dokumentima i kontakt podacima koji su na njoj dostupni, na maternjem jeziku organizacije i na engleskom jeziku,
- dokumentacija – sva dokumenta koja su potrebna za proces sertifikacije treba da se čuvaju na jednom mestu, i dostupna članovima CERT tima, jer se time olakšava posao tokom sertifikacije,
- online interna baza znanja – umesto dugih dokumenata pogodnije je imati online bazu znanja, koja se i lakše ažurira ukoliko se za tim ukaže potreba,
- rotacija – na poslovima ažuriranja dokumentacije i pripreme za sertifikaciju svake godine treba postaviti nove članove tima, jer je to dobat način da svako od njih stekne odličan uvid u poslovanje CERT organizacije, i visok nivo razumevanja za sve procese unutar organizacije,
- edukacija i treninzi – procesi obuke zaposlenih treba da budu dokumentovani, jer to olakšava njihovo sprovođenje,
- saradnja sa eksternim organizacijama – učešće nacionalnih i državnih CERT organizacija u međunarodnim organizacijama je ključno za razumevanje okruženja i delatnosti tih organizacija, i olakšava da CERT organizacija postane uspešan i produktivan deo zajednice,
- samoocenjivanje – pre sertifikacije treba sprovesti proces samoocenjivanja, kako bi se kasniji proces sertifikacije olakšao i ubrzao, i ENISA može da pomogne CERT timovima u tom poslu,
- stalni napredak – i posle izvršene sertifikacije ne treba stati, organizacija stalno mora da se razvija i poboljšava. Treba razviti strategiju stalnog razvoja, sa fokusom na oblasti u kojima je tim u prethodnom periodu postigao slabije rezultate.

Takođe, postoje i stvari koje CERT organizacije treba da izbegavaju:

- sertifikacija ne treba da bude cilj sama po sebi, radije treba raditi na stalnom razvoju organizacije, kako bi TI sertifikat bio prirodan rezultat takvog rada,
- ne treba biti neiskren u procesu samoocenjivanja i u procesu sertifikacije, jer će u tom slučaju dostizanje višeg nivoa razvoja organizacije biti nemoguće,
- proces sertifikacije ne treba da obeshrabri CERT organizaciju, jer često izgleda teže nego što se u realnosti dešava,
- u proces sertifikacije ne treba ulaziti pre nego što se istraže sve dostupne informacije i resursi, i obave konsultacije sa drugim CERT timovima, ekspertima TI organizacije i ENISA-e.

Postoje CERT timovi koji smatraju da je glavni cilj da u svim parametrima, o kojima je bilo reči, napreduju do nivoa „4“ SIM³ modela. Obično je ovo nepotrebno u mnogim slučajevima, jer bi se revizija svih aspekata poslovanja CERT organizacije mogla smatrati

gubitkom vremena i resursa. Kada postoje dokumenta koja su potvrđena i odobrena od rukovodstva CERT organizacije (što odgovara nivou „3“ SIM³ modela), ona su već od velike koristi za organizaciju, jer su ih svi članovi tima svesni i koriste ih u radu. Za mnoge parametre nivo „4“ je nepotreban, a često je i nemoguće postići ga.

Ukoliko se desi da između procesa sertifikacije i re-sertifikacije CERT tim promeni svoju strukturu, bitno je potvrditi da svi procesi i dalje normalno funkcionišu, iako je struktura tima promenjena.

Sazrevanje CERT organizacija je proces za koji je potrebno vreme, kako bi se organizacije unapredile u raznim aspektima svog delovanja. Šema TI sertifikacije je alat koji omogućava CERT timu da proceni svoje performanse u spram zadataka koji se pred njih postavljaju, i da se otkriju manjkavosti na kojima je potrebno dodatno raditi. Sertifikacija je posao koji se tiče razumevanja procesa i pronalaženja uzroka problema, više nego dobijanja povoljnih ocena.

4. OBLASTI DELOVANJA I ODGOVORNOSTI CERT ORGANIZACIJE

4.1 UVOD

U cilju razumevanja značaja i uloge Nacionalnog centra za prevenciju bezbednosnih rizika u IKT (informaciono-komunikacionim) sistemima (u daljem tekstu „Nacionalni CERT“), potrebno je jasno definisati šta se uopšteno podrazumeva pod pojmom CERT-a, kao i neke druge osnovne pojmove koji se koriste u vezi sa tim, kao što su:

- **Konstituenti** - U skladu sa svrhom postojanja CERT timova, implicitno postoje i njegovi konstituenti. To je grupa korisnika, njihovih lokacija i mreža, ili organizacija kojima CERT tim pruža svoje servise. CERT tim mora biti prepoznat i priznat od strane svojih konstituenata da bi mogao efikasno da obavlja svoje poslove.
- **Bezbednosni incident** - To je bilo kakav neželjeni događaj koji kompromituje neke aspekte bezbednosti računarskih sistema ili mreža. Definicija incidenta može da varira između različitih organizacija, ali neke od generalnih kategorija koje se koriste su sledeće:
    - gubitak poverljivosti informacija,
    - kompromitovanje integriteta informacija,
    - onemogućavanje pružanja servisa,
    - zloupotreba servisa, sistema ili informacija,
    - oštećenje sistema.

  Ovo su vrlo uopštene kategorije. Primera radi, zamena nekog dela sistemskog programa malicioznim softverom, tzv. ,,trojancem" predstavlja primer „kompromitovanja integriteta“, dok je uspešno otkrivanje lozinke primer „gubitka poverljivosti“. Ovi napadi, čak i ako su neuspešni u slučaju kvalitetne zaštite sistema, moraju biti posmatrani kao bezbednosni incidenti.
  U okviru definicije incidenta koristi se reč „kompromitovan“. Nekada administrator može samo da „sumnja“ na incident, a tokom njegovog razrešavanja je potrebno utvrditi da li se on zaista i dogodio.

- **CERT -** Na osnovu definicija bezbednosnog incidenta i konstituenata, CERT je organizacija koja omogućava i koordinira razrešenja bezbednosnih incidenata, koji uključuju lokacije i sisteme definisanih konstituenata.
  Da bi neka organizacija mogla da se nazove CERT-om, potrebno je da:
  - omogući bezbedne kanale za dobijanje prijava o potencijalnim bezbednosnim incidentima,
  - obezbedi podršku svojim konstituentima za rešavanje ovih incidenata,
  - distribuira informacije o incidentima svojim konstituentima ili drugim relevantnim organizacijama.

  Treba primetiti da se u okviru ove definicije ne podrazumevaju policija ili istražni organi, koji, takođe, mogu istraživati kriminalne aktivnosti u vezi sa računarskim sistemima.

- **Vendor -** Vendor je entitet koji proizvodi i razvija mrežnu ili računarsku tehnologiju i odgovoran je za tehničke aspekte te tehnologije. Primeri tehnologije uključuju hardver (računari, ruteri, svičevi ...) i softver (operativni sistem, *e-mail* sistem...). Treba primetiti da vendor ne mora nužno biti i isporučilac tehnologije. Na primer, provajder Internet servisa može svojim korisnicima isporučiti rutere na korišćenje, ali vendor je njihov proizvođač, i on je odgovoran za tehničke aspekte njihovog funkcionisanja.

- **Ranjivost sistema -** Pojam ranjivosti odnosi se na krakteristiku dela tehnološkog rešenja koja se može iskoristiti u kreiranju bezbednosnog incidenta. Na primer, ukoliko program slučajno omogući običnim korisnicima da izvršavaju proizvoljne komande operativnog sistema, koje bi trebalo da budu dostupne samo u privilegovanom modu, onda se ova karakteristika označava kao ranjivost sistema.

Dakle, u najširem smislu, CERT je organizacija koja sprovodi, koordinira, i daje podršku u odbrani od bezbednosnih rizika u IKT sistemima, za potrebe svojih klijenata (koji se drugačije nazivaju i „konstituentima“). Bilo koja organizacija, koja igra ulogu CERT-a za određenu grupu svojih konstituenata, mora da reaguje na prijavljene bezbednosne incidente, i pretnje po bezbednost IKT sistema svojih konstituenata, na način koji je u okviru te zajednice generalno dogovoren.

S obzirom da je od ključne važnosti da svaki član zajednice konstituenata zna šta može očekivati od svog CERT tima, CERT bi morao jasno da definiše kojoj vrsti konstituenata može da pruži podršku, i da definiše usluge, tj. servise, koje kao organizacija nudi svojim konstituentima. Dodatno, potrebno je da CERT objavi načela, tj. politike svoga delovanja, kao i svoje operativne procedure. Slično tome, potrebno je da konstituentima bude poznato šta se od njih očekuje kako bi na uspešan način koristili servise svog CERT-a, tj. CERT mora da objavi i objasni na koji način im se bezbednosni incidenti prijavljuju. Potrebno je naglasiti da je bez aktivne uloge samih korisnika servisa koje CERT nudi, efikasnost učinka ovih servisa znatno umanjena, i to naročito kada se radi o prijavi incidenata. U najmanju ruku korisnici moraju da budu svesni da je potrebno da prijavljuju bezbednosne incidente, i samim tim mora im biti poznat način na koji to mogu da učine.

U mnogim slučajevima, bezbednosni incidenti potiču izvan granica lokalne zajednice konstituenata koje opslužuje odgovarajuća CERT ogranizacija, kao što i sama ta zajednica može biti izvor bezbednosnih incidenata za druge zajednice konstituenata, tj. njihove CERT-ove. Iz tog razloga, rešavanje bezbednosnih incidenata može da obuhvati različite zajednice konstituenata, tj. različite CERT organizacije, te je samim tim potrebna saradnja, kako u okviru iste zajednice, tako i između različitih zajednica konstituenata, tj. njihovih CERT-ova.

U tom smislu, konstituenti nekog CERT-a moraju biti upoznati na koji način će njihov CERT sarađivati sa drugim CERT organizacijama, i koje informacije će tom prilikom biti deljene. Takođe, većina interakcija između konstituenata i njihovih CERT-ova, kao i saradnja između različitih CERT organizacija, obavlja se preko javne telekomunikacione infrastrukture koja se mora obezbediti, a, pored toga, i jasno naznačiti na koji način je ta komunikacija zaštićena.

4.2 DELOVANJE CERT ORGANIZACIJA

Postoje različite vrste CERT organizacija u zavisnosti od širine zajednice konstituenata kojima se servisi nude. Ali nezavisno od toga, svaki korisnik koji ima pristup servisima neke CERT organizacije, trebalo bi unapred da zna što je moguće više o servisima koji se nude, kao i načinu interakcije, tj. komunikacije sa svojom CERT organizacijom. Jasna objava o politikama i procedurama CERT organizacije pomaže konstituentima da razumeju koji je najbolji način da prijave bezbednosni incident, i koju vrstu podrške potom mogu da očekuju. Da li će CERT operativno pomagati u razrešenju incidenta, da li će obezbediti pomoć da se ta vrsta incidenta izbegne u budućnosti... – jasne odrednice, a naročito jasno naglašena ograničenja u servisima koje CERT nudi svojim korisnicima, učiniće interakciju sa korisnicima efikasnijom.

4.2.1 Objavljivanje načela i procedura delovanja

Sve politike i procedure koje su relevantne za konstituente, moraju biti dokumentovane i javno dostupne. Pod pojmom relevantne, podrazumeva se da nisu baš sve politike i procedure značajne za konstituente. Primera radi, nije potrebno da konstituenti razumeju unutrašnju organizaciju funkcionisanja CERT-a da bi bili u stanju da sa njim komuniciraju, ali je potrebno da razumeju kako se incident prijavljuje, ili kako se uz pomoć podrške CERT-a analizira bezbednost sistema, ili razrešava incident koji je narušio bezbednost sistema.

Preporuka je da se ova vrsta dokumenata objavljuje u standardizovanoj formi, na Internet stranicama CERT ogranizacija, što ih čini lako dostupnim svim konstituentima. To, takođe, omogućava raznim grupama korisnika da pretragom na Internetu identifikuju CERT organizaciju koja im može biti od pomoći u kriznim situacijama.

Bez obzira na izvor, tj. način na koji neki korisnik ili zajednica konstituenata identifikuje neku CERT organizaciju koja im može pružiti podršku, korisnik mora proveriti autentičnost te informacije. Od velike je važnosti da ovakva vitalna dokumenta CERT organizacija budu zaštićena digitalnim potpisom kako bi korisnici mogli da verifikuju njihovu autentičnost.

4.2.2 Odnosi između različitih CERT organizacija

U današnjim uslovima funkcionisanja IKT sistema, tj. shodno izloženosti rizicima globalnih razmera, teško je očekivati da neka grupa konstituenata, tj. njihova CERT organizacija, može da funkcioniše samo u okvirima svoje zajednice. Izvesno je da će CERT organizacije sarađivati na razrešenju raznih incidenata sa drugim CERT-ovima. U tom smislu, zajednica konstituenata mora da ima jasnu predstavu o prirodi i obimu te saradnje, s obzirom da se u tom procesu mogu objaviti neke osetljive informacije o pojedinim članovima te zajednice.

Saradnja između CERT-ova može obuhvatiti savetodavnu saradnju po pitanju nekih vrsta incidenata, razmenu znanja i iskustava na temu razrešenja incidenata, kao i operativnu saradnju u kriznim situacijama kada je potrebno otkloniti uzroke ili posledice nekih bezbednosnih incidenata. Prilikom uspostavljanja te saradnje, CERT-ovi moraju odlučiti koja vrsta ugovora mora da postoji između njih, kako bi uspešno razmenjivali informacije, kao i da li se detalji tog odnosa mogu obznaniti, do koje mere, i kome. U nekim slučajevima CERT-ovi imaju čvrste ugovore i aktivno sarađuju na razrešenju incidenata i dele relevantne informacije, a u nekim drugim se međusobno kontaktiraju samo radi traženja savetodavne pomoći. U svakom slučaju, jasno je da je saradnja među različitim timovima u mnogim situacijama neophodna, ali je na samim timovima da odluče na koji način i do koje mere će međusobno sarađivati.

4.2.3 Uspostavljanje bezbednih kanala komunikacije

Bilo da se radi o komunikaciji, tj. razmeni informacija, između CERT organizacije i njenih konstituenata, ili između različitih CERT-ova, potrebno je omogućiti da se ova komunikacija odvija na bezbedan način. U ovom slučaju se termin „bezbedan" odnosi na proces prenosa podataka između različitih strana, a ne na način upotrebe informacija koje su stigle do neke od strana u komunikaciji.

Ciljevi bezbedne komunikacije su da se obezbedi:

- poverljivost (da niko drugi ne može da pristupi sadržaju informacije),
- integritet (da niko ne može da menja sadržaj informacije), i
- autentifikacija (da se sa sigurnošću zna ko je druga strana sa kojom se komunicira).

Primera radi, veoma je lako poslati krivotvoren *e-mail*, ili se lažno predstaviti tokom telefonskog razgovora, ali je uz pomoć kriptografskih tehnika (PGP-*Pretty Good Privace*, PEM-*Privacy Enhanced Mail*...) u slučaju elektronske pošte, ili uz odgovarajuću opremu u slučaju komunikacije preko telefona, moguće osigurati bezbednu komunikaciju. Međutim, korišćenje ovakvih mehanizama podrazumeva postojanje odgovarajuće infrastrukture, pa je u tom smislu neophodna priprema. Kada su u pitanju kriptografski ključevi potrebno je osigurati njihovu autentičnost, tj:

- kada su u pitanju javni ključevi (za tehnike enkripcije kao što su PEM, ili PGP), s obzirom da su oni dostupni preko Interneta, potrebno je proveriti njihovu autentičnost pre upotrebe,
- kada su u pitanju tajni ključevi (za tehnike enkripcije kao što su AES – *Advanced Encryption Standard* ili PGP), potrebno ih je na bezbedan način (putem bezbednog kanala komunikacije) razmeniti pre nego što dve strane u komunikaciji počnu da ih koriste.

U svakom slučaju, bezbedna komunikacija je kritična u svim aspektima razrešavanja bezbednosnih incidenata. U tom smislu, sve neophodne informacije o načinima na koji neka CERT organizacija osigurava bezbednost komunikacije moraju biti dokumentovane, i dostupne konstituentima kako bi bili u prilici da ih na odgovarajući način koriste.

4.3. INFORMACIJE, POLITIKE I PROCEDURE

Kako bi se olakšalo razumevanje svih aspekata saradnje između CERT organizacija i njihovih konstituenata, preporučljivo je da CERT objavi sve informacije, politike i procedure koje se tiču njihovih konstituenata, u formi dokumenta, na bazi univerzalnog obrasca (tzv. RFC 2350 obrazac), tj. forme na koju se oslanja većina CERT organizacija. Tipičan sadržaj RFC 2350 dokumenta opisan je u nastavku.

4.3.1 Informacije o dokumentu

Detalji o samoj CERT organizaciji se tokom vremena menjaju, pa je potrebno da RFC 2350 dokument, koji je opisuje, nosi oznaku kada je poslednji put ažuriran, i, pri tome, potrebno je obezbediti informaciju kako se dolazi do poslednje ažurne verzije ovog dokumenta. U tom smislu dokument treba da sadrži:

- datum poslednjeg ažuriranja,
- listu za distribuciju dokumenta (mejling liste su pogodan mehanizam za distribuiranje ažurnih informacija ka velikom broju korisnika, i pri tome je za ove poruke potrebno koristiti digitalni potpis), i
- lokaciju dokumenta (to je najčešće lokacija na *web* stranici CERT organizacije gde se nalazi poslednja verzija dokumenta, i pri tome i taj dokument koji je javno dostupan na *web* stranici mora biti digitalno potpisan).

4.3.2 Kontakt informacije

Ovde treba navesti sve detalje o tome kako konstituenti mogu da kontaktiraju svoju CERT organizaciju, tj. dokument treba da sadrži:

- ime CERT organizacije,
- adresu elektronske pošte (*e-mail* adresa),
- vremensku zonu (što je jako korisno u slučaju saradnje sa CERT-ovima koji postoje u drugim državama, tj. različitim vremenskim zonama),
- broj telefona,
- broj faksa,
- adresu *web* stranice,
- neki drugi vid komunikacije,
- javne ključeve i metode enkripcije,
- nabrojane članove tima (opciono),
- radno vreme (uz napomenu o radu i načinu komunikacije za vreme vikenda ili praznika ukoliko nije organizovana 24/7 služba dežurstva), i
- dodatne napomene.

Može se dati i više detalja o kontaktima u slučaju da postoje različite tačke, ili načini kontakta za različite servise. U slučaju da postoje specifične procedure za pristup nekim servisima, ovde ih treba navesti i objasniti njihovo korišćenje (na primer, korisnik želi da ostavi svoju *e-mail* adresu za prijavu na mejling listu za obaveštavanje).

4.3.3 Povelja

Svaka CERT organizacija treba da ima povelju, tj. mandat, kojim se specificiraju njena zaduženja, kao i ovlašćenja putem kojih će ih sprovoditi. Povelja u najkraćem treba da sadrži:

- definiciju misije CERT organizacije,
- ciljane konstituente, tj. korisnike servisa koje CERT obezbeđuje,
- informaciju o široj organizaciji ili instituciji u okviru koje CERT organizuje svoje aktivnosti, i
- ovlašćenja.

Misija treba da ukaže na aktivnosti koje su srž delovanja CERT-a, a koje su već sadržane u samoj definiciji CERT-a. Da bi se neka organizacija nazvala CERT-om, potrebno je da svojim klijentima pruža podršku prilikom prijave bezbednosnih incidenata, kao i u razrešavanju tih incidenata. Ciljevi i svrha postojanja CERT-a su od izuzetne važnosti, i potrebno je da budu jasno i nedvosmisleno definisani.

Konstituenti, tj. klijenti neke CERT organizacije, mogu biti određeni na više načina. Na primer, to mogu biti zaposleni u nekoj kompaniji, ili pretplatnici usluga te kompanije, ili se mogu definisati na bazi tehnoloških odrednica kao što su na primer korisnici nekog operativnog sistema. Definisanjem konstituenata od interesa, određuju se okviri zajednice kojoj će CERT pružati svoje usluge. Zatim se definisanjem politika, o kojima će biti reči kasnije, definiše kako će se postupati u slučaju zahteva za uslugama koji dolaze izvan okvira ove zajednice. Ukoliko CERT organizacija odluči da ne objavi ko su njeni konstituenti, mora da navede i razlog za takvu odluku (na primer, to može biti slučaj ukoliko postoji ugovorna obaveza o tajnosti podataka sa nekim od korisnika servisa CERT-a). Naravno, moguće je da postoji i preklapanje konstituenata različitih CERT organizacija. Primera radi, konstituenti nekog CERT-a mogu istovremeno biti korisnici servisa nekih drugih kompanija, kao što su na primer provajderi telekomunikacionih servisa, koji i sami imaju svoje CERT organizacije ili funkcije, i u tom slučaju odnosi između ovih CERT-ova moraju biti jasno definisani u okvirima ovlašćenja kojima svaki od ovih CERT-ova raspolaže.

Zatim, potrebno je objaviti i detalje o organizaciji ili instituciji u okviru koje CERT organizuje svoje aktivnosti, tj. iz koje crpi ovlašćenja za svoje delovanje. Zahvaljujući ovome, korisnici servisa mogu da sagledaju pozadinu delovanja CERT-a, što je jedna od ključnih informacija za izgradnju poverenja između jednog CERT-a i korisnika njegovih usluga.

Ovlašćenja kojima u svom delovanju raspolažu različite CERT organizacije razlikuju se u zavisnosti od odnosa koji postoje između CERT-ova i korisnika njihovih usluga, tj. konstituenata. Na primer, u okviru neke konkretne organizacije ili kompanije, ovlašćenja CERT-a definiše rukovodstvo te organizacije, dok CERT-ovi koji opslužuju šire zajednice konstituenata uobičajeno imaju samo savetodavnu ulogu. CERT može, ali i ne mora, imati ovlašćenja da interveniše u operativnom smislu na sistemima unutar okvira svojih delovanja ili konstituenata. U svakom slučaju potrebno je u ovom smislu definisati jasnu granicu operativnog delovanja, naročito u delu koji povlači i odgovarajuće odgovornosti za sisteme koji su predmet delovanja. Ukoliko postoje i druge CERT organizacije koje deluju u okvirima istih konstituenata preporučuje se i konsultacija sa pravnim timovima radi što jasnijeg razgraničenja delovanja i odgovornosti.

4.3.4 Politike

Izuzetno je važno da CERT organizacija definiše politike svoga delovanja i da ih na odgovarajući način objavi unutar zajednice svojih konstituenata. Pod politikama se pre svega podrazumevaju nivoi podrške koji se obezbeđuju za razrešavanje različitih tipova incidenata, način saradnje i deljenja informacija sa konstituentima ili drugim CERT-ovima, kao i način za osiguranje bezbednosti same komunikacije.

Tipove incidenata koje je CERT u stanju da obradi, kao i nivo podrške koju CERT može da ponudi svojim konstituentima, treba sažeti u formi liste koja se objavljuje u dokumentu koji opisuje konkretni CERT. Zatim je moguće, u posebnom odeljku tog dokumenta, detaljnije opisati svaki od servisa, kao i način na koji se tretiraju teme koje nisu u vezi sa konkretnim bezbednosnim incidentima. Nivo podrške može zavisiti od raznih faktora, kao što su nivo zauzetosti tima drugim poslovima u datom trenutku, ili nivo kompletnosti informacija koje CERT dobije o nekom konkretnom incidentu. Takvi faktori moraju biti navedeni i objašnjeni, kao i uticaj koji svaki od njih ima na pružanje servisa. Naravno, ukoliko se dogodi incident koji ne potpada ni pod jednu od navedenih kategorija incidenata ili servisa, i u takvim situacijama mora postojati neki podrazumevani nivo podrške. Takođe, CERT treba da navede da li će delovati na bazi informacija koje dobije na temu bezbednosne ranjivosti nekih sistema, a ukoliko se za to odluči, najčešće se to definiše kao neka vrsta opcionog proaktivnog servisa, pre nego kao bazični obavezujući servis.

Kada su u pitanju saradnja, komunikacija, tj. razmena informacija, potrebno je eksplicitno navesti sa kojim grupama (konstituenata ili drugih CERT-ova) CERT uobičajeno komunicira. Ova komunikacija ne mora uvek biti na temu razrešenja nekih tekućih incidenata, već i u cilju poboljšanja saradnje, ili su u pitanju opšte teme vezane za tehnologije ili servise. Pri tome, nije potrebno otkrivati detalje neke saradnje, ili ugovora o saradnji, već je suština da se konstituentima pruži osnovno razumevanje o tome kakve sve vrste interakcija postoje, i koji je njihov smisao.

Saradnja između različitih CERT-ova može biti olakšana korišćenjem usaglašenih procedura za razmenu informacija, u kombinaciji sa standardizovanim sistemima za vođenje evidencije o prijavljenim incidentima, kako bi se izbegli nesporazumi u komunikaciji, ili rasipanje energije i napora u rešavanju incidenata. Takođe, politikama o izveštavanju, ili razmeni informacija, treba jasno definisati ko dobija informacije od nekog CERT-a, kao i da li se jedan CERT bavi incidentima koje je prijavio konstituent nekog drugog CERT-a tako što direktno komunicira sa tim korisnikom, ili preko njegovog „matičnog“ CERT-a. Grupe sa kojima CERT-ovi uobičajeno sarađuju ili komuniciraju su sledeće:

- T**imovi za rešavanje incidenata -** Timovi različitih CERT-ova često sarađuju između sebe, na primer CERT neke kompanije obraća se za pomoć nacionalnom CERT-u, a nacionalni CERT drugim nacionalnim CERT-ovima u slučaju bezbednosnih incidenata širih razmera. Ova saradnja može dovesti do razmene poverljivih informacija kao što su:
    - izveštaji o incidentima koji mogu sadržati mesto ili metu napada, koji u tom slučaju postaju javna informacija za različite CERT-ove, pa čak i širim krugovima interesenata (na primer medijima),
    - postupanje po incidentima prijavljenim van okvira zajednice koju neki CERT opslužuje,
    - prosleđivanje informacija o uočenim ranjivostima nekih sistema njihovim proizvođačima, partnerskim CERT-ovima, ili direktno pogođenim konstituentima drugih CERT-ova,

- davanje povratnih informacija o uočenim ranjivostima, ili po dobijenim prijavama incidenata,
- prosleđivanje kontakt informacija nekog od svojih konstituenata, ili članova drugih zajednica konstituenata, drugim CERT-ovima ili istražnim organima.

- **Proizvođači opreme** - Neki proizvođači opreme imaju svoje CERT timove, dok ih neki drugi nemaju. U tom slučaju CERT mora direktno da komunicira sa proizvođačem opreme, radi sugerisanja poboljšanja ili modifikacija opreme ili sistema, analize tehničkih problema, ili testiranja ponuđenih rešenja. U tom smislu, proizvođači opreme imaju posebno važnu ulogu, ukoliko je bezbednosni incident koji je prijavljen posledica ranjivosti njihove opreme ili sistema.
- **Istražni organi** - Ovo uključuje policiju ili druge istražne agencije. CERT-ovi, kao i njihovi konstituenti podložni su lokalnom zakonodavstvu i propisima, što se može jako razlikovati u različitim zemljama. CERT može podeliti informaciju o tehničkim aspektima nekog bezbednosnog incidenta, ili tražiti savet od istražnih organa na temu nekog tekućeg incidenta, a po pitanju pravnih implikacija tog incidenta. Lokalni zakoni i propisi mogu podrazumevati neke specifične procedure po pitanju očuvanja poverljivosti informacija, ili izveštavanja o nekim vrstama incidenata.
- M**ediji** - Može se povremeno desiti da se CERT-ovima obrate mediji radi dobijanja informacija ili komentara o nekim događajima ili incidentima. U tom slučaju dobro je da postoji eksplicitna politika o načinu deljenja informacija, naročito ukoliko se one odnose na konstituente, jer oni mogu biti uzdržani prema kontaktu sa medijima.
- D**rugi** - U opštem slučaju misli se na istraživačke aktivnosti ili odnose sa organizacijom ili institucijom u okviru koje je CERT uspostavljen.

Podrazumevani status svih informacija koje se stiču u okviru CERT-a je „poverljivo“, ali kako bi se sprečilo da to bude prepreka u komunikaciji ili saradnji sa konstituentima ili drugim CERT-ovima, potrebno je dokumentovati koje klase informacija mogu biti deljene kroz prijave incidenata ili izveštaje o incidentima, i to sa kime, i u kom trenutku.

S obzirom na razlike u zakonodavstvu i propisima, kao i u skladu sa različitim očekivanjima pojedinih konstituenata, ova pravila moraju biti jasno dokumentovana i objavljena, kako bi se ispoštovali principi tajnosti podataka, ali istovremeno i omogućila efikasna saradnja. Takođe, ukoliko u svom radu neki CERT prikuplja i distribuira neke statističke podatke, i to mora biti dokumentovano, a partnerske organizacije i konstituenti upućeni kako do takvih izveštaja mogu da dođu.

Kao što je ranije već naglašeno, neophodno je da postoji politika koja opisuje metode bezbedne komunikacije, bilo između konstituenata i CERT-a, ili između različitih CERT-ova. RFC 2350 dokument, koji opisuje CERT, treba da sadrži javne ključeve, ili druge metode zaštite komunikacije, zajedno sa uputstvom kako ih iskoristiti da bi se proverila autentičnost i kako treba postupiti ako se utvrdi da su neki podaci kompromitovani. Najmanje što je preporučeno je da svaki CERT ima dostupan PGP ključ, a može koristiti i druge mehanizme (npr, PEM, MOSS - *Minimum Operating Security Standards*, S/MIME - *Secure/Multipurpose Internet Mail Extensions*), u skladu sa svojim potrebama, ili potrebama svojih konstituenata. Treba, ipak, napomenuti da su CERT, kao i njegovi konstituenti, podložni lokalnom zakonodavstvu i propisima. Neke države ne dozvoljavaju previše jaku enkripciju, a neke sprovode specifične politike po pitanju korišćenja tehnologija za enkripciju. Kao dodatak na korišćenje enkripicije kad god je ona moguća, komunikacija bi trebalo da sadrži i digitalni

potpis. Kada se radi o komunikaciji putem telefona ili faksa, CERT može da primeni tajne metode autentifikacije, kao što je unapred dogovorena lozinka, koja naravno neće biti javno objavljena, ali informacija o tome da postoji lozinka za ove namene može biti objavljena.

4.3.5 Servisi

Servisi koje CERT nudi svojim korisnicima grubo se mogu podeliti u dve kategorije: aktivnosti u realnom vremenu koje se odnose na rešavanje bezbednosnih incidenata, ili proaktivne aktivnosti koje olakšavaju aktivnosti na rešavanju incidenata. Ova druga kategorija, a i neki delovi prve kategorije, spadaju u servise koji su opcioni, tj. ne nude ih svi CERT-ovi podjednako.

Rešavanje incidenata obično uključuje obradu i procenu pristiglih prijava, odnosno trijažu incidenata, i aktivnosti na njihovom razrešavanju u saradnji sa konstituentima, drugim CERT-ovima, ili provajderima telekomunikacionih i Internet servisa. Treći red aktivnosti, u koje bi na primer mogla da spada operativna pomoć konstituentu da se oporavi od incidenta, obično se sastoji od opcionih servisa koje ne nude svi CERT-ovi.

Trijaža incidenata uključuje:

- procenu prijavljenih incidenata (njihovu interpretaciju, prioritetizaciju, i utvrđivanje veze sa drugim tekućim incidentima ili trendovima), i
- verifikaciju (utvrđivanje da li se bezbednosni incident zaista dogodio, i obim tog događaja).

Koordinacija u razrešavanju incidenata obično uključuje:

- kategorizaciju informacija (kao što su log fajlovi, kontakt informacije i druge informacije o incidentu, a u skladu sa politikom o razmeni poverljivih informacija), i
- koordinaciju (obaveštavanje svih strana kojima je neophodno pružiti informaciju, a u skladu sa politikom o razmeni poverljivih informacija).

Operativna pomoć u rešavanju incidenata, obično se tretira kao dodatni ili opcioni servis, a može obuhvatati:

- tehničku podršku (analiza kompromitovanog sistema),
- otklanjanje uzroka incidenta (npr, eliminacija uočene ranjivosti sistema, ili ukidanje pristupa sistemu za napadača), i
- oporavak (pomoć pri vraćanju sistema ili servisa u funkcionalno stanje, tj. na status pre izbijanja incidenta).

Proaktivni servisi koji, takođe, spadaju u opcione, mogu uključivati:

- pružanje informacija (to može biti arhiva poznatih ranjivosti sistema, „zakrpa" ili načina razrešavanja nekih prethodnih incidenata, ili distribuiranje savetodavnih poruka putem elektronske pošte),
- bezbednosne alate (razni alati koje korisnik može da koristi za procenu bezbednosti svog sistema),
- edukaciju i treninge,
- procenu proizvoda,
- procenu bezbednosti sistema nekog korisnika, i konsultantske usluge na poboljšanju te bezbednosti.

4.3.6.Forme izveštaja o incidentima

Korišćenje unificiranih formi za izveštavanje čini proces rešavanja incidenata jednostavnijim i za CERT organizacije i za korisnike njihovih servisa. Korisnik može da pripremi odgovore na razna važna pitanja čak i pre nego što kontaktira CERT tim, tako da tim CERT-a u startu dobija sve neophodne informacije i može efikasno da nastavi sa svojim poslom. U zavisnosti od ciljeva i servisa kojima se bave pojedinačni CERT-ovi, može postojati više različitih formi. Primera radi, forma za prijavu tekućeg incidenta može biti različita od forme za prijavu neke uočene ranjivosti sistema koja još nije zloupotrebljena.

Najefikasnije je da forme za prijavu incidenata budu dostupne preko Internet stranice CERT organizacije. Takođe, RFC 2350 dokument, koji opisuje CERT i njegove aktivnosti, treba da sadrži pokazivače na ove forme, zajedno sa izjavom kako se one pravilno koriste, i uputstvom kako i kada ih treba koristiti. Ukoliko postoje i posebne *e-mail* adrese za slanje ili prijem ovih formi, i njih treba navesti.

4.3.7 Odricanje od odgovornosti

Iako RFC 2350 dokument koji opisuje CERT ne podrazumeva ugovornu obavezu, iz opisa njegovih ciljeva ili servisa može da proističe i određena vrsta odgovornosti. Zbog toga je potrebno da taj dokument na svom kraju sadrži i odricanje od odgovornosti, čime se korisnik jasno upozorava na tu vrstu ograničenja ukoliko ono postoji.

Druga situacija u kojoj je ovo jako bitno je kada je ovaj dokument potrebno prevesti na drugi jezik, koji nije matični datom CERT-u. Tada je potrebno naglasiti odricanje od odgovornosti u smislu svih nedoumica koje proističu iz lošeg prevoda, ili loše intepretiranog smisla neke izjave u okviru dokumenta koji se prevodi.

Korišćenje ovog mehanizma je uslovljeno i definisano lokalnim zakonodavstvom i propisima, kojih CERT treba da bude svestan, i da u smislu njihovog korišćenja, u slučaju bilo kakvih nedoumica, potraži pomoć pravnika.

4.4 NACRT DOKUMENTA DEFINICIJE CERT-A

Radi definisanja oblasti delovanja i odgovornosti CERT organizacije, preporučeno je da se izradi dokument (po obrascu RFC 2350) koji definiše aktivnosti CERT-a i odnose sa njegovim konstituentima. U nastavku je dat nacrt dokumenta koji tačku po tačku sumira sve neophodne informacije o CERT-u, njegove politike, procedure i sve druge informacije koje su relevantne za njegove konstituente, kao i spoljnje organizacije sa kojima CERT sarađuje:

1. Informacija o dokumentu:
    1.1. Datum poslednje izmene,
    1.2. Lista za distribuciju obaveštenja, i
    1.3. Lokacija na kojoj se ovaj dokument može pronaći.

2. Kontakt informacije:
    2.1. Naziv tima,
    2.2. Adresa,
    2.3. Vremenska zona,

2.4. Broj telefona,
2.5. Broj faksa,
2.6. Drugi telefoni,
2.7. Adresa elektronske pošte,
2.8. Javni ključevi i informacije o enkripciji,
2.9. Članovi tima,
2.10. Ostale informacije, i
2.11. Tačke kontakta sa korisnicima.

3. Povelja:
3.1. Definicija misije,
3.2. Konstituenti,
3.3. Krovna organizacija / Osnivač CERT-a, i
3.4. Nadležnost i ovlašćenja.

4. Politike:
4.1. Tipovi incidenata i nivo podrške,
4.2. Saradnja, komunikacija i razmena informacija,i
4.3. Bezbedna komunikacija i autentifikacija.

5. Servisi:
5.1. Rešavanje incidenata:
5.1.1. Trijaža incidenata,
5.1.2. Koordinacija u rešavanju incidenata, i
5.1.3. Operativna pomoć,

5.2. Proaktivno delovanje.

6. Forme za izveštavanje o incidentima.

7. Odricanje od odgovornosti.

U nastavku je, kao primer, predstavljen RFC 2350 dokument austrijskog nacionalnog CERT-a, prenet u izvornom obliku na engleskom jeziku, onako kako je objavljen na Internet stranici te organizacije.

RFC 2350

Version: 0.9
Date: Thu, 27 Mar 2014 15:40:19 +0100
Author: L. Aaron Kaplan <kaplan@cert.at>

1. Document information

This document contains a description of CERT.at according to RFC 2350. It provides basic information about the CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of last update

Thu, 27 Mar 2014 15:40:19 +0100

1.2 Distribution list for notifications

There is no distribution list for notifications as of 2014/03.

1.3 Locations where this document may be found

The current version of this document can always be found at http://www.cert.at/about/rfc2350/rfc2350.html . For validation purposes, a GPG signed ASCII version of this document is located at http://www.cert.at/static/rfc2350.txt. The key used for signing is the CERT.at key as listed under 2.8.

2. Contact information

2.1 Name of the team

CERT.at Computer Emergency Response Team Austria

2.2 Address

CERT.at nic.at GmbH Karlsplatz 1/9 1010 Vienna Austria

2.3 Time zone

We are located in the central European timezone (CET) which is GMT+0100 (+0200 during day-light saving time).

2.4 Telephone number

+43 1 5056416 78

2.5 Facsimile number

+43 1 5056416 79

2.6 Other telecommunication

None.

2.7 Electronic mail address

Please send incident reports to reports@cert.at. Non-incident related mail should be addressed to team@cert.at.

2.8 Public keys and encryption information

CERT.at uses a master signing key to sign all keys used for operational purposes. This trust anchor is:

pub 4096R/998C1CC6C2E0E6A7 2014-03-19 [expires: 2019-03-18]
Key fingerprint = FB59 8F2F 6B68 0211 F85D 2A0C 998C 1CC6 C2E0 E6A7
uid CERT.at master key <signing-only-key-no-mail@cert.at>
sub 4096R/9D1B02A6B0454903 2014-03-19 [expires: 2019-03-18]

and can be found on most key-servers. Please DO NOT use this key for communications with us. All official communication by CERT.at will be signed by the current team key, which is as of 2014/03:

pub 4096R/8D2F23E111334B61 2014-03-19 [expires: 2019-03-18]
Key fingerprint = AD35 20E5 2CE8 8BA2 50B2 8507 8D2F 23E1 1133 4B61
uid CERT.at (General Communications) <team@cert.at>
uid CERT.at (Incidents) <reports@cert.at>
sub 4096R/CC28457FA810F7AA 2014-03-19 [expires: 2019-03-18]

Encrypted communications with CERT.at should use this - and only this - operational key.

All keys (including the keys of individual team members) can be found at http://www.cert.at/static/pgpkeys.asc.

Since the team key and the master signing key expire regularly, CERT.at will always sign younger master signing keys with the older master signing keys as well. The current master signing key always signs the team key. See also the key transition document at http://www.cert.at/static/key-transition-2014.txt.

2.9 Team members

The team leader of CERT.at is Otmar Lendl. Other team members are listed in the "About Us" / Team page on our webpage. Management, liaison and supervision are provided by Robert Schischka, Technical Manager of nic.at.

2.10 Other information

-

2.11 Points of customer contact

The preferred method for contacting CERT.at is via e-mail. For incident reports and related issues please use reports@cert.at. This will create a ticket in our tracking system and alert the human on duty. For general inquiries please send e-mail to team@cert.at.

If it is not possible (or advisable due to security reasons) to use e-mail, you can reach us via telephone at +43 1 5056416 78.

CERT.at's hours of operation are generally restricted to local regular business hours: Mon-Fri, 8 a.m. - 6 p.m. CET/CEST.

3. Charter

3.1 Mission statement

The purpose of CERT.at is to coordinate security efforts and incident response for IT-security problems on a national level in Austria.

3.2 Constituency

The constituency of CERT.at is basically the whole country of Austria.

CERT.at will first try to coordinate with IT-security teams and more specific CERTs in Austria.

Note that usually no direct support will be given to end users; they are expected to contact their ISP, system administrator, network administrator, or department head for assistance. CERT.at will support the latter.

Pro-active and educational material are provided for the general public.

3.3 Sponsorship and/or affiliation

CERT.at is an initiative of nic.at, the Austrian domain registry and the Austrian Federal Chancellery.

Funding is provided by nic.at GmbH, http://www.nic.at/

3.4 Authority

The main purpose of CERT.at in incident handling is the coordination of incident response. As such, we can only advise our constituency and have no authority to demand certain actions.

We have indirect authority over AS30971 and AS1921 and are in very close contact with the Austrian CERT Verbund (union of CERTs) and the Austrian Trust Circle (ATC).

4. Policies

4.1 Types of incidents and level of support

CERT.at is authorised to address all types of computer security incidents which occur, or threaten to occur, in our constituency (see 3.2) and which require cross-organisational coordination. The level of support given by CERT.at will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and our resources at the time. Special attention will be give to issues affecting critical infrastructure.

CERT.at is committed to keeping its constituency informed of potential vulnerabilities, and, where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, interaction and disclosure of information

CERT.at will cooperate with other organisations in the field of computer security. This cooperation also includes and often requires the exchange of vital information regarding security incidents and vulnerabilities. Nevertheless CERT.at will protect the privacy of reporters, partners and our constituents, and therefore (under normal circumstances) pass on information in an anonymised way only unless other contractual agreements apply. CERT.at operates under the restrictions imposed by Austrian law. This involves careful handling of personal data as required by Austrian Data Protection law, but it is also possible that - according to Austrian law - CERT.at may be forced to disclose information due to a court order.

CERT.at treats all submitted information as confidential per default, and will only forward it to concerned parties in order to resolve specific incidents when consent is implicit or expressly given.

For example: incoming report "Malware on www.example.com/malware, please get it cleaned up". In this case, we would forward the information only to the concerned parties (domain-holder, hoster/ISP) to help them quickly fix the problem. Especially we will not forward information about incidents to government authorities or the press without explicit prior permission by the submitting party.

4.3 Communication and authentication

For normal communication not containing sensitive information CERT.at might use conventional methods like unencrypted e-mail or fax. For secure communication PGP-encrypted e-mail or telephone will be used. If it is necessary to authenticate a person before communicating, this can be done either through existing webs of trust (e.g. FIRST, TI,) or by other methods like call-back, mail-back or even face-to-face meeting if necessary.

5. Services

5.1 Incident response

CERT.at will assist IT-security teams in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident triage

- *determining whether an incident is authentic*
- *assessing and prioritizing the incident*

5.1.2. Incident coordination

- *determine the involved organizations*
- *contact the involved organizations to investigate the incident and take the appropriate steps*
- *facilitate contact to other parties which can help resolve the incident*
- *send reports to other CERTs*

We mainly see ourselves as information hub which knows where to send the right incident reports to in order to help and facilitate the clean-up of IT security incidents.

5.1.3. Incident resolution

- *advise local security teams on appropriate actions*
- *follow up on the progress of the concerned local security teams*
- *ask for reports*
- *report back*

CERT.at will also collect statistics about incidents within its constituency.

5.2 Proactive activities

CERT.at tries to

- *raise security awareness in its constituency*
- *collect contact information of local security teams*
- *publish announcements concerning serious security threats*
- *observe current trends in technology*
- *distribute relevant knowledge to the constituency*
- *provide fora for community building and information exchange within the constituency*

6. Incident reporting forms

There are no local forms available.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, CERT.at assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

5. ANALIZA NACIONALNIH CERT-OVA U EVROPI

5.1 UVOD

Nacionalni, ili državni CERT-ovi (*Computer Emergency Response Team*), su timovi koji služe vladama država radi pomoći u zaštiti bezbednosti ključne informacione infrastrukture. Nacionalni/državni CERT ima ključnu ulogu u koordiniranju upravljanja bezbednosnim incidentima, zajedno sa relevantnim organizacijama ili zajednicama na nacionalnom nivou. Oni su, takođe, odgovorni za saradnju sa nacionalnim i državnim timovima drugih zemalja.

Zaštita ključne informacione infrastrukture (*Critical Information Infrastructure Protection* – CIIP), bez sumnje, ne zaustavlja se na granicama jedne države, i potreban je koordinirani pristup na nivou cele Evrope kako bi se efikasno suprotstavili bezbednosnim pretnjama i napadima. Jedan način da se to postigne jeste podrška CERT organizacijama u razvoju saradnje između nacionalnih/državnih CERT-ova, radi razmene informacija i koordinacije u razrešavanju incidenata.

European Network and Information Security Agency (ENISA) je agencija koja je središte ekspertize računarske i mrežne bezbednosti Evropske Unije (EU), njenih država članica, privatnih organizacija i građana. ENISA sarađuje sa svim ovim grupama na razvoju saveta i preporuka radi primene dobre prakse u zaštiti informacione bezbednosti. Ona pomaže članicama EU u implementaciji relevantne zakonske regulative i radi na poboljšanju otpornosti ključne informacione infrastrukture i mreža u Evropi. ENISA ulaže napore da poboljša postojeći nivo ekspertize u državama članicama EU tako što podržava razvoj organizacija za međudržavnu saradnju, radi poboljšanja informacione i mrežne bezbednosti širom EU.

Ključni problem u međudržavnoj saradnji je raznolikost u kapacitetima (mogućnostima i sposobnostima), što se oslikava ili u potpunom nepostojanju nacionalnih/državnih CERT ogranizacija u nekim državama, ili u onome što bi se moglo nazvati adekvatnim nivoom „zrelosti“ CERT organizacija u nekim državama. Odgovor ENISA-e na ove probleme je konstantno insistiranje na potrebi da se u svim državama Evrope formiraju CERT timovi, što podržava svojom stručnošću, treninzima i iskustvom. Takođe, samim definisanjem osnovnih kapaciteta, tj. bazičnih oblasti delovanja jedne CERT

organizacije, ENISA daje svoj prilog usmeravanju napora ka „sazrevanju“ određene CERT organizacije, kako bi se na uspešan način uklopila u širu zajednicu ovih organizacija.

Postojanje nacionalnog/državnog CERT-a, koji ispunjava zahteve „osnovnih kapaciteta“ koji će u nastavku biti opisani, od velikog je značaja za zaštitu ključne informacione infrastrukture jedne zemlje. Međutim, ovi timovi nisu jedina potrebna i dovoljna mera zaštite ovih sistema, tj. njihova zaštita mora biti planirana unutar sveobuhvatne strategije informacione bezbednosti jedne zemlje, gde je nacionalni/državni CERT važan, ali ne i jedini deo.

U cilju razmevanja značaja i uloge nacionalnog/državnog CERT-a potrebno je definisati neke osnovne pojmove koji se koriste u vezi sa tim, kao što su:

- **CERT/CSIRT (*Computer Security Incident Response Team*) -** CERT je skup eksperata na polju informacione bezbednosti čiji je osnovni posao rad na razrešavanju bezbednosnih incidenata. Ovaj tim pruža servise i podršku svojim konstituentima na rešavanju incidenata i oporavku posle takvih događaja. U cilju smanjenja broja incidenata većina CERT-ova pruža svojim korisnicima i preventivne servise, ili usluge edukacije. Konstituenti, što je uobičajeni pojam za korisnike servisa nekog CERT-a, obično pripadaju nekim specifičnim sektorima, kao što su akademski, poslovni, državni, vojni, i sl.
- **Nacionalni CERT** - Neformalna definicija bi glasila: CERT koji deluje kao tačka kontakta na nacionalnom nivou radi razmene informacija (kao što su prijave incidenata, informacije o ranjivostima, i sl.), sa drugim nacionalnim CERT-ovima među državama EU, ili na nivou celog sveta. Nacionalni CERT se može posmatrati i kao poslednja instanca koja ima ulogu u koordinaciji rešavanja incidenta u okviru jedne države. U mnogim slučajevima nacionalni CERT ima i ulogu državnog CERT-a, iako ova defincija može varirati od države do države.
- ***De facto* nacionalni CERT** - Neformalna definicija bi glasila: *de facto* nacionalni CERT deluje kao tačka kontakta u zemljama u kojima država još uvek nije ustanovila nacionalni CERT. Obično se prva CERT organizacija koja se uspostavi u nekoj državi posmatra od strane CERT timova u drugim zemljama kao *de facto* nacionalni CERT. *De facto* nacionalni CERT je nezamenljiva instanca u razrešavanju bezbednosnih incidenata širokih razmera kada je neophodna međudržavna saradnja, dok zvanični nacionalni CERT nije uspostavljen, ili dok prethodni *de facto* nacionalni CERT ne dobije zvanični mandat za delovanje od svoje države.
- **Državni CERT** - Neformalna definicija bi glasila: CERT koji je odgovoran za zaštitu mreža državne administracije. Samim tim, konstituenti državnog CERT-a su vlada i njene javne institucije. U mnogim slučajevima državni CERT ima istovremeno i ulogu nacionalnog CERT-a. Definicije mogu varirati od države do države.
- **Termin „državni/nacionalni” CERT** - Neformalne definicije državnog CERT-a i nacionalnog CERT-a ne reflektuju na jedinstveni način statuse tih organizacija, njihove uloge i odgovornosti. Zato se često koristi i združeni termin „državni/nacionalni“ CERT, čija šira definicija obuhvata:
  - ulogu zvanične nacionalne tačke kontakta za nacionalne/državne CERT-ove drugih država, i
  - odgovornost za zaštitu kritične informacione infrastrukture u svojoj zemlji.

  Stoga termin „nacionalni/državni“ CERT obuhvata sve kapacitete, nacionalnih CERT-ova, državnih CERT-ova, i nacionalne tačke kontakta za druge države članice EU.

5.2 OSNOVNI KAPACITETI DRŽAVNIH/NACIONALNIH CERT-OVA

Osnovni skup kapaciteta, tj. sposobosti i mogućnosti nacionalnih/državnih CERT-ova, može se podeliti u četiri osnovne kategorije:

- portfolio servisa – koji obuhvata servise koje CERT tim obezbeđuje za svoje konstituente, ili ih interno koristi za svoje funkcionisanje,
- mandat, ili zvanični okvir delovanja – koji obuhvata ovlašćenja koja CERT tim dobija od države kojoj pripada,
- operativni kapaciteti – obuhvata tehnike i operativne zahteve koje tim mora da ispunjava, i
- kapaciteti za saradnju – obuhvata zahteve i procedure u vezi sa razmenom informacija sa drugim CERT timovima.

5.2.1 Portfolio servisa

Od svih servisa koje bi jedna CERT organizacija trebalo da pokriva, rešavanje incidenata, analiza i izveštavanje, sumirano kao upravljanje incidentima, je jedini servis koji bi se morao smatrati obaveznom aktivnošću, tj. servisom koji bi svaki nacionalni CERT morao da nudi svojim konstituentima. Pored ovoga preporučuje se i nuđenje servisa za alarmiranje, tj. upozoravanje i obaveštavanje konstituenata, i u reaktivnom i u proaktivnom smislu. Razmena informacija u vezi sa bezbednosnim incidentima, radi trenutnog alarmiranja ili obaveštavanja u slučaju nadolazećih pretnji, i dobra korisnička praksa na srednji i duži rok radi podizanja svesti o bezbednosnim rizicima, čine merljivu dodatnu vrednost za konstituente, uz smanjeni nivo troškova i napora. Bezbednosna upozorenja i druge informacije za konstituente, povećavaju prepoznatljivost CERT-a i svrhe njegovog postojanja, i doprinose izgradnji poverenja u mogućnosti i sposobnosti tima.

5.2.1.1 Angažovanje spoljnjih saradnika (Outsourcing)

Dok su upravljanje incidentima i slanje upozorenja servisi koje bi CERT tim trebalo da pruži kao svoje interne servise, korisno je razmišljati da se neke od funkcija, tj. servisi čiji je karakter srednjoročni, ili na duži rok, pružaju angažovanjem spoljnjih saradnika.

5.2.1.2 Interno funkcionisanje

Radi internog funkcionisanja nacionalnih CERT organizacija, potrebno je implementirati i neke dodatne servise i mere. Generalno rečeno, potrebno je da tim u svakom trenutku bude svestan dešavanja u mrežama svojih konstituenata, svojoj sopstvenoj mreži, mrežama svojih partnera, kao i na Internet mreži u celini. Konstantna budnost u tom smislu u mnogome se poboljšava praćenjem tehnologija, treninzima i praksom. U principu, svi ovi servisi se mogu smatrati opcionim, tj. nuđenje ovih servisa zavisi od potreba konstituenata.

5.2.2 Mandat

Jedna od najvažnijih stvari u delovanju nacionalnog CERT-a je dobijanje mandata od strane države, tj. ovlašćenja da u okvirima svog delovanja predstavlja svoju državu u zajednici

CERT organizacija. Mandat mora da obuhvata odredbe kojima se definiše da je nacionalni CERT zvanična tačka kontakta, na nacionalnom nivou, u komunikaciji sa CERT-ovima drugih zemalja, i drugim članovima bezbednosne zajednice. Kao takav on je nezamenljivi element u očuvanju bezbednosti ključne informacione infrastrukture u okviru svoje države. Generalna preporuka je da se nacionalni CERT uspostavi, i bude prihvaćen, kao vrhovna instanca u slučajevima bezbednosnih pretnji koje zahtevaju hitnu akciju, i njegova dužnost je da obaveštenja o tekućim incidentima (kao i druge informacije u vezi sa informacionom bezbednošću) prosleđuje odgovarajućim konstituentima u svojoj zemlji.

Međutim, nije uvek neophodno, a ponekad je i kontraproduktivno, da se nacionalni CERT učini odgovornim za upravljanje incidentima svih mogućih kategorija u okvirima jedne države. Umesto toga, preporuka je da se nacionalnom CERT-u pronađe adekvatna uloga u okvirima bezbednosne zajednice, kako bi se na odgovarajući način uklopio u organizaciju očuvanja bezbednosti ključne informacione infrastrukture svoje države.

5.2.2.1 Uloga na nacionalnom nivou

Da bi nacionalni CERT napredovao, tj. dorastao svojoj ulozi i odgovornostima, potreban je kooperativni pristup svih članova bezbednosne zajednice u jednoj državi, koji ga moraju prihvatiti i afirmisati kao jednog od ključnih članova te zajednice, na način i u smislu mandata koji mu je poveren od strane države.

5.2.2.2 Komunikacija

Neophodno je da se uloga i odgovornosti nacionalnog CERT-a na jasan način predstave svim relevantnim članovima bezbednosnih zajednica drugih zemalja. Sve nejasnoće i osobenosti organizacije na nacionalnom nivou treba „sakriti“ od članova bezbednosnih organizacija drugih zemalja, kako bi se sprečila bilo kakva konfuzija, ili kašnjenje u razmeni bezbednosnih informacija. U tom smislu, potrebno je ohrabriti sve države, tj. njihove vlade, da učine neophodne korake ka pojednostavljenju i standardizaciji pravnih okvira u kojima deluju nacionalne CERT organizacije. Ovo uključuje specifikaciju uloge CERT tima, njegovih prava, obaveza, odgovornosti i mandata, sa ciljem da se kreira jedinstveni pravni okvir za delovanje CERT organizacija širom Evrope.

5.2.2.3 Organizacioni model

Radi definisanja organizacionog modela, preporuka je da se proceni uloga nacionalnog CERT-a u okviru državnih struktura, kako bi se donela odluka kojem sektoru, ministarstvu, agenciji ili drugoj strukturi, nacionalni CERT treba da pripada.

5.2.3 Operativni kapaciteti

5.2.3.1 Resursi

U početnoj fazi osnivanja nacionalnog CERT-a jako je teško dati procenu o potrebnom brojnom stanju osoblja, jer na to utiču razni faktori. Na bazi postojećih iskustava, preporuka je da to bude najmanje 3 do 5 stalno zaposlenih, za slučaj da se servisi pružaju samo tokom regularnog radnog vremena. Ukoliko je cilj da se ustanove samo najosnovniji servisi,

minimalno je potrebno da postoji rukovodilac tima, jedan iskusan član tima za trijažu i upravljanje incidentima, i dodatno još i ekspert za informacione tehnologije i bezbednost. Međutim, s obzirom da je svrha nacionalnog CERT-a da nosi deo odgovornosti za bezbednost ključne informacione infrastrukture u državi, kao i da sarađuje sa drugim bezbednosnim organizacijama na nacionalnom i međunarodnom nivou, preporuka je da se od početka delovanja predvidi adekvatan broj ljudi za taj nivo posla i odgovornosti (6 do 8 stalno zaposlenih).

5.2.3.2 Radno vreme

S obzirom na ulogu nacionalnog CERT-a, smatra se neophodnim da tim bude dostupan u režimu 24/7/365, kako za svoje konstituente, tako i za druge bezbednosne organizacije na nacionalnom i međunarodnom nivou. U zavisnosti od portfolija servisa, strukture organizacije i odgovornosti koju nosi, potrebno je doneti odluku da li je neophodno stalno fizičko prisustvo članova tima na radnom mestu, ili je dovoljno da budu dostupni putem telefona, ali u svakom slučaju je neophodno garantovati njihovu brzu reakciju po prijavi bezbednosnih incidenata.

5.2.3.3 Komunikacijski servisi

Telefon, *e-mail* i Internet stranica se smatraju minimalnim skupom sredstava za komunikaciju sa nacionalnim CERT-om. Takođe, u slučaju *e-mail* komunikacije potrebno je da ona bude zaštićena enkripcijom, radi osiguranja bezbednosti (PGP, S/MIME (*Secure/Multipurpose Internet Mail Extensions*)...). Isto tako, smatra se obaveznim pristup Internet stranici CERT-a putem enkriptovane konekcije, u slučaju kada se na ovaj način CERT-u dostavljaju poverljive informacije (kada postoji mogućnost prijave bezbednosnog incidenta popunjavanjem formulara na Internet stranici CERT-a).

5.2.3.4 Fizičko obezbeđenje

Fizičko obezbeđenje radnog okruženja CERT organizacije često je potcenjen faktor, ali s obzirom na prirodu posla i poverljivost informacija kojima raspolaže, potrebno je obezbediti i adekvatan nivo fizičke bezbednosti na radnim mestima. Ovo je izuzetno važno, tim pre što nacionalni CERT raspolaže ne samo bezbednosnim informacijama relevantnim u okvirima svoje države, već i onih koje dobija od saradnika na međunarodnom nivou. U tom smislu fizičko obezbeđenje radnog okruženja je i važan faktor u izgradnji poverenja u CERT organizaciju.

5.2.4 Kapaciteti za saradnju

Jedan od kljućnih faktora uspešnog delovanja nacionalnog CERT-a je održiva i efikasna saradnja sa drugim CERT organizacijama, kako na nacionalnom, tako i na međudržavnom nivou. To nije bitno samo u procesu razrešavanja tekućih incidenata, nego i u svakodnevnom operativnom radu. U tom smislu postoje tri ključna elementa:

- poverenje, i izgradnja poverenja,
- kvalitet i održivost informacija i reakcija, i
- zajednička terminologija i operativne procedure.

5.2.4.1 Poverenje i izgradnja poverenja

Ovo je veoma kompleksna tema na koju utiču razni faktori, tako da je teško definisati konkretne zahteve u ovoj oblasti. Iz tog razloga najbolje je osloniti se na uopštene preporuke koje su plod višegodišnjeg iskustva na polju saradnje između različitih CERT organizacija.

5.2.4.2 Lična poznanstva

Lična poznanstva i reputacija se još uvek smatraju najvažnijim kriterijumom za izgradnju poverenja, a samim tim i za uspešnu saradnju. Iz tog razloga ključna je integracija sa relevantnim zajednicama CERT organizacija (FIRST, TF-CSIRT, ...). Potrebno je da timovi steknu dobru reputaciju tokom vremena, svojim delovanjem i angažovanošću, a ova reputacija (koja se na egzaktan način ne može izmeriti) je usko povezana sa reputacijom samih članova CERT tima. Bez ove reputacije veoma je teško da timovi postignu uspešnu saradnju sa drugim timovima, ili da se uopšte uključe u postojeće tokove saradnje. Takođe, do reputacije se može doći na dva načina: zahvaljujući dobroj reputaciji pojedinačnih članova tima, ili tako što timovi koji već imaju dobru reputaciju garantuju za kvalitet novih timova i uključuju ih u postojeće tokove saradnje. Naravno, kada je savladana ova prva prepreka uključivanja u tokove saradnje, neophodno je da svaki novi tim svojim delovanjem tokom vremena gradi svoju sopstvenu reputaciju.

5.2.4.3 Reputacija

Ne postoji zlatno pravilo kako se gradi dobra reputacija. Integracija sa postojećim zajednicama CERT timova je svakako neophodna. Važan faktor je i aktivna i proaktivna uloga u diskusijama i projektima koji se iniciraju tokom sastanaka u okviru zajednice. Takođe, dokazana tehnološka ekspertiza, kao i smisleno delovanje pojedinačnih članova tima u svakom slučaju doprinosi izgradnji dobre reputacije tima kao celine. Naravno, potrebno je da se tim i njegovi članovi tokom vremena dokazuju kao pouzdani i diskretni. Ukratko, poverenje između timova se gradi tokom vremena, a lična poznanstva i međusobno uvažavanje su ključni faktori u tom smislu.

5.2.4.4. Neformalne grupe

Interesantno je da se neformalna saradnja i aktivnosti na razmeni informacija, među njihovim akterima, ponekad smatraju korisnijim od formalnih okvira saradnje. Činjenica je da se, zahvaljujući svojoj fleksibilnosti, neformalne grupe smatraju efikasnijim kada god je u saradnju uključeno više od dve organizacije. Ipak, s obzirom da su standardne operativne procedure, u formalnim okvirima saradnje, te koje nose potreban nivo odgovornosti za ono što je potrebno učiniti, definitivno je potrebno uložiti napore da se neformalne grupe uvedu u formalne okvire saradnje, kako bi se poboljšala razmena informacija i saradnja u celini.

5.2.4.5 Nacionalna i međunarodna saradnja

Svi gore navedeni principi važe i za uspešnu saradnju i razmenu informacija i na nacionalnom nivou. Jasno je da nacionalni CERT treba da ima ključnu ulogu u organizovanju i koordinaciji saradnje među relevantnim bezbednosnim organizacijama u svojoj zemlji. Samo u slučaju kada saradnja dobro funkcioniše na nacionalnom nivou, nacionalni CERT može da ispuni svoju ulogu na međunarodnom nivou, gde se on smatra tačkom kontakta za razmenu

informacija za svoju državu. Jedan od vrhovnih ciljeva nacionalnog CERT-a treba da bude izgradnja čvrste zajednice sastavljene od ključnih aktera na očuvanju informacione bezbednosti te države.

5.2.4.6 Kvalitet i količina informacija

Razmena informacija između nacionalnih CERT-ova na duže staze može biti uspešna ukoliko su ispunjena dva uslova: sve uključene strane daju svoj doprinos, i nivo kvaliteta informacija koje pristižu od svih članova zajednice je u većoj ili manjoj meri jednak. Prvi uslov se odnosi na činjenicu da svaki CERT mora da ponudi neke informacije zajednici, da bi mogao da očekuje da nešto od nje i dobije za uzvrat. Drugi uslov se odnosi na činjenicu da informacije koje jedan tim deli treba da imaju neku upotrebnu vrednost za druge članove zajednice. Oba uslova zajedno znače da je tim sposoban da ponudi informacije koje imaju dodatnu vrednost za druge članove zajednice, bilo u smislu da su im do tada bile nepoznate, ili da im pomažu da potvrde već uočene bezbednosne pretnje. Treba naglasiti da je ispunjenost ovih uslova teško merljiva, ali ih, ipak, ne treba zanemariti kako bi se saradnja i razmena informacija uspešno razvijali tokom vremena.

5.2.4.7 Održivo reagovanje

Još jedan važan faktor je i vrsta reakcije koju je jedan nacionalni CERT tim u stanju da pruži, kao odgovor na informacije koje dobija, a naročito kada su u pitanju prijave incidenata. U idealnom slučaju, tim treba da bude kadar da trenutno reaguje po prijavi incidenta koju dobije od drugog tima, i da, primera radi, sistemima nekog napadača onemogući pristup mreži. Ovo je jedino moguće ukoliko CERT ima direktan pristup odgovarajućoj infrastrukturi, ili ukoliko ima mandat, tj. ovlašćenja u okviru svoje države, da takvu akciju zahteva od vlasnika te infrastrukture. Ipak, čest je slučaj da nacionalni CERT nema takvu vrstu ovlašćenja, i tu ponovo dolazi do izražaja njegova uloga na polju saradnje između timova u okviru svoje države. Dobro ustanovljena saradnja između svih ključnih aktera na nacionalnom nivou, kao što su CERT-ovi, provajderi Internet servisa, i drugi, na uspešan način doprinosi rešavanju incidenata čak i kada ne postoji direktan pristup infrastrukturi, ili mandat da se nekome od njih naloži neka vrsta reakcije. U suprotnom, nacionalni CERT može samo da prima prijave incidenata u koje su uključeni neki od njegovih konstituenata, ali ukoliko nije u stanju da po njihovom prijemu na adekvatan način reaguje, on ne može ispuniti obaveze u okviru svoje uloge, i pre ili kasnije će biti eliminisan iz procesa saradnje i razmene informacija.

5.2.4.8 Zajednička terminologija i operativne procedure

Samo po sebi je jasno da razmena informacija ima smisla samo ukoliko između partnera u komunikaciji postoji zajedničko razumevanje teme i terminologije koja je opisuje. Ovime se sprečava da dođe do nesporazuma u komunikaciji, i posledično do pogrešnih reakcija. Nacionalni CERT-ovi koji su uključeni u međudržavnu saradnju moraju da poštuju i određene operativne procedure, na primer po pitanju klasifikacije informacija, ili enkripcije informacija. U tom smislu, uvek se preporučuje primena dobre prakse do koje se došlo putem ranijih iskustava.

5.3 PREGLED STANJA NACIONALNIH CERT ORGANIZACIJA U EVROPI

5.3.1 Uvod

Prvi projekat na definisanju mininalnog skupa osnovnih kapaciteta nacionalnih CERT organizacija ENISA je sprovela tokom 2009. i 2010. godine. Taj skup je podrazumevao aktivnosti na očuvanju kritične informacione infrastrukture jedne zemlje, i davanje doprinosa saradnji i razmeni informacija među CERT organizacijama u različitim državama. Međutim, definisanje ovih kapaciteta je proces koji stalno traje, u skladu sa promenama u bezbednosnim aspektima informacionog okruženja, i tehnološkom napretku uopšte. Iako su, od 2010. Godine, pa do danas, mnoge države formirale svoje CERT organizacije, kapaciteti ovih timova u svim aspektima (mandat, portfolio servisa, operativno delovanje, saradnja...) jako variraju od države do države. Ove različitosti u mnogome otežavaju i njihovu međusobnu saradnju. Stoga je 2012. godine ENISA pokrenula novi projekat čiji je cilj da se preispita minimalni skup kapaciteta CERT organizacija, u skladu sa promenama u informacionom okruženju, ali i da se proceni trenutno stanje i status CERT organizacija na tlu Evrope.

U analizi iz 2012. godine *(Deployment of Baseline Capabilities of national/governmental CERTs: Status Report 2012*, ENISA) obuhvaćeno je 27 zemalja članica EU, i dodatno Island, Norveška i Švajcarska. Velika većina zemalja članica EU već je formirala državni/nacionalni CERT, iako među njima postoje značajne razlike u pogledu ovlašćenja u okvirima mandata, njihove uloge u pogledu razvoja nacionalne strategije informacione bezbednosti, tipa CERT organizacije (nacionalni, *de facto* nacionalni, državni/nacionalni, državni...), ili godinama iskustva u operativnom delovanju koje se manifestuje kroz zrelost tima.

Uopšteno rečeno, i dalje postoji izvestan nivo konfuzije u tome kako CERT-ovi sagledavaju svoju ulogu, u pogledu definicija nacionalni, državni, *de facto* nacionalni... Ipak, postoji ravnoteža između broja nacionalnih, državnih i državnih/nacionalnih CERT organizacija, dok se manji broj CERT-ova posmatra kao *de facto* nacionalni.

Spisak ovih CERT timova, uključujući i CERT tim EU institucija, po abecednom redu, predstavljen je u tabeli 5.1.

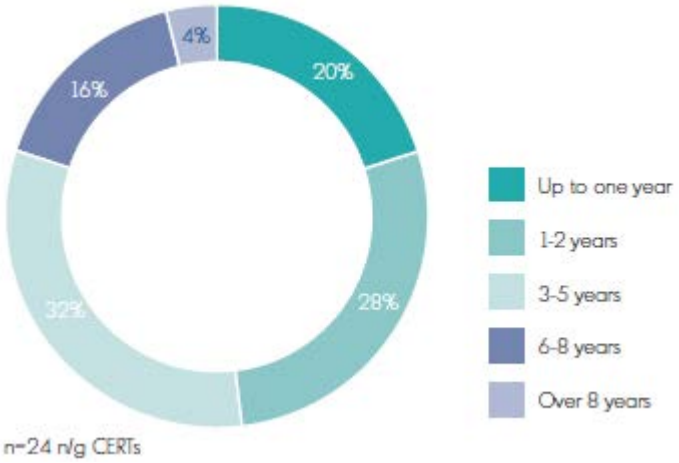
Takođe, postoje i značajne razlike u pogledu vremena postojanja državnih/nacionalnih CERT organizacija. U trenutku izrade preseka stanja, tj. 2012. godine, najveći deo organizacija (oko 32%) bile su već operativne u periodu 3-5 godina. Nacionalne CERT organizacije sa najdužim vekom trajanja su one koje su originalno formirane radi zaštite nacionalnih istraživačkih i obrazovnih institucija. Presek stanja u pogledu vremena postojanja CERT organizacija predstavljen je na slici 5.1.

Nivo implementacije osnovnih kapaciteta državnih/nacionalnih CERT organizacija definiše njihov nivo zrelosti, tj. razvijenosti. Raznolikost u nivou razvoja pojedinačnih CERT organizacija širom Evrope je jako izražena, pri čemu najveći broj organizacija definiše svoj nivo razvijenosti kao srednji (*defined*). Ovaj nivo razvijenosti podrazumeva: organizacija je u međunarodnoj zajednici prepoznata kao tačka kontakta na nacionalnom nivou, ima definisane i dokumentovane standardne procese koji se odnose na pružanje osnovnih servisa, i pruža dodatne servise (sa dodatnom vrednošću).

Skoro jednako velika grupa timova smatra da je dostigla sledeći, napredniji, nivo razvoja (*managed*), što pored prethodno definisanog, podrazumeva merljivost učinka i posedovanje zvaničnog mandata u pogledu pojedinih svojih aktivnosti.

Tabela 5.1: Spisak dražavnih/nacionalnih CERT organizacija na području Evrope

Država	Naziv CERT organizacije	Web sajt
Armenia	CERT AM	http://www.cert.am
Austria	CERT.AT	http://www.cert.at
Belgium	CERT.BE	https://www.cert.be
Bulgaria	CERT Bulgaria	http://govcert.bg
Croatia	HR-CERT	http://www.cert.hr
Czech Republic	CSIRT.CZ	http://www.csirt.cz/
Denmark	Danish GovCERT	http://www.govcert.dk/
Estonia	CERT-EE	http://www.cert.ee/
EU	CERT-EU	http://www.cert.europa.eu
Finland	NCSC-FI	http://www.cert.fi/
France	CERT-FR	http://www.cert.ssi.gouv.fr
Georgia	CERT-GOV-GE	http://www.cert.gov.ge/
Germany	CERT-BUND	https://www.bsi.bund.de/IT-Krisenmanagement
Greece	NCERT-GR	http://www.cert.gov.gr
Hungary	CERT-Hungary	http://www.cert-hungary.hu
Iceland	CERT-IS	http://cert.is/
Ireland	CSIRT.IE	http://www.dcenr.gov.ie/
Israel	CERTGOVIL	http://www.cert.gov.il/
Italy	CERT Pubblica Amministrazione	http://www.agid.gov.it/
Italy	CERT Nazionale Italia	https://www.certnazionale.it
Latvia	CERT.LV	http://www.cert.lv/
Lithuania	CERT-LT	http://www.cert.lt/
Luxembourg	CIRCL	http://www.circl.lu/
Montenegro	CIRT.ME	http://www.cirt.me/
Netherlands	NCSC-NL	http://www.govcert.nl
Norway	NorCERT	http://www.cert.no
Portugal	CERT.PT	http://www.cncs.gov.pt/
Romania	CERT-RO	http://www.cert-ro.eu/?lang=en
Slovakia	CSIRT.SK	http://www.csirt.gov.sk/
Slovenia	SI-CERT	http://www.cert.si/
Spain	CCN-CERT	https://www.ccn-cert.cni.es
Spain	INTECO-CERT	http://cert.inteco.es
Spain	"CERTSI"	http://certsi.es
Sweden	CERT-SE	http://www.cert.se
Switzerland	SWITCH-CERT	http://www.switch.ch/cert/
Turkey	TR-CERT	http://www.usom.gov.tr/
United Kingdom	CSIRTUK	http://www.cpni.gov.uk/
United Kingdom	GovCertUK	http://www.govcertuk.gov.uk/

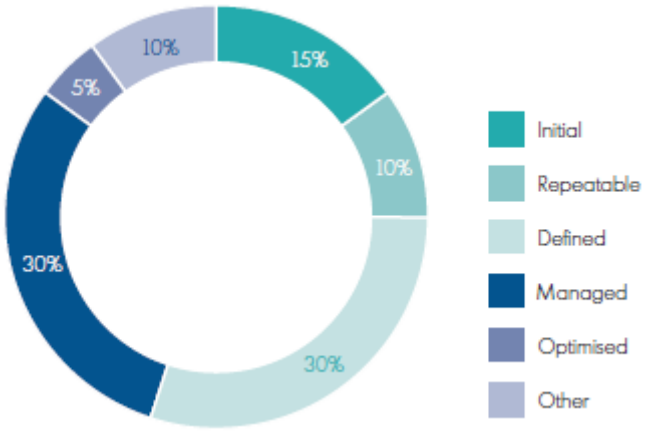


Slika 5.1: Vreme postojanja državnih/nacionalnih CERT organizacija na području Evrope

Timovi koji imaju najkraće vreme postojanja nalaze se u *initial* ili *repeatable* fazi razvoja. Jedan od razvijenijih timova deklarisao se da se dostigao najviši nivo razvoja (*optimized*), što podrazumeva da ima zvanični mandat za sve svoje aktivnosti, i ima dugotrajnu uspešnu saradnju sa svojim konstituentima, praćenu izuzetnim nivoom poverenja.

U svakom slučaju, bez obzira na nivo sa kojim se svaki od timova deklariše, ambicije svih su da povise svoj nivo razvoja u najkraćem mogućem roku, a često je to u vezi sa procesom učlanjenja u odgovarajuće međunarodne bezbednosne organizacije, tj. procesom akreditacije u organizacijama kao što su FIRST, ili TI (*Trusted Introducer*).

Deklarisani nivo razvijenosti nacionalnih CERT organizacija prikazan je na slici 5.2.



Slika 5.2: Nivo razvijenosti dražavnih/nacionalnih CERT organizacija na području Evrope

5.3.2 Mandat i strategija

Države svojim CERT organizacijama dodeljuju mandat, tj. ovlašćenja za delovanje, na nekoliko načina: kroz postojanje nacionalnih strategija za informacionu bezbednost u kojima se pominje i definiše uloga državnog/nacionalnog CERT-a (npr. u Slovačkoj), ili usvajanjem specijalnih zakona (Danska, Grčka, Finska, Španija...) koji se u nekim delovima oslanjaju na CERT-ove. Ovi zakoni se odnose na nekoliko oblasti: pravni okvir u oblasti telekomunikacija, zaštita podataka o ličnosti, zaštita ključne informacione infrastrukture u državi, i informaciona bezbednost. Pri tome, nivo učešća CERT organizacija u donošenju ovih zakona je zadovoljavajući (više od 90% CERT-ova je na neki način uključeno), mada je dubina angažovanja različita od zemlje do zemlje.

U nekim zemljama, uprkos postojanju nacionalne strategije informacione bezbednosti, ili odgovarajućih zakona, mandat je CERT organizacijama dodeljen vladinim dekretom (Mađarska, Rumunija, Slovačka), ili zakonskom naredbom (Litvanija). Poseban primer je i Češka, gde mandat ima formu memoranduma između države i administratora nacionalnog domena. Primer države u kojem nacionalni CERT postoji i funkcioniše, ali bez formalno dodeljenog mandata je Portugal.

Primetno je da i dalje postoji prostor na polju razjašnjenja mandata, jer postoje primeri u kojima predviđeni skup servisa nadilazi kapacitete formiranog CERT-a. Dodatno, ponekad je potrebno više detalja i smernica kada je u pitanju saradnja sa istražnim ili pravosudnim organima, ili kada je potrebno obezbediti finansiranje u delu koji se tiče aktivnosti državnog CERT-a.

Nacionalne CERT organizacije u različitim državama formiraju se u okviru različitih organizacija i institucija. Primera radi, u Finskoj je nacionalni CERT ustanovljen u okviru nacionalne regulatorne agencije, što mu donosi određene prednosti u nekim kriznim situacijama, kada pod okriljem autoriteta regulatorne agencije može da izvrši uticaj, na primer, na provajdere telekomunikacionih usluga. Jedan trend, koji se čini globalnim, ogleda se u formiranju centara za informacionu bezbednost, koji su odgovorni za implementaciju strategije informacione bezbednosti. Ovakve strukture su već formirane u Velikoj Britaniji i Holandiji, a i u Irskoj se čine napori u tom smeru. Sa druge strane, u nekim državama usvojen je pristup da se nacionalne/državne CERT organizacije formiraju u institucijama pravosuđa, javne bezbednosti, istražnim agencijama, kao i u okviru ministarstava ili izvršnih organa vlasti (na primer, Francuska, Grčka, Poljska, Španija, Švedska...).

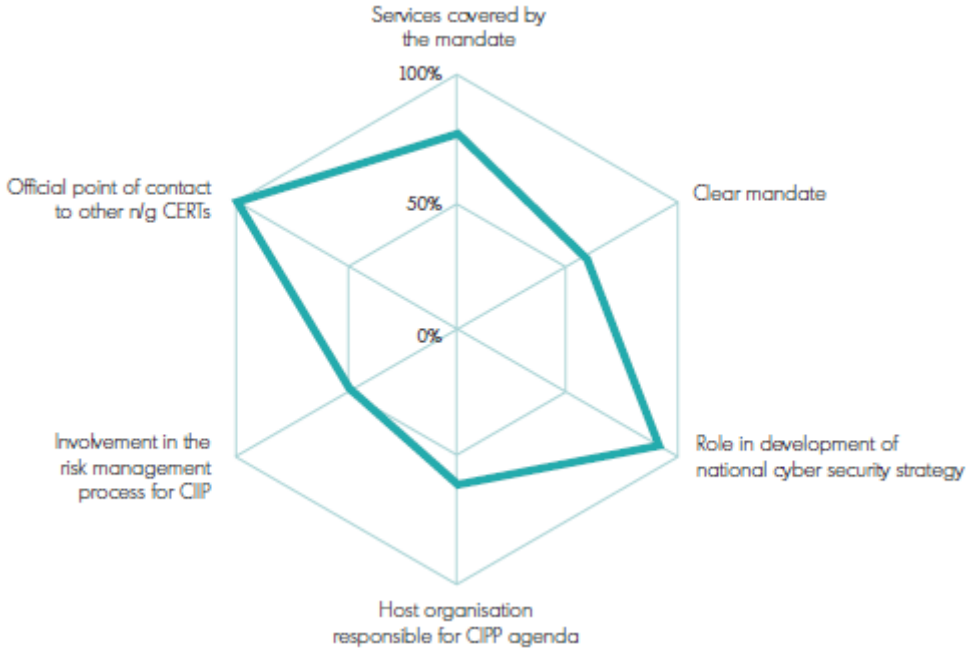
Na slici 5.3 dat je prikaz implementacije pojedinih aspekata delovanja CERT organizacija u okvirima njihovog mandata. Iz ovoga je evidentno da postoje najveće potrebe za dodatnim angažovanjem na polju definisanja mandata i dubljeg uključivanja nacionalnih CERT-ova u procese procene bezbednosnih rizika i očuvanja ključne informacione infrastrukture.

5.3.2.1 Izvor mandata

Od izuzetne je važnosti da nacionalni CERT ima jasan mandat za obavljanje svojih delatnosti, kako bi mogao zvanično da nastupa kao ključni igrač u očuvanju bezbednosti, razmeni informacija, i koordinaciji u borbi sa raznim vrstama napada na ključnu nacionalnu informacionu infrastrukturu.

Postoji više načina na koje se ovaj mandat dodeljuje. Ukoliko u državi postoji definisana strategija informacione bezbednosti, što je slučaj u oko polovine zemalja članica

EU, uloga nacionalnog CERT-a mora biti definisama u okviru tog dokumenta. Precizniji okviri mandata obično su definisani u okviru posebnih odluka vlade, dekreta i naredbi, što je slučaj u oko dve trećine zemalja članica EU. U nekim ređim slučajevima mandat je definisan i posebnim ugovorom između vlade i CERT organizacije. Zakoni na koje se nacionalne organizacije oslanjaju u svom delovanju su opšti zakoni o telekomunikacijama, zaštiti podataka ličnosti, javnoj bezbednosti ili bezbednosti ključne informacione infrastrukture. Postoje i slučajevi, u bar dve države, gde ne postoji formalno definisan mandat nacionalnog CERT-a, ali on, ipak, obavlja svoje funkcije.



Slika 5.3: Prikaz implementacije pojedinih aspekata delovanja CERT organizacija

5.3.2.2 Trajanje mandata

U više od 80% država mandat nacionalne CERT organizacije nije vremenski ograničen. Ali, i u slučajevima kada je ograničen, radi se o formalnom isteku ugovora pre nego što mandat postane stalan, ili je u vezi sa očekivanjima za prijem u odgovarajuće bezbednosne organizacije ili zajednice na nivou EU. Dakle, postoji apsolutni trend da trajanje mandata nacionalnih CERT-ova ne bude vremenski ograničeno.

5.3.2.3 Servisi izvan mandata

Blizu 80% CERT organizacija imaju stav da su servisi koje oni nude pokriveni mandatom koji im je poveren. Postoje i CERT organizacije koje su identifikovale dodatne servise koje nude van okvira svojih mandata, a neki od tih servisa su:

- organizovanje treninga za osoblje drugih organizacija na polju informacione bezbednosti,
- prikupljanje podataka o uočenim bezbednosnim incidentima, koji potiču od mreža u okviru države, i slanje zahteva za verifikaciju incidenata krajnjim korisnicima,
- da bude sertifikacioni autoritet za platforme građanske inicijative, i
- istraga u slučajevima narušavanja ili pretnji po informacionu bezbednost.

5.3.2.4 Potreba za razjašnjenjem mandata

Oko 63% CERT organizacija tvrdi da su uloge i odgovornosti njihovih timova jasno definisane u okviru mandata, što je istovremeno i utisak oko 70% korisnika njihovih usluga. Pri tome, CERT-ovi su naglasili nekoliko oblasti u kojima postoje potrebe za pojašnjenjima:

- opseg servisa koji su opisani u okvirima mandata ne odgovara kapacitetima formiranih timova, a najčešće se problemi javljaju zbog nedostatka osoblja u novoformiranim CERT organizacijama,
- potrebne su promene u pogledu obaveštavanja o bezbednosnim incidentima, naročito u delu gde zakonom nije jasno definisano kome i u kojim situacijama provajderi Internet servisa i telekomunikacioni operatori treba da prijave incidente,
- potrebna su razjašnjenja u pogledu saradnje sa istražnim i pravosudnim organima,
- postoji problem sa finansiranjem državnih CERT organizacija, tj. dela posla koji pokriva nacionalni CERT dok se ne formira državni CERT, i
- potrebno je da servisi nacionalnog CERT-a budu dostupni širem građanstvu, i utoliko je potrebno više raditi na predstavljanju i komunikaciji ovih organizacija sa javnošću.

Iako postoje potrebe za razjašnjenjima, opšti stav je da odredbe mandata treba da ostanu u određenoj meri generalne, jer je teško predvideti potencijalne dodatne aktivnosti CERT-ova, koje mogu da se jave tokom vremena.

5.3.2.5 Uloga u izradi nacionalne strategije informacione bezbednosti i osiguranja bezbednosti ključne informacione infrastrukture

Prema izveštajima nacionalnih CERT organizacija, za oko 60% njih mandat uključuje i ulogu u razvoju nacionalne strategije informacione bezbednosti i odgovarajućih zakona. Ovo uključuje procenu rizika, izradu plana za upravljanje rizicima u vezi sa ključnom informacionom infrastrukturom, implementaciju plana, verifikaciju njegovog učinka, kao i redovnu evaluaciju i poboljšanja na tom polju. Još oko 30% nacionalnih CERT organizacija sprovode ovu ulogu na neformalan način.

Međutim, dubina do koje su nacionalne CERT organizacije uključene u ove poslove jako varira od države do države, i u određenom broju slučajeva se svodi samo na formalnu savetodavnu aktivnost. Sa druge strane, u oko 50% zemalja se radi na izradi zakona koji će ovu ulogu nacionalnih CERT organizacija osnažiti.

Što se tiče uloge u proceni rizika i obezbeđenju ključne informacione infrastrukture, nivo angažovanja nacionalnih CERT organizacija je samo oko 50%. Njihova uloga je uglavnom posredna, i to na polju tehničke ekspertize. Na primer, postoje države u kojima je nacionalni CERT tačka kontakta u slučajevima incidenata sa ključnom informacionom infrastrukturom, ali krovna organizacija u okviru koje CERT funkcioniše ima i poseban sektor koji se bavi razrešavanjem ovih incidenata.

5.3.2.6 Krovne organizacije i njihova uloga u razvoju strategije informacione bezbednosti

Nacionalne CERT organizacije u 90% slučajeva funkcionišu u okviru drugih krovnih organizacija ili institucija, kao što su ministarstva, regulatorne agencije, istraživačke institucije i slično. Više od 60% tih organizacija odgovorno je za izradu nacionalne strategije informacione bezbednosti u svojoj zemlji, uključujući i upravljanje kriznim situacijama radi obezbeđenja ključne informacione infrastrukture. Oko 80% nacionalnih CERT organizacija je potvrdilo da imaju direktnu liniju odgovornosti prema izvršnim vlastima svoje zemlje u slučajevima kriznih situacija, putem svojih krovnih organizacija.

5.3.2.7 Promene radi ojačanja mandata

Iako u velikoj većini nacionalnih CERT organizacija postoji mišljenje da su njihove uloge i odgovornosti manje ili više pokrivene njihovim mandatima, većina njih je ipak predstavila i neke ideje, koje sve češće postaju sastavni deo novih zakona na ovom polju, kako bi se taj mandat u nekim slučajevima mogao ojačati:

- zahtevanje od telekomunikacionih operatora i provajdera Internet servisa da prijavljuju incidente koji se dešavaju u njihovim mrežama,
- razjašnjenje odnosa između nacionanih CERT-ova i njihovih konstituenata,
- dugoročno planiranje na temu finansiranja ovih organizacija,
- poboljšanje i bolja usaglašenost među propisima koji se odnose na ključnu informacionu infrastrukturu i elektronske komunikacije,
- stimulisanje i razvoj zajednica bezbednosnih organizacija,
- davanje dozvola nacionalnim CERT organizacijama da proaktivno skeniraju infrastrukturu i prijavljuju otkrivene ranjivosti njenim vlasnicima,
- donošenje regulative kojom se nacionalnim CERT organizacijama omogućava korišćenje podataka o ličnosti kako bi se ubrzao proces razrešenja bezbednosnih incidenata, i
- uključivanje nacionalnih CERT organizacija u rad nacionalnih centara za informacionu bezbednost, sa centralnom ulogom u olakšavanju komunikacije sa drugim nacionalnim agencijama koje se bave bezbednošću ključne informacione infrastrukture u okviru svoje zemlje.

Sa ovim idejama su se u velikoj meri saglasili i konstituenti nacionalnih CERT organizacija. Oni, takođe, očekuju da nacionalni CERT-ovi imaju i više resursa, kako bi poboljšali svoje delovanje i proširili obim servisa, sa više proaktivnog angažovanja. Sa druge strane telekomunikacioni operatori imaju stav da je potrebno izbeći povećanje birokratskog opterećenja prema njihovim organizacijama, u smislu paralelnog izveštavanja o incidentima i nacionalnih regulatornih organizacija i CERT organizacija.

5.3.2.8 Zvanična tačka kontakta za nacionalne CERT organizacije drugih zemalja

Uloga zvanične tačke kontakta za nacionalne CERT organizacije drugih zemalja je jedna od najvažnijih specifičnosti ovih organizacija. Takođe, to podrazumeva i mandat dobijen od strane države da se zemlja predstavlja u međunarodnim zajednicama CERT organizacija, kao što su FIRST, i eventualno EGC (*European Government CERTs*).

Više od 70% nacionalnih CERT organizacija ima zvaničnu ulogu nacionalne tačke kontakta, dok u ostalim slučajevima nezvanično preuzimaju ovu ulogu, bez formalnog mandata. Interesantno je iskustvo koje ukazuje da je, za izgradnju reputacije jedne nacionalne CERT organizacije na međunarodnom planu, proaktivni pristup u okvirima njenog delovanja izuzetno važan, dok je na domaćem planu za reputaciju važnije imati zvanični mandat.

5.3.3 Portfolio servisa

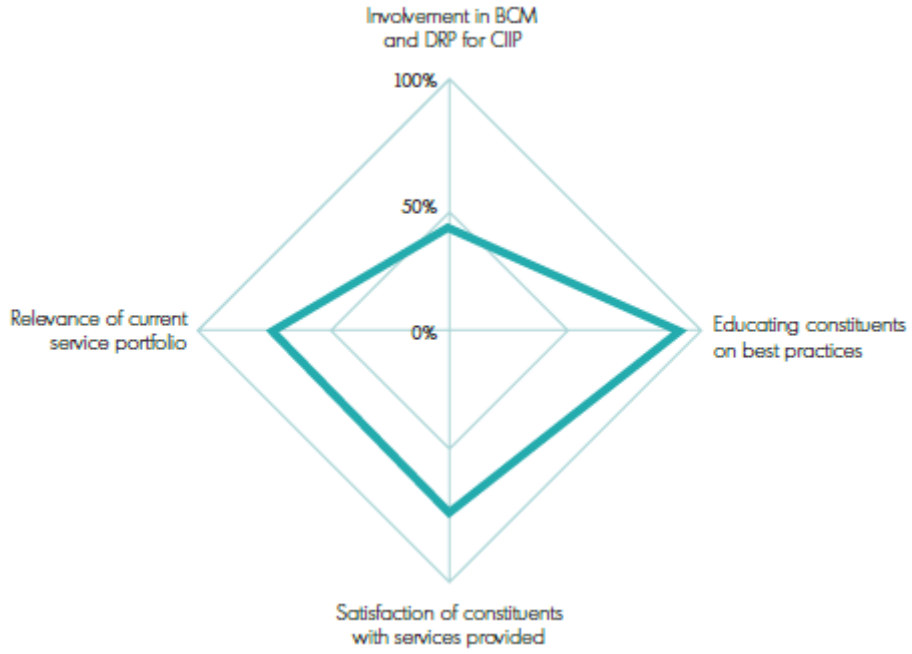
Nacionalne CERT organizacije obezbeđuju razne kategorije servisa, iz skupa osnovnih servisa, među kojima su reaktivni servisi, proaktivni servisi i servisi upravljanja kvalitetom bezbednosti. Nacionalne CERT organizacije sa više iskustva, ili sa više resursa, mogu da ponude naprednije servise iz svih ovih kategorija, za svoje ključne konstituente kao što su državne institucije, ili javni operatori ključne informacione infrastrukture. Međutim, treba napomenuti da je upravljanje incidentima jedini univerzalni servis koji sve nacionalne CERT organizacije obezbeđuju za svoje konstituente.

Nacionalni CERT-ovi tokom vremena izgrađuju svoju tehnološku ekspertizu na polju informacione bezbednosti, što kasnije može biti od koristi i drugim državnim organima, kao što su istražni ili pravosudni organi. Takođe, članovi tima često imaju ulogu konsultanata u izradi strategija i zakona na temu obezbeđenja ključne informacione infrastrukture u svojoj zemlji. Oko 90% nacionalnih CERT organizacija učestvuje u organizaciji seminara i obuka na temu informacione bezbednosti. Sa druge strane, samo oko 40% CERT organizacija navodi da je angažovano na izradi planova za oporavak od katastrofalnih incidenata (*disaster recovery* – DRP) i obezbeđivanje kontinuiteta poslovanja (*business continuity management* – BCM). Nivo ovog angažovanja zavisi od mandata koji organizacija ima, kao i odnosa koji ima sa svojom krovnom organizacijom.

Neki od bolje organizovanih timova, sa više iskustva i resursa, mogu svojim konstituentima da ponude i neke dodatne servise, izvan okvira svojih uobičajenih aktivnosti. U to mogu spadati projekti na podizanju svesti o informacionoj bezbednosti, ili uloga koordinacije u testovima informacione bezbednosti. Ponekada ti testovi mogu obuhvatati ključnu informacionu infrastrukturu svoje zemlje, ili koordinisane testove na teritorijama, ili sistemima, više zemalja. Postoje i slučajevi kada nacionalne CERT organizacije daju i servise za građanstvo, kojima ih upozoravaju na kompjuterske viruse, ili drugi maliciozni softver.

Pregled aktivnosti, i raznih aspekata servisa nacionalnih CERT organizacija dat je na slici 5.4.

Sa slike 5.4 vidi se i da postoji visok nivo zadovoljstva (oko 73%) konstituenata servisima koje obezbeđuju nacionalne CERT organizacije. To se, takođe, ogleda i u činjenici da 9 od 10 organizacija obezbeđuje svojim konstituentima programe edukacije i treninga, što doprinosi izgradnji poverenja i boljoj međusobnoj saradnji.



Slika 5.4: Pregled aktivnosti, i raznih aspekata servisa nacionalnih CERT organizacija

5.3.3.1 Konstituenti nacionalnih CERT organizacija

Konstituenti, tj. korisnici usluga nacionalnih CERT organizacija, trebalo bi po teoriji da budu svi entiteti unutar granica jedne države, pri čemu javne službe i državne institucije treba da imaju poseban tretman. U tom smislu, nacionalne CERT orgaizacije često imaju i ulogu državnih CERT organizacija. U nekim državama, kao što su Poljska, Španija, Švajcarska ili Velika Britanija, postoje odvojene CERT organizacije za konstituente na nacionalnom, tj. državnom nivou.

Provajderi ključne informacione infrastrukture, takođe, mogu biti korisnici servisa nacionalnih CERT organizacija, ali često imaju i svoje timove koji se bave razrešavanjem bezbednosnih incidenata, i u tim situacijama nacionalni CERT ima samo ulogu podrške.

CERT organizacije koje vode poreklo iz istraživačkih ili obrazovnih institucija, koji su vremenom izrasli u *de facto* nacionalne CERT-ove, nastavljaju da pružaju servise svojim originalnim konstituentima. Drugi potencijalni korisnici obično dobijaju samo podskup osnovnih servisa, dok se građanstvo najčešće upućuje na provajdere Internet servisa, za slučaj sumnje da su postali žrtva informacionog napada.

5.3.3.2 Rešavanje incidenata i drugi reaktivni servisi

Ključni servis koji svaka nacionalna CERT orgaizacija mora da obezbedi svojim konstituentima je rešavanje incidenata, analiza i koordinacija, što sve spada u termin upravljanje incidentima. Reaktivni servisi obuhvataju četiri osnovne kategorije: alarmi i upozorenja, upravljanje incidentima, nadgledanje ranjivosti sistema i prikupljanje dokaza o incidentima. Što je nacionalni CERT iskusniji i sposobniji, to se trudi da ponudi reaktivne servise iz što više kategorija. U državama u kojima postoji jako razvijena nacionalna mreža u okviru koje funckionišu brojne CERT organizacije, kao što su Velika Britanija i Nemačka, nacionalni CERT-ovi nude čitav spektar reaktivnih servisa. Ovi nacionalni CERT-ovi su deo nacionalnih centara za informacionu bezbednost ili sličnih institucija, te samim tim imaju

dovoljno ljudskih i tehnoloških resursa da pružaju ne samo reaktivne, već i druge vrste servisa.

Univerzalni način izveštavanja nacionalnih CERT organizacija je izdavanje alarma i upozorenja. Oni prikupljaju informacije, ili automatski (preko raznih sistema koji to omogućavaju), ili od drugih organizacija koje se bave sličnim poslom. Upozorenja uključuju procenu rizika i davanje saveta kako da se ti rizici preduprede (koje sistemske „zakrpe“ treba primeniti, koji softver treba izbegavati, koje komunikacione portove treba blokirati na mrežnom nivou, i slično). Takođe, s obzirom da je za upravljanje incidentima često potrebna međunarodna saradnja, postoji konstantna težnja da se forme za razmenu podataka o incidentima na neki način standardizuju, kako bi se saradnja i razmena informacija olakšala.

Kada se procenjuju kapaciteti CERT organizacije da odgovori na zadatke upravljanja incidentima, od velike je važnosti prikupiti informacije i utiske konstituenata o tome koliko su zadovoljni radom svoje CERT organizacije. Telekomunikacioni operatori i državne institucije uglavnom imaju pozitivan stav (u oko 75% slučajeva) o radu svojih nacionalnih CERT organizacija.

5.3.3.3 Proaktivni servisi

Cilj pružanja proaktivnih servisa je da se smanji broj bezbednosnih incidenata primenom preventivnih mera. Ovi servisi uključuju: najave, praćenje tehnologija, revizije i procene bezbednosti sistema, konfigurisanje i nadzor bezbednosnih alata, aplikacija, infrastrukture i servisa, razvoj bezbednosnih alata, servise za detektovanje upada u sisteme ili mreže, razmenu informacija na temu informacione bezbednosti.

Veća pažnja koja se u poslednje vreme poklanja proaktivnim servisima utiče i na nacionalne CERT organizacije da ih sve više praktikuju. Sada je već uobičajeno da nacionalne CERT organizacije objavljuju savete na temu bezbednosnih događaja i incidenata koji bi mogli imati posebnu važnost za njihove konstituente. Informacije se prosleđuju različitim kanalima, u zavisnosti od tipa informacija (putem *web*-a, mejling listi, društvenih mreža, i slično). Zahvaljujući ovim informacijama, koje su lako dostupne, svaka konstituentska organizacija može imati korist u smislu unapređenja svoje informacione bezbednosti.

Takođe, objavljivanje statističkih informacija o upravljanju incidentima postaje sve traženiji servis među konstituentima, jer je to dobar izvor za praćenje aktivnosti i uspešnosti rada CERT organizacije koja ih opslužuje. Stoga je ovaj tip servisa sve više zastupljen među nacionalnim CERT organizacijama, mada se podaci, čak iako se redovno ažuriraju, ne objavljuju uvek javno.

5.3.3.4 Nestandardni servisi

Iako se trenutni servisni portfolio nacionalnih CERT organizacija generalno smatra odgovarajućim, neke organizacije omogućavaju i neke nestandardne servise na zahtev svojih konstituenata. Ovi servisi se među CERT organizacijama nazivaju „novim“ servisima, i oko 25% nacionalnih CERT-ova je u stanju da ih ponudi. Neki od ovih servisa mogu se ticati otkrivanja ranjivosti sistema, davanja pravne podrške, razvoja alata za proaktivno delovanje, ili analizu i upravljanje razrešavanjem incidenata.

Takođe, postoje i servisi koji se pružaju na zahtev provajdera ključne informacione infrastrukture, ili državnih institucija, kao što su projekti na podizanju javne svesti o informacionoj bezbednosti koje finansira država, ili uloga koordinacije u testovima informacione bezbednosti na nivou cele države. Postoje čak i aktivnosti kao što je organizovanje radnih grupa koje se bave pojedinim aspektima informacione bezbednosti u

okviru jedne zemlje, a u nekim državama (npr. Nemačka) postoje i servisi za upozoravanje građanstva na pretnje od kompjuterskih virusa ili drugog malicioznog softvera.

5.3.3.5 Angažovanje spoljnjih saradnika (outsourcing)

Upravljanje incidentima i alarmiranje i obaveštavanje su obavezni servisi koje nacionalni CERT treba da pruža, ali neki drugi servisi koji nisu vremenski kritični, mogu biti delegirani drugim organizacijama, ili spoljnjim saradnicima. To je praksa koja je prisutna u oko jedne četvrtine nacionalnih CERT organizacija. U ove servise najčešće spadaju: pravna pomoć, razvoj softvera, pisanje bezbednosnih preporuka za javne ustanove, razvoj alata za prikupljanje informacija.

5.3.3.6 Učešće u izradi planova za disaster recovery (DRP) i business continuity management (BCM) za potrebe ključne informacione infrastrukture

Plan oporavka od katastrofalnih incidenata (*disaster recovery planning* – DRP) i obezbeđenje kontinuiteta poslovanja (*business continuity management* – BCM) su ključni aspekti nacionalnog plana za obezbeđenje ključne informacione infrastrukture, i oni su važna komponenta upravljanja kvalitetom bezbednosti sistema.

Nešto manje od polovine nacionalnih CERT organizacija potvrdilo je da je učestvovalo u DRP i BCM aktivnostima, pri čemu nivo njihovog angažmana zavisi od dobijenog mandata i odnosa sa krovnom organizacijom. Neke su angažovane na razvoju regulative u ovoj oblasti, a neke druge pružaju konsultantske usluge odgovarajućim entitetima koji su angažovani na ovim poslovima. Takođe, angažovanje nacionalnih CERT organizacija u ovom smislu odnosi se i na povećanje svesti o informacionoj bezbednosti, uspostavljanje mehanizama za razmenu informacija sa operatorima, procenu bezbednosnih rizika i organizaciju bezbednosnih testova.

5.3.3.7 Servisi edukacije i treninga

U zavisnosti od resursa kojima raspolažu, nacionalne CERT organizacije često sprovode napredne obuke i treninge za svoje konstituente, na najaktuelnije teme na polju informacione bezbednosti. Ovi servisi spadaju u grupu servisa za upravljanje kvalitetom bezbednosti, koje su nacionalne CERT organizacije sposobne da ponude zahvaljujući svojoj ekspertizi na polju informacione bezbednosti. Istraživanje kaže da više od 90% nacionalnih CERT organizacija sprovodi ovakve aktivnosti. U ove servise spadaju organizovanje konferencija, seminara, kurseva, tutorijala, kao i organizovanje velikih testova informacione bezbednosti na nacionalnom nivou, u čemu učestvuje oko polovine nacionalnih CERT organizacija. Učestanost ovih događaja može da zavisi od zahteva konstituenata, a često je to i predmet ugovorne obaveze sa konstituentima.

Veliki testovi informacione bezbednosti na nacionalnom nivou, tj. testovi bezbednosti ključne informacione infrastrukture, obično se izvode jednom u godinu ili dve dana, ali neke CERT organizacije sa boljim resursima i nivoom ekspertize u stanju su da ih izvode i više puta godišnje. Takođe, postoji tendencija da se ovakvi testovi sprovode i na teritorijama više zemalja, kako bi se testirala i poboljšala komunikacija i spremnost za rešavanje bezbednosnih incidenata na međunarodnom nivou.

5.3.3.8 Održivost trenutnog obima servisa

S obzirom na česte i velike promene u informacionom okruženju, često se postavlja pitanje da li je trenutni obim servisa nacionalnih CERT organizacija koji su u ponudi adekvatan, i oko tri četvrtine organizacija deli mišljenje da jeste.

Ipak, određeni broj nacionalnih CERT organizacija poziva na ulaganje više napora u vezi sa pravnom problematikom, i saradnjom sa istražnim i pravosudnim organima. Postoji i generalni utisak da su, pored tehničke ekspertize koja je ključna, nacionalnim CERT organizacijama sve više potrebne i pravne kompetencije.

Konstituenti sa svoje strane stalno očekuju poboljšanja na implementaciji postojećih servisa, kao i uspostavljanju novih. Operatori imaju potrebu za servisima koji se više tiču telekomunikacionih mreža, kao i detaljnije savetodavne aktivnosti, dok druge CERT organizacije često imaju primedbu da nacionalne CERT organizacije, naročito one sa ulogom državnog CERT-a, često nisu voljne, ili u mogućnosti, da razmenjuju određene relevantne informacije.

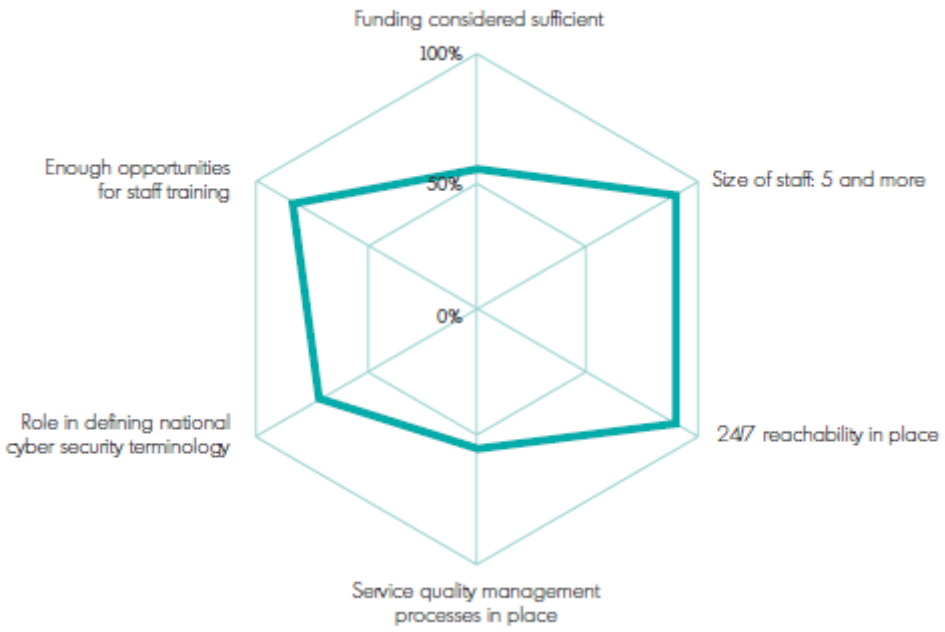
5.3.4 Operativni kapaciteti

Postoje četiri oblasti u kojima se ogledaju operativni kapaciteti nacionalnih CERT organizacija: ljudski resursi, infrastruktura, isporuka servisa i kontinuitet poslovanja. Iako faktori kao što su mandat, regulativa, veličina države i radno vreme u mnogome određuju veličinu nacionalne CERT organizacije, generalno se smatra da je na evropskom nivou tim od 6 do 8 ljudi dovoljan za isporuku prihvatljivog nivoa servisa. Ipak, u većini zemalja članica EU timovi broje više od 8 ljudi, a u nekim slučajevima taj broj je i višestruko veći. Isto tako, postoje i timovi od samo 4 ili 5 ljudi. Međutim, kada se tumače ovi brojevi, treba imati u vidu da CERT timovi česti uživaju podršku informacione službe svoje krovne organizacije ili institucije. Kada je u pitanju kontakt sa javnošću, neki timovi na svojoj Internet stranici objavljuju kontakt informacije, ili čak i slike svojih članova, dok je kod nekih drugih timova dostupna samo osnovna adresa elektronske pošte.

Sa druge strane, ne postoje velike razlike u pogledu potrebe da se omogući više načina komunikacije sa nacionalnim CERT-om, što je *de facto* pravilo koje važi za sve organizacije. Takođe, da bi se obezbedila kvalitetna isporuka servisa i kontinuitet poslovanja, nacionalni CERT-ovi u najvećem broju slučajeva rade u režimu 24/7. Čak i kada je radno vreme ograničeno na uobičajeno dnevno radno vreme, i u slučajevima kada se timovi suočavaju sa manjkom resursa, u najvećem broju slučajeva, ipak, postoji dežurna osoba koja je dostupna preko telefona, ili neko od članova tima prati stanje preko elektronske pošte.

Mnoge nacionalne CERT organizacije podvlače problem finansiranja svojih aktivnosti, naročito u državama gde se timovima ne dozvoljava da dodatno zarađuju novac kroz implementaciju dodatnih servisa. Finansiranje se najčešće obezbeđuje kroz krovnu organizaciju koja je osnivač nacionalnog CERT-a, ili iz državnog budžeta. U slučaju da je osnivač nacionalnog CERT-a neka od nacionalnih regulatornih agencija, deo sredstava se stiče direktno od operatora u formi malog dela njihove godišnje dobiti.

Na slici 5.5 dat je prikaz nekih aspekata operativnih kapaciteta, na bazi informacija dobijenih od samih nacionalnih CERT organizacija.



Slika 5.5: Aspekti operativnih kapaciteta nacionalnih CERT organizacija

Sa slike 5.5 može se uočiti da većina nacionalnih CERT organizacija ima bar 5 ili više članova tima, s tim da svi imaju planove da povećaju broj osoblja, dok malo više od polovine organizacija smatra da ima dovoljno sredstava za obavljanje poslova iz okvira svog mandata. Takođe, preko 80% timova tvrdi da ulaže velike napore da osoblje bude na odgovarajući način edukovano i osposobljeno, preko 90% timova je dostupno u režimu 24/7, i tako dalje.

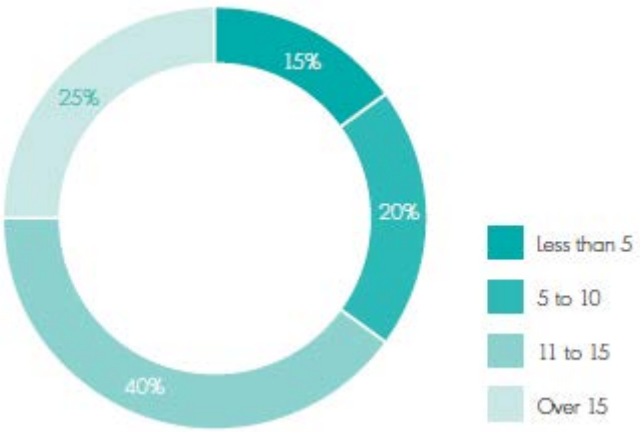
5.3.4.1 Model finansiranja

Da bi bili u mogućnosti da obezbede kvalitetne servise za svoje konstituente, nacionalne CERT organizacije moraju imati na raspolaganju dovoljno finansijskih sredstava za osoblje i opremu. U tom smislu, situacija se olakšava ukoliko se kroz nove bezbednosne strategije i mandate, nacionalne CERT organizacije više prepoznaju kao ključni igrač na polju informacione bezbednosti.

Finansiranje nacionalnih CERT organizacija obično se obezbeđuje iz dva izvora – iz budžeta vladinih institucija, ili kroz budžet krovne organizacije koja je osnivač nacionalnog CERT-a. Ipak, postoje tendencije da ove organizacije samostalno zarađuju novac, kroz razne komercijalne i istraživačke aktivnosti gde njihova ekspertiza dolazi do izražaja.

5.3.4.2 Veličina i sastav tima i njegove odgovornosti

Već je pomenuto da je za normalno poslovanje nacionalne CERT organizacije, u režimu 24/7, kako na domaćem planu za potrebe svojih konstituenata, tako i na planu međunarodne saradnje u rešavanju bezbednosnih incidenata, potrebno bar 6 do 8 članova tima. Većina nacionalnih CERT organizacija ispunjava ovaj uslov, što se vidi na slici 5.6, gde je prikazana procentualna zastupljenost broja članova tima po raznim organizacijama na tlu Evrope.



Slika 5.6: Procentualna zastupljenost broja članova tima

Treba napomenuti, da i u slučajevima jako malih timova, deo zadataka obavlja osoblje matične organizacije, kroz svoje uobičajene aktivnosti. Takođe, finansijske i pravne poslove, takođe, preuzimaju odgovarajuće službe krovne organizacije ili institucije. Ipak, tendencija svih nacionalnih CERT organizacija je da povećaju brojno stanje osoblja kako bi kvalitetnije odgovorili na svoje obaveze u okvirima servisa koje pružaju, a takva su i očekivanja njihovih konstituenata.

Sastavi timova obično su u skladu sa generalnim preporukama na ovu temu, tj. postoji rukovodilac tima, nekoliko ljudi koji se bave upravljanjem incidentima, i nekoliko tehnoloških eksperata. Nacionalne CERT organizacije koje imaju više resursa, obično imaju i više specijalizovanih eksperata, na primer u oblastima kao što su istraživanje i razvoj, ili na poslovima pravne prirode. Kada se alocira osoblje koje treba da se bavi određenim servisima, teško je predvideti egzaktne brojke, jer je čest slučaj da se članovi tima bave sa više različitih poslova ili servisa. Takođe, timovi često imaju problem da pronađu i angažuju pojedine tipove stručnjaka, na primer u oblastima digitalne forenzike, programiranja i razvoja bezbednosnih alata, ili pravne eksperte na polju informacione bezbednosti. Nacionalni CERT timovi pokušavaju da privuku ovakve osobe ponudom jedinstvenog posla, na kojem osoba može lično i profesionalno da se razvija i napreduje, uz pristup najmodernijim tehnologijama, i u saradnji sa ekspertima iz drugih zemalja.

5.3.4.3 Obuka osoblja

Nacionalna CERT organizacija mora da obezbedi da njeni zaposleni imaju odgovarajući nivo znanja i ekspertize, što implicira stalno investiranje u ljudske resurse, u obimu koji to dozvoljavaju budžet i vreme koje imaju na raspolaganju za ove aktivnosti. Naravno, stoji i činjenica da je najbolja obuka koju čovek može dobiti sam rad u jednom takvom timu, gde se vremenom stiču veliko znanje i iskustvo. Razni tipovi obuka koje se organizuju na nacionalnom ili međunarodnom nivou obuhvataju i treninge ili seminare koje organizuju razne međunarodne organizacije u okviru CERT zajednice, kao što su TERENA (*Trans-European Research and Education Networking Association*)/TRANSIT, SANS (*System Administration, Networking, and Security*) ili ENISA, ili obuke koje organizuju specijalizovane IT kompanije.

Treba ipak napomenuti da su ovi treninzi jako dobri za nove timove, koji tek grade svoje znanje i iskustvo, ali ih stariji i zreliji timovi ponekad smatraju previše jednostavnim, a postoji i generalno mišljenje da je čak i na tlu cele Evrope teško doći do kvalitetnog treninga koji ide dovoljno duboko u tehničke detalje, i da se takve obuke najčešće organizuju samo na terotiriji SAD.

5.3.4.4 Načini i bezbednost komunikacije

Za konstituente, i sve one koji imaju potrebu da prijave bezbednosni incident, važno je da znaju na koji način to mogu da učine, tj. kako mogu da kontaktiraju nacionalni CERT. U današnje vreme, standard za sve nacionalne CERT organizacije jeste da imaju svoj Internet sajt gde su objavljeni detalji o kontaktima (poželjno i na engleskom jeziku). Elektronska pošta (osigurana PGP-om) je preferirani način komunikacije, a trebalo bi da postoje i dostupne telefonske linije. Širem krugu konstituenata omogućava se i komunikacija preko *web* formi na Internet sajtu organizacije. Naravno, neki od specifičnih konstituenata, kao što su državne institucije, ili operatori ključne informacione infrastrukture, kontakt najčešće obavljaju preko telefona.

Osim što su javno dostupni na Internet sajtu organizacije, kontakti se objavljuju i na razne druge načine, na primer tokom sastanaka sa konstituentima, u zvaničnim pismima, na prezentacijama, konferencijama, seminarima, pa čak i preko društvenih mreža. Konstituenti su generalno zadovoljni načinima za kontakt i razmenu informacija, ali napominju da bi razmena informacija trebalo da bude u većoj meri automatizovana.

Bezbednost komunikacije se najčešće osigurava PGP enkripcijom, ili korišćenjem S-MIME, ACID, CHIASMUS, HTTPS (uopšteno SSL), SSH, ili kriptovanom komunikacijom sa javnim institucijama. Takođe, potrebno je obezbediti i redundansu u komunikacionim kanalima (korišćenjem usluga više različitih telekomunuikacionih operatora) radi održanja kontinuiteta poslovanja u kriznim situacijama.

5.3.4.5 Režim rada 24/7

Rad nacionalne CERT organizacije u režimu dostupnosti 24/7/365 omogućava njenim konstituentima da prijave bezbednosni incident u bilo koje vreme, što povećava nivo poverenja između nacionale CERT organizacije i korisnika njenih servisa. Velika većina organizacija radi u ovakvom režimu dostupnosti, sa tendencijom da sve CERT organizacije funkcionišu na ovaj način, tj. da izgrade svoje resurse kako bi to mogli da podrže. Za slučaj da ne postoji osoblje dostupno na radnom mestu van redovnog radnog vremena, uvek postoji osoba koja je na dežurstvu i dostupna preko telefona ili na neki drugi način.

5.3.4.6 Mere fizičkog obezbeđenja

S obzirom da nacionalne CERT organizacije raspolažu poverljivim informacijama, što onim koje dobiju od svojih konstituenata, što od timova drugih zemalja, potrebno je obratiti posebnu pažnju i na fizičko obezbeđenje prostorija u kojima tim funkcioniše. U najvećem broju slučajeva radne prostorije obezbeđuje fizičko obezbeđenje u režimu 24/7, uz pristup prostorijama preko identifikacionih kartica. Ima i slučajeva kada CERT tim, koji ima prostorije u okviru svoje matične organizacije, ima odvojeni ulaz u svoj deo objekta. Takođe, ponekad se eventualnim posetiocima ne dozvoljava upotreba nikakvih ličnih uređaja u prostorijama tima.

5.3.4.7 Upravljanje kvalitetom bezbednosti

Radi upravljanja kvalitetom servisa nacionalni CERT timovi treba da imaju sistem preko kojeg mogu da prate svoj učinak što doprinosi konstantnom poboljšanju nivoa usluga koje nude, a samim tim doprinosi i informacionoj bezbednosti. Ipak tek nešto više od polovine nacionalnih CERT organizacija imaju izvesne procese upravljanja kvalitetom servisa bazirane na različitim standardima (ISO 27001, ISO 9001). Takođe, pokazala se kao jako korisna upotreba alata za servis upravljanja incidentima, u smislu beleženja i praćenja statusa incidenata preko *ticketing* sistema, pri čemu se najčešće koriste OTRS (*Open-source Ticket Request System*), RTIR (*Request Tracker for Incident Response*) ili *Abuse Helper* sistemi.

5.3.4.8 Najbolje prakse i uloga nacionalnih CERT timova u širenju bezbednosne terminologije

Identifikacija, prilagođavanje i primena najboljih praksi koje se preuzimaju od drugih organizacija u okviru zajednice, je dobar način da se poboljša proces upravljanja kvalitetom servisa CERT organizacija. Ove najbolje prakse se odnose na primenu formi za prijavu incidenata, primenu šema za klasifikaciju informacija, i sve druge aktivnosti koje se tiču prioritetizacije i obaveštavanja o incidentima. Kao izvori najbolje prakse, najčešće se uzimaju primeri koje daju međunarodne organizacije u okviru CERT zajednica, kao što su ENISA ili CERT/CC (CERT *Coordination Center*).

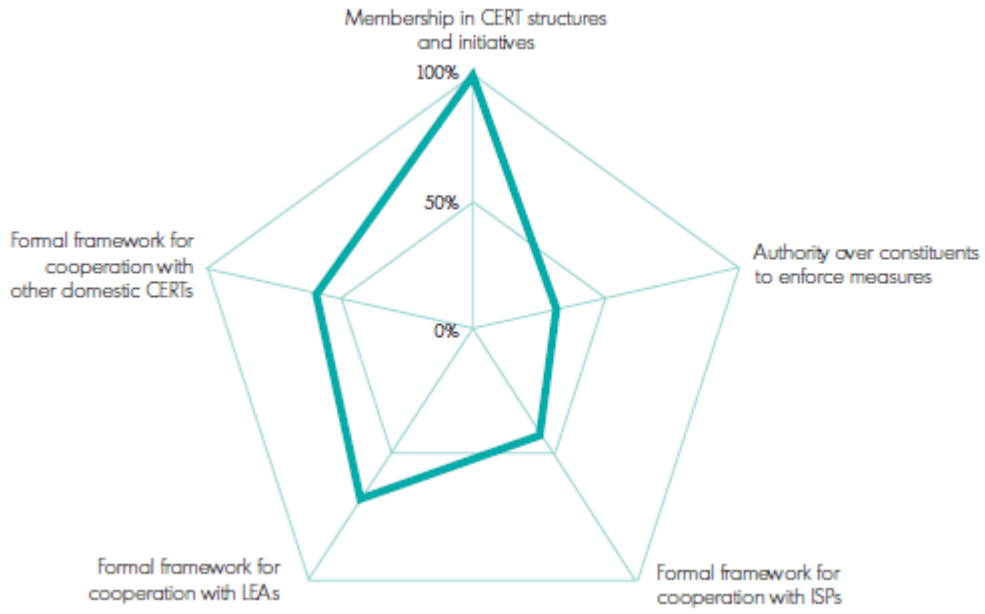
Lekcije koje se nauče, i veštine i ekspertiza koji se vremenom grade, mogu se dalje koristiti za širenje i definisanje terminologije na temu informacione bezbednosti na nacionalnom nivou. Više od dve trećine nacionalnih CERT timova učestvuje u ovakvim aktivnostima.

5.3.5 Saradnja

S obzirom na globalnu prirodu informacione bezbednosti, potrebno je da nacionalne CERT organizacije uspostave što je više moguće veza sa svojim konstituentima, kao i činiocima ključne informacione infrastrukture svoje zemlje. U tom smislu važno je da mandat nacionalne CERT organizacije bude precizno definisan, tako da nema sukoba među raznim CERT organizacijama na domaćoj sceni. Ipak, čest je slučaj da se preporuke nacionalne CERT organizacije ne mogu sprovesti u delo, tj. da se konstituenti prema njima odnose po sopstvenom nahođenju.

Takođe, nacionalne CERT organizacije često su u prilici da sarađuju sa istražnim i pravosudnim organima, po pitanjima informatičkog kriminala. Međutim, ova saradnja je uglavnom jednostrana, s obzirom da su istražni organi često ograničeni u mogućnostima razmene informacija dok traje neka istraga.

Jednako mnogo napora se ulaže i u međunarodnu saradnju na polju informacione bezbednosti, u čemu nacionalne CERT organizacije imaju nezamenljivu ulogu. Nacionalne CERT organizacije zemalja članica EU angažovane su u raznim međunarodnim i evropskim forumima, kao što su FIRST, TF-CSIRT, *Trusted Introducer* i ENISA. Preduslov za prijem u ove organizacije su procedure koje treba da obezbede da je jedna nacionalna CERT organizacija prepoznata od drugih timova kao sposobna i od poverenja u borbi za informacionu bezbednost. Na slici 5.7 dat je prikaz implementacije nekih aspekata kapaciteta za saradnju CERT organizacija.



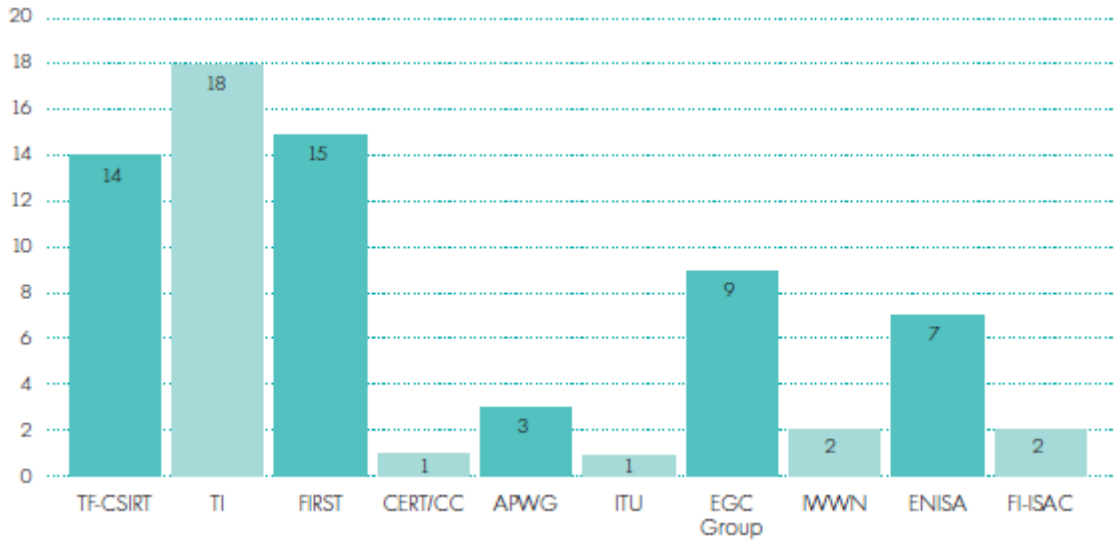
Slika 5.7: Prikaz implementacije nekih aspekata kapaciteta za saradnju CERT organizacija

Na slici 5.7 vidi se da su sve nacionalne CERT organizacije u Evropi uključene u asocijacije CERT organizacija, ili se kreću u tom smeru (ako su u pitanju tek formirani timovi), dok su okviri za saradnju sa domaćim konstituentima i partnerima manje formalni.

5.3.5.1 Članstvo u CERT strukturama i inicijativama

Članstvo u različitim CERT inicijativama široko je rasprostranjeno među nacionalnim CERT organizacijama u Evropi, gde su osim par izuzetaka, sve organizacije članice jedne ili više ovih inicijativa. Najčešće strukture kojima nacionalne CERT organizacije pripadaju su *Trusted Introducer*, FIRST i TF-CSIRT. Još neke od popularnih su EGC grupa, ENISA-ine radne grupe i *Anti-Phishing Working Group* (APWG). Vrednost ovih inicijativa u pogledu saradnje i razmene informacija u velikoj meri zavisi od tipa organizacije. Postoji generalno mišljenje među nacionalnim CERT-ovima, da su ove organizacije pogodne za susrete sa drugim CERT organizacijama u okviru zajednice, ali i da bi one mogle biti efikasnije u pogledu deljenja tehnoloških platformi za razmenu podataka o incidentima u realnom vremenu.

Raspodela nacionalnih CERT organizacija u Evropi po različitim međunarodnim inicijativama prikazana je na slici 5.8.

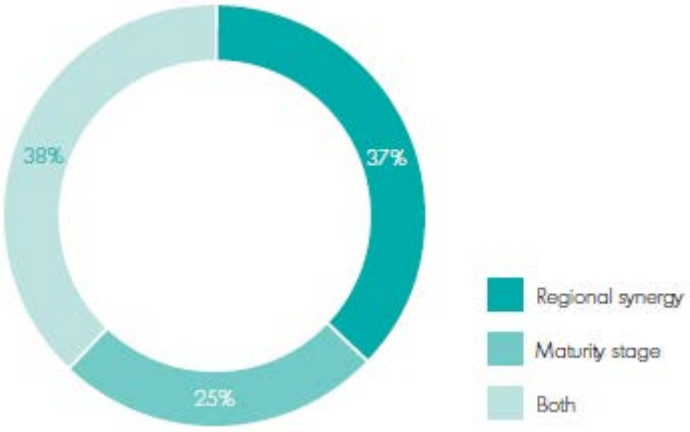


Slika 5.8: Raspodela nacionalnih CERT organizacija u Evropi po različitim međunarodnim inicijativama (ITU- *International Telecommunication Union*, IWWN- *International Watch and Warning Network*, FI-ISAC-*Financial Services Information Sharing and Analysis Center*)

5.3.5.2 Bilateralna saradnja

Osim što učestvuju u različitim međunarodnim inicijativama, nacionalne CERT organizacije aktivno sarađuju sa ekvivalentnim organizacijama u drugim zemljama, na nivou Evrope i globalno. One to čine na bazi zajedničkih interesa, radi deljenja znanja i ekspertize, kao i radi saradnje na specifičnim zadacima koji su vezani za neki geografski region, ili između dve ili više susednih zemalja.

U mnogim slučajevima, saradnja se uspostavlja na bazi hitnih potreba da se odgovori na neku bezbednosnu pretnju. U nekim drugim slučajevima saradnja funkcioniše na bazi redovnih sastanaka ili razmene informacija, najčešće putem elektronske pošte, telefonskih razgovora, na konferencijama i slično. Priroda ove saradnje je obično neformalna, naročito kada nacionalne CERT organizacije žele da razmene iskustva i dobre prakse. Ponekad postoje i formalni ugovori o saradnji u formi Memoranduma o razumevanju između dve organizacije. U slučajevima kada je neophodna operativna saradnja potpisuju se i ugovori o poverljivosti informacija (NDA – *Non-Disclosure Agreement*). U svakom slučaju, formalizacija saradnje, koja za sobom povlači pravnu odgovornost, često je ometajući faktor za efikasnu saradnju među članovima timova, i zbog toga se ponekad izbegava, a kao dva najvažnija faktora za dobru saradnju ističu se regionalna povezivanja i ujednačeni nivoi zrelosti, tj. sposobnosti timova. Učešće različitih faktora u saradnji među različitim CERT organizacijama prikazano je na slici 5.9.



Slika 5.9: Učešće različitih faktora u saradnji među različitim CERT-ovima

5.3.5.3 Važnost kriterijuma poverenja za saradnju među nacionalnim CERT-ovima

Saradnja između različitih CERT organizacija generalno se zasniva na poverenju. Bez poverenja ne bi bilo razmene informacija, niti volje da se zajednički radi na razrešavanju bezbednosnih incidenata. Osnovni kriterijumi kojima se CERT organizacije rukovode u izgradnji poverenja sa drugim organizacijama su: dokazana tehnička ekspertiza, članstvo u CERT inicijativama, sposobnost da se tim brzo i aktivno uključi u razrešavanje incidenata, kao i stabilnost tima.

5.3.5.4 Nivoi ovlašćenja

Nacionalne CERT organizacije često imaju mala ovlašćenja u odnosu na široke krugove svojih konstituenata, u smislu primoravanja konstituenata da sprovedu neke specifične zaštitne mere. U tom smislu u nekim zemljama postoje inicijative da se ova problematika zakonski reguliše. U najvećem broju slučajeva veza između nacionalnih CERT organizacija i njihovih konstituenata je neformalna i neobavezujuća, mada postoji tendencija da se određena polja saradnje definišu i utvrde ugovornim obavezama. Ovo može uključivati na primer kodeks ponašanja u slučaju pojave velikih bezbednosnih incidenata, kojeg se konstituenti moraju pridržavati kada se radi o merama bezbednosti u njihovim mrežama.

Takođe, saradnja između nacionalnih CERT-ova i provajdera telekomunikacionih servisa i Interneta, je najčešće na dobrovoljnoj bazi, osim u retkim slučajevima zemalja gde je ta saradnja na određenim poljima definisana striktnim ugovorima. Neformalna saradnja podrazumeva povremene sastanke i razgovore sa predstavnicima operatora na *ad hoc* bazi.

5.3.5.5 Saradnja sa istražnim i pravosudnim organima

Razmena informacija o incidentima između nacionalnih CERT organizacija i istražnih organa u državi, može biti od velike važnosti u borbi protiv informatičkog kriminala. Informacije koje prikupe CERT organizacije tokom svojih testiranja mogu da pomognu istražnim organima u njihovim radnjama. Isto tako, istražni organi mogu svojim podacima da pomognu u razrešavanju bezbednosnih incidenata i napada na informacione sisteme. Takođe,

s obzirom da CERT organizacije često nemaju ovlašćenja da narede sprovođenje određenih mera, one to mogu da forsiraju kroz istražne ili pravosudne organe.

Ankete pokazuju da većina nacionalnih CERT organizacija imaju saradnju sa istražnim organima u okviru svoje zemlje, i ocenjuju je kao pozitivnu. Ta saradnja se u više od 70% slučajeva bazira na potpisanim ugovorima, tj. formalizovana je u mnogo većoj meri od saradnje sa drugim entitetima. U nekim slučajevima ova saradnja može biti jednosmerna, pre svega u situacijama kada istražni organi ne smeju da dele informacije sa drugim entitetima dok traje istraga o nekom krivičnom delu, a kada jednom dođu u priliku da te informacije objave one najčešće više nisu relevantne. Za razliku od domaćih istražnih organa, saradnja sa međunarodnim istražnim organima se među nacionalnim CERT organizacijama najčešće ocenjuje kao zanemarljiva.

5.3.5.6 Radne grupe i asocijacije za saradnju unutar države

Oko 60% nacionalnih CERT organizacija organizovalo je radne grupe, ili druge tipove zajedničkih aktivnosti, kojima se članovi informaciono bezbednosne zajednice okupljaju na redovne sastanke gde se razmenjuju informacije i znanja. Radne grupe obično okupljaju različite CERT organizacije u okviru države, ili širi krug organizacija koje se bave informacionom bezbednošću, kao što su telekom i internet provajderi, akademske institucije, javna administracija, predstavnici zakonodavstva, predstavnici bankarskog sektora, i slično. U retkim slučajevima ove grupe uključuju predstavnike državnih bezbednosnih agencija ili vojske. Ove radne grupe se sastaju dva do tri puta godišnje.

Smisao postojanja radnih grupa je da omoguće redovnu razmenu ideja, priliku da se izgrađuju standardi, postave očekivanja, diskutuje o evoluciji bezbednosnih pretnji i incidenata, i možda najvažnije – da se izgrađuje međusobno poverenje među učesnicima ovih foruma. Ipak, postoje i neka ograničenja u funkcionisanju ovih radnih grupa, a ona se najčešće tiču nemogućnosti pojedinih učesnika da učestvuju u deljenju informacija jer ih u tome sprečavaju oštri propisi u okviru delatnosti kojom se bave, ili odnosi sa konkurencijom.

5.3.5.7 Poseban odnos prema provajderima ključne informacione infrastrukture

Nacionalne CERT organizacije opslužuju širok krug konstituenata, sa različitim stepenom implementacije informacione infrastrukture i rešenja, i to od nacionalnih telekomunikacionih operatora do velikih privatnih multinacionalnih kompanija sa mrežama u više zemalja. S tim u vezi, nacionalne CERT organizacije imaju izazov kako da pozicioniraju svoje servise i da se na odgovarajući način odnose prema različitim potrebama svojih konstituenata.

U takvim uslovima može se desiti da neke organizacije dobijaju veći nivo pažnje, na račun nekih drugih, imajući u vidu ograničene resurse nacionalnih CERT organizacija. Stanovište većine nacionalnih CERT organizacija je da nivo pažnje koja se poklanja nekom korisniku mora da zavisi od kritičnosti koju infrastruktura te organizacije ima po nacionalnu bezbednost. Tu se pre svega misli na kompanije koje se bave energetikom, vodosnabdevanjem, finansijama, nacionalnom bezbednošću i drugim. S obzirom na ovu činjenicu, ove kompanije bi morale imati i veću obavezu da se povinuju zahtevima za informacionom bezbednošću, nego male kompanije koje nemaju taj značaj. To naravno ne sme da znači da ove druge mogu da budu manje oprezne, a dodatno, ranjivosti nekih tehnologija i infrastrukture predstavljaju jednaku pretnju bez obzira na veličinu ili tip organizacije koja tu tehnologiju koristi.

6. ORGANIZACIONA STRUKTURA NACIONALNOG CERT-A

Kada je reč organizacionoj strukturi CERT organizacija, treba se osvrnuti na različite aspekte, kao što su predlog same (interne i eksterne) organizacione strukture, tj. modela organizacije, ali i predlog ljudskih i materijalnih resursa. Takođe, u ovom poglavlju biće reči i o elementima operativnog delovanja, kao i o četiri osnovna aspekta operativnog delovanja: osnovnim politikama, osiguranju kontinuiteta poslovanja, upravljanju bezbednošću i upravljanju ljudskim resursima tima.

6.1 PREDLOG INTERNE I EKSTERNE ORGANIZACIONE STRUKTURE

Odgovarajuća organizaciona struktura CERT organizacije u mnogome zavisi od postojeće strukture njene krovne organizacije, kao i konstituenata koje treba da opslužuje. Takođe, ona zavisi i od dostupnosti, tj. mogućnosti da se u CERT organizaciji zaposle, ili po potrebi angažuju, iskusni eksperti na polju informacione bezbednosti.

Tipična CERT organizacija podrazumeva sledeće uloge u okviru tima:

- direktor/rukovodilac organizacije,
- osoblje opštih poslova:
  - asistent rukovodioca organizacije,
  - računovođa,
  - konsultant za komunikacije sa javnošću,
  - konsultant za pravne poslove,
- operativno tehničko osoblje:
  - rukovodilac tehničkog tima,
  - tehničko osoblje koje rade na isporuci servisa,
  - istraživači/analitičari,
- eksterni konsultanti koji se angažuju po potrebi.

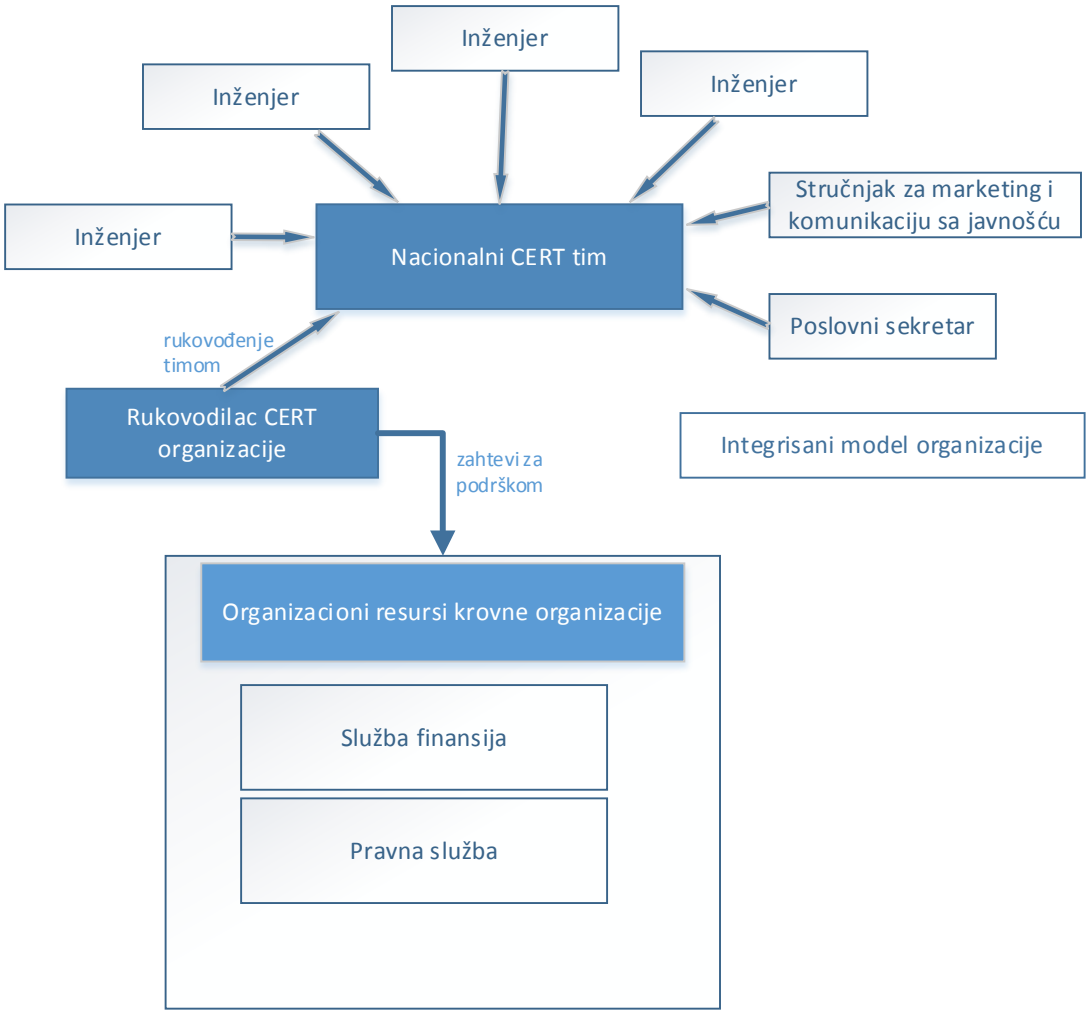
Treba napomenuti da je izuzetno važno imati na raspolaganju specijalistu za pravne poslove, naročito u početnoj fazi rada CERT organizacije. Time se podižu troškovi ljudstva,

ali se istovremeno mnogo dobija na uštedi u vremenu, i izbegavanju eventualnih problema po pravnim pitanjima u budućnosti.

Takođe, u zavisnosti od nivoa „tehnološke pismenosti“ konstituenata, a naročito ukoliko je prisustvo CERT organizacije jako izraženo u medijima i na javnoj sceni uopšte, pokazalo se veoma korisnim da u okviru CERT tima postoji i ekspert za komunikacije sa javnošću. Njegov posao je da se fokusira na „prevođenje“ teške tehnološke tematike i sadržaja na jezik, odnosno poruke, koje su razumljive širokom krugu konstituenata, partnera u medijima, ili javnosti uopšte. Naravno, princip važi i u obrnutom smeru, ekspert za komunikacije može obezbediti i povratne informacije od konstituenata i javnosti, za potrebe tehničkog dela CERT tima, olakšavajući time sveukupnu komunikaciju između ovih entiteta.

Postoji više različitih organizacionih modela za CERT organizacije. CERT organizacija može biti u potpunosti nezavisna sa svim sopstvenim funkcijama i osobljem, može biti integrisana u svoju krovnu organizaciju odakle crpi neke neophodne materijalne ili ljudske resurse, može biti distribuirana na više entiteta koji obavljaju sličan posao na različitim lokacijama, ili može biti formirana od strane grupe eksperata na neformalnoj i dobrovoljnoj bazi.

S obzirom na prirodu i ciljeve Nacionalnog CERT-a Republike Srbije, kao i činjenicu da se on formira od strane RATEL-a, kao krovne organizacije, najsvrsishodnije je da se ova organizacija formira po integrisanom modelu, prikazanom na slici 6.1.



Slika 6.1: Integrisani model organizacije

Kao što se sa slike 6.1 može videti, ovaj model podrazumeva da ovakva CERT organizacija poseduje pre svega tehničko osoblje i rukovodioca organizacije, koji su u potpunosti posvećeni uobičajenim poslovima i servisima CERT tima, dok se za ostale funkcije, kao što su računovođa, ili pravnik, oslanjaju na ljudske resurse svoje krovne organizacije.

Kada je u pitanju broj tehničkog osoblja, veoma je teško dati striktnu procenu o tome, ali postoje neke preporuke na bazi iskustava u funkcionisanju postojećih CERT organizacija:

- da bi se pružili osnovni servisi, kao što su upravljanje incidentima i distribucija obaveštenja i upozorenja, tokom redovnog radnog vremena, potrebno je minimalno 4 zaposlena,
- za širi krug servisa, koji bi npr. obuhvatali i analizu artefakata, i otkrivanje i objavljivanje ranjivosti sistema, ili servise upravljanja kvalitetom bezbednosti (procena rizika, konsultantske usluge...), kao i za samostalno održavanje svih internih sistema, tokom redovnog radnog vremena, procena je da je potrebno minimalno 6 do 8 stalno zaposlenih, i
- u slučaju da se želi pokriti radno vreme u režimu 24/7 (sa dve smene van redovnog radnog vremena, uz rad za vikend i praznike), minimalni procenjeni broj je oko 12 stalno zaposlenih.

Takođe, kao što je već pomenuto u analizi nacionalnih CERT-ova u Evropi, u glavi 5, najveći broj CERT organizacija (njih oko 40%) ima između 11 i 15 stalno zaposlenih.

Kada je u pitanju Republika Srbija, shodno obavezama Nacionalne CERT organizacije koje proističu iz Zakona o informacionoj bezbednosti, ali i uzimajući u obzir primere dobre prakse iz drugih zemalja, pre svega zemalja članica EU, potrebno je da ona bude organizovana u režimu rada 24/7, i shodno tome treba obezbediti i odgovarajuće ljudske resurse u tehničkom timu.

U početnoj fazi razvoja CERT organizacije, uz rukovodioca tima moraju postojati još tri člana tima, tj. inženjera koji će se baviti uspostavljanjem i izgradnjom njenih tehničkih i organizacionih resursa. Pod tim se podrazumevaju uspostavljanje informacione infrastrukture za potrebe same CERT organizacije (uspostavljanje telekomunikacione infrastrukture, *e-mail* sistema, Internet portala, sistema za upravljanje incidentima ...), uspostavljanje bezbednosnih politika i procedura, uspostavljanje komunikacije sa drugim CERT oganizacijama u zemlji i inostranstvu, početak implementacije osnovnih servisa, i slično. Naravno, u ovakvom brojnom stanju moguće je obezbediti funkcionisanje organizacije tokom redovnog radnog vremena, uz mogućnost ostavljanja dežurnog kontakta za pozive i prijave incidenata van radnog vremena.

Nakon ove inicijalne faze, odnosno čim se za to steknu uslovi, potrebno je preći u potpuni režim rada 24/7 za pokrivanje osnovnih servisa, i postepeno uvoditi nove servise, i angažovati dodatno osoblje kako bi svi servisi bili kvalitetno pokriveni. Procena je da u periodu od pet godina od početka rada na uspostavljanju CERT organizacije, ona treba da ima barem 8 zaposlenih inženjera operativaca, i 3 zaposlena inženjera analitičara u tehničkom timu, koji bi se bavili svim neophodnim poslovima upravljanja incidentima u režimu 24/7. Naravno, ukoliko se u tom periodu prepozna prilika za uvođenje dodatnih usluga ili servisa na komercijalnim osnovama, koje bi bile izvor dodatnih prihoda za CERT organizaciju, treba razmotriti i angažovanje dodatnih eksperata iz raznih oblasti informacione bezbednosti koje su od interesa, i to kao stalno zaposlenih, ili angažovanjem po potrebi.

Kada je u pitanju netehničko osoblje (poslovni sekretar, računovođa, pravnik, ekspert za komunikacije...), procena je da u inicijalnoj fazi razvoja CERT organizacije, na većini pozicija, ne postoji potreba za angažovanjem takvih ljudi u punom radnom vremenu. Otuda predlog da se CERT organizacija kreira po integrisanom modelu, kako bi se koristile

odgovarajuće službe krovne organizacije, tj. RATEL-a, i time smanjili troškovi za ovaj profil zaposlenih. Od prve godine, neophodno je angažovanje poslovnog sekretara u punom radnom vremenu, ali je angažovanje pravnika i ekonomiste procenjeno na pola radnog vremena, bez potrebe da se tokom vremena to angažovanje povećava, uz mogućnost da se angažovanje ekonomiste čak i smanji na 30% radnog vremena. Angažovanje stručnjaka za marketing i komunikacije sa javnošću neophodno je planirati u drugoj godini poslovanja CERT organizacije, i to u punom radnom vremenu. Dinamika zapošljavanja, odnosno kumulativna raspodela zaposlenih tokom prvih pet godina rada CERT organizacije, prikazani su u tabelama 6.1 i 6.2.

Tabela 6.1: Dinamika zapošljavanja tokom prvih pet godina rada CERT-a

Dinamika zapošljavanja	Direktor	Inženjer - operativac	Inženjer - analitičar	Sekretarica	Pravnik	Marketing stručnjak	Ekonomista
1. godina	1	2	1	1	0.5		0.3+0.2*
2. godina		2	1			1	
3. godina		1	1				
4. godina		3					
5. godina							
Ukupno:	1	8	3	1	0.5	1	0.3

* - jedino u prvoj godini se zahteva nešto veće angažovanje stručnjaka ekonomske struke

Tabela 6.2: Kumulativna raspodela tokom prvih pet godina rada CERT-a

Kumulativna raspodela zaposlenih	Direktor	Inženjer - operativac	Inženjer - analitičar	Sekretarica	Pravnik	Marketing stručnjak	Ekonomista
1. godina	1	2	1	1	0.5	0	0.5
2. godina	1	4	2	1	0.5	1	0.3
3. godina	1	5	3	1	0.5	1	0.3
4. godina	1	8	3	1	0.5	1	0.3
5. godina	1	8	3	1	0.5	1	0.3

6.2 PREDLOG MATERIJALNIH RESURSA

6.2.1 Elementi operativnog delovanja

Elementi operativnog delovanja su gradivni blokovi funkcionisanja CERT tima, koji se odnose na sve aspekte poslovanja, od sistema elektronske pošte, do radnog vremena. U daljem razmatranju biće analizirani elementi koji su u vezi sa pružanjem servisa za upravljanje incidentima, kao najbitnije aktivnosti svakog CERT tima.

6.2.1.1 Radno vreme

Ovaj element definiše razliku između redovnog radnog vremena i aktivnosti van tog vremenskog okvira, i uključuje organizaciju smenskog rada (uključujući i angažovano osoblje), angažovanje van radnog vremena (npr, obezbeđenje i kontakt centar), dežurstva i aktivnosti u vanrednim okolnostima. Kada se govori o radnom vremenu, važno je imati na umu da je posle dva sata rutinskog posla potrebno organizovati pauzu, ali i da je jedan sat napornog posla u stresnoj situaciji razrešavanja incidenata dovoljno da iscrpi koncentraciju osoblja. Kada se planira radno vreme najvažnije je obezbediti kontinuitet u radu, jer je to jedan od najvažnijih ciljeva CERT organizacije.

6.2.1.2 Telekomunikacioni servisi

Ovaj element podrazumeva tradicionalne telekomunikacione servise kao što su telefon, faks, mobilni telefon, govorni automati, *call* centar, i slično. Ovaj tehnološki element (zajedno sa drugim komunikacijama) je neophodan kako bi CERT organizacija i njeni članovi bili dostupni u skladu sa svojim potrebama i obavezama, tj. kako bi bili u mogućnosti da uspostave komunikaciju sa svojim konstituentima i drugim entitetima. Implementacija ovih servisa zavisi od misije CERT tima i karakteristika njegovih servisa.

Treba imati u vidu da ne postoji apsolutna dostupnost ovakvih servisa, tj. da se može desiti da sistemi fiksne ili mobilne telefonije nekada ne rade, ili da postoje situacije u kojima se članovi tima ne jave na poziv, koji god da je razlog u pitanju. Takođe, konstituenti će generalno biti nezadovoljni ukoliko se iz više pokušaja niko ne javi na njihov poziv, ili im se u trenucima hitne potrebe umesto osobe javi govorni automat. Ukoliko tom prilikom ostave poruku i niko im se ne javi u roku od 15-tak minuta, to je još jedan razlog za dodatno nezadovoljstvo. U ovakvim situacijama od izvesne koristi može biti servis govorne pošte, gde konstituenti mogu dobiti potvrdu da je njihov poziv registrovan i kakvu dalju akciju mogu da očekuju i u kojim vremenskim okvirima.

6.2.1.3 Elektronska pošta

Potreba za kvalitetnim sistemom elektronske pošte je nešto što se u današnjem poslovanju podrazumeva. Takođe, tehnološki je moguće kreirati robustan sistem koji je jednostavan za korišćenje, a u isto vreme je u skladu sa najmodernijim težnjama i standardima u pogledu vrste poruka koje se prenose i bezbednosti komunikacije. Međutim, s obzirom na dodatne zadatke i potrebe koji se postavljaju pred CERT timove (kvalitetan metod filtriranja poruka, kvalitetan sistem pretraživanja poruka, alati za slanje automatskih odgovora ...), implementacija ovakvog sistema nije tako lak zadatak.

Uobičajeno je da CERT timovi sami implementiraju svoje sisteme za razmenu elektronske pošte, na bazi standardnih alata, i korišćenjem dodatnih alata ili skripti kojima se postižu nestandardne funkcionalnosti koje zadovoljavaju njihove specifične potrebe. Takođe, jako je dobro i u praksi se pokazuje kao korisno da postoji neki interfejs između sistema elektronske pošte i sistema za upravljanje procesima rada, kako bi se većina informacija koje pristižu u CERT organizaciju na odgovarajući način i „automatski“ integrisala u informacioni sistem organizacije. Sistem elektronske pošte je jednostavan način za razmenu informacija, a ukoliko se npr. na njega na neki način nadogradi funkcionalnost za prioritetizaciju dolaznih poruka, to onda može biti način da se značajno poveća efikasnost rada CERT organizacije. Ovaj način komunikacije zapravo štedi puno vremena članovima CERT tima, za razliku od npr. direktnog razgovora sa korisnicima servisa, iako postoje situacije kada je tu vrstu

interakcije nemoguće izbeći. U svakom slučaju, treba voditi računa o tome da, koji god sistem komunikacije da se koristi, konstituenti će uvek očekivati neku povratnu informaciju, i to u što je moguće kraćem roku.

6.2.1.4 Alati za upravljanje procesom rada

Alati kojima se omogućava upravljanje procesima rada, i protok informacija, zadataka i obaveza između zaposlenih koji rade u različitim sekcijama CERT organizacije, ili u različitim smenama, su od ključne važnosti za operativno delovanje timova koji su suočeni sa velikim obimom posla. Pod „alatom“ se u ovom smislu podrazumeva softver, tj. baza podataka i odgovarajući program, kojim se omogućava CERT timu da prati tok ili dodaje neophodne informacije o događajima koji su mu od interesa (kao što su bezbednosni incidenti, tekući zahtevi ili analize ...). Naravno, bitan parametar ovakvih alata je i njihova bezbednost, bilo da se koriste u zaštićenom okruženju (unutar lokalne mreže CERT organizacije), ili da je neophodno pristupiti im spolja. Kao što je ranije već pomenuto, dobro je i da postoji mogućnost da se ovakav sistem spregne sa sistemima elektronske pošte, i telekomunikacionim servisima generalno, kako bi se što više automatizovao proces prikupljanja informacija.

6.2.1.5 Internet stranica

WWW (*World Wide Web*) je u današnje vreme sveprisutni i najpopularniji medijum koji se koristi za razmenu informacija, i stoga se podrazumeva za jedan od bitnijih elemenata infrastrukture CERT timova. Jasno je da *web* servisi, ili bilo koji serveri ili informacije CERT organizacije koji su javno dostupni preko Interneta, moraju biti implementirani na bezbedan način kako bi se izbegla situacija da se sadržajem tih informacija ili servisa manipuliše bez odgovarajuće autorizacije. Jedan od načina bezbedne implementacije podrazumeva da se *web* serveri zaštite u DMZ (*demilitarized zone*) zoni mreže CERT organizacije, zaštićeni *firewall* uređajima, sa odgovarajućim bezbednosnim polisama i procedurama koje podrazumevaju redovno praćenje i kotrolu bezbednosti sistema. Dodatni način da se sačuva autentičnost i integritet podataka je da se podaci čuvaju na glavnim serverima koji su u lokalnoj mreži CERT organizacije, zaštićeni od pristupa spolja, i da se kopije podataka na redovnoj bazi, tj. u određenim vremenskim razmacima prebacuju na javno dostupan *web* server. Naravno, preporučuje se i primena raznih kriptografskih tehnika radi dodatne zaštite.

6.2.1.6 Upotreba IP adresa i domena (DNS - Domain Name System)

Da bi se interna mreža, iz razloga bezbednosti, odvojila od svih drugih mreža, potrebno je da CERT organizacija poseduje određeni broj javnih IP adresa koje će koristiti za svoje potrebe, nezavisno od svoje krovne organizacije, ili nekog drugog entiteta. Naravno, CERT organizacija može koristiti i privatne opsege IP adresa za potrebe adresiranja u svojoj lokalnoj mreži, i implementirati NAT (*Network Address Translation*) funkcionalnost na *firewall* uređajima ka javnoj Internet mreži.

Kada je u pitanju DNS sistem, treba voditi računa da osetljive informacije, kao što su operativni sistem na kojem sistem radi, ili kompletna lista internih sistema u organizaciji, nikada ne budu javno dostupne, jer to može da pomogne napadačima u izvođenju akcija protiv CERT organizacije. Najbolja praksa je da CERT organizacija registruje Internet domen odgovarajućeg naziva, preko kojeg će promovisati svoje postojanje i misiju, i biti lako dostupna za svoje kostituente, kao i druge entitete radi razmene informacija.

6.2.1.7 Bezbednost mreže i sistema

U okviru svake CERT organizacije, svi interni sistemi, mreža i konekcije sa spoljnjim sistemima ili mrežama, moraju biti implementirani i konfigurisani na način da se obezbedi maksimalna bezbednost i otpornost na bezbednosne napade. To znači da je potrebno na odgovarajući način segmentirati i zaštiti lokalnu mrežu, prema različitim funkcijama u okviru CERT organizacije, i obezbediti da svaki segment mreže ima izlaz ka drugim segmentima ili javnoj Internet mreži preko naprednih *firewall* uređaja, radi maksimalne bezbednosti. U najmanju ruku, potrebno je da postoje dva segmenta u internoj mreži: operativna mreža, gde su implementirani svi sistemi koje CERT organizacija koristi za svoje servise, i mreža za sprovođenje bezbednosnih testova ili analiza artefakata (ukoliko CERT tim uopšte sprovodi takve aktivnosti). Ova dva segmenta treba međusobno povezati samo ukoliko je to apsolutno neophodno, i to preko *firewall* uređaja, uz maksimalno restriktivne polise pristupa iz jedne u drugu mrežu. Naravno, moguće je ovakvo povezivanje obavljati samo „po potrebi“, na privremenoj bazi, ali i tada treba biti maksimalno oprezan i restriktivan u polisiranju saobraćaja na *firewall* uređajima.

Tip i model *firewall* uređaja koji će biti implementiran zavisi od budžeta koji je dostupan za te svrhe. Obično se *firewall* zaštita implementira kroz dve instance, jednu koja je okrenuta javnoj Internet mreži, i drugu koja opslužuje segmente interne mreže, sa odgovarajućim polisama koje omogućavaju komunikaciju lokalnih i javnih mreža. Dodatno, obično se radi dodatne zaštite klijenti iz interne mreže (računari koje koriste zaposleni u okviru organizacije, ili serveri kojima je potreban pristup Internetu) povezuju sa serverima na javnoj Internet mreži preko *proxy* servera, da bi se sprečila „direktna“ komunikacija između ovih entiteta. Takođe, svi serveri CERT organizacije koji su javno dostupni preko Interneta (*web* serveri, serveri elektronske pošte, ftp serveri ...), treba da budu smešteni u DMZ zoni mreže, tj. treba da budu odvojeni *firewall* uređajima i od lokalne mreže i od javne Internet mreže, radi kontrole pristupa i zaštite od bezbednosnih napada.

Podrazumeva se da svi sistemi u okviru CERT organizacije treba da funkcionišu na ažurnim verzijama operativnih sistema, sa implementiranim najnovijim bezbednosnim zakrpama, i da je potrebno da se u tom smislu redovno održavaju. Potrebno je implementirati sisteme i softver za prikupljanje logova sa svih sistema, i alate koji mogu pomoći u aktivnostima bezbednosne zaštite sistema, tj. sprečavanje neovlašćenog pristupa sistemima. Preporučuje se čak i kontrola i zaštita sistema, ili računara, koje zaposleni poseduju kod svoje kuće, a koriste ih za pristup sistemima i mreži CERT organizacije, za slučaj rada od kuće, ili u drugim sličnim situacijama.

Posebno opasna kategorija bezbednosnih napada kojima treba posvetiti pažnju, jer mogu uticati na rad, tj. dostupnost servisa CERT organizacije, su tzv. *denial-of-service* (DoS) napadi. Jedan od načina da se CERT organizacija suprotstavi ovom tipu napada je da ima konektivnost sa javnom Internet mrežom preko više različitih provajdera Internet servisa, tako da u slučaju DoS napada može da obezbedi minimum konektivnosti, tj. dostupnosti, za potrebe ključnih sistema za razmenu informacija, kao što je npr. elektronska pošta. Naravno, nove generacije *firewall* uređaja obezbeđuju manje ili više efikasnu zaštitu i od ovakvih vrsta napada, ali njihova implementacija može zavisiti od budžeta koji je na raspolaganju CERT organizaciji za te svrhe.

6.2.2 Funkcije i način realizacije Nacionalnog CERT-a u Srbiji

Prema Zakonu o informacionoj bezbednosti Republike Srbije, operatori IKT sistema od posebnog značaja imaju obavezu obaveštavanja Nadležnog organa (Ministarstvo trgovine, turizma i telekomunikacija - MTTT) što implicitno znači da će Nadležni organ morati da formira odgovarajuću organizacionu jedinicu koja će se baviti ovim poslovima. S druge strane, pošto je Nacionalni CERT podređen Nadležnom organu u smislu kontrole rada, ne postoji obaveza obaveštavanja Nacionalnog CERT-a od strane Nadležnog organa o ovim bezbednosnim incidentima. Ostavljeno je Nadležnom organu da proceni u kojoj meri će o bezbednosnim incidentima obaveštavati Nacionalni CERT. Zakonom je predviđena saradnja Nacionalnog CERT-a i posebnih CERT-ova u zemlji, ali nivo ove saradnje nije preciznije definisan. Iz prethodno navedenog proizlazi zaključak da Nacionalni CERT nije direktno odgovoran za IKT sisteme od posebnog značaja. S druge strane, u cilju profesionalnog obavljanja funkcija Nacionalnog CERT-a, u okviru istog će morati da postoji adekvatan informacioni sistem sa dovoljnim brojem stručnih kadrova. Imajući u vidu prethodno navedeno, stiče se utisak da će biti potrebno napraviti približno isti informacioni sistem na dva mesta, u okviru Nadležnog organa (MTTT) i u okviru Nacionalnog CERT-a. U cilju smanjivanja troškova i formiranja efikasnih institucija i organizacija, bilo bi opravdano da Nacionalni CERT na sebe preuzme kompletnu tehničku realizaciju informacionog sistema za prijem i obradu informacija o bezbednosnim incidentima. Pri tome, Nadležni organ bi imao potpuni pristup ovom informacionom sistemu. Navedenim načinom realizacije sistema za prijem informacija o bezbednosnim incidentima obezbedilo bi se efikasno deljenje informacija između Nadležnog organa i Nacionalnog CERT-a. Bez obzira na zajedničko korišćenje informacionog sistema, pravo odlučivanja o daljoj distribuciji informacija o bezbednosnim incidentima i dalje bi ostalo kod Nadležnog organa. Kroz zajednički informacioni sistem funkcija kontrole rada Nacionalnog CERT-a od strane Nadležnog organa će biti daleko efikasnije implementirana, jer će Nadležni organ u svakom trenutku imati puni uvid u rad Nacionalnog CERT-a.

Prethodno navedeno rešenje je i u skladu sa evropskom direktivom o mrežnoj i informacionoj sigurnosti (*Network and information security* – NIS – direktiva). U okviru NIS direktive je posebno prepoznata funkcija podrške za kritične IKT sisteme (u zakonodavstvu Republike Srbije su identifikovani kao IKT sistemi od posebnog značaja) zbog osetljivosti tih sistema. Ovakav princip rada je upravo osmišljen zbog kontrole toka osetljivih informacija koje se tiču sigurnosti IKT sistema od posebnog značaja. S druge strane, NIS direktiva ničim nije uslovila da funkcija CERT-a za potrebe IKT sistema od posebnog značaja mora da bude realizovana kao fizički poseban CERT. U evropskoj praksi postoje Nacionalni CERT-ovi kod kojih je ova funkcija objedinjena sa ostalim funkcijama Nacionalnog CERT-a. Imajući u vidu sve prethodno navedeno, ovom Studijom je predviđeno da funkcija CERT-a za potrebe IKT sistema od posebnog značaja (osim za one IKT sisteme za koje je Zakon predvideo postojanje posebnih CERT-ova) bude tehnički objedinjena sa tehničkim sistemom Nacionalnog CERT-a.

Pored prethodno opisanih funkcija Nacionalnog CERT-a, postoji veliki slobodan prostor za delovanje u oblasti informacione bezbednosti. Aktivnosti koje Nacionalni CERT može da ponudi na komercijalnoj osnovi su:

- forenzika IKT sistema u slučajevima kada je došlo do bezbednosnih incidenata,
- *security auditing* IKT sistema.
- analiza rizika IKT sistema,
- izrada politike sigurnosti prilikom korišćenja IKT sistema,
- obuka i sertifikovanje kadrova iz oblasti informacione bezbednosti,

- istraživački rad iz oblasti informacione bezbednosti i publikovanje rezultata i preporuka,
- pružanje konsultantskih usluga za postojeće i nove IKT sisteme iz oblasti informacione bezbednosti, i
- servis direktnog slanja preporuka i informacija iz oblasti informacione bezbednosti.

Sve prethodno navedene dodatne aktivnosti otvaraju prostor za ostvarivanje značajnih komercijalnih rezultata. Preduslov za sve navedene aktivnosti je postojanje odgovarajućih stručnih timova koji bi se time bavili. Na domaćem tržištu postoje komercijalne firme koje u nekoj meri pokrivaju neke od navedenih aktivnosti. S obzirom da je kod informacione bezbednosti, pored stručnosti, veoma bitan element i poverenje naručioca u sposobnosti i diskreciju izvršioca neke aktivnosti, postoji slobodan prostor za uspostavu Nacionalnog CERT-a kao pružaoca ovih usluga, koji bi bio referentna institucija za oblast informacione bezbednosti. Kod komercijalnih firmi koje pružaju usluge iz oblasti informacione bezbednosti pitanje poverenja uvek se prepliće sa sopstvenim interesima tih komercijalnih firmi i njihovim vezama sa firmama koje su konkurenti na tržištu potencijalnim korisnicima usluga iz oblasti informacione bezbednosti. Nacionalni CERT kao državno telo nema takav problem i ima mogućnost da se nametne tržištu kao referentna ustanova za oblast informacione bezbednosti.

6.2.3 Logička struktura mreže

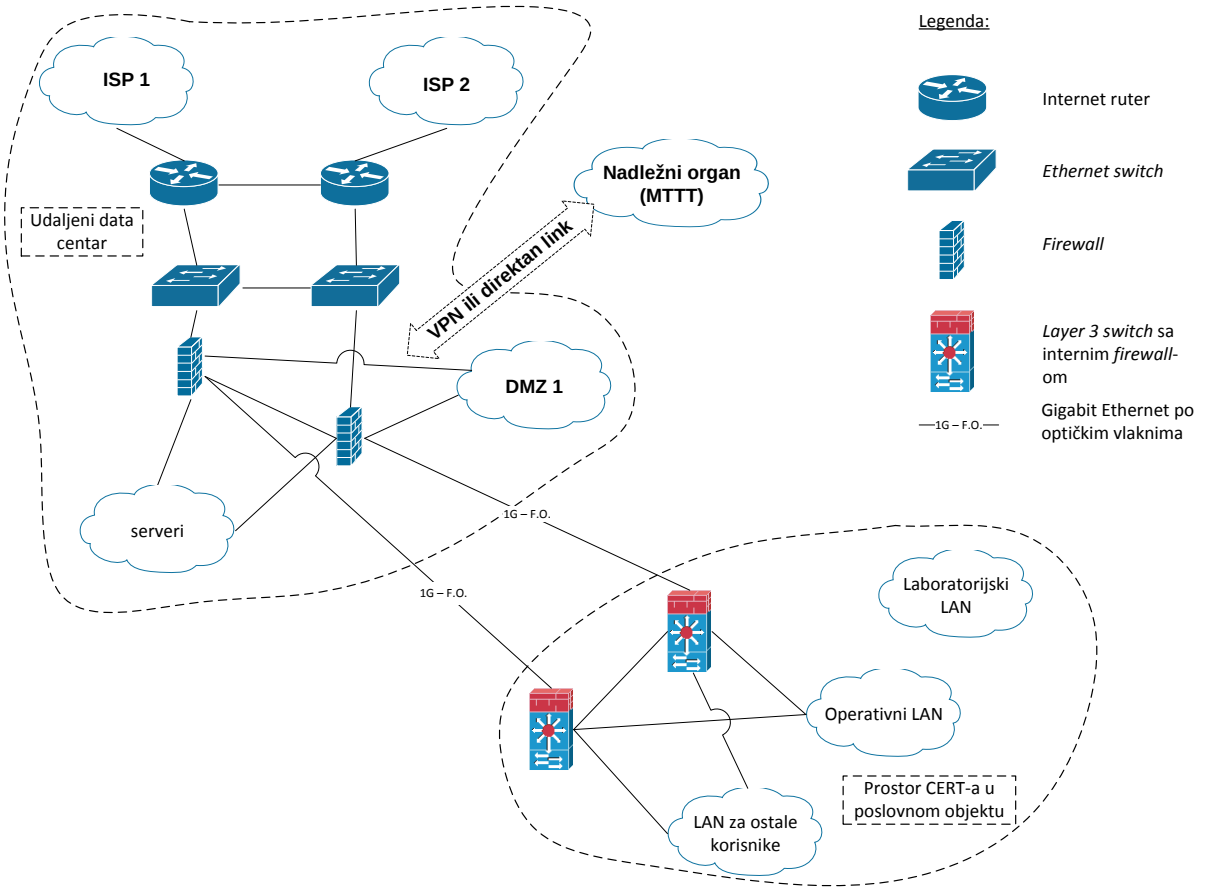
Polazeći od prethodno navedenih zahteva po pitanju operativnog rada Nacionalnog CERT-a, predložena je logička topologija mreže predstavljena na slici 6.2. Imajući u vidu potrebne tehničke resurse da bi se obezbedio smeštaj i uslovi za rad nekoliko servera koji čine informacioni sistem Nacionalnog CERT-a, RATEL se opredelio da sva kritična oprema stoji u profesionalnom *data* centru. Na slici 6.2 predloženo je rešenje kod koga se sva aktivna oprema i Internet linkovi nalaze u udaljenom *data* centru. Pošto će ljudi koji čine Nacionalni CERT sedeti i raditi u posebnom poslovnom objektu, izdvojenom u odnosu na *data* centar, potrebno je obezbediti adekvatne komunikacione kapacitete za povezivanje ove dve lokacije. Iz razloga pouzdanosti, lokaciju udaljenog *data* centra treba povezati optičkim kablovima i to po dva različita pravca tako da se izbegne mogućnost da prekidom optičkog kabla dođe do prekida komunikacije sa lokacijom Nacionalnog CERT-a. Po navedenim optičkim vlaknima bi se koristila gigabit *Ethernet* tehnologija.

Nacionalni CERT treba da ima svoj PI (*Provider Independent*) IPv4 adresni prostor veličine jedne C klase (256 adresa) i AS broj. Taj opseg treba da obezbedi osnovnu konektivnost u radu. Za potrebe rada sistema u uslovima DoS napada, potrebno je od svakog *Internet Servis Provajder*-a (ISP) uzeti manji opseg IPv4 adresa koje pripadaju navedenom ISP-u. Na tim adresama će biti rezervni sistemi koji će se koristiti u slučaju DoS napada ili sličnog problema u komunikaciji preko osnovnih PI adresa. Pored IPv4 adresnog prostora, Nacionalni CERT treba da ima i svoj IPv6 adresni prostor koji, takođe, treba da bude PI. IPv6 adresni prostor treba da se nabavi preko lokalnog Internet registra (LIR – *Local Internet Registry*).

Za potrebe povezivanja na dva različita ISP-a, potrebno je da postoje dva rutera koji mogu da prihvate kompletnu (tzv. f*ull*) BGP (*Border Gateway Protocol*) tabelu rutiranja. U slučaju pada jednog od ova dva rutera ili linka do nekog ISP-a, BGP protokol će automatski da prerutira kompletan saobraćaj na drugi link. Dva *firewall* uređaja koji se vide na slici 6.2 imaju zadatak da obezbede osnovnu zaštitu mreže Nacionalnog CERT-a od napada sa Interneta. Na *firewall* uređaje je priključena i demilitarizovana zona (DMZ 1 na slici 6.2) gde

će se nalaziti *mail* i *web* server. Na *firewall* uređaje direktno je priključena i lokalna mreža sa serverima na kojima se nalaze sve informacije o incidentima. U istoj mreži se nalazi server za nadzor i upravljanje mrežom Nacionalnog CERT-a, lokalni NTP server za sinhronizaciju tačnog vremena na svim mrežnim uređajima i radnim stanicama Nacionalnog CERT-a. Zadatak *firewall* uređaja biće i terminiranje VPN konekcija za udaljeni pristup informacionom sistemu Nacionalnog CERT-a putem Interneta.

Pristup informacionom sistemu Nacionalnog CERT-a za zaposlene kod Nadležnog organa u cilju zajedničkog korišćenja sistema za smeštanje i analizu prijava sigurnosnih incidenata može da se realizuje na dva načina. Jedan način je da povezivanje bude realizovano na isti način kako je to urađeno za Nacionalni CERT, tj. da postoji direktan link od prostorije Nadležnog organa do udaljenog *data* centra. Drugi način je da zaposleni kod Nadležnog organa koriste VPN pristup, na isti način na koji će to koristiti i zaposleni u Nacionalnom CERT-u u slučaju da se nalaze negde na terenu, izvan poslovnog prostora Nacionalnog CERT-a. Na Nadležnom organu je da izabere način pristupa informacionom sistemu koji njima najviše odgovara.



Slika 6.2: Logička struktura metro mreže Nacionalnog CERT-a

Na lokaciji poslovnog prostora Nacionalnog CERT-a nalaze se dva rutera/*layer* 3 *switch*-a sa integrisanom funkcijom *firewall*-a. Zadatak ovih uređaja je da obezbede komunikaciju između lokacije poslovnog prostora Nacionalnog CERT-a i udaljenog *data* centra, kao i da zaštite operativni LAN (deo mreže gde su povezani administratori i analitičari Nacionalnog CERT-a koji se bave operativnim poslom i koji rade sa kritičnim podacima koji moraju da budu zaštićeni). Na ovoj lokaciji se nalazi i lokalna mreža za povezivanje svih

ostalih zaposlenih u Nacionalnom CERT-u (direktor, sekretarica, pravnik, ekonomista...) koji ne rade sa kritičnim informacijama, ali imaju potrebe da pristupaju Internetu.

6.2.4 Prostorije za smeštanje opreme i ljudi

Nacionalni CERT treba da se nalazi na dve lokacije u gradu. Jedna lokacija je poslovni prostor gde će se nalaziti kancelarije i radni prostor zaposlenih u Nacionalnom CERT-u, a druga lokacija je udaljeni *data* centar u kome će se nalaziti serveri koji su neophodni za svakodnevni rad Nacionalnog CERT-a.

Za smeštanje servera i komunikacione opreme u *data* centar, potreban je jedan rek orman, visine 42U, dubine 1000 mm (tzv. serverski rek), sa metalnim vratima koja se zaključavaju i sa prednje i sa zadnje strane. Rek orman mora da ima dve nezavisne grane za napajanje električnom energijom koje su zaštićene sistemom za neprekidno napajanje. Rek orman mora da ima i sistem fizičke kontrole pristupa unutrašnjosti rek ormana. U cilju kontrole beleženja pristupa opremi, unutar rek ormana treba da se nalazi IP kamera čiji je zadatak snimanje svih aktivnosti na opremi u rek ormanu. Rek orman mora da bude opremljen sistemom detekcije otvaranja rek ormana i sistemom daljinskog očitavanja temperature vazduha, da bi administratori Nacionalnog CERT-a mogli iz svoje kancelarije da provere stanje u rek ormanu.

Na lokaciji poslovnog prostora za potrebe Nacionalnog CERT-a potrebno je izdvojiti prostor za:

- kancelariju za direktora Nacionalnog CERT-a,
- kancelariju za sekretaricu Nacionalnog CERT-a,
- kancelariju za administrativno osoblje Nacionalnog CERT-a (marketing stručnjak, pravnik i ekonomista kada dolaze u Nacionalni CERT),
- kancelariju za administratore i analitičare Nacionalnog CERT-a,
- laboratorijski prostor za rad administratora,
- prostor za sastanke, i
- rek orman za smeštanje komunikacione opreme za potrebe Nacionalnog CERT-a.

Sve kancelarije zaposlenih u Nacionalnom CERT timu, uključujući i laboratorijski prostor, moraju biti zaštićene sistemom za kontrolu pristupa (sigurnosna vrata sa šifrom, ili nekim drugim mehanizmom kontrole ulaska i izlaska). Podrazumeva se i postojanje sistema za video nadzor u prostorijama Nacionalnog CERT tima (kancelarije, ulaz, pristupni hodnik/hol). Takođe, neohodno je da članovi Nacionalnog CERT tima imaju mogućnost da borave u poslovnim prostorijama u režimu 24/7, tj. da u svakom trenutku bude moguće da uđu u prostorije, ili da ih napuste. Sve kancelarije treba da budu pokrivene sistemom za neprekidno napajanje električnom energijom. Operativno delovanje Nacionalnog CERT tima ne sme da bude dovedeno u pitanje usled nestanka električne energije u javnoj mreži.

Na osnovu prethodno navedenih zahteva, procena je da je za Nacionalni CERT potreban poslovni prostor površine 100m^2. Prilikom određivanja veličine potrebnog prostora pošlo se od pretpostavke da po jednom zaposlenom treba obezbediti minmalno 6m^2 (planirano je da Nacionalni CERT u zreloj fazi zapošljava oko 15 ljudi), dok je za smeštaj IKT opreme potrebno još oko 10 m^2.

6.2.5 Aktivna oprema

Za realizaciju sistema datog u poglavlju 6.2.4, potrebna je sledeća aktivna oprema:

- Internet ruter (2 komada) – minimalno 3 x 1000BaseT ili 1000BaseX interfejsa, podrška za BGPv4, dovoljno RAM memorije da može da prihvati 3 pune BGP tabele rutiranja, interni *firewall* za potrebe zaštite samog rutera od nedozvoljenog pristupa, sa podrškom za sledeće protokole: BGPv4, MP-BGP, IPv4 i IPv6 rutiranje, SSHv2, SNMPv3, NTP, Netflow;
- ruter/*layer* 3 *switch* za povezivanje lokacije u RATEL-u sa udaljenim *data* centrom (2 komada) – uređaj sa minimalno 4 x 1000BaseX interfejsima i sa integrisanom *firewall* funkcionalnošću, sa podrškom za sledeće protokole: OSPFv2 i OSPFv3, IPv4 i IPv6 rutiranje, SNMPv3, SSHv2, NTP, Netflow;
- *firewall* (2 komada) – uređaj sa minimalno 5 x 1000BaseT interfejsima, sposobni da rade *load balancing* saobraćaja u *active/active* režimu. Zadatak ovog *firewall* uređaja je zaštita mreže od upada sa Interneta, interna kontrola pristupa zaštićenim serverima u serverskoj mreži i u DMZ-u, i terminiranje VPN tunela udaljenih korisnika;
- *workgroup switch* (6 komada) – namena ovih *Ethernet switch*-eva je povezivanje komunikacione opreme, servera i radnih stanica; minimalno 24 x 10/1000BaseT interfejsima, upravljivi, sa podrškom za sledeće protokole: SSHv2, SNMPv3, LACP, Rapid STP, IEEE 802.1x, Radius, *Port-based* VLAN, BPDU *Guard*, *port autonegotiation*, *Automatic media-dependent interface crossover*, IGMP *snooping* v1 i v2, *Switch Port Analyzer*, *Remote Switch Port Analyzer*, NTP *synchronization*;
- serveri za informacioni sistem na kojima će se čuvati podaci o incidentima (2 komada);
- serveri za *mail* podsistem (3 fizička servera). – *Mail* podsistem se sastoji od dva *mail* servera čiji je zadatak prijem i distribucija *e-mail* poruka, dva servera za anti spam i anti virus proveru svih poruka i jednog servera na kome će se nalaziti sami nalozi korisnika;
- server za DNS servis (1 komad);
- server za *web* portal (2 komada) – Na ovom serveru treba da se nalazi *web* stranica Nacionalnog CERT-a sa portalom za prijem prijava o sigurnosnim incidentima. Zbog važnosti ovog servisa, ovaj server mora da bude udvojen;
- oprema za laboratorijski LAN: serveri (2 komada), radne stanice (3 komada), *Ethernet switch* (24 x 100/1000BaseT, upravljivi), laptop računar (3 komada), mobilni telefon sa iOS operativnim sistemom (1 komad), mobilni telefon sa Android operativnim sistemom (1 komad), mobilni telefon sa *Windows Phone* operativnim sistemom (1 komad);
- radne stanice za zaposlene;
- štampači (4 komada);
- mobilni telefoni za svakodnevni rad zaposlenih;
- fax aparat (1 komad), ;
- televizor (1 komad) – za praćenje aktuelnih događanja;
- video projektor (1 komad) – za prezentacije.

6.2.6 Infrastruktura

Za funkcionisanje tima Nacionalnog CERT-a, potrebno je obezbediti sledeću infrastrukturu:

- linkove ka dva nezavisna Internet servis provajdera (izabrani Internet servis provajderi moraju da imaju međusobno nezavisne izlaze ka Internetu) minimalnog kapaciteta 100 Mb/s,
- dve optičke veze (dva vlakna, *dark fiber*, po fizički odvojenim putanjama) između lokacije udaljenog *data* centra i poslovnog prostora gde će biti sedište Nacionalnog CERT-a,
- minimalno 5 direktnih telefonskih linija u poslovnom prostoru Nacionalnog CERT-a:
    - direktor – 1 linija,
    - sekretarica – 1 linija
    - fax aparat – 1 linija
    - prostorija za administrativno osoblje – 1 linija,
    - prostorija za administratore i analitičare – 1 linija,

- VPN grupu mobilnih pretplatničkih brojeva – za svakog zaposlenog po jedan broj i mobilni telefon,
- pasivni deo računarske mreže u poslovnom prostoru gde će biti sedište Nacionalnog CERT-a, i
- odgovarajuće opremanje poslovnog prostora koje obuhvata: protiv provalni alarmni sistem, detektore požara, sistem video nadzora ispred prostorija, neprekidno napajanje električnom energijom u okviru samog objekta, klimatizaciju prostorija.

6.2.7 Potrebni informacioni sistemi

Za funkcionisanje Nacionalnog CERT-a u skladu sa zadacima navedenim u prethodnim poglavljima, potrebno je obezbediti sledeće informacione sisteme:

- informacioni sistem za vođenje evidencije o primljenim prijavama o sigurnosnim incidentima, trenutnom statusu, načinu za rešavanje problema, statistici incidenata. Sistem mora da ima mogućnost uspostavljanja korelacije između prijava o sigurnosnim incidentima;
- besplatni pristup „IBM X-Force Exchange“ sistemu sa evidencijom o trenutno aktivnim sigurnosnim problemima u svetu;
- pristup bazi podataka sa do sada poznatim vrstama kompromitacije IKT sistema i načinima odbrane i zaštite IKT sistema;
- podsistem za elektronsku poštu.

6.2.8 Softverski alati

Za funkcionisanje Nacionalnog CERT tima, u skladu sa zadacima navedenim u prethodnim glavama, potrebno je obezbediti sledeće softverske pakete:

- Windows 10 operativni sistem za radne stanice zaposlenih,
- Windows 8.1 operativni sistem za radne stanice zaposlenih,
- anti-virus softver za radne stanice zaposlenih,
- MS *Office* softverski paket,

- *WebSite-Watcher* – softverski paket za praćenje promena na *web* sajtovima na kojima se objavljuju informacije o sigurnosnim problemima i rešenjima,
- *netflow collector* sa odgovarajućim softverom za analizu podataka,
- *wireshark* besplatan softver za snimanje i analizu mrežnog saobraćaja,
- GnuPG (www.gnupg.org) – besplatan softver za kriptovanje i digitalno potpisivanje dokumenata, i
- RTIR (https://bestpractical.com/rtir/) – besplatan *open source* softver za vođenje evidencije o sigurnosnim incidentima.

6.3 OSNOVNE POLITIKE POSLOVANJA

Određene politike poslovanja CERT organizacija smatraju se fundamentalnim, jer moraju biti implementirane nezavisno od skupa servisa ili nivoa usluga koje CERT tim pruža. O ovoj temi je bilo reči i u ranijim glavama, ali cilj narednog izlaganja je da se detaljnije opišu politike koje su bazične sa stanovišta operativnog delovanja Nacionalnog CERT tima. Naravno, treba imati u vidu da na formulaciju osnovnih politika utiču sami servisi koje Nacionalni CERT tim pruža, tj. garancije kvaliteta servisa na koje se tim obavezuje prema svojim konstituentima.

6.3.1 Kodeks ponašanja

Kodeks ponašanja je skup opštih pravila u okviru organizacije koje upućuju sve zaposlene na način ophođenja prema klijentima, a u skladu sa misijom organizacije i njenim organizacionim karakteristikama. Kodeks ponašanja odnosi se na sve članove tima, na svim nivoima organizacije, bez razlike. Njime se definišu uputstva na koji način se reaguje u specifičnim situacijama i uspostavlja baza za sve interakcije u okviru CERT tima, kao i sa spoljnim entitetima.

Kodeks ponašanja se može posmatrati i kao politika na koju se svaki zaposleni može osloniti u slučajevima kada nijedna druga politika, procedura ili pravilo nisu primenljivi. To treba da postane način ponašanja iskusnog člana tima, ili novog člana koji treba da se uklopi u način poslovanja i ophođenja u okviru organizacije.

Sadržaj dokumenta kodeksa ponašanja ne mora biti duži od jedne stranice teksta, ali ne škodi i ako se dopuni nekim konkretnim primerima situacija sa kojima se zaposleni najčešće susreću. Ovaj dokument nije potrebno opterećivati procedurama, to je poseban tip dokumenta. Ukoliko je dokument kratak i koncizan lakše je podeliti ga članovima tima, ali i sa spoljnim saradnicima, jer ovaj dokument po svojoj prirodi nije poslovna tajna. Objavljivanje ovakvog dokumenta olakšava razumevanje između strana koje su upućene na međusobnu saradnju.

Jedan jednostavan primer kodeksa ponašanja mogao bi izgledati ovako:

- Demonstrirajte potreban nivo radoznalosti, ali istovremeno imajte na umu i odgovarajući nivo uzdržanosti.
- Temeljno informišite sve one kojima su informacije neopodne, ali ne širite glasine.
- Svakome posvetite potrebnu pažnju, ali ne zaboravite na prioritete.
- Uvek budite pristojni i konstruktivni u komunikaciji, ali nikome ne verujte bez prethodne provere informacija.

- Upoznajte se sa procedurama i poštujte ih, ali nikada ne gubite iz vida da je misija tima na prvom mestu.

Ovo je jedan od mogućih primera kodeksa ponašanja, ali treba imati na umu da on pre svega proističe iz formulacije misije i karaktera svake CERT organizacije ponaosob.

6.3.2 Politika kategorizacije informacija

Svaki CERT tim mora da ima politiku kategorizacije informacija, kako bi se izbegla situacija da svaki član tima po sopstvenom utisku vrši kategorizaciju različitih informacija, ili ih uopšte ne kategorizuje. Nepostojanje konzistentne politike kategorizacije informacija u krajnjoj instanci može dovesti do lošeg servisa koji se obezbeđuje konstituentima.

Kompleksnost politika za kategorizaciju informacija zavisi od misije CERT tima i tipa njegovih konstituenata. Primera radi, najjednostavnija politika bi bila podeliti informacije na „osetljive/poverljive“ i „sve ostale“. Sa osetljivim informacijama treba postupati izuzetno pažljivo, dok se sve druge informacije mogu smatrati javnim.

Korak dalje bi bilo definisanje kategorija kao što su „interno poverljivo“, tj. za upotrebu samo u okviru CERT tima, „interno javno“, za poverljive informacije koje je po potrebi moguće deliti sa drugim CERT timovima sa kojima se sarađuje. Kategorija „za eksterne partnere“ bi mogla da se odnosi na informacije koje je moguće razmenjivati sa konstituentima, ili drugim CERT timovima, a „eksterna javna“ bi bila kategorija informacija koje je moguće potpuno otvoreno i javno objavljivati. Naravno, suština ovog izlaganja nije u nazivima kategorija, već je suštinski potrebno da svaki član tima razume i sprovodi dogovorene metode za kategorizaciju informacija. U tom smislu dobra preporuka je da se napravi inicijalna šema kategorizacije informacija, i da se onda prepusti svakom od članova tima da izvrši kategorizaciju nekog proizvoljnog skupa dokumenata ili informacija. Krajnji cilj ovog postupka bi trebalo da bude da se iz stavova različitih članova tima, i argumenata koje su izneli za svoje odluke o kategorizaciji, izvuče neka zajednička logika, i dođe do šeme kategorizacije koja je svima razumljiva i prihvatljiva, tj. koja će se sprovoditi na konzistentan način.

Treba imati u vidu da dodeljena kategorija utiče na način na koji se postupa sa informacijama (kako se informacija čuva, objavljuje ili uništava). Rezultat toga je da za svaku kategoriju moraju biti definisane odgovarajuće politike i procedure. Taj skup politika i procedura se zatim primenjuje na sve informacije u određenoj kategoriji, bez obzira na njihov konkretan sadržaj. Politike i procedure moraju da definišu način na koji se operativno postupa sa informacijama u okviru svake kategorije. Ovo uključuje i specificiranje podrazumevanih kategorija informacija (velika je razlika u tome da li je podrazumevana kategorija „interno“ ili „javno“).

Ponekad se može desiti situacija u kojoj nije jednostavno odrediti kako treba kategorizovati neku informaciju, jer informacija ima karakteristike iz više različitih kategorija. U takvim situacijama treba primenjivati princip „bolje sprečiti nego lečiti“, odnosno, izabrana kategorija treba da bude takva da se obezbedi viši nivo zaštite informacije, sve dok se ne pojave novi detalji, ili dodatne informacije koje će pomoći u adekvatnoj kategorizaciji.

6.3.3 Politike objavljivanja informacija

Jedna od najvažnijih stvari o kojima CERT tim mora da vodi računa je poverenje koje u njega imaju njegovi konstituenti i članovi drugih CERT timova. Bez tog poverenja i poštovanja CERT tim nije u mogućnosti da uspešno i efikasno sprovodi svoje aktivnosti, jer će drugi timovi, ili konstituenti, imati otpor prema razmeni informacija sa takvim CERT timom. Veoma je važno da CERT tim definiše politike o objavljivanju i razmeni informacija, u okvirima servisa za upravljanje incidentima, ali i van toga. Bez takve politike osoblje CERT tima nema smernice šta, kome i kada može da prosledi od informacija, tokom interakcije sa konstituentima ili drugim CERT timovima.

Većina CERT timova tretira sve informacije koje do njih dođu kao strogo poverljive, i ne razmenjuju ih van okvira svoje organizacije i članova tima. Izuzetak od ovoga mogu biti opšte informacije o trendovima, koje su statističke prirode, ili informacije za koje su sve uključene strane dale saglasnost da se mogu razmenjivati sa drugim entitetima, u posebnim slučajevima kada je to neophodno (sa drugim lokacijama ili konstituentima koji su mete istog tipa bezbednosnog napada, sa drugim CERT timovima u cilju efikasnijeg razrešenja incidenata, sa istražnim i pravosudnim organima, i slično).

Politika objavljivanja informacija mora da uzme u obzir restrikcije nad informacijama koje se postavljaju kao zahtev od drugih entiteta, ili krovne organizacije u kojoj CERT funkcioniše (u nekim slučajevima to mogu biti restrikcije pravne prirode, koje se kontrolišu u redovnim postupcima revizije ovih organizacija). Primera radi, postavlja se pitanje šta konstituenti nekog CERT tima mogu da očekuju u pogledu razmene informacija, u situacijama kada njihov tim dobije prijavu incidenta od nekog drugog CERT tima? Da li će se takva informacija proslediti rukovodstvu CERT tima, ili možda istražnim ili pravosudnim organima? Politikom treba da se definišu sva ograničenja u razmeni informacija, koja treba učiniti javno dostupnim za konstituente i druge zainteresovane strane. Takođe, pod kojim uslovima CERT tim može da prosledi osetljive informacije (npr. kontakt informacije) istražnim ili pravosudnim organima? Politika objavljivanja informacija često mora da se usaglasi i sa lokalnim zakonodavstvom, u pogledu zaštite poverljivosti informacija.

Primera radi, može se pretpostaviti scenario u kojem Nacionalni CERT Republike Srbije dobije prijavu incidenta od lokalnog CERT tima koji se bavi bezbednošću neke akademske institucije. I neka je pretpostavka da se u okviru te akademske institucije dogodio incident tokom kojeg je napadač preko sistema institucije izveo uspešan napad na sisteme u stranoj zemlji. CERT akademske institucije može sve log fajlove i artefakte proslediti Nacionalnom CERT-u i zahtevati da se neophodni detalji proslede nacionalnoj CERT organizaciji države u kojoj se nalazi konstituent koji je meta napada. Oni, pri tome, treba da naglase da li su saglasni da se informacije proslede i drugim entitetima koji su potencijalne mete napada, ili su na neki način uključeni u taj incident. Takođe, CERT organizacija akademske institucije može proslediti i kontakt informacije sistem administratora sistema koji je izvor napada Nacionalnom CERT-u, uz napomenu da ta informacija nije za dalju distribuciju. Sve ove informacije mogu koristiti Nacionalnom CERT-u da izgradi širu sliku bezbednosnog incidenta koji se dogodio, i da eventualno prepozna veze sa nekim drugim incidentima koji su u toku, ili su se desili u prošlosti. Zatim, Nacionalni CERT može proslediti povratnu informaciju lokalnom CERT-u, ali i CERT timu države u kojoj se nalazi meta napada, zahvaljujući kojoj će se obe lokacije lakše izboriti sa posledicama napada, i sprečiti njegovo dalje širenje.

Kao što postoje restrikcije na objavljivanje informacija koje CERT tim dobija od drugih entiteta, isto tako mora da postoji politika koja tretira zahteve drugih entiteta za

dobijanjem informacija koje su u posedu CERT tima. Obično su to zahtevi za dobijanje detaljnih tehničkih informacija, ili drugih osetljivih informacija.

U osnovi, postoje tri faktora koji određuju da li, u kojoj meri, i na koji način je moguće objavljivati, ili razmenjivati neke informacije. To su: razlog objavljivanja informacije, ciljna grupa, i kategorija informacije.

Za objavljivanje bilo kojih informacija mora da postoji odgovarajući razlog, tj. mora da postoji neko ko ima potrebu da sazna te informacije. Ovaj princip se može primeniti na bilo koji tip informacija.

Termin ciljna grupa se odnosi na entitete kojima je neka konkretna informacija od interesa (konstituenti CERT tima, drugi CERT timovi, interno rukovodstvo organizacije, istražni i pravosudni organi, mediji, tehnološki eksperti, ili šira javnost ...). Naravno, nivo restriktivnosti je značajno viši kada se informacije dele sa javnošću, nego npr. interno sa članovima tima.

Kategorija informacija se definiše na bazi politike kategorizacije informacija, kao što je u poglavlju 6.3.2 već opisano. Kada treba doneti odluku da li će se neka informacija objaviti ili ne, jasno je da postoji razlika u tome da li je ta informacija poverljive prirode, ili je npr. javna. Kategorizacija utiče na to kako će se informacija zaštiti prilikom objavljivanja. Primera radi, javne informacije je moguće objavljivati putem elektronske pošte, koja je uobičajeno zaštićena autentičnošću digitalnog potpisa, dok se poverljive informacije štite korišćenjem enkripcije i bezbednih kanala komunikacije.

Neka postoji jasan razlog da se objavi neka informacija i ukoliko se donese odluka da se to učini, onda će sadržaj informacije, njena kategorija i ciljna grupa uticati na način na koji će biti objavljena, koji delovi informacija će biti objavljeni, i kome. Primera radi, ukoliko se desi bezbednosni incident širokih razmera, koji uključuje hiljade hostova širom sveta, CERT timovi će prikupiti određenu količinu detaljnih log fajlova sa sistema na napadnutim lokacijama. Pri tome će jedan CERT tim, koji dođe do određenih informacija, razmenjivati te informacije na sledeći način:

- CERT timovima, i sa kojima postoji saradnja i odnos poverenja, predaće delove log fajlova koji se odnose na njih ili njihove konstituente,
- ostalim žrtvama napada predaće zapise iz log fajla koji su relevantni samo za njih, kako bi mogli da izvrše poređenje i kontrolu svojih log fajlova, zajedno sa smernicama kako da se zaštite od sličnih napada u budućnosti,
- istražni i pravosudni organi se mogu obavestiti o razmerama incidenta, i opštim informacijama o njegovom uzroku,
- mediji se mogu obavestiti o razmerama incidenta i uz uopšteno upozorenje,
- ekspertima od poverenja se mogu predati sve detaljne informacije, kako bi se što pre istražili svi detalji incidenta i ranjivosti koje su do njega dovele, izolovao „otisak“ napadača, i sprovele aktivnosti na saniranju posledica incidenta.

6.3.3.1 Objavljivanje posredno dobijenih informacija

Kada jedan entitet razmeni informacije sa drugim entitetom, vrlo je verovatno da će taj drugi entitet nastaviti da širi informacije dalje. Naravno, to je najčešći slučaj sa medijima, sa drugim entitetima ne mora uvek biti tako. Veoma je važno prilikom razmene informacija predočiti drugoj strani šta sa tim informacijama sme da uradi. Jednom kada se neka informacija otkrije, stvari lako mogu da izmaknu kontroli. Čak i kada postoji ugovor između dve strane, koji definiše postupanje sa informacijama, ipak je moguće da informacije „cure“,

što može imati loše posledice za onoga ko je inicijalno objavio neku informaciju (loš uticaj na reputaciju, pa čak i pravno gonjenje).

Primera radi, kada su u pitanju mediji, obično se od njih zahteva da se „radna verzija“ neke vesti koju žele da objave, na bazi informacija koje dobiju od CERT tima, prvo pošalje CERT timu na pregled i odobrenje. Nažalost, u praksi mediji veoma retko ispoštuju takav zahtev, tako da informacija bude objavljena u formi kako su je predstavnici medija razumeli, bez bilo kakve autorizacije od strane izvora informacija. Kada su u pitanju drugi CERT timovi sa kojima se sarađuje, sa njima se obično dele informacije u punom obimu, pod pretpostavkom da će te informacije dalje biti korišćene samo u svrhu upravljanja incidentima, u korist CERT tima ili njegovih konstituenata, bez daljeg objavljivanja široj javnosti.

Jedan koristan pristup razmeni informacija je da se svaka informacija pre razmene „obeleži“, tj. dopuni napomenom o mogućem načinu korišćenja te informacije (na primer „samo za internu upotrebu CERT tima“). Ovaj pristup je naročito koristan u slučaju razmene osetljivih informacija.

6.3.3.2 Vremenski okviri objavljivanja informacija

Pravovremeno objavljivanje informacija je izazov svoje vrste, na koji CERT tim treba da bude kadar da odgovori. S jedne strane, dobro je biti siguran u sve činjenice pre nego što se bilo kakva informacija objavi, ali ponekad je za to potrebno previše vremena. Sa druge strane, potencijalne žrtve napada je potrebno što pre obavestiti o potencijalnoj opasnosti, čak i kada informacija nije kompletna ili potpuno tačna. Šta više, u oba ova slučaja CERT tim može imati problema pravne prirode, naročito ukoliko je u ugovornoj obavezi sa svojim konstituentima, i oni pretrpe nekakvu štetu zbog loše procene vremena za objavljivanje neke bezbednosne informacije.

Ovakve situacije retko se dešavaju CERT timovima koji nisu u ugovornoj obavezi, i nemaju operativne ingerencije nad sistemima svojih konstituenata, već je njihova uloga više savetodavnog karaktera, kao što je to npr. slučaj sa nacionalnim CERT organizacijama.

Treba imati u vidu da je osnovna funkcija nacionalnog CERT-a zaštita kritične infrastrukture jedne zemlje. U tom smislu, prilikom objavljivanja informacija, prvo je, svakako, potrebno obavestiti ostale CERT-ove u zemlji, kao i operatore kritičnih IKT sistema. Tek kada svi prethodno navedeni budu obavešteni i ostavljeno im dovoljno vremena za zaštitu IKT sistema, navedena informacija može da bude i javno objavljena (ukoliko je priroda informacije takva da ona može da bude javno objavljena). Ukoliko bi informacija bila suviše rano javno objavljena, to bi ostavilo mogućnost potencijalnim napadačima na kritični IKT sistem, koji nisu svesni sigurnosnog propusta, da izvrše napad i kompromituju IKT sistem.

6.3.4 Politika odnosa sa medijima

Mediji mogu biti moćan i koristan alat za javno objavljivanje informacija širokim krugovima korisnika, i CERT timovi sa medijima treba da razvijaju dobre odnose. S tim u vezi, očigledno je potrebno imati definisanu politiku odnosa sa medijima. Čak i kada postoje kvalitetne politike upravljanja informacijama, odnos sa medijima može biti posebno osetljivo i teško pitanje.

Glavni zadatak je odrediti gde je, tj. ko je glavni „interfejs“ za saradnju sa medijima, tj. da li je to neko unutar tima, ili van njega. S obzirom da CERT timovi raspolažu tehničkim podacima poverljive prirode, preporučuje se da CERT tim ima saradnika za odnose sa

medijima koji nije član CERT tima. Na taj način se obezbeđuje da ta osoba nema pristup poverljivima podacima, jer se toj osobi saopštava samo onoliko koliko je neophodno da ispuni svoju funkciju odnosa sa medijima, na način na koji je to definisano odgovarajućom politikom CERT organizacije. Obično su takve informacije detaljno prečišćene, čime se sprečavaju pravne posledice usled objavljivanja informacija putem medija. Naravno, ukoliko je osoba za saradnju sa medijima van CERT organizacije, mora postojati i neko u okviru same organizacije ko će joj prenositi adekvatne informacije na redovnoj osnovi, i na definisan način.

6.3.4.1 Uspostavljanje liste kontakata sa medijima

U izboru medija sa kojima se sarađuje treba biti izuzetno pažljiv, i lista kontakata treba da sadrži samo one medije ili novinare sa dobrom tehničkom pozadinom, sa kojima je lako sarađivati bez bojazni o načinu na koji će oni predstaviti neku vest. Čak i kada mediji imaju na raspolaganju kvalitetne novinare koji se bave temama informacione bezbednosti, treba imati u vidu i bezbednost informacija koje se na ovaj način razmenjuju.

6.3.4.2 Pravila angažovanja

Ovim pravilima se predstavnici medija informišu o tome šta mogu da očekuju od CERT tima, i na koji način će se uopšte odvijati ta interakcija. Neka od ovih pravila mogu biti:

- da mediji kontaktiraju jedino sa osobom ovlašćenom za te poslove ispred CERT organizacije,
- da ne smeju menjati sadržaj i smisao informacija koje dobiju,
- da omoguće predstavniku za medije CERT tima da ima uvid u vest, i može da je prokomentariše, ili odobri pre objavljivanja, i
- da će bilo kakvo kršenje ovih pravila dovesti do prekida saradnje sa medijskom kućom koja ih prekrši.

6.3.4.3 Obaveštavanje medija unapred

Kada je u pitanju davanje objašnjenja o tekućim događajima, često je bolje imati inicijativu nego čekati da se mediji obrate CERT organizaciji sa zahtevom za nekim informacijama. Na taj način CERT tim može i da se pripremi za očekivana pitanja. Korak dalje bi bio da se medijima unapred objasni uloga i misija CERT tima, kako bi mediji unapred imali uopštenu sliku o tome.

6.3.4.4 Pravila ponašanja u interakciji sa medijima

Članovi CERT tima, kao i njihov predstavnik za odnose sa medijima, koji se pojavljuje u javnosti ispred CERT organizacije, moraju u svakoj situaciji biti pripremljeni na kontakt sa medijima. Ukoliko se takva situacija desi u neočekivanom trenutku, jedan od pristupa interakcije bi mogao biti „bez komentara“. Naravno, ovaj pristup može da važi za članove tima, ali ne i za predstavnika za odnose sa medijima. Elegantniji pristup bi bio da se članovi tima obuče u tome šta je to što medijima smeju da kažu, i na koji način, radije nego da se obučavaju šta je to što ne smeju da govore. Ovakav pozitivan pristup ima dobar efekat na odnose sa medijima, čak i kada oni nisu zadovoljni informacijama koje dobiju.

6.3.5 Politike bezbednosti

U današnje vreme, svaka organizacija koja drži do sebe tvrdi da ima politike bezbednosti koje se tiču svih aspekata bezbednosti, počev od brava na vratima, pa do *back-up*-a informacionih sistema, ili upotrebi lozinki, *firewall*-a i enkripcije.

Kada su u pitanju CERT organizacije, one su prisiljene da rade u kompleksnom mrežnom okruženju, oslonjene na puno informacionih sistema i telekomunikacionih servisa, te su samim tim izuzetno izložene bezbednosnim rizicima i podložne napadima. Pri tome, s obzirom na svoju delatnost, kao i vrstu informacija sa kojima raspolažu, CERT organizacije su jako popularna meta svih vrsta napadača. Stoga je primarni faktor rizika za CERT organizacije da će usled napada ostati u nemogućnosti da reaguju na bezbednosne incidente, a nije mali rizik ni od gubitka poverenja njihovih kostituenata ukoliko se sa ovakvim situacijama ne izbore na brz i efikasan način.

Politika bezbednosti je pod izuzetno velikim uticajem drugih politika, s obzirom da ciljevi svih drugih politika podrazumevaju odgovarajući nivo bezbednosti. Politika bezbednosti treba da pokriva sve aspekte koji se tiču informacionih sistema i računarskih mreža na koje se oslanja CERT tim u svom radu, kao i komunikacione linkove ka drugim organizacijama, i to:

- fizičko obezbeđenje,
- planove oporavka od incidenata (*back-up* sistema, i slično),
- bezbednost lokalne računarske mreže,
- bezbednost lokalnih informacionih sistema,
- bezbednost eksternih komunikacija,
- upravljanje lokalnim bezbednosnim incidentima, i
- upravljanje kriznim situacijama i obezbeđenje kontinuiteta poslovanja.

6.4 OBEZBEĐENJE KONTINUITETA POSLOVANJA

Osnova poslovanja uspešnog CERT tima je kontinuitet u pružanju pouzdanih i konzistentnih servisa. To je je faktor koji direktno utiče na percepciju sposobnosti CERT tima od strane njegovih konstituenata, i nivo poverenja koji će postojati. Obezbeđenje kontinuiteta poslovanja je opšta kategorija koja podrazumeva mnoge važne aspekte operativnog delovanja, od kojih se tri posebno ističu: upravljanje procesom rada, kontinuitet servisa van regularnog radnog vremena, i rad na daljinu.

6.4.1 Pretnje po kontinuitet poslovanja

Sa stanovišta ustaljene prakse, postoje tri osnovne kategorije pretnji po kontinuitet poslovnaja sa kojima se CERT timovi susreću: kratkoročni problemi (koji mogu trajati nekoliko dana i nedelja), srednjoročni problemi (koji mogu trajati mesecima), i dugoročni problemi (koji mogu pratiti poslovanje CERT tima godinama).

6.4.1.1 Kratkoročni problemi

Pretnje po kontinuitet poslovanja koje se manifestuju tokom nekoliko dana ili nedelja, najčešće su operativne prirode. Najčešće je to jedan od sledeća četiri faktora: nedostatak vremena, nedostupnost nekog od ključnih članova tima, promena zaposlenih u slučaju rada po smenama, ili nedostupnost elemenata infrastrukture.

6.4.1.1.1 Nedostatak vremena

Nedostatak vremena može biti posledica nekog tekućeg incidenta, ali može biti i strukturne prirode. Ukoliko je strukturne prirode, onda je najčešće posledica manjka zaposlenih zbog nedostatka sredstava za finansiranje CERT tima, i tada to više nije kratkoročni problem. Ukoliko je u pitanju iznenadni pritisak na zaposlene usled pojave incidenta širokih razmera, onda se takvom situacijom upravlja politikama prioritetizacije. U ekstremnim situacijama potrebno je primeniti i krizno upravljanje, kako bi se servisi tima održali u funkciji. Kada je tim preopterećen poslom potrebno je voditi beleške o svim dešavanjima, što je jako korisno kada se predaje posao drugim članovima tima, u slučajevima rada po smenama.

6.4.1.1.2 Nedostupnost članova tima

Nedostupnost nekog od ključnih članova tima je događaj koji se ne može izbeći, jer se dešavaju razni nepredvidivi događaji, kao što su odsustvo zbog bolesti, ili razne nezgode. Da bi se izbegli ovakvi događaji, dobro je da svaki od ključnih članova tima ima svoju adekvatnu zamenu. Naravno, treba izbegavati situaciju da oni imaju slobodne dane u isto vreme. Jedan od dobrih načina da se među članovima tima širi znanje i smanjuje rizik je da se zaposleni rotiraju na različitim poslovima. Takođe, najkritičniji periodi u pogledu radnog vremena su vreme neposredno pre i posle radnog vremena, kada su članovi tima na putu od kuće do posla i obratno. Da bi se izbegla situacija da su svi članovi tima nedostupni može se organizovati „smaknuto“ radno vreme, što bi podrazumevalo da neki članovi tima rade npr. od 7 do 15 časova, a drugi od 9 do 17 časova. Takođe, kritične su i situacije kada je određeni broj članova tima na obukama ili konferencijama, a preostali članovi tima moraju da nadoknade njihovo odsustvo. Naravno, moguće je obezbediti i daljinski pristup za članove tima koji su van kancelarije, ali to sa sobom nosi razne poteškoće, ali i bezbednosne rizike.

6.4.1.1.3 Rad po smenama

Promena zaposlenih tokom smenskog rada je jedna od situacija u kojoj do izražaja dolazi kvalitet upravljanja procesima rada. U zavisnosti od okolnosti treba obratiti pažnju na dve situacije: promena zaposlenih tokom redovnog radnog vremena, i prelazak iz režima rada „u radno vreme“ i „van radnog vremena“. U ovom prvom slučaju treba rezervisati neko vreme za usmenu komunikaciju i predaju poslova između različitih članova tima, kako bi smena koja dolazi prikupila sve neophodne informacije i nastavila sa poslom tamo gde je prethodna smena stala. U drugom slučaju (pokrivanje servisa van radnog vremena) se pojavljuju problemi koji se tiču samog načina obavljanja posla van radnog vremena, tj. osoblja koje je angažovano van radnog vremena (a najčešće su to samo čuvari i agenti centra za prijem poziva koji nisu obučeni za naprednije poslove upravljanja incidentima).

6.4.1.1.4 Nedostupnost elemenata infrastrukture

Nedostupnost kritičnih telekomunikacionih servisa, ili operativnih elemenata kao što su sistem elektronske pošte, ili Internet prezentacije tima, dovodi do nemogućnosti da tim sprovodi svoje aktivnosti na efikasan način, i u predviđenim vremenskim rokovima. To može dovesti do žalbi konstituenata, ali čak i do pravnih posledica po CERT tim, u slučaju da postoje ugovorne obaveze prema nekim od konstituenata.

6.4.1.2 Srednjoročni problemi

Kako bi se obezbedio kontinuitet rada tima na srednjoročnom nivou, korisno je da članovi tima zajednički analiziraju situacije u kojima se nalaze u svakodnevnom radu, kako bi svoje servise učinili boljim. U tom smislu, potrebno je analizirati i procedure i politike, kako bi se došlo do zaključka da li postoji potreba da se akcije sprovode na efikasniji i bolji način. Ovakve sastanke treba planirati na redovnoj bazi. Drugi srednjoročni problem može biti nedostatak sredstava za finansiranje aktivosti tima, što može uticati na operativne sposobnosti tima, i nivo kvaliteta servisa koji se obezbeđuje konstituentima. Takođe, zasićenje zaposlenih članova tima može biti problem u organizovanju svakodnevnih aktivnosti, zbog čega im je potrebno obezbediti što bolje uslove za rad. Dobro je potencirati da članovi tima imaju redovne odmore, ali i da se rotiraju na radnim mestima i zadacima u okviru tima. Takođe, dobra motivacija za zaposlene mogu biti i razni programi edukacije, koja im se omogućava kako bi održali korak sa izazovima na polju informacione bezbednosti. Naravno, ovo donosi prednosti i samoj CERT organizaciji, jer dobro obučeni članovi tima doprinose kvalitetu servisa koje organizacija nudi.

6.4.1.3 Dugoročni problemi

Sposobnost CERT tima da se prilagodi promenama, u pogledu tehnologije, ili servisa koji su neophodni konstituentima, doprinosi tome da CERT organizacija ima duži vek trajanja. Samim tim, obučavanje osoblja je dugoročna investicija u kontinuitet poslovanja CERT organizacije. Štaviše, preporučuje se edukacija više članova tima za istu oblast delovanja, kako tim ne bi bio pogođen odlaskom, ili nedostupnošću nekog od članova tima. Jedan od faktora koji vremenom može postati važan su radne navike, naročito ako se sastav tima ne menja tokom dužeg vremenskog perioda. Upadanje u neku vrstu stabilnog i rutinskog poslovanja je dobro, ali nije garancija kontinuiteta poslovanja. Rutina može da ograniči sposobnost tima da se prilagodi promenama, ili da se greške u radu ignorišu, jer su prikrivene procedurama koje se ne preispituju i ne menjaju. Sposobnost da se reaguje u dinamičnom okruženju upravljanja bezbednosnim incidentima je kontinuirani proces učenja, i članova tima, i tima kao celine, a fleksibilnost je neophodna jer su stalne promene sastavni deo svakodnevnog funkcionisanja tima. Samim tim, iako su politike i procedure neophodan preduslov poslovanja CERT timova, one se moraju redovno analizirati i revidirati, kako bi ostale u toku sa realnim dešavanjima i kako bi ih članovi tima poštovali i sprovodili.

6.4.2 Upravljanje procesom rada

Kao što mu i ime kaže, upravljanje procesom rada je upravljanje tokovima događaja koji su deo svakodnevnog rada pojedinačnih članova tima, tima u celini, ili čitave CERT organizacije. Ukratko, upravljanje procesom rada se primenjuje na svim nivoima organizacije.

Obezbeđenje kontinuiteta poslovanja u poslovima upravljanja incidentima je problematično zbog činjenice da se CERT timovi bave sa puno incidenata tokom dužih vremenskih perioda, pri čemu se stalno pojavljuju nove informacije i događaji, a menjaju se i ljudi koji na njima rade (osoblje se menja po smenama, usled odlaska na odsustva, usled promene radnih mesta, ili napuštanja CERT organizacije). Stoga je potrebno da se informacije o svim događajima (problemima, incidentima, ranjivostima sistema, artefaktima incidenata i slično) čuvaju u dužem vremenskom periodu, i budu dostupne svim članovima tima u bilo koje vreme. Pored informacija o samom incidentu o kojem je reč, mora se voditi i evidencija o svim akcijama koje je CERT tim preduzeo tim povodom, kao i akcijama koje je potrebno sprovesti u budućnosti, i sve to mora biti dostupno svim članovima tima u svakom trenutku. Na ovaj način olakšava se preusmeravanje posla na odgovarajuće članove tima, koji tada na jednom mestu mogu pronaći sve relevantne informacije.

Primera radi, treba se osvrnuti na osnovne načine na koje informacije stižu do CERT tima: elektronska pošta, log fajlovi, telefonske zabeleške, ili pisma konstituenata. Evidentirati sve ove informacije nije jednostavan zadatak. Prva stvar koju treba učiniti je da se sve informacije označe odgovarajućim identifikatorom, koji ih povezuje sa incidentom ili događajem sa kojim su u vezi, o čemu je već bilo reči u prethodnim poglavljima. Kada se to učini, sve informacije se čuvaju u informacionom sistemu, odakle su dostupne svim članovima tima. Pri tome, cilj treba da bude da baza podataka sa svim informacijama bude jedinstvena, što uveliko olakšava posao članovima tima u trenucima kada je vreme za reakciju na neki događaj kritičan faktor. Iako postoji težnja da se sve informacije i dokumenta, bez obzira na koji način dođu do CERT organizacije, čuvaju u elektronskom obliku, treba obratiti pažnju i na zahteve pravne prirode, koji se odnose na čuvanje dokumenata u originalnoj formi u određenom vremenskom periodu, kako je propisano zakonima države u kojoj CERT tim funkcioniše.

Najbolji način da se evidentiraju incidenti, i sve informacije i akcije koje su u vezi sa njima, je da se koriste namenski sistem i softver, koji omogućavaju što veći stepen automatizacije procesa rada i arhiviranja informacija. Pri tome treba voditi računa o bezbednosti celog rešenja, kako bi jednako efikasno moglo da se koristi u lokalnoj mreži, ali i u distribuiranom okruženju, kroz daljinski pristup, ili preko *web*-a.

6.4.3 Kontinuitet procesa rada van radnog vremena

Ukoliko specifikacija servisa koje CERT tim pruža podrazumeva i podršku van radnog vremena, treba jasno naglasiti koji nivo podrške konstituenti tada mogu da očekuju. U skladu sa tim definicijama vrši se i organizacija procesa rada. Naravno, parametri kvaliteta servisa (kao što je npr. vreme odziva na prijavu incidenta), mogu se značajno razlikovati tokom i van regularnog radnog vremena. Zbog toga je potrebno obezbediti jasne opise i uputstva, u skladu sa odgovarajućim politikama i procedurama, koji će pomoći konstituentima da utvrde nivo svojih očekivanja u pogledu podrške CERT tima van radnog vremena.

6.4.3.1 Hitni pozivi

Postoje različiti načini da se reši problem prijema telefonskih poziva van radnog vremena. Najvažnije je definisati ko se javlja na hitne pozive van radnog vremena: član tima koji je na dežurstvu, neki drugi član tima, automat za govornu poštu, ili dežurni centar

telekomunikacionog provajdera. Kada se donese takva odluka poziv se može preusmeriti na odgovarajući telefonski broj, ili se konstituentima može pružiti informacija o alternativnim kontaktima CERT tima. U krajnjem slučaju dežurni član tima može provoditi vreme u poslovnim prostorijama tima, gde će se javljati na hitne pozive.

6.4.3.2 Eskalacije

Za slučajeve da situacija sa incidentima eskalira van radnog vremena dobra praksa je da postoji barem jedan član tima koji je dostupan, tj. može biti operativan u kratkom vremenskom roku. Takođe se preporučuje da postoji i „dežurni rukovodilac“, kako bi se olakšalo donošenje odluka i skratilo vreme reakcije u kriznim situacijama van radnog vremena.

6.4.3.3 Dostupnost članova drugih CERT timova ili konstituenata van radnog vremena

Uobičajena je praksa da sve CERT organizacije imaju dežurno osoblje van radnog vremena, a nejčešće je to slučaj i sa organizacijama konstituenata. Stoga je dobra praksa da se izgrađuju veze sa drugim CERT timovima i konstituentima, i da se razmene kontakti koji mogu da se koriste u kriznim situacijama van radnog vremena, jer to može biti od ključne važnosti za efikasno razrešavanje incidenata. Pri tome treba povesti računa o vremenskim zonama, pa čak i rasporedu državnih praznika u raznim zemljama, kako bi se na vreme utvrdilo na koji način, tj. preko kojih kontakata je moguće doći do pomoći drugih timova ili konstituenata.

6.4.4 Rad na daljinu

Rad na daljinu se razlikuje od rada van radnog vremena u tom smislu da članovi tima moraju biti u stanju da isporuče svoje servise u punom obimu čak i ako nisu u prilici da budu locirani u svojim poslovnim prostorijama. Razlozi za ovakav scenario mogu biti različiti, od toga da su poslovne prostorije nedostupne zbog neke krizne situacije (npr. vremenski uslovi), do toga da neki članovi tima mogu biti odsutni sa posla, zbog prisustva obukama ili konferencijama van mesta rada, ili su prisiljeni da rade sa neke rezervne udaljene lokacije. U svakom slučaju, za razliku od rada van radnog vremena, u ovim situacijama se od tima očekuje da pruži servise u punom obimu, i da sve funkcioniše „normalno“, kao da su svi članovi tima na svojim radnim mestima u poslovnim prostorijama tima. Konstituenti ne treba da budu svesni da CERT tim funkcioniše u nekim specifičnim uslovima. Očigledno je da ovakav scenario poslovanja nosi brojne komplikacije, i zato ga treba redukovati na apsolutni minimum.

Lokacija sa koje će članovi tima biti prinuđeni da obavljaju svoje zadatke ne mora biti unapred poznata. To sa sobom nosi dodatne bezbednosne probleme i izazove koje treba u kratkom vremenu proceniti i razrešiti. U zavisnosti od okolnosti potrebno je doneti odluku da li da se nivo bezbednosti smanji kako bi se neki specifični servis uopšte isporučio, ili da visok nivo bezbednosti bude prioritet, čak i ako se time sprečava pristup resursima CERT tima, i samim tim efikasna isporuka servisa. U ovakvim situacijama prevagu treba da odnese bezbednost infrastrukture CERT tima.

Obično postoje dobri razlozi zašto su članovi tima odsutni iz poslovnih prostorija (mogu biti na obukama, konferencijama, ili angažovani na lokacijama konstituenata ...) i u takvim situacijama dolaze do izražaja procesi prioritetizacije posla. Svaki zadatak mora imati

unapred i jasno definisan prioritet, kojim bi članovi tima mogli da se rukovode u sprovođenju aktivnosti, tj. kako bi odredili šta može da sačeka njihov povratak u sedište tima, a šta je neophodno uraditi odmah, bez obzira na lokaciju na kojoj se nalaze.

6.5 UPRAVLJANJE BEZBEDNOŠĆU

Očigledno je da CERT timovi moraju da ulože posebne napore za očuvanje bezbednosti svojih sopstvenih sistema i mreže. Kada se govori o cijevima upravljanja bezbednošću informacione infrastrukture, CERT organizacija treba obratiti pažnju na sledeće osnovne faktore:

- poverljivost: omogućiti pristup samo neophodnim informacijama, i ne više od toga,
- dostupnost: da informacije budu dostupne u svakom željenom trenutku,
- integritet: omogućiti da se informacije čuvaju u nepromenjenom obliku,
- autentičnost: da se pouzdano zna izvor svake informacije,
- ekskluzivitet: da informacija bude dostupna samo onome kome je namenjena,
- privatnost: da se garantuje zaštita identiteta i interesa ličnosti i organizacija sa kojima se sarađuje, i
- posvećenost: da se obaveze izvršavaju u potpunosti i na vreme.

6.5.1 Korišćenje enkripcije i digitalnih potpisa

Primena enkripcije i korišćenje digitalnih potpisa trebalo bi da bude obavezna u poslovanju i komunikaciji svakog CERT tima. Time se povećava bezbednost podataka koji se čuvaju u informacionim sistemima CERT organizacija, ili tokom prenosa kroz neobezbeđene mreže. Kriptografskim metodama se obezbeđuju i konekcije i autentifikacija prilikom pristupa infrastrukturi CERT tima sa eksternih mreža. Primera radi, može se vršiti i enkripcija log fajlova o bezbednosnim incidentima, prilikom razmene podataka sa konstituentima putem *e-mail*-a, kako bi se zaštitile informacije o napadnutim sistemima. Kada je u pitanju razmena informacija sa spoljnjim entitetima treba koristiti uobičajene protokole, kao što su PGP, GPG, ili S/MIME.

6.5.2 Upravljanje ključevima i sertifikatima

Korišćenje enkripcije nosi sa sobom probleme upravljanja ključevima i sertifikatima. Primera radi, S/MIME, ili PGP/GPG koriste asimetričnu enkripciju (poznata i kao enkripcija privatnim ključevima) radi obezbeđenja jake autentifikacije. Na ovaj način se izbegavaju slabosti simetrične enkripcije, gde tajni ključ mora biti poznat svim entitetima u komunikaciji. Samim tim nemoguće je izvršiti autentifikaciju jer je ključ poznat svima, tj. učesnici u komunikaciji ga „dele“. Kod asimetrične enkripcije koriste se dva ključa, koji su u međusobnoj relaciji, za svaka dva učesnika u komunikaciji. Javni ključevi se mogu distribuirati svima, bez bojazni od kompromitacije, a privatni se moraju čuvati u tajnosti, poput lozinke.

Primera radi, kod asimetrične enkripcije, ako Petar šalje Jovani enkriptovani *e-mail*, Petar koristi Jovanin javni ključ da obezbedi sadržaj poruke koju će napisati i poslati Jovani, i pri tome je Jovana jedina koja može dekriptovati taj tekst svojim privatnim ključem. Pri tome,

Petar koristi svoj privatni ključ da potpiše tekst poruke koju šalje, a Jovana može da potvrdi originalnost poruke korišćenjem Petrovog javnog ključa.

Problem upravljanja ključevima odnosi se i na privatne i na javne ključeve. Privatni ključevi se moraju adekvatno obezbediti, jer ako neko preuzme kontrolu nad privatnim ključem može da dekriptuje sve njime zaštićene poruke. Privatni ključevi se dodatno štite lozinkom, koju je, takođe, potrebno bezbedno čuvati. Privatni ključevi se nekada nose na prenosnim medijumima, kao što su USB diskovi, koje, takođe, treba držati na bezbednom mestu.

Dodatno, treba imati u vidu sve aspekte bezbednosti metoda enkripcije. Na primer, ukoliko za zaštitu privatnog ključa koristi lozinka od tri karaktera, to svakako nije adekvatna zaštita, tj. kida se ceo lanac bezbednosti. Dakle, implementacija jakih bezbednosnih metoda nije sama po sebi dovoljna, bitan je i način na koji se one koriste.

Još jedan problem prilikom upotrebe javnih ključeva je da se utvrdi njihova autentičnost, tj. da li pripadaju osobi u čije ime se distribuiraju. Za te svrhe su potrebni nezavisni autoriteti za sertifikaciju (*Certificate Authorities* - CA), tj. kompanije kao što je *Verisign*, koje krajnjim korisnicima prodaju parove javnih i privatnih ključeva, i garantuju za njihovu autentičnost i privatnost.

Ukoliko korisnici sami prihvataju i potpisuju, tj. garantuju jedni drugima za autentičnost ključeva, onda se takve akcije baziraju na međusobnom poverenju. Sa tim u vezi, postavlja se pitanje da li, i kada CERT tim treba da potpisuje ključeve drugih entiteta? Rizik je u tome, da ukoliko bi se otkrilo da je CERT tim greškom garantovao za autentičnost nečijeg ključa, onda bi se takav tim smatrao nepouzdanim za saradnju. Stoga CERT timovi treba da izbegavaju ovakve situacije, koje mogu imati negativan uticaj na njihovo poslovanje.

6.5.3 Bezbednost mrežne infrastrukure

U idealnom slučaju mrežna infrastruktura CERT tima je od spoljnih mreža zaštićena dobro dizajniranim *firewall* uređajima. Pri tome se kao spoljna mreža može posmatrati i mreža krovne organizacije u okviru koje CERT tim posluje. Pored *firewall* uređaja, kao dodatnu meru treba praktikovati i odgovarajuću autentifikaciju i autorizaciju na svim nivoima infrastrukture. Takođe, potrebno je praktikovati i odgovarajuće mere administracije i kontrole, kako bi se sprečili napadi i upadi u sisteme i mrežu CERT organizacije. *Firewall* uređaji su beskorisni ukoliko ne postoji procedura redovne provere log fajlova i praćenja sumnjivih aktivnosti na dnevnom nivou. U tom smislu je pogodno koristiti i softverska rešenja za automatizaciju ovih procesa kako bi članovi tima na vreme bili upozoreni u slučaju opasnosti po bezbednost svoje infrastrukture.

Takođe, treba razmišljati i o redundansi na svim nivoima, ne samo *firewall* uređaja ili bitne mrežne opreme, već i serverske infrastrukture i baza podataka. Naravno, za svu opremu treba obezbediti neprekidno napajanje električnom energijom. U situacijama bezbednosnih kriza ili prirodnih katastrofa, pogodno je imati rezervnu lokaciju sa svom neophodnom infrastrukturom, na kojoj se čuvaju sveže kopije svih podataka, i koje u slučaju nužde mogu postati operativne u kratkom vremenskom roku. Naravno, svi sistemi na rezervnoj lokaciji moraju biti implementirani poštujući preporuke o informacionoj bezbednosti koje važe i za primarnu lokaciju. U tom smislu, metode enkripcije treba praktikovati na svim podacima i u lokalnoj mreži, kako bi se podaci dodatno osigurali u slučaju da *firewall* uređaji nisu u stanju da blokiraju svaki napad.

6.5.4 Izolovane mreže za testiranje

Ukoliko CERT tim vrši testiranja malicioznog softvera, analizu artefakata, ili bilo kakvog nepoznatog softvera, to se mora vršiti u izolovanom mrežnom okruženju, i na opremi koja se ni na koji način ne koristi u produkcionim sistemima. Time se osigurava bezbednost ključne infrastrukture CERT tima, koja je neophodna za svakodnevno obavljanje posla i isporučivanje servisa svojim konstituentima, i sprečava kompromitacija imidža CERT organizacije u javnosti. Naročito bi neprijatno moglo biti ako bi mreža neke CERT organizacije postala izvor napada na druge sisteme na Internetu, ili bezbednosnih rizika za svoje konstituente.

6.5.5 Udaljeni pristup infrastrukturi CERT tima

Posebnu pažnju u smislu bezbednosti treba obratiti na situaciji kada je članovima CERT tima potrebno omogućiti pristup lokalnim resursima i infrastrukturi sa udaljenih lokacija, preko javne Internet mreže. Pravljenje „rupa“ u *firewall* zaštiti svakako nije preporučljivo u ovakvim situacijama. Jedini pravi način da se ovaj problem reši je da se korišćenjem jakih metoda enkripcije i autentifikacije kreira bezbedan „tunel“, ili virtuelna privatna mreža (VPN), kroz javnu Internet mrežu i omogući pristup internim resursima CERT organizacije. Naravno, nije dovoljno obezbediti samo kanal komunikacije koji se koristi za daljinski pristup, već i sisteme koji u tome učestvuju (npr. računar člana tima koji on koristi za daljinski pristup može biti zaražen virusom koji bi se tada mogao proširiti na internu mrežu CERT-a, ili neki maliciozni softver na njemu može neprimetno kopirati poverljive podatke ...). Ponekad je najbolje rešenje da se prilikom udaljenog pristupa internoj mreži CERT-a, nivo pristupa svede na najmanju moguću meru, samo na zaista neophodne sisteme, tj. da se onemogući pristup delovima sistema koji su posebno osetljivi.

6.5.6 Fizička bezbednost

Fizičko obezbeđenje prostorija u kojima borave članovi CERT tima, ili se nalaze njihova oprema i sistemi, je problem na koji CERT tim najčešće ne može samostalno da odgovori. Fizičko obezbeđenje je obično u domenu krovne organizacije u kojoj CERT tim funkcioniše, sa dodatnim merama zaštite koje su neophodne sa stanovišta posebnih bezbednosnih potreba CERT tima. Fizički upadi u prostorije CERT tima mogu biti jednako opasni, kao i upadi u njihove sisteme. Potrebno je razmišljati o režimima zaključavanja i pristupa prostorijama, o izbegavanju ostavljanja bilo kakve dokumentacije na vidnom mestu ili na radnom stolu posle radnog vremena, autorizaciji osoblja, kao i načinu na koji se organizuju posete i sastanci u prostorijama CERT tima. Pisana dokumenta treba čuvati na bezbednim mestima, ili u sefovima, a ona koja su nepotrebna treba na odgovarajući način fizički uništiti. Takođe, faks aparati, dežurni telefoni, štampači, skeneri i slična oprema treba da bude na bezbednom mestu. U slučaju da se u prostorijama CERT tima nalaze spoljni posetioci, oni ne treba da budu u mogućnosti da čuju razgovore članova CERT tima, koje oni obavljaju između sebe ili preko telefona.

Kada je u pitanju mrežna infrastruktura, lokacije mrežnih čvorišta, kao i samo kabliranje, treba da bude izvedeno tako da nije moguće prisluškivanje, ili neovlašćeno povezivanje na mrežu, kao ni fizički pristup tim prostorijama bilo kome sem ovlašćenih

članova CERT tima. Isto važi i za prostorije u kojima se nalaze ostali elementi informacionog sistema CERT tima, kao što su serveri baza podataka, i slično.

Takođe, treba obratiti pažnju i na osoblje koje se bavi higijenskim održavanjem prostorija tima, ili održavanjem elektro instalacija, ili bilo kakve druge kancelarijske opreme. Ove osobe su obično „nevidljive“, tj. ne smatraju se bezbednosnim rizikom, ali svakako treba obratiti pažnju i na njihovo prisustvo i ponašanje u prostorijama tima.

6.5.7 Upravljanje kriznim situacijama

U slučaju izrazite krizne situacije, ili katastrofe, bilo da je ona u vidu destruktivnog upada u mrežu i sisteme CERT organizacije, ili da je u pitanju sabotaža, požar, ili nekakva prirodna katastrofa, potrebno je da postoje šeme i procedure za eskalaciju i prioritetizaciju koje daju odgovore na pitanja šta je potrebno učiniti bez odlaganja, i koga treba obaveštavati o razvoju situacije. Potrebno je i da postoji nekakva formalna definicija kada tim prelazi u krizni režim rada, i pod kojim uslovima se vraća u normalni režim rada. Kada je neka krizna situacija u toku, dešava se da u prostorije CERT tima dolaze ljudi kojima tu inače nije dozvoljen pristup, da bi što pre dobili potrebne informacije. Međutim, politike bezbednosti moraju da važe i u ovakvim situacijama, bez razlike.

Primera radi, u slučaju požara može se desiti da prostorije tima u kratkom roku budu pune vatrogasaca, ili ljudi koji se bave hitnim intervencijama. U takvim situacijama je dobro da postoji osoba u okviru tima, koja će u slučaju objave opasnosti od požara, ne dovodeći pri tome svoju bezbednost u veliku opasnost, pokupiti svu dokumentaciju sa radnih stolova, dokumenta sa štampača ili faks aparata, prenosne medijume sa podacima (USB, CD ...), prenosne računare i svu drugu opremu koja bi mogla da „nestane“ u situaciji kada puno ljudi ima pristup prostorijama tima, bez ikakve kontrole.

U slučaju da krizna situacija potraje, potrebno je obezbediti poslovanje CERT tima sa rezervne lokacije, u što kraćem mogućem roku, kako bi se ispoštovale potrebe konstituenata.

6.5.8 Upravljanje internim bezbednosnim incidentima

Sve organizacije imaju težnju da o internim bezbednosnim incidentima ne govore. Ukoliko ne postoji politika ponašanja u ovakvim situacijama u pisanoj formi, koja bi nekoga obavezala na nekakvu konkretnu reakciju, prirodna težnja svake organizacije je da se ovakve situacije „sakriju“. Ali ovo je najčešće pogrešan pristup. Osim u izuzetnim sličajevima namernih internih napada, najčešće ovakvi incidenti, bez obzira što izgledaju kao da su interni, imaju nekakve veze sa entitetima ili događajima izvan CERT organizacije. Posledica toga je da drugi entiteti mogu javno objaviti informacije o ovakvim dešavanjima u okviru CERT organizacije. Na taj način incident postaje javan, čak i ako se CERT tim nije tim povodom oglašavao, ili na bilo koji način evidentirao ovakav incident.

Svaka CERT organizacija bi trebalo da „praktikuje ono što propoveda“, i interni napadi na CERT organizacije ne smeju biti ignorisani, već evidentirani kao i bilo koji drugi bezbednosni incident. CERT timovi moraju da se pripreme za takve incidente i da na njih odgovore, ne samo iz očiglednog razloga da se oni na adekvatan način razreše, već i zbog toga što naknadno objavljivanje takvih incidenata u javnosti može jako loše da utiče na reputaciju CERT organizacije i njene odnose sa konstituentima. Naravno, CERT organizacije, više nego bilo koje druge treba da vode računa o bezbednosti svoje infrastrukture, jer poverenje konstituenata se teško stiče, i ukoliko se incident dogodi, a pri tome se njegova suština skriva, ili bez kontrole procuri u javnost, onda to može biti nepopravljiva šteta po reputaciju CERT

organizacije. Stoga interni incidenti moraju imati visok prioritet u razrešavanju, naravno ne na štetu servisa koji se pružaju konstituentima, ali odgovarajući resursi se moraju dodeliti ovakvim incidentima kako bi se njihove posledice što pre uklonile.

6.6 UPRAVLJANJE LJUDSKIM RESURSIMA

Bez obzira na količinu vremena i resursa koje CERT organizacija troši na uspostavljanje i dokumentovanje svojih politika i procedura, ona mora odgovarajuću pažnju da posveti svojoj osnovnoj delatnosti, a to je isporuka servisa svojim konstituetnima. U tom smislu CERT organizacije se oslanjaju na kompetencije i posvećenost svojih zaposlenih, koji moraju na efikasan način sprovoditi politike i procedure svoje organizacije, demostrirajući pri tome i diplomatske sposobnosti u odnosu sa svojim konstituentima. Stoga osoblje CERT tima ima centralnu ulogu u ostvarivanju misije svoje organizacije, u operativnom delovanju na isporuci servisa njihovim krajnjim korisnicima.

6.6.1 Osoblje CERT tima

Postoji jedna pretpostavka, koja je u velikoj meri netačna, da je najvažnija osobina članova CERT tima njihova tehnička osposobljenost i iskustvo. Iako je to važna i poželjna osobina, još važniji kriterijum je individualna spremnost i želja svakog člana tima da sledi politike i procedure CERT organizacije, i da se na odgovoran i profesionalan način odnosi prema konstituentima, klijentima i drugim entitetima sa kojima CERT organizacija sarađuje. U tom smislu, praktičniji pristup je zaposliti ljude koji imaju manje tehničkog iskustva ili sposobnosti, ali imaju dobre sposobnosti za komunikaciju i saradnju, pa ih zatim obučiti u poslovima tehničke prirode kojima se CERT timovi bave, nego obratno.

Posedovanje dobrih osobina za komunikaciju i međuljudske odnose je jako važno, jer su članovi tima u stalnoj komunikaciji i saradnji, kako između sebe, tako i sa spoljnim saradnicima, drugim CERT timovima, ili konstituentima. Reputacija čitavog tima se bazira na profesionalnoj interakciji svakog člana tima sa spoljnim entitetima, stoga je stalni rad na razvoju međuljudskih odnosa i tehnika komunikacije sa drugima izuzetno važan.

Sledeće karakteristike članova tima su izuzetno važne za uspešno ostvarivanje misije tima kao celine:

- zdrav razum i efikasnost u donošenju prihvatljivih odluka, kada god se član tima nađe u nepredviđenoj situaciji, ili je pod stresom usled intenziteta događaja i kratkog vremena za adekvatnu reakciju,
- sposobnost efikasne usmene i pisane komunikacije (na maternjem i stranim jezicima) u saradnji sa konstituentima, ili drugim CERT timovima,
- diplomatsko ophođenje u saradnji sa spoljnim entitetima, naročito sa konstituentima i predstavnicima medija,
- sposobnost i volja da se prate i poštuju politike i procedure svoje CERT organizacije,
- želja da se stalno edukuje i prate trendovi na polju informacione bezbednosti,
- sposobnost da se bori sa stresom i efikasno radi pod pritiskom,
- sposobnost timskog rada,
- svest o reputaciji CERT organizacije, i sposobnost da se deluje na njenom očuvanju,
- spremnost da se prizna greška u radu, ili nepoznavanje neke materije,
- sposobnost snalaženja u novim i nepredviđenim situacijama,
- sposobnost upravljanja vremenom, kako bi se koncentrisali na ono što su prioriteti.

Iz tehničke perspektive, svaki član tima koji se bavi bezbednosnim incidentima mora imati osnovno razumevanje tehnologija koje su u pozadini dešavanja i problema, na kojima će bazirati svoju kasniju ekspertizu. Priroda ovih veština i sposobnosti je slična, bez obzira na konkretne softverske ili hardverske tehnologije koji koristi CERT tim, ili njegovi konstituenti.

Članovi CERT tima moraju imati osnovna tehnološka znanja iz sledećih oblasti:

- tehnologija javnih mreža za prenos podataka (FR, ATM, MPLS...),
- Internet protokola i mreža (od aspekata koji se tiču istorije razvoja i arhitekture mreže, do budućih stremljenja i filozofije u njihovoj pozadini),
- mrežnih protokola (IP, ICMP, TCP, UDP ...),
- elemenata mrežne infrastrukture (ruteri, DNS, serveri elektronske pošte ...),
- mrežnih aplikacija, servisa i protokola u vezi sa njima (SMTP, HTTP, HTTPS, FTP, TELNET, SSH, IMAP, POP3 ...),
- osnovnih principa bezbednosti,
- rizika i pretnji po informacione sisteme i mreže,
- bezbednosne ranjivosti i slabosti sistema, i napada koji su u vezi sa njima (maliciozni softveri, IP *spoofing*, Internet *sniffers*, DoS napadi ...),
- elemenata bezbednosti mreža (*firewall* tehnologije, VPN tehnologije ...),
- metoda enkripcije (DES, 3DES, AES ...), digitalnih potpisa (RSA, DSA, DH ...) i kriptografskih algoritama (MD5, SHA-1, SHA-2 ...),
- elemenata bezbednosti računarske i serverske infrastrukture, sa stanovišta korisnika i administratora sistema (operativni sistemi, instalacija bezbednosnih zakrpa, *back-up* sistema ...).

Pri svemu ovome, imperativ je da bar neki članovi tima poseduju duboko razumevanje čitavog spektra tehnologija i sistema koji se koriste u okviru same CERT organizacije, ali i kod njenih konstituenata. Ovaj viši nivo ekspertize je osnova za širenje i produbljivanje tehnoloških znanja i mogućnosti čitavog tima, kroz odgovarajuće interne obuke, treninge ili dokumentaciju. Time se, takođe, omogućava i efikasna isporuka servisa svojim konstituentima. Kao dodatak na prethodno navedena tehnološka znanja, poželjan je viši nivo ekspertize iz sledećih oblasti:

- programiranje i administriranje mrežnih komponenata (ruteri, svičevi, *firewall* uređaji ...) i operativnih sistema (UNIX, Linux, Windows, ...),
- iskustvo u međuljudskim odnosima i komunikaciji, iskustvo u prezentovanju na konferencijama i obukama, ili rukovođenje grupom,
- iskustvo u organizaciji procesa rada.

Ne postoji jedinstven skup veština koji bi bio primenljiv na bilo kojoj poziciji u okviru CERT tima. Potrebno je i imati uvid u sisteme konstituenata i skup tehnologija koje oni koriste, kako bi se utvrdilo koje veštine i znanja članovi CERT tima treba da poseduju. Kada god je to moguće treba angažovati pojedince koji svojim sposobnostima mogu da pokriju više tehnologija, kako nijedan član tima ne bi bio nezamenljiv. Sa druge strane, manji timovi moraju da imaju bar jednog čoveka za svaku bitnu tehnologiju, koji u toj oblasti poseduje visok nivo ekspertize, da bi na profesionalan način mogao da odgovori na potrebe konstituenata.

6.6.2 Prijem novih članova CERT tima

Kada se razmatra izbor kandidata za upražnjeno radno mesto, važno je unapred definisati procedure i kriterijume za izbor najboljih kandidata. Primeri iz prakse pokazuju da čak i kada izgleda da neki kandidat poseduje odgovarajući nivo sposobnosti, ipak na kraju nije u stanju da se uklopi u radno okruženje CERT tima. Dodatno, kada dođe do neke krizne situacije, može se desiti da neki kandidati ne budu u stanju da se izbore sa svojim obavezama i poslom. Dobar pristup je da kandidat prođe kroz proces zapošljavanja, koji je osmišljen tako da do izražaja dođu svi njegovi kvaliteti, ali i slabosti. Na bazi informacija koje tim dobije tokom procesa probnog rada, tim može lakše da donese odluku da li je neki kandidat pogodan da se investira u njegovu obuku, na poslovima koji su od interesa CERT timu, ili da odluči da ga uopšte ne angažuje.

U pogledu zapošljavanja CERT timovi mogu biti ograničeni raznim faktorima, kao što su zahtevi njihove krovne organizacije, ili zakonska ograničenja. U svakom slučaju, u procesu zapošljavanja treba sprovoditi sledeće korake, kada god je to moguće:

- provera dokumentacije pre razgovora sa kandidatom,
- uvodni telefonski razgovor sa potencijalnim kandidatom,
- intervjui sa kandidatom na razne teme, od tehničkih sposobnosti, preko socijalnih veštima, do uklapanja u timski način rada,
- tehnička prezentacija kandidata,
- provera referenci, uključujući i kriminalni dosije, ukoliko je potrebno.

U zavisnosti od specifičnih potreba krovne organizacije, ili konstituenata, ponekad mogu biti potrebne dodatne bezbednosne provere kandidata.

Sve u svemu, proces zapošljavanja treba da bude osmišljen tako da se utvrdi da li kandidat ima odgovarajuće karakteristike u pogledu međuljudskih odnosa, i da li ima sposobnosti, ili može biti obučen do odgovarajućeg nivoa tehničkog znanja za obavljanje poslova u okviru CERT tima. U interakciji sa potencijalnim kandidatom treba da učestvuje što je moguće više članova CERT tima, bilo kroz formalne intervjue, ili kroz neformalne sastanke, ili kao posmatrač tehničke prezentacije kandidata. Pri tome treba voditi računa da se članovi tima što manje opterećuju ovim zadacima, ali da se postigne maksimalni mogući efekat njihovog prisustva.

Uvodni telefonski razgovor sa kandidatom, i prethodna provera njegove dokumentacije imaju za cilj da se utvrdi da li je kandidat vredan pažnje i nastavka procesa zapošljavanja kroz intervjue i prezentacije. Tom prilikom treba utvrditi opšti nivo zainteresovanosti kandidata za teme informacione bezbednosti, i potvrditi neke od navoda iz njegove biografije. Ali, možda najvažnije je da je to prilika da se utvrde veštine kandidata u verbalnoj komunikaciji.

Kako bi se postojeći članovi tima na što bolji način pripremili za potrebe intervjuisanja novih kandidata, potrebno je unapred definisati pogodne teme za razgovor (tehničke, etičke, socijalne ...), i odrediti ko su najpogodniji članovi tima koji u tim razgovorima mogu učestvovati. Sve informacije koje se na ovaj način dobiju od potencijalnog kandidata mogu se naknadno prodiskutovati među svim članovima tima, kako bi se njegove sposobnosti i ograničenja sagledali iz različitih uglova, i donela najbolja odluka u interesu CERT tima.

Zahtev kandidatu da održi tehničku prezentaciju pred članovima tima predstavlja mogućnost da se procene tehničke i prezenterske kompetencije kandidata. To je prilika i da se proceni ponašanje kandidata u situaciji koja je donekle stresna za njega, kao i neke od

njegovih opštih osobina, kao što su tehnička preciznost, obraćanje pažnje na detalje, ili sposobnost da odgovara na pitanja i izazove u realnom vremenu.

Jednom kada kandidat postane član tima potrebno je uložiti još dodatnih napora da se on uspešno integriše u CERT organizaciju. Uobičajeno je da novi zaposleni u prvo vreme ima treninge i obuke za redovne poslove tima, i da mu se dozvoli pristup ograničenom skupu sistema i informacija, pre nego što posle nekog vremena obuke i upoznavanja sa politikama i procedurama CERT organizacije, kao i procene njegove sposobnosti i podobnosti, ne dobije pun pristup svim sistemima i informacijama.

6.6.3 Procedure ulaska u CERT tim i napuštanja tima

S obzirom na prirodu i osetljivost informacija koje su u posedu CERT organizacije, potrebno je razviti posebne procedure koje se primenjuju za prijem novih članova tima, ili kada neki od zaposlenih napusti CERT organizaciju. Procedura prijema novih zaposlenih u CERT organizaciju može da podrazumeva potpisivanje dodatnih ugovora, mimo standardnog ugovora o radu, koji se tiču poverljivosti informacija, ili čuvanju intelektualne svojine. Takođe, dodatni dokumenti mogu da se tiču pravila objavljivanja informacija, karakteristika mrežnog povezivanja, ili interakcije sa medijima.

Takođe, pre nego što neki član tima napusti CERT organizaciju (čak i ako se radi o promeni radnog mesta koje podrazumeva angažovanje u okviru krovne organizacije koja je osnivač CERT tima) potrebno je ispoštovati proceduru izlaska, koja može podrazumevati:

- promenu svih lozinki (ličnih i sistemskih),
- vraćanje bilo kakvih uređaja, ili bezbednosnih uređaja, ili medijuma (laptop, telefon, USB, CD ...),
- oduzimanje svih ključeva (fizičkih ili digitalnih),
- izlazni intervju, kako bi se sagledala stečena iskustva osobe koja napušta tim, i prikupile ideje za poboljšanja u okviru tima, kao i da se osoba upozori na odredbe ugovora koje i dalje mora da nastavi da poštuje iako više nije član tima,
- obaveštavanje konstituenata i drugih entiteta koji treba da imaju informaciju da je neka osoba napustila CERT tim, uključujući i gašenje njegove adrese za elektronsku poštu, i preusmeravanje komunikacija na druge kontakte u okviru tima.

Ukoliko neka osoba napušta CERT tim po svojoj volji, dobro je otkriti razloge za takvu odluku. To može da pomogne timu da prepozna okolnosti na koje treba obratiti pažnju kako bi se izbegla situacija da još članova tima napusti organizaciju.

Sa druge strane, ukoliko organizacija odluči da otpusti nekog člana tima, to može podrazumevati različite izlazne procedure, u zavisnosti od pozadine događaja i razloga da se takva odluka donese. U tim situacijama naročito treba povesti računa o bezbednosnim aspektima, koji se tiču promene lozinki, ključeva, oduzimanja službenog računara, prenosnih medijuma, i slično.

6.6.4 Obučavanje zaposlenih

Obučavanje zaposlenih u CERT organizaciji je neophodno iz najmanje tri razloga: dovođenje novih članova tima na odgovarajući nivo stručnosti za obavljanje svakodnevnih zadataka, proširenje sposobnosti postojećih članova tima radi ličnog razvoja ili prosperiteta

tima kao celine, i generalno održavanje nivoa sposobnosti čitavog tima u skladu sa novim tehnologijama i izazovima pred koje napadači stavljaju CERT organizacije.

Kada se sagledavaju potrebe za obučavanje CERT tima, treba voditi računa o veštinama koje su neophodne svakom članu tima, kao i o skupu veština i mogućnosti koje tim treba da poseduje kao celina. Nove članove tima treba odmah obučavati u svim aspektima koji su neophodni da oni u što kraćem roku postanu produktivni članovi tima. CERT organizacija treba da ima politike i procedure kojima se pokriva barem inicijalni nivo treninga neophodan novim članovima tima, ali je potrebno predvideti i obuke koje su neophodne kao podrška novim servisima ili oblastima delovanja CERT tima. Ponekad je potrebno sprovoditi i kurseve kojima se članovima tima skreće pažnja na to zašto je neophodno da se pridržavaju uspostavljenih politika i procedura. Takođe, potrebno je sprovoditi i vežbe u kojima će članovi tima biti u prilici da, na bazi politika i procedura poslovanja, ali i sopstvenog rasuđivanja, donose odluke i sprovode aktivnosti sa kojima se mogu susresti u realnim situacijama tokom rada.

Kao dodatak na tehničke aspekte, kao i aspekte međuljudskih odnosa o kojima je ranije bilo reči, veoma je važno da svaki član tima bude obučen u specifičnim oblastima servisa za upravljanje incidentima, u okruženju i na način na koji ih dotična CERT organizacija realizuje. Takvi treninzi treba da pokrivaju sledeće oblasti:

- razvoj novih tehnologija,
- politike i procedure lokalnog tima,
- razumevanje i razotkrivanje tehnika koje koriste napadači,
- komunikacija sa spoljnim entitetima,
- analiza incidenata,
- vođenje evidencije o incidentima,
- izgradnja timskog duha,
- organizacione tehnike i delegiranje poslova.

Inicijalni treninzi novih zaposlenih su jako povezani sa aktivnostima na radnom mestu i na njih treba obratiti posebnu pažnju. U mnogim profesijama, pa i kada su u pitanju CERT organizacije, oni se svode na čitanje dostupne dokumentacije, posmatranje poslovnih procesa i učenje na bazi iskustva. Naravno, u situacijama kada je jako malo dokumentacije dostupno, novi članovi su još više upućeni na razmenu iskustava sa svojim starijim kolegama, i učenje na bazi primera iz svakodnevnog procesa rada.

Naravno, u današnje vreme postoje mnoge zajednice i organizacije čija je misija da proces edukacije novih članova tima, kao i CERT timova u celini, učine lakšim, kroz izradu materijala za kurseve i treninge u oblastima koje su u vezi sa servisom upravljanja incidentima, u svim njegovim aspektima. Ti materijali pokrivaju aspekte tehničke ekspertize iz raznih oblasti koje su u opisu delovanja CERT organizacija, ali i teme koje se tiču formiranja ovih organizacija, ili efikasnog angažovanja i upravljanja takvim organizacijama.

Za nove članove timova je jednako važno da stalno pregledaju i upoznaju se sa internim dokumentima, kao što su politike i procedure, ali i studijama raznih slučajeva sa kojima se mogu susresti tokom rada, ili izveštajima o incidentima koji su ranije zabeleženi i ostali sačuvani u arhivi CERT tima.

Kada su u pitanju poverljive informacije, čak i najiskusniji članovi tima doživljavaju određeni nivo stresa kada barataju sa takvim informacijama. Taj nivo stresa potiče od činjenice da su svesni razmera posledica koje se mogu dogoditi ukoliko bi zbog nesmotrenosti došlo do neželjenog otkrivanja nekih informacija. Kada su u pitanju novi članovi tima, oni su uglavnom preopterećeni količinom informacija i veština koje treba da steknu kako bi se uklopili u poslovanje CERT tima, i njih ne treba u prvo vreme izlagati mogućnosti da imaju

posla sa osetljivim informacijama, sve dok ne prođu određeni nivo obuke i ne steknu dovoljno iskustva kako bi se na zadovoljavajući način odnosili prema osetljivim informacijama. Treba učiniti sve da se njima omogući da se uključuju u posao, bez opasnosti da naprave skupocene greške. Uobičajeni pristup je da svaki novi član tima ima iskusnijeg mentora, koji ga uvodi u posao kroz upoznavanje sa politikama i procedurama tima, kao i kroz obuku za osnovne funkcije trijaže i upravljanja incidentima, pre nego što im se omogući da počnu samostalno da se bave manjim bezbednosnim incidentima.

Interne obuke na radnom mestu mogu biti dobro rešenje i za starije članove tima, kojima je potrebna obuka iz neke oblasti koja nije u fokusu njihovog svakodnevnog delovanja.U uslovima brzog tehnološkog razvoja i jednog tako dinamičnog okruženja koje podrazumevaju poslovi na očuvanju informacione bezbednosti, razmena iskustava između članova tima je od vitalne važnosti za uspeh celog tima. Kao dodatak na ovo preporučuje se da članovi tima redovno učestvuju na stručnim skupovima i konferencijama, da uzmu učešće u međunarodnim forumima i organizacijama koje se bave informacionom bezbednošću i da tako stečena znanja i veštine šire među ostalim članovima tima.

6.6.5 Očuvanje osoblja CERT tima

Kao što je ranije već pomenuto, jako je teško doći do kvalitetnih kadrova za potrebe CERT timova, i cena njihovog rada i obuke može biti jako velika. Samim tim, s obzirom na vreme i resurse koje je potrebno angažovati za pronalaženje i obučavanje kvalitetnih zaposlenih, potrebno je uložiti i odgovarajuće napore da se oni zadrže u okvirima CERT organizacije. Dva glavna razloga zbog kojih ljudi napuštaju CERT organizaciju su zasićenje poslom, i finansijski razlozi.

Mnogi članovi CERT timova pate od zasićenja poslom u situacijama kada su svakodnevno suočeni sa stresom i pritiskom obaveza koje sa sobom nosi pružanje servisa za upravljanje incidentima, i kada to počne da utiče na njihov privatni život. Često se dešava da zaposleni postaju zamoreni rutinskim aktivnostima koje svakodnevno obavljaju, psihički su umorni, gube pažnju za detalje, i mogu da počnu da prave velike greške u svakodnevnom radu. Kada su u pitanju finansijski aspekti, potrebno je članovima CERT tima obezbediti zarade koje su uporedive sa sličnim radnim mestima u drugim organizacijama koje se bave informacionom bezbednošću, ali im omogućiti i lični razvoj i napredovanje u stručnom smislu, kako bi bili motivisani da ne napuštaju CERT organizaciju. Kako bi se osoblje CERT tima što duže zadržalo u okvirima organizacije treba učiniti sledeće:

- vršiti rotaciju zaposlenih po radnim mestima u okviru tima, kako bi se sprečilo zapadanje u rutinu i zasićenje jednoličnim poslom,
- nijedan zaposleni ne treba da provodi više od 80% svog radnog vremena na poslovima upravljanja incidentima,
- svi zaposleni treba da prisustvuju treninzima, obukama i stručnim skupovima, vezano za svoju konkretnu oblast interesovanja i angažovanja,
- zaposleni treba da učestvuju u radnim grupama gde bi proširili delokrug svojih aktivnosti i sticali iskustva u saradnji sa širom zajednicom eksperata iz svoje oblasti,
- treba posvetiti pažnju internim obukama i razmeni iskustava između zaposlenih unutar organizacije.

CERT organizacije koje imaju najbolje rezultate u očuvanju svog stručnog kadra puno napora ulažu na održanje timskog duha i dobre saradnje članova tima, kako na poslovnom planu, tako i u ličnim kontaktima i druženju. U takvim organizacijama se svakom članu tima

posvećuje dužna pažnja i odaje poštovanje za trud koji svaki pojedinac ulaže u uspeh tima kao celine.

6.6.6 Proširenje osoblja CERT tima

Postoje situacije u kojima CERT organizacije nisu u mogućnosti da angažuju adekvatno osoblje, iz razloga što ne mogu da pronađu adekvatne ljude, nisu u mogućnosti da ih obuče, ili nemaju sredstava da ih angažuju. U takvim situacijama CERT timovi su obično prinuđeni da razviju mrežu spoljnih saradnika, koji su eksperti u određenim oblastima koje CERT organizacija samostalno ne može da pokrije. Takođe, postoje i situacije kada nivo posla i angažovanja može toliko da naraste (na primer zbog nekog incidenta velikih razmera) da CERT organizacija nije u mogućnosti da samostalno odgovori na taj izazov, i tada je prinuđena da angažuje spoljne saradnike da joj pomognu u nekim aspektima posla. Stoga je neophodno da CERT organizacije imaju procedure koje se primenjuju u ovakvim situacijama, kao i da identifikuje pojedince ili organizacije kojima će se obratiti za pomoć u slučaju nužde. Te organizacije ili pojedinci mogu biti:

- drugi timovi za informacionu bezbednost u okviru krovne organizacije koja je osnivač CERT-a,
- druge grupe u okviru krovne organizacije koja je osnivač CERT-a,
- druge grupe ili eksperti iz konstituentskih organizacija,
- druge CERT organizacije,
- eksterni eksperti za pojedine specifične oblasti informacione bezbednosti.

Kada je u pitanju osoblje koje će uzeti ulogu u pomoći CERT timu, za njih moraju važiti ista pravila kao i za stalne članove CERT tima. Takođe, potrebno je unapred definisati sledeće procese, kako bi se dodatno osoblje moglo angažovati u što kraćem roku:

- definisati kriterijume pod kojim uslovima se pristupa angažovanju dodatnih članova tima,
- potrebno je ugovorno definisati odnose sa dodatnim osobljem (ugovori o poverljivosti informacija, memorandumi o saradnji i razumevanju, i slično ...),
- održavati ažurnom bazu kontakata sa ovakvim organizacijama ili pojedincima,
- sprovesti procedure za bezbednu komunikaciju,
- obučiti dodatno osoblje za rad po procedurama o politikama CERT organizacije.

Jako je važno da se ovom dodatnom osoblju omogući da povremeno ima priliku da sarađuje sa članovima tima, na realnim poslovima i u radnom okruženju CERT tima, kako bi iz prve ruke bili upoznati sa procedurama i načinom obavljanja posla, tj. kako bi se na kvalitetan način uključili u aktivnosti onda kada je to zaista neophodno.

7. PROCESI I PROCEDURE U RADU CERT ORGANIZACIJA

Upravljanje incidentima je osnovna delatnost svake CERT organizacije, i u ovom poglavlju biće opisane sve komponente ovog servisa, kao i procedure i procesi koje su u njegovoj osnovi. Opis svakog servisa treba da ima barem dva aspekta:

- opis, tj. specifikaciju servisa (logički aspekt) - Ovo je opis namene i strukture servisa i njegovih funkcija, i
- način implementacije servisa (tehnički aspekt) - Ovde se specificira skup alata, procedura, i uloga koje su neophodne za implementaciju specificiranih procesa, na definisani način.

7.1 OPIS SERVISA

Servisi koje nudi CERT organizacija treba da budu jasno definisani. Potrebno je da svaka definicija bude razumljiva i dostupna, kako unutar CERT organizacije, tako i spoljnim saradnicima i konstituentima. Pri tome, definicije namenjene za internu, tj. spoljašnju upotrebu mogu sadržati različite nivoe apstrakcije.

7.1.1 Ciljevi servisa za upravljanje incidentima

CERT organizacija treba da ima jasnu definiciju svojih ciljeva kako bi se olakšala izrada procesa i procedura u okviru organizacije. Kada je u pitanju servis upravljanja incidentima, ciljevi ovog servisa izvode se iz definisane misije CERT organizacije, koja je opet rezultat definicije misije tima za informatičku bezbednost, ili krovne organizacije u okviru koje CERT funkcioniše. Zatim se u vezi sa navedenim ciljevima CERT organizacije definišu opseg i razmere procesa za upravljanje incidentima, koji su neophodni kako bi se ispunili definisani ciljevi ovog servisa.

Na primeru nacionalnog CERT-a ovaj skup definicija predstavljen je u tabeli 7.1.

Tabela 7.1: Skup ciljeva servisa za upravljanje incidentima nacionalne CERT organizacije

TIP CERT ORGANIZACIJE	PRIRODA MISIJE	MOGUĆI CILJEVI SERVISA
Nacionalni CERT	Predstavlja kontakt na nacionalnom nivou za pitanja informacione bezbednosti i radi na smanjenju broja bezbednosnih incidenata u okviru svoje zemlje, bilo da oni potiču iz te zemlje, ili su usmereni na sisteme u toj zemlji.	Obezbeđuje tehničku podršku, na zvaničnom jeziku i u okviru pripadajuće vremenske zone, kao odgovor na bezbednosne incidente. Obezbeđuje neophodne tehničke informacije radi detekcije, prevencije i oporavka od uočenih ranjivosti sistema. Predstavlja vezu sa nacionalnim istražnim i pravosudnim organizacijama.

7.1.2 Definicija servisa za upravljanje incidentima

Pre nego što se krene u opis kako će servis za upravljanje incidentima biti implementiran, važno je razumeti obim i dubinu servisa koje treba obezbediti, a u skladu sa raspoloživim resursima. Za početak, dobro je identifikovati ograničavajuće faktore, koji utiču na nivo servisa koji može da se ponudi svojim konstituentima. Ograničavajući faktori mogu biti sami definisani ciljevi servisa, kao i resursi (fizički, finansijski, nivo stručnosti ...) koje CERT tim ima na raspolaganju, ali i autoritet koji CERT tim ima nad svojim konstituentima. Sledeći primeri pokazuju kako različiti servisi mogu postići svoju svrhu i imati zadovoljavajuću ulogu u očuvanju informatičke bezbednosti, uprkos različitim ograničavajućim faktorima.

Primer 1: Najčešći ograničavajući faktor za CERT organizacije je njihov budžet, koji utiče kako na broj zaposlenih, tako i na fizičke resurse koji su im na raspolaganju za implementaciju servisa. Međutim, mnogi CERT timovi koji danas postoje obezbeđuju minimalni servis za upravljanje incidentima koji se sastoji od jednostavne trijaže, upravljanja razrešenjem incidenta i davanja povratnih informacija konstituentima, sve to kombinovano u jedan „servis“.

Primer 2: CERT organizacije različitih tipova (na nacionalnom nivou, u okviru privatnih kompanija, ili kod provajdera telekomunikacionih ili Internet servisa ...), koje imaju ograničene budžete za svoje delovanje, fokusiraju se na aktivnosti za zadovoljenje potreba samo svojih konstituenata, umesto da se bave širim krugom potencijalnih korisnika kojima bi davali operativnu podršku. Ovi timovi igraju ulogu centralne tačke kontakta za potrebe svojih konstituenata, radi razmene informacija o incidentima sa entitetima koji su zahvaćeni tim incidentima.

Primer 3: Postoje situacije kada CERT organizacija ima sredstva da zaposli nekoliko članova tima, ali nije u prilici da privuče, obuči, ili zadrži osoblje koje ima dovoljan nivo tehničke stručnosti. U takvoj situaciji tim ne može da ponudi sveobuhvatan servis za upravljanje incidentima, koji bi u svim funkcijama bio nezavisan od pomoći izvan organizacije. U tom slučaju CERT tim mora da se oslanja na informacije koje dobija od

drugih timova, koji imaju više tehničkih znanja, i da te informacije prosleđuje svojim konstituentima.

Dakle, imajući u vidu resurse koji su na raspolaganju, ograničavajuće faktore, kao i mehanizme na kojima se bazira struktura same CERT organizacije, i ciljeve koji se žele postići, treba definisati servis za upravljanje incidentima. Naročito treba obratiti pažnju na nivo servisa koje je CERT organizacija sposobna da ponudi, a zatim tako definisan servis treba razbiti na niz procesa koji su neophodni za implementaciju servisa.

Nekada je dobro napraviti dva opisa servisa, bazirana na istom skupu kriterijuma i definicija. Jedan opis, koji bi bio dostupan spoljnjim entitetima (konstituenti i/ili partneri), sadržao bi informacije o tome kome je servis dostupan, kako se do njega dolazi, i kakvu vrstu podrške korisnik može da očekuje. Drugi opis, za internu upotrebu, pored prethodno navedenih informacija (ko-kako-šta ...), treba da sadrži i detaljnije uputstvo za internu implementaciju servisa. To obuhvata i administrativna pitanja, kao što su način prikupljanja i čuvanja informacija (uključujući i ko je odgovoran za ovaj proces), specificirane načine za prioritetizaciju aktivnosti, kao i striktne odrednice šta je tačno dostupno korisnicima unutar granica definicije servisa.

Dakle, eksterni opis treba da bude podskup internog opisa servisa. U zavisnosti od tipa konstituenata, eksterni opis može biti formulisan na način koji je razumljiv ljudima koji nisu eksperti na polju informatičke bezbednosti. Takođe, u situacijama kada se nivo servisa može promeniti usled pojave neočekivanih okolnosti, potrebno je obezbediti dodatne informacije u tom smislu, koje bi bile dostupne korisnicima servisa.

7.1.3 Opis procesa u okviru servisa za upravljanje incidentima

Servis za upravljanje incidentima generalno obuhvata izveštavanje, analizu i tehničku podršku. Ovaj servis se može dalje opisati u svetlu svoja četiri osnovna procesa: trijaža, razrešavanje, izdavanje obaveštenja i davanje povratnih informacija korisnicima.

Svaki od ovih procesa je potrebno interno dokumentovati, u okviru CERT organizacije, u vidu jasnih opisa. Ovi opisi se zatim koriste za generisanje procedura za implementaciju pojedinačnih procesa.

Definicije procesa trebalo bi u najmanjem da sadrže:

- cilj procesa,
- detalje implementacije, sa osvrtom na pripadajuće procedure,
- kriterijume za prioritetizaciju,
- nivo servisa koji se obezbeđuje, i
- kriterijume za uspostavljanje i garanciju kvaliteta servisa.

7.1.4 Dostupnost servisa za upravljanje incidentima

Definisanje dostupnosti servisa nije samo odgovor na pitanje „ko i kada može nekoga da kontaktira“, već i „pod kojim uslovima“:

- Ko može da koristi servis - Da li su neki aspekti servisa dostupni samo za deklarisane konstituente (kao što je izdavanje obaveštenja ili tehnička podrška na razrešavanju incidenata), i da li su neki drugi aspekti dostupni širem krugu korisnika (na primer prihvatanje informacija o incidentima od bilo koga, u slučaju da mogu imati uticaja na deklarisane konstituente) ?

- Vreme tokom kojeg je servis dostupan - Da li su u različito doba dostupni različiti nivoi servisa ? Na primer, funkcija davanja povratnih informacija može biti dostupna samo tokom regularnog radnog vremena, dok funkcija razrešavanja incidenata može biti dostupna tokom radnog vremena, ili na bazi 24/7, za sve, ili samo za neke tipove incidenata, ili za neki poseban podskup konstituenata.
- Uslovi pod kojima je servis dostupan - Na primer, prijava incidenta se prihvata samo preko formulara CERT organizacije, pri čemu je potrebno ostaviti sve informacije koje su u formularu označene kao obavezne.

7.1.5 Garancija kvaliteta servisa za upravljanje incidentima

Korisnicima servisa treba dati informacije na osnovu kojih mogu da baziraju nivo svojih očekivanja u pogledu servisa koji se nudi. Pri tome, tim treba da ponudi viši nivo očekivanja za svoje deklarisane konstituente, ili krovnu organizaciju u okviru koje funkcioniše, u odnosu na druge entitete koji mu nisu u primarnom fokusu. Potrebno je jasno navesti šta servis obuhvata, tj. šta ne podrazumeva. Dobro je i navesti vremenski okvir kada korisnik može da očekuje odgovor ili aktivnost CERT organizacije, po prijavi bezbednosnog incidenta, kao i na koji način se CERT organizacija odnosi prema različitim tipovima informacija do kojih dolazi. Takođe, skup očekivanja treba da bude usaglašen i sa kriterijumima za prioritetizaciju u okviru posmatranog servisa.

7.1.6 Saradnja i razmena informacija

Korisnici servisa moraju razumeti način na koji mogu sa komuniciraju i sarađuju sa CERT organizacijom, kao i način na koji se postupa sa informacijama koje se tom prilikom razmenjuju (na primer, šta se dešava sa artefaktima ili log fajlovima koje oni predaju CERT organizaciji u procesu razrešavanja incidenta; da li se i pod kojim uslovima ti podaci dele sa drugim CERT organizacijama, stručnjacima za bezbednost, proizvođačima opreme i slično).

7.1.7 Koordinacija sa drugim servisima

U zavisnosti od skupa svih servisa koje CERT organizacija nudi svojim korisnicima, mogu postojati razni kriterijumi i tačke u kojima se protok informacija deli između različitih procesa ili servisa. Na primer, proces trijaže je zajednički za sve tipove servisa, i obično postoji kao jedinstveni proces za sve servise koje CERT organizacija nudi.

7.1.8 Prioritetizacija

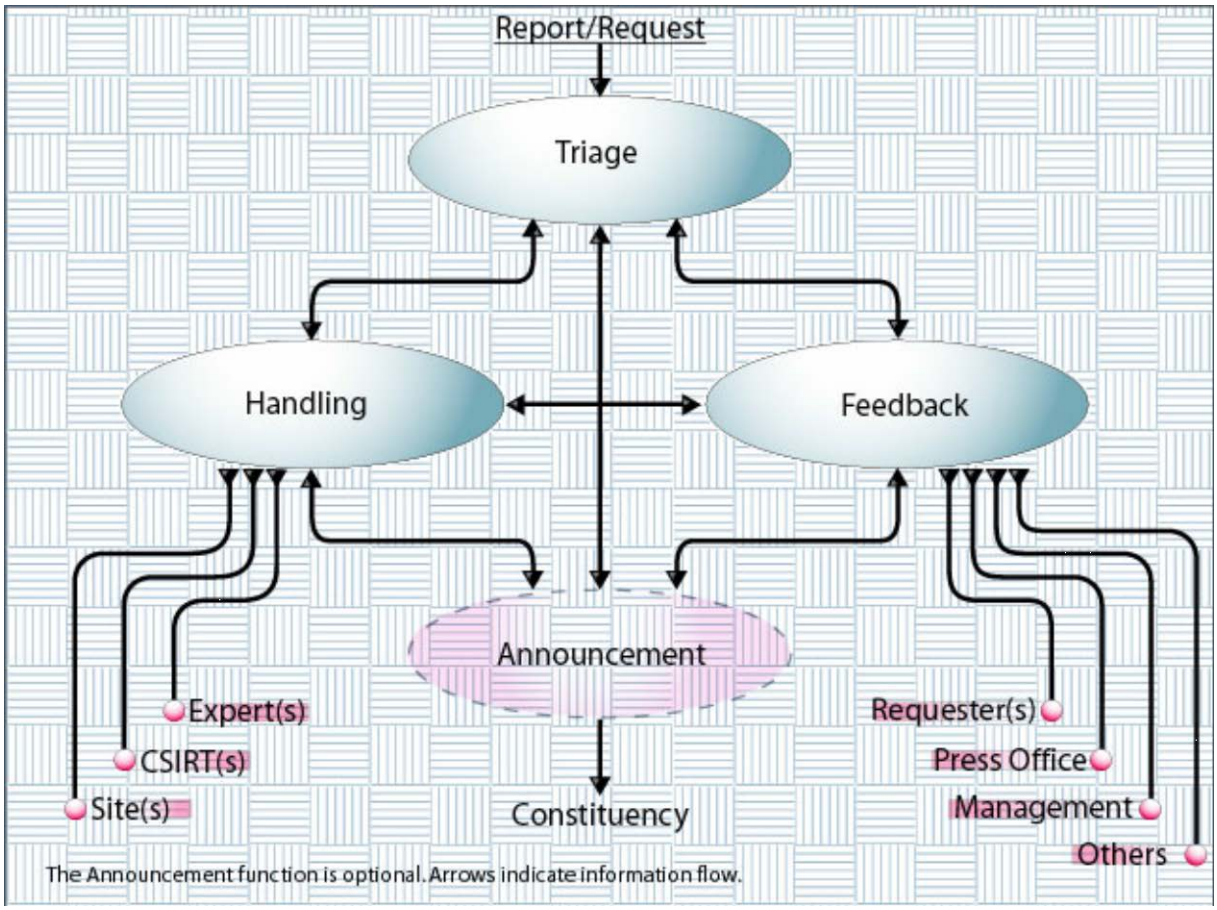
Prioritetizacija događaja, tj. aktivnosti, je izuzetno važna u okviru svakog od procesa, ali je isto tako važno razumeti međusobni odnos između različitih procesa u okviru jednog servisa, kao i međusobni odnos servisa za upravljanje incidentima u odnosu na druge servise koje CERT orgaizacija nudi. Potrebno je dodeliti odgovarajuće prioritete različitim ciljevima CERT tima, kao i servisima koje on nudi. Ukoliko su resursi limitirani, proces razrešavanja incidenata obično ima prednost u odnosu na izdavanje obaveštenja, ili davanje povratnih informacija. Takođe, treba ovde naglasiti da je proces trijaže preduslov za dobru efikasnost u procesu razrešavanja incidenata, tako da ovaj proces mora da ima svoje mesto tokom prioritetizacije aktivnosti.

7.2 PREGLED SERVISNIH PROCESA

Kao što je već navedeno, servis upravljanja incidentima sastoji se od različitih aktivnosti (trijaža, razrešavanje incidenata, izdavanje obaveštenja i davanje povratnih informacija korisnicima) koje sačinjavaju njegove procese, kao što je predstavljeno na slici 7.1.

Važno je napomenuti da danas postoje mnoge CERT organizacije koje pružaju servise za upravljanje incidentima, koji su funkcionalno organizovani na gore pomenuti način, ali su velike razlike među njima u načinu implementacije. Te razlike su posledica raznih faktora kao što su: finansiranje, nivo stručnosti, ili organizaciona struktura.

Primera radi, u malim timovima servisni procesi ne moraju biti „individualizovani“, tj. jedna osoba, sa odgovarajućim nivoom stručnosti, može biti nosilac posla u okviru različitih procesa. Sa druge strane, veći timovi mogu da uspostave *help-desk* službu koja se bavi poslovima trijaže i davanja povratnih informacija korisnicima servisa, dok se poslovi u okviru procesa razrešavanja incidenata prebacuju na članove tima sa višim nivoom tehničke osposobljenosti.



Slika 7.1: Procesi servisa za upravljanje incidentima

Proces trijaže obezbeđuje jedinstvenu tačku kontakta za prihvatanje, prikupljanje, sortiranje, i prosleđivanje dobijenih informacija, u okviru servisa koji se pružaju konstituentima. Dodatno, ovaj proces može biti kanal preko kojeg se prosleđuju sve relevantne informacije ka spoljnjim entitetima. On podržava različite kanale za prijem informacija, koji su pogodni za CERT tim i njegove konstituente. Prilikom svake nove prijave

koja pristigne dodeljuje se inicijalni prioritet događaja i odgovarajući broj za identifikaciju prijave. Kao deo ovog procesa mogu se preduzeti i dodatne aktivnosti (kao što su arhiviranje, prevođenje ili konverzija) kako bi se olakšale aktivnosti u okviru procesa razrešenja incidenata.

Proces razrešavanja incidenata podrazumeva davanje podrške, tj. aktivnosti koje su u vezi sa razrešavanjem sumnjivih ili potvrđenih bezbednosnih incidenata, pretnji ili napada. Ovaj proces može da uključuje veliki broj različitih aktivnosti. Da bi se utvrdio uzrok incidenta pristupa se pregledu prijave incidenta, analiziraju se dokazni materijali (kao što su npr. log fajlovi), utvrđuje se ko je uključen u incident (ili ko tim povodom treba da bude kontaktiran), i koja vrsta podrške i u kojoj meri je potrebna. Potrebno je da CERT tim na odgovarajući način reaguje (u skladu s svojom misijom, ciljevima i definicijama servisa), i potrebno je da o tome obavesti onoga ko je prijavio incident, ili svoje konstituente generalno.

Proces izdavanja obaveštenja podrazumeva generisanje obaveštenja, u različitim formatima, i prema potrebama svojih konstituenata, o aktuelnim pretnjama po informacionu bezbednost i koracima koji se mogu preduzeti kako bi se te pretnje neutralisale. Ili to mogu biti prečišćene informacije o obimu i prirodi nedavnih bezbednosnih incidenata i napada koji su prijavljeni CERT timu. U ovom slučaju na izdavanje obaveštenja se gleda kao na proces u okviru servisa upravljanja incidentima. Ali, za CERT organizacije koje pružaju širi spektar servisa, izdavanje obaveštenja može da se posmatra i kao nezavisan servis, koji se temelji na širem skupu informacija koje se dobijaju od različitih servisa, kao što su analiza ranjivosti sistema, ili analiza artefakata incidenata.

Proces davanja povratnih informacija odnosi se na komunikaciju sa korisnicima o prijavljenim incidentima, ali i sa drugim entitetima kojima je potrebno dostaviti informaciju, bilo na zahtev (na primer na zahtev medija, povodom nekog tekućeg incidenta ili pretnje po informatičku bezbednost širih razmera), ili na regularnoj osnovi (na primer u formi godišnjih izveštaja). Takođe, ovaj proces treba da obezbedi minimalan skup informacija u formi odgovora na najčešće postavljena pitanja, koja su dostupna medijima i široj javnosti.

7.3 PROCES TRIJAŽE

Cilj ovog procesa je da se obezbedi da se sve informacije koje su relevantne za servis upravljanja incidentima, kanališu kroz jedinstvenu tačku pristupa, bez obzira na metod kojim informacije ili prijave incidenata pristižu (elektronskom poštom, faksom, telefonom, pismom ...), kako bi se na odgovarajući način redistribuirale radi razrešenja incidenata. Ovaj cilj se uobičajeno postiže postavljanjem procesa trijaže u fokus komunikacije, kao jedinstvene tačke kontakta za ukupan servis upravljanja incidentima. Ukoliko CERT tim želi da ograniči mogućnost da konstituenti, ili drugi entiteti, zaobiđu proces trijaže, ne smeju se objavljivati kontakt informacije pojedinačnih članova tima (kao što su broj telefona ili adresa elektronske pošte).

CERT timovi uobičajeno objavljuju jedinstvenu „adresu“, tj. tačku kontakta za celu svoju organizaciju, bez obzira na vrstu servisa koja se traži, jer se za sve servise primenjuje zajednički proces trijaže. Osoblje koje je angažovano u okviru procesa trijaže prima i odgovara na sve poruke primljene preko elektronske pošte, otvara svu poštu, pregleda sve pristigle fax poruke i odgovara na sve telefonske pozive. Uobičajeno je i da se svi telefonski pozivi upućeni pojedinačnim članovima tima prosleđuju na osoblje koje se bavi trijažom kako bi se osiguralo da se svi pozivi koji imaju veze sa prijavom incidenata obrađuju centralizovano.

Da bi se stimulisalo prijavljivanje incidenata i prikupljanje relevantnih informacija, konstituentima se moraju omogućiti jednostavni i efikasni mehanizmi za prijavu incidenata:

- jasno definisana tačka kontakta,
- navedeni detalji dostupnosti definisane tačke kontakta,
- jednostavne, ali striktne procedure koje treba slediti,
- jasno uputstvo o tipovima događaja koje treba prijaviti,
- adekvatna dokumenta za potrebe korisnika (forme za prijavu problema sa referencama na drugu dostupnu dokumentaciju).

Kada deo CERT tima koji se bavi trijažom dobije neku informaciju ili prijavu problema, šalje se potvrda pošiljaocu da je poruka primljena, a zatim se informacija sortira, prioritetizuje, dodaje joj se jedinstveni idenitifikator, i prosleđuje se drugim procesima u okviru implementiranih servisa. Dodatno, proces trijaže mora da obavi dekripciju enkriptovanih poruka i proveru digitalnih potpisa, da sačuva ovu informaciju za kasniju upotrebu, i da zapravo omogući uvid u sadržaj poruke. Da bi se izvršio ovaj zadatak, proces trijaže mora imati pristup bazama podataka koje koriste svi drugi procesi u okviru servisa za upravljanje incidentima.

Na osnovu dobijenih informacija, i podataka koji se odnose na tekuće poslove u okvirima servisa, obavlja se inicijalno sortiranje dobijenih podataka kako bi se identifikovalo koja funkcija u okviru servisa za upravljanje incidentima treba da preduzme odgovarajuće akcije. Sledeći korak je da se utvrdi da li je pristigla informacija u direktnoj vezi sa bilo kojim od tekućih ili nedavnih događaja. Ukoliko takva veza postoji, informacija se označava kao sastavni deo tog događaja. U suprotnom, biće označena kao novi događaj, specificiranog tipa, i biće joj dodeljen novi identifikator. Dodatno, dodeljuje se i inicijalni prioritet u skladu sa šemom prioritetizacije u okvirima funkcija servisa. Ukoliko se informacija primi u formi štampanog dokumenta, uobičajeno je da se u procesu trijaže unose podaci u informacioni sistem za praćenje incidenata.

Proces unošenja podataka, pristupa informacijama, identifikacija informacija i događaja može se znatno olakšati i donekle automatizovati upotrebom alata, tj. softvera za obradu i pretragu podataka. Takvi alati omogućavaju osoblju koje se bavi procesom trijaže da identifikuje:

- nove događaje (prijave incidenata, izveštaje o ranjivostima sistema, razna obaveštenja),
- informacije koje su direktno povezane sa nekim tekućim događajem,
- informacije koje su direktno povezane sa nekim već zatvorenim incidentom,
- događaje koji se prate odvojeno, ali mogu biti direktno povezani,
- informacije koje se mogu smatrati irelevantnim sa stanovišta servisa za upravljanje incidentima.

Ukoliko informacije ne sadrže dovoljno detalja, ili su nekompletne, postoji mogućnost da i proces trijaže bude neefikasan, tj. spor i neprecizan u ispunjenju svoje uloge. U tom slučaju može biti potrebno da se od pošiljaoca traže dodatne informacije, pre nego što se odradi odgovarajuća trijaža, što donekle usporava proces. Kao dodatak na korišćenje alata koji olakšavaju trijažu primenjuju se i drugi koraci kojima se poboljšava kvalitet informacija, kao što su dodeljivanje jedinstvenog identifikacionog broja, korišćenje standardizovanih formi za prijavu incidenata, kao i prethodna registracija korisnika.

7.3.1 Dodeljivanje jedinstvenog identifikacionog broja

Proces trijaže se jako olakšava ukoliko CERT tim koristi šeme za dodeljivanje jedinstvenog brojnog identifikatora tokom prijave incidenata, i poželjno je da zahteva od drugih entiteta da se referenciraju na dodeljene identifikatore kasnije pri komunikaciji na temu prijavljenog incidenta. Kako bi se proces automatizovao, šema dodeljivanja identifikatora trebalo bi da bude jednostavna, tj. lako razumljiva i za ljude i za softverske alate. U robusnom sistemu za praćenje incidenata, sistem koristi ove identifikatore da automatski sortira pristigle informacije i odredi da li su one u korelaciji sa nekim tekućim događajima ili incidentima, bez potrebe za ljudskom intervencijom u ovoj inicijalnoj fazi. Ovo ubrzava posao i omogućava da se proces trijaže više fokusira na određivanje korelacije među, na prvi pogled, nepovezanim informacijama. Identifikacioni brojevi se kasnije mogu koristiti tokom komunikacije, kao referenca u naslovima elektronske pošte, zaglavljima dokumenata ili faks poruka, tj. tokom govorne komunikacije.

Identifikacione brojeve bi trebalo koristiti za praćenje događaja u okviru svakog procesa servisa za upravljanje incidentima. Pri tome se za različite servise mogu koristiti različiti prefiksi. S obzirom da je moguća i komunikacija sa eksternim entitetima, deo identifikatora bi trebalo da ukaže i na tim koji je „vlasnik“ tog identifikatora. Takođe, svaka od kategorija: povratna informacija, incident i obaveštenje bi trebalo da ima svoj tip identifikatora.

Primera radi, identifikator za praćenje incidenata može da sadrži prefiks CERT#, identifikator za praćenje informacija o ranjivostima sistema može da ima prefiks VU#, a druge informacije nižeg prioriteta mogu da imaju prefiks INFO#. Naravno, mogu postojati i drugi dodatni prefiksi za potrebe različitih internih i eksternih dokumenata.

7.3.1.1 Jedinstveni brojni identifikatori za internu upotrebu

Osnovna pretpostavka za identifikacioni broj je da on mora biti jedinstven. Uobičajeno je da se za šemu numeracije koristi neki opseg celih brojeva. U okvirima servisa za upravljanje incidentima, ali i svih drugih servisa koje pruža neki CERT tim, najbolja praksa je da se koriste jedinstveni prefiksi za svaki proces pojedinačno, kao i da se obezbedi da je identifikacioni broj koji sledi posle prefiksa jedinstven. Ukoliko se isti broj koristi u više od jednog procesa, a da se pri tome ne koriste prefiksi, to može dovesti do konfuzije i poteškoća u komunikaciji na temu nekog događaja. Ukoliko se brojevi za identifikatore „recikliraju“ potrebno je obezbediti da prođe dovoljno vremena od zatvaranja nekog incidenta pre nego što se isti identifikator iskoristi za neki novi događaj.

7.3.1.2 Jedinstveni brojni identifikatori za eksternu upotrebu

Identifikacioni brojevi moraju biti jedinstveni ne samo u okviru same CERT organizacije, nego i među različitim konstituentima i partnerskim organizacijama. Ukoliko je više CERT organizacija uključeno u razrešavanje nekog incidenta, svaka od njih će koristiti svoj identifikator za taj isti događaj. Ukoliko to nije slučaj može se desiti da dve CERT organizacije koriste isti identifikator za dva različita incidenta, što dovodi do konfuzije i kašnjenja u sprovođenju odgovarajućih akcija na razrešenju incidenta.

Takođe, može biti od velike koristi ukoliko alati za vođenje evidencije o incidentima prepoznaju različite formate identifikatora koje koriste različiti CERT timovi, jer se time dodatno olakšava proces trijaže. Poželjno je da se različiti CERT timovi, tokom komunikacije

na temu tekućih incidenata, referenciraju na sve identifikatore posmatranog incidenta (interne i eksterne), kako bi se on lakše identifikovao i efikasnije procesirao.

7.3.1.3 Identifikacioni brojevi kao javna informacija

S obzirom da se jedinstveni identifikatori koriste tokom razmene informacija sa spoljnim entitetima, oni se mogu smatrati javnom informacijom, i stoga ne treba da sadrže poverljive informacije, kao što su imena hostova ili domena koji su deo nekog bezbednosnog incidenta. Najbolja praksa je da se za kreiranje jedinstvenog identifikatora koriste slučajno generisani brojevi.

7.3.1.4 Životni ciklus jedinstvenih identifikatora

Ukoliko se za praćenje nekog događaja koristi jedinstveni identifikator, onda identifikator koji se inicijalno alocira za neki događaj ostaje vezan za taj događaj od trenutka kada je taj događaj prijavljen CERT timu do trenutka kada je, iz perspektive CERT tima taj događaj zatvoren, tj. incident razrešen. Međutim postoje situacije u kojima ovaj jednostavan model mora da se preispita:

- Trijaža informacija nije korektno obavljena - Tokom trijaže može se neki događaj proglasiti novim iako je on direktno povezan sa nekim tekućim događajem.
- Informacije nisu korektno označene - Ukoliko informacija stigne sa nekorektnim identifikatorom, neće biti korektno praćena
- Zatvoreni događaj se ponovo otvara - Ukoliko se neki događaj ili incident zatvori, a pristigne nova informacija na temu tog događaja, onda se taj događaj mora ponovo aktivirati.
- Više događaja se spaja u jedan - Može se desiti da pristigne informacija koja povezuje dva događaja koja su pre toga evidentirani kao nezavisni događaji ili incidenti. U takvim slučajevima treba razmotriti da se dva događaja spoje u jedan, tj. da im se dodeli novi zajednički jedinstveni identifikator.

7.3.2 Korišćenje standardizovanih formi za prijavu incidenata

Korišćenjem standardizovanih formi za prijavu incidenata olakšava se proces dobijanja potpunih i tačnih informacija za potrebe CERT tima. Ovime se povećava efikasnost rada i olakšava posao prosleđivanja informacija odgovarajućim procesima u okviru servisa za upravljanje incidentima, tj. olakšava se posao na razrešenju incidenata. Za većinu servisa je moguće kreirati odgovarajuće forme za prijavu incidenata ili događaja.

U okvirima servisa za upravljanje incidentima, mogu se napraviti forme za prijavu bezbednosnih incidenata, ili za zahteve za razmenu informacija. Da bi bile od koristi, ove forme moraju biti što jasnije i konciznije, i lako dostupne onima kojima su potrebne. Da bi bile korisne za potrebe procesa trijaže, ali i procesa razrešenja incidenata, forme za prijavu incidenata obično sadrže sledeće tipove informacija:

- kontakt informacije o podnosiocu prijave, ili bilo kom drugom entitetu uključenom u prijavljeni incident,
- imena i mrežne adrese hostova koji su uključeni u incident,
- prirodu aktivnosti,

- opis aktivnosti i relevantne informacije (kao što su log fajlovi sa uključenom informacijom o vremenskoj zoni, ili drugi artefakti ...),
- identifikacioni broj koji je možda već dodeljen od strane lokalnog CERT-a, ili neke spoljnje CERT organizacije.

Ponekad postoji otpor korisnika servisa prema ovom načinu prijave incidenata, što može dovesti do toga da oni potpuno prestanu da prijavljuju incidente. U tom slučaju CERT tim može da donese odluku da „žrtvuje“ dobitak nekih inicijalnih informacija u zamenu za to da mu se incident prijavi, pa makar to bilo preko telefona, ili u nekoj slobodnoj formi putem elektronske pošte. Efekat ovoga je da će CERT tim morati da potroši više resursa, tj. vremena da iz takve prijave incidenta izvuče relevantne informacije i unese ih u svoj sistem za praćenje incidenata.

Dakle, forme moraju biti što jednostavnije i konciznije, a treba razmotriti i mogućnost da se za sve vrste interakcija sa CERT timom (prijave incidenata, zahtevi za dobijanje informacija ...) koristi jedna osnovna zajednička forma ili dokument. Naravno, CERT tim stalno treba da radi na tome da podiže svest o korisnosti ovakvih formi kod svojih konstituenata, i da ih ohrabruje u njihovom korišćenju.

Jedan primer forme za prijavu bezbednosnih incidenata prikazan je na slici 7.2.

7.3.3 Prethodna registracija korisnika

Kao dodatak na korišćenje formi za prijavu incidenata, a u zavisnosti od broja i prirode konstituenata nekog CERT tima, moguće je preduzeti neke proaktivne mere kako bi se unapred dobile neke informacije koje mogu biti korisne u procesu trijaže. Ovaj proces se može proširiti i na dobijanje informacija unapred, i od nekih drugih entiteta, kao što su drugi CERT timovi, ili istražni i pravosudni organi. Ovaj proces prethodne registracije, može da eliminiše potrebu za standardnim inicijalnim pitanjima koja se postavljaju tokom prijave incidenata, ili komunikacije sa CERT timom generalno. U tom smislu uobičajeno je da se tokom registracije navedu:

- tačke kontakta od poverenja, sa pridruženim kontakt informacijama (koje se moraju povremeno verifikovati, barem jednom godišnje),
- restrikcije u pogledu razmene informacija, i
- (verifikovani) ključevi za enkripciju, ili razmenu informacija sa digitalnim potpisom.

Takođe, u nekim slučajevima može biti korisno da se tokom registracije ostave i informacije kao što su imena domena, ili vremenske zone.

7.4 PROCES RAZREŠAVANJA INCIDENATA

Cilj ovog procesa je da se za prijavljene bezbednosne incidente ili pretnje obezbedi odgovor CERT tima u vidu podrške konstituentima. Minimalni skup atributa koje ovaj proces obuhvata su:

- tačka izveštavanja – lokacija za prijem prijava incidenata konstituenata,
- analiza – podrazumeva određeni nivo verifikacije prijavljenog incidenta i tehničko razumevanje aktivnosti koje su do njega dovele. Ovo uključuje i pronalaženje odgovora na prijavljeni incident, koji će se proslediti korisniku,

- obaveštavanje – prosleđivanje odgovora, tj. informacija neophodnih za razrešenje incidenta ili saniranje njegovih posledica. Odgovor se prosleđuje konstituentu koji je prijavio posmatrani bezbednosni incident, a po potrebi i drugim konstituentima i CERT organizacijama u vidu upozorenja.

Definicija pojma „odgovora“ na incident varira od tima do tima, u zavisnosti od načina na koji CERT tim definiše incidente i ciljeve svog servisa za upravljanje incidentima. Dodatno i drugi faktori mogu biti uzeti u obzir, a među njima je jedan od važnijih nivo prioriteta koji je dodeljen prijavljenom incidentu, kao i lokacije, tj. konstituenti koji su njime zahvaćeni (u smislu da li pripadaju zajednici konstituenata CERT tima ili su u pitanju neki eksterni entiteti).

INCIDENT REPORTING FORM

Please fill out this form and Fax or email it to: ……..
*Lines marked with * are required.*

Name and Organisation
1. Name*:
2. Name of Organisation*:
3. Sector type:
4. Country*:
5. City:
6. E-Mail address*:
7. Telephone number*:
8. Other:

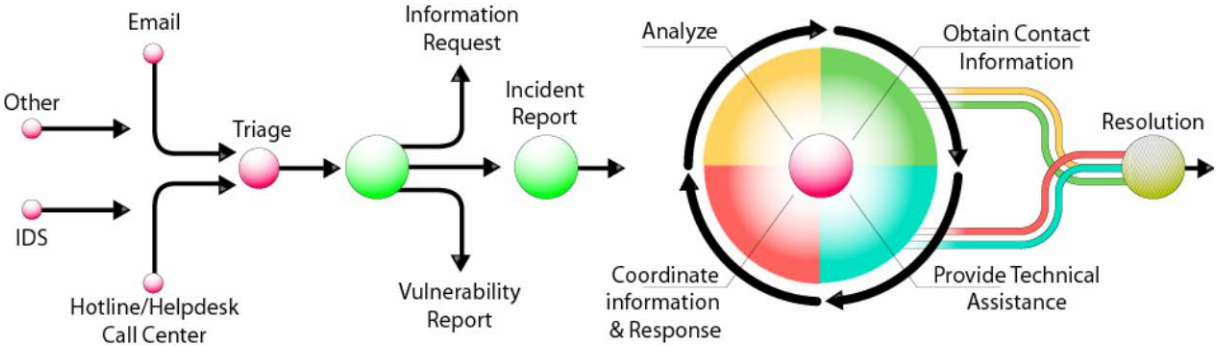
Affected Host(s)
9. Number of Hosts:
10. Hostname & IP*:
11. Function of the Host*:
12. Time-Zone:
13. Hardware:
14. Operating System:
15. Affected Software:
16. Affected Files:
17. Security:
18. Hostname & IP:
19. Protocol/port:

Incident
20. Reference number ref #:
21. Type of Incident:
22. Incident Started:
23. This is an ongoing incident: YES NO
24. Time and Method of Discovery:
25. Known Vulnerabilities:
26. Suspicious Files:
27. Countermeasures:
28. Detailed description*:

Slika 7.2: Primer sadržaja forme za prijavu bezbednosnih incidenata

7.4.1 Životni ciklus incidenta

Na koji god način da CERT tim definiše pojam bezbednosnog incidenta, on će u najvećem broju slučajeva imati sličan životni ciklus. Već je pomenuto da se deo životnog ciklusa bezbednosnog incidenta odvija u procesu trijaže, gde se incident inicijalno kategorizuje, i identifikuje kao novi događaj ili deo nekog postojećeg događaja koji se već razrešava. U skladu sa tim dodeljen mu je i odgovarajući jedinstveni identifikator. Treba napomenuti da se novi incident može otkriti i u toku procesa razrešenja, kao rezultat nekorektne informacije dobijene od procesa trijaže, ili informacije koja do tima stiže sa lošim identifikatorom, ili novih informacija do kojih se dođe tokom dublje tehničke analize incidenta u toku procesa razrešenja. Na slici 7.3 data je ilustracija životnog ciklusa procesa upravljanja bezbednosnim incidentima.



Slika 7.3: Životni ciklus procesa upravljanja bezbednosnim incidentima

Jednom kada je incident otvoren on može prolaziti kroz razne statuse, sa svim informacijama koje su u vezi sa tim incidentom (situacije i preduzete akcije), do trenutka kada, iz perspektive CERT tima, nije više potrebna nikakva dodatna akcija („kružni tok“ na ilustraciji sa slike 7.3), odnosno dok se inicident konačno ne zatvori. Naravno, važno je primetiti da incident, ili događaj, može kružiti kroz ciklus analize više puta tokom aktivnosti u okviru njegovog životnog ciklusa.

Zatvaranje incidenta se normalno dešava kada nijedna strana, koja je uključena u incident, ne može da identifikuje ili prijavi nikakvu novu informaciju CERT timu, koji je u međuvremenu već preduzeo neophodne akcije na razrešenju incidenta, i o tome obavestio sve zainteresovane strane. Takođe, CERT tim može da odluči da zatvori incident i u slučaju kada se očekuju nove informacije povodom nekog incidetna, ali ne postoji mogućnost da CERT tim svojim aktivnostima doprinese razrešenju tog incidenta.

Primera radi, CERT tim može u dužem periodu vremena da dobija informacije o pojavi nekog računarskog virusa, ali je već po prvoj primljenoj prijavi incidenta taj događaj evidentiran, analiziran, razrešen, i konstituenti su o tome obavešteni. I pored novih prijava koje pristižu ne postoji ništa dodatno što bi CERT tim trebao ili mogao da uradi povodom pojave tog virusa i incident se zatvara.

Sa druge strane, ukoliko neki istražni ili pravosudni organi vrše istragu povodom pojave nekog bezbednosnog incidenta, takav incident se ne može zatvoriti, bez obzira na njegovo razrešenje, dok se istražne radnje ne završe.

Tokom svog životnog ciklusa incident može prolaziti kroz razna stanja, kao što su:

- potrebna je akcija – očekuje se da CERT tim odgovori na incident, i
- čekanje – kada CERT tim čeka na reakciju ili informaciju od spoljnjih entiteta.

Kada CERT tim odluči da zatvori neki incident, mora da obezbedi da sve zainteresovane strane budu o tome obaveštene. Ovime se zadovoljavaju očekivanja korisnika i izbegavaju konfuzne situacije u kojima se može desiti da korisnik smatra da je incident još uvek otvoren, ali ne dobija nikakve informacije od CERT-a na temu tog incidenta. Kada zatvori incident, tim o tome može obavestiti sve strane odjednom, ili to može činiti parcijalno tokom prepiske sa zainteresovanim stranama u toku procesa razrešenja incidenta. Prvi način zahteva više vremena, i može generisati „poplavu" trivijalnih povratnih poruka kojima se potvrđuje prijem informacije, a može se čak i desiti da se status incidenta vrati u stanje „potrebna je akcija". Drugi način omogućava da učesnici u prepisci obezbede ili imaju uvid u informacije na vreme, što je svakako efikasnije s obzirom na ograničene resurse kojima raspolažu CERT timovi.

Može se dogoditi da se zatvoreni incident ponovo otvori u slučaju da je CERT tim dobio neke nove informacije, na primer da se isti incident ponovo pojavio kod nekog od konstituenata uprkos preduzetim merama. U tom slučaju dobro je da se ovom incidentu ponovo dodeli isti identifikator, ukoliko je to moguće. Naravno, ukoliko se aktivnosti koje treba preduzeti ne mogu smatrati nastavkom već preduzetih aktivnosti, potrebno je otvoriti novi incident i dodeliti mu novi identifikator.

Slično ovome, može se desiti da se pojavi nova informacija koja povezuje dva incidenta koji su do tada tretirani kao nezavisni događaji. U tom slučaju CERT tim mora da donese odluku da li će ta dva događaja da spoji u jedan incident (i u tom slučaju da odredi koji će od dva identifikatora nadalje da se koristi, i da o tome obavesti sve zainteresovane strane), ili će da nastavi da ih tretira kao dva incidetna koji su povezani. Koja god šema da se usvoji, sve procedure, alati i baze podataka moraju da podržavaju takve postupke.

7.4.2. Analiza bezbednosnih incidenata

Tokom životnog ciklusa bezbednosnog incidenta, proces analize obezbeđuje informacije koje igraju važnu ulogu u procesu donošenja odluka o narednim koracima u razrešenju incidenata, koji su u skladu sa politikama i procedurama CERT tima.

Prva akcija u analizi incidenta zapravo se dešava u procesu trijaže, tj. u trenutku kada pristižu nove informacije o nekom incidentu. Međutim, ono što je važnije od toga je proces analize koji se dešava u okviru procesa razrešenja incidenta, kada se ide dublje u tehničke detalje, na bazi analize log fajlova, ili malicioznog koda.

Različiti tipovi analiza mogu se odvojiti u posebne servise CERT tima, nezavisno od servisa za upravljanje incidentima. Primera radi, tragovi koje napadač ostavi na delovima napadnutih sistema nazivaju se artefaktima, i pretraga i analiza ovih artefakata, sa ciljem da se saniraju posledice napada na sistem, mogu se tretirati kao poseban servis. Naravno, s obzirom na prirodu aktivnosti u procesu razrešavanja incidenata, analiza artefakata je uobičajen postupak i u okvirima servisa za upravljanje incidentima.

Generalno, postoje dve klase analize incidenata koje treba uzeti u obzir:

- Interna analiza incidenta - U ovom slučaju analiza se tiče striktno samo posmatranog incidenta, i to:
    - analiza bilo kojeg artefakta koji ostane kao trag iza napadača (log fajlovi, virusi, maliciozni softver ...),
    - analiza softverskog okruženja u kojem se incident dogodio.

- Eksterna analiza incidenta - Ovde se analiziraju okolnosti koje bi mogle dovesti u međusobnu vezu više različitih incidenata, tj. koje mogu da upute na isti uzrok incidenta ili na istog napadača.

Dakle, analiza bezbednosnog incidenta je jako široko područje delovanja, i to je kritična aktivnost koja doprinosi efikasnom razrešenju bezbednosnih incidenata.

7.4.2.1 Kreiranje „šire slike“

U sagledavanju rezultata analize važno je zadržati uvid u sve aspekte incidenta koji se analizira, tj. potrebno je kreirati „širu sliku“, tj. širi kontekst dešavanja u vezi sa posmatranim bezbednosnim incidentom. Šira slika se uglavnom odnosi na trendove (moguće tipove napada u budućnosti, poboljšanja na polju informacione bezbednosti), statistike (broj hostova koji su uključeni u bezbednosne incidente, učestalost prijava incidenata), ili studije slučaja (sa ciljem da se stekne uvid u aktivnosti napadača i njihovih zajednica, ili uticaj koji neki incidenti mogu imati na specifične sisteme ili aplikacije). Svaka CERT organizacija gradi svoju širu sliku u kontekstu onoga što je najrelevantnije za zajednicu njihovih konstituenata.

Kreiranje šire slike može biti težak proces jer se različiti članovi tima mogu baviti različitim aspektima nekog incidenta, sprovodeći različite tipove analiza. Različiti ljudi u okviru tima imaju uvid u različite informacije koje su rezultat njihovog dela analize. Da bi se dobila šira slika na bazi svih informacija koje su dostupne različitim članovima tima potrebno je ustanoviti proces objedinjavanja i usaglašavanja informacija u okviru tima. Ovo se postiže redovnim sastancima članova tima radi razmene informacija, ili uspostavljanjem funkcije supervizora incidenata koji prikupljaju i ukrštaju sve relevantne informacije koje su u vezi sa nekim incidentom.

Identifikovanje šireg konteksta nekog događaja naročito je važno u procesu učenja i izgradnje iskustva kojim se olakšava posao tokom rešavanja novih incidenata u budućnosti. Proučavanjem slučajeva i iskustava iz prošlosti olakšava se proces donošenja ispravnih odluka u budućnosti i skraćuje vreme rešavanja incidenata. U tom smislu, izrada baze znanja kojom se potpomaže ovaj proces je jako korisno, naročito u smislu očuvanja kontinuiteta, jer za razliku od zaposlenih koji mogu napustiti CERT organizaciju, ova baza ostaje kao trajna pomoć za sve članove CERT tima. Takođe, izrada studija slučaja može biti od velike pomoći u procesu obuke novih članova tima.

Izuzetno je korisno, i preporučuje se, da se pomenute baze znanja i studija slučaja učine dostupnim i drugim CERT timovima ili državnim istražnim organima. To se može činiti na razne načine, i u različitim formatima, ali jedinstveni cilj je da se konstituenti stalno obaveštavaju o novim dešavanjima i trendovima, i da se podiže svest o važnosti informatičke bezbednosti. Pored ovoga postoje i konstanti napori između CERT timova na međunarodnom nivou, na aktivnostima u razmeni znanja, tj. na kreiranju zajedničkih formi za prikupljanje, arhiviranje i razmenu informacija o bezbednosnim incidentima (uključujući tu upozorenja, rezultate analiza, arhive incidenata, statistike, izveštaje, i slično).

7.4.2.2 Dubina analize

Dubina analize, tj. odgovor na pitanje do kog nivoa detalja treba ići u toku analize nekog incidenta, i koliko resursa tima treba u tom smislu utrošiti, je kompleksan i zavisi od niza faktora. Neki od tih faktora su sledeći:

- Misija i tehničke mogućnosti tima - Tim čija je misija da osigurava bezbednost svojih konstituenata u obavezi je da se više i temeljnije bavi analizom tekućih incidenata, i za to su mu potrebne adekvatne tehničke mogućnosti i ekspertiza. Ukoliko CERT timu fale tehničke mogućnosti, ili potreban nivo znanja, onda su i rezultati analize manje detaljni, i u takvim slučajevima se ovi poslovi mogu delegirati i nekom spoljnjem entitetu koji raspolaže takvim resursima.
- Ozbiljnost incidenta - Ukoliko CERT tim raspolaže sa dovoljno materijalnih sredstava i ljudskih resursa, čak se i incidenti nižeg prioriteta mogu istraživati do višeg nivoa detalja, ali pošto vrlo često to nije slučaj, potrebno je da tim bude veoma selektivan po ovom pitanju, i najčešće se fokusira na dublju analizu samo kada su u pitanju incidenti najvišeg prioriteta.
- Verovatnoća ponavljanja incidenta - Ukoliko postoji mogućnost da napadač ponovi svoju aktivnost na drugom mestu ili u drugo vreme, onda je svrsishodno potrošiti više resursa za analizu takvog incidenta. Na ovaj način se smanuje efekat koji taj incident može imati u slučaju ponavljanja, jer se relevantne informacije unapred prosleđuju konstituentima, drugim CERT timovima, pa čak i istražnim organima. Naravno, ovakva vrsta analize povoljno utiče i na već pomenuto kreiranje šire slike, koja pomaže svim članovima tima u razrešavanju incidenta.
- Mogućnost identifikovanja novih metoda napadača - Ukoliko postoji sumnja da napadač koristi neki novi metod ili alat za izvođenje napada, ili je u pitanju nova varijanta neke već postojeće metode ili alata, onda je za razumevanje takvih aktivnosti potrebna detaljna analiza.
- Podrška od strane konstituenata - Ukoliko neko prijavi bezbednosni incident, ali ne obezbedi sve neophodne informacije koje su potrebne za izvođenje detaljne analize, onda se može desiti da se proces analize prekine.

Postoji čitav spektar aktivnosti koje CERT može da preduzme ako ima dovoljno resursa da detaljno analizira događaje, i da na adekvatan način podeli rezultate tih analiza sa svojim konstituentima i drugim timovima:

- analiza log fajlova,
- analiza malicioznog koda i softverskog okruženja,
- obezbeđivanje privremenih rešenja ili ispravki,
- aktivno razrešavanje incidenata, i
- analiza bezbednosti sistema ili računarske mreže na nekoj lokaciji.

7.4.2.3 Analiza log fajlova

Svaka hardverska platforma i operativni sistem, kao i mnoga softverska rešenja, imaju mogućnost slanja alarma, tj. upozorenja, kao i generisanja log fajlova. Alarmi su dizajnirani da se aktiviraju i privuku pažnju u slučaju da se desi neki unapred definisani događaj. Logovi su fajlovi u koje se upisuje pojavljivanje raznih događaja (i bezopasnih i opasnih). Alarm se obično aktivira kada neki zapis u okviru log fajla ima vrednost koja je definisana kao kriterijum za podizanje alarma.

Alarmi su uglavnom interesantni ljudima koji se bave održavanjem konkretnih sistema, dok log fajlovi imaju širi značaj, naročito zbog obilja detalja o događajima koji se u

njima mogu pronaći, kao i zbog činjenice da su ti fajlovi prenosni (moguće je iskopirati ih sa sistema i poslati bilo kome). U log fajlovima se mogu pronaći informacije kao što su:

- ko se povezivao na sistem, u koje vreme i sa koje lokacije ili sistema,
- koja vrsta konekcije se desila (SSH, telnet, rlogin ...),
- na koju destinaciju je poslata neka poruka, ili elektronska pošta,
- koje greške su se desile u sistemu, i slično.

Ljudi koji operativno održavaju sisteme treba da obezbede da u log fajlovima postoji dovoljan nivo detalja o pojedinim događajima. Naravno, svaki CERT tim ima svoje preporuke u tom smislu, i on ih prenosi svojim konstituentima, kako tokom procesa razrešenja nekog konkretnog incidenta, tako i stalnim prenošenjem znanja o dobroj praksi na svoje konstituente, radi prevencije incidenata. Uloga CERT tima je da tokom razrešavanja incidenta preuzme relevantne log fajlove, procesira ih, i preduzme akcije u skladu za rezultatima analize.

Primera radi, izmene koje se obave na DNS (*Domain Name System*) sistemima mogu dovesti do toga neka imena domena, ili IP adrese više nisu validne, tj. mogu upućivati na neke pogrešne hostove. U tim smislu, da bi log fajlovi imali širi smisao nego samo tokom rešavanja incidenata, oni moraju posedovati određene karakteristike, i potrebno je analizirati ih u što kraćem roku. Dodatno, puna korist od analize log fajlova se postiže ako se uporedo sa njima izvrši i analiza konfiguracionih fajlova sistema, ili alata koji generiše te log fajlove. Naravno, CERT tim koji se bavi prihvatanjem i procesiranjem log fajlova mora da ispoštuje određene zahteve u smislu bezbednosti podataka, i njihovog arhiviranja ili uništavanja od trenutaka kada oni više nisu potrebni za dalju analizu.

Bitne karakteristike log fajlova su sledeće:

- Vremenski markeri - Za svaki događaj koji se registruje u log fajlu bitno je da postoji oznaka tačnog vremena kada se događaj desio. U tom smislu preporučuje se korišćenje softvera za sinhronizaciju vremena (NTP – *Network Time Protocol*), kako bi se izbegla konfuzija u slučaju poređenja log fajlova koji su pristigli sa različitih sistema ili lokacija. Iz istog razloga potrebno je da vremenski markeri sadrže i informaciju o vremenskoj zoni.

- Izvor log fajla - Moraju se prikupiti svi detalji sistema koji je generisao log fajl (kao što su njegovo ime, mrežna adresa, tip sistema ...). Važno je znati i koji sofver (uključujući njegovu tačnu verziju) je generisao log fajl, zajedno sa njegovim konfiguracionim fajlovima.

- Autentifikacija log fajla - Bez autentifikacije nije moguće utvrditi da li je log fajl autentičan, tj. da li je kreiran ili menjan pre, tokom ili posle pojavljivanja incidenta. U slučajevima kada postoje pravne implikacije nekog incidenta uobičajeno je da dvoje ljudi garantuju autentičnost log fajla (npr. svojim potpisom na štampanoj verziji). Alternativni pristup je da se log fajlovi sa nekog sistema kopiraju na drugi sistem kojem se pristupa na veoma kontrolisan način.

7.4.2.3.1 Kategorizacija log fajlova

Često se postavlja pitanje u koju kategoriju tajnosti (tajni ili javni) potpada neki log fajl. U tom smislu potrebno je da CERT organizacija ima politiku kategorizacije informacija,

koja se primenjuje već tokom procesa trijaže, a zatim se sa svim informacijama postupa u skladu sa dodeljenom kategorijom.

U slučaju log fajlova često je potrebno pridružiti im više od jedne kategorije. Opšte informacije su generalno manje osetljive od specifičnih informacija kojima se otkrivaju imena sistema, mrežne adrese, ili imena zaposlenih.

Kreiranje šire kategorizacije log fajlova mora biti učinjeno pre prijema konkretnih log fajlova, jer svaka kategorija (dodeljena na bazi onoga što je očigledni sadržaj log fajla) podrazumeva određeni skup ograničenja po kojima se postupa sa log fajlom.

7.4.2.3.2 Prijem log fajlova

Log fajlovi treba da budu isporučeni CERT timu sa potrebnim nivoom pažnje, s obzirom na kategoriju informacija koje log fajl sadrži. Osetljive informacije moraju biti prenete na bezbedan način (preko enkriptovanih kanala), dok se manje osetljive informacije mogu prenositi i u otvorenom teksu putem elektronske pošte. Naravno, ukoliko se radi o velikim količinama podataka mogu se koristiti odgovarajući prenosni medijumi (trake, diskovi i slično ...).

7.4.2.3.3 Verifikacija log fajlova

Kako bi se moglo garantovani da je primljeni fajl autentičan potrebno je sa pošiljaocem log fajla dogovoriti metodu autentifikacije. Ovaj problem se često rešava korišćenjem digitalnih potpisa (na bazi MD5 (*Message-Digest*) i RSA (*Ron Rivest, Adi Shamir and Leonard Adleman*) algoritama i protokola). Naravno, nijedna od ovih metoda ne može garantovati da sadržaj samog log fajl pre slanja nije promenjen od strane napadača ili nekog drugog entiteta.

7.4.2.3.4 Čišćenje log fajlova

Najbolje je odmah u startu prečistiti primljeni log fajl od osetljivih informacija koje nemaju suštinski značaj u procesu analize. Time se izbegava mogućnost slučajnog otkrivanja osetljivih informacija tokom procesa analize. Primera radi, ukoliko se u log fajlu nalaze lozinke za pristup opremi dobra praksa je da se te informacije odmah odstrane iz fajla.

7.4.2.3.5 Objavljivanje delova log fajlova

Ukoliko se tokom razrešavanja incidenta, tokom analize log fajlova, utvdi da bi isti incident mogao da pogodi i neke druge konstituente, ili je o rezultatima analize potrebno obavesiti druge CERT timove, može se desiti da je tom prilikom neophodno proslediti im i neke delove analiziranih log fajlova. Pravilo je da se nikada ne šalje kompletan log fajl, već se izvlače samo pojedini delovi koji mogu biti relevantni za druge entitete.

7.4.2.4 Analiza artefakata

Obično se dešava da na napadnutim sistemima, kao trag napada ostane čitav niz različitih fajlova, od kojih neki mogu biti log fajlovi sa alata za presretanje mrežne komunikacije, fajlovi sa lozinkama, maliciozni kodovi ili skripte koji su delovi nekih softverskih alata, i slično. Sve ove zaostale fajlove, sa potencijalno malicioznom namenom, nazivaju se artefaktima. Neki od ovih fajlova ne moraju biti maliciozni, ali se to obično ne zna

dok se ne završi proces analize. Korektan pristup je da se svaki od ovih fajlova smatra malicioznim dok se analizom ne dokaže suprotno.

Primera radi, dešava se da napadači zamene uobičajene fajlove, tako da se oni po sadržaju razlikuju od originala, ali nose isto ime. Ovakvi programi se nazivaju „trojanci“ i jako su popularni među napadačima. Ovakvi programi rade sve ono što je i inače namena originalnih programa, ali na „pogrešan način“, ili što može biti još opasnije, sve rade ispravno, ali i dodatno obaveštavaju napadača o svim aktivnostima, šalju osetljive informacije u skrivene log fajlove, ili ih prosleđuju na eksterne lokacije, tj. sisteme napadača.

Da li CERT organizacije treba da se bave analizom malicioznog koda u sklopu servisa za upravljanje incidentima je važno pitanje prema kojem različite organizacije imaju različite stavove. Neki CERT timovi ne raspolažu resursima i tehničkim znanjem da bi se ovime bavili, i moraju se osloniti na pomoć eksperata iz drugih CERT timova. Sa druge strane, timovi koji se bave obezbeđivanjem mreža i sistema svojih korisnika na komercijalnoj bazi, obično će obaviti ove analize u punom obimu.

Ipak, određena analiza malicioznog koda treba da se obavi, bez obzira ko preuzima takvu obavezu na sebe. Time se uzima „otisak“ napadača, koji se može iskoristiti za sprečavanje ponovljenih napada na druge sisteme ili lokacije. Ponekad ne postoji drugi način da se usmeri istraga nekog incidenta ukoliko se ne ispita šta maliciozni kod pokušava da učini u sistemu. Samo uništavanje artefakata, i podizanje sistema od „nule“, kao odgovor na bezbednosni incident, je skupo i oduzima previše vremena, a i naivno je očekivati da se incident neće ponoviti ukoliko se njegov uzrok pravilno ne ispita i ne ukloni mogućnost ponovljenog napada.

7.4.2.4.1 Gde se analiziraju artefakti

Obično se maliciozni kod ne analizira na samom sistemu žrtve napada. Ogranizacije koje su žrtve napada imaju potrebu da u najkraćem mogućem roku povrate normalno funkcionisanje sistema, i cilj CERT organizacije nije da nadalje ugrožava njihovo poslovanje i funkcionisanje sistema. Pri preuzimanju artefakta treba povesti računa o tome da se ne iskopira samo artefakt, već i čitavo okruženje, tj. ako je to moguće, treba „preslikati“ sistem u kojem se incident desio. Ovaj posao mora da uradi osoblje CERT orgaizacije, sa adekvatnim nivoom tehničkog znanja, u saradnji sa osobljem organizacije koja je napadnuta.

U idealnom slučaju artefakti se analiziraju u laboratorijskom okruženju, na opremi koja služi samo za potrebe raznih vrsta testiranja, i koja je izolovana od bilo koje druge računarske mreže ili sistema. Bilo kakav gubitak podataka na takvoj opremi ne sme imati nikakve konsekvence po bilo koji sistem ili računarsku mrežu. Za slučaj da je ovoj opremi, iz praktičnih razloga, ipak potrebno omogućiti pristup spolja, potrebno je takvo okruženje izolovati veoma restriktivnim *firewall* polisama.

7.4.2.4.2 Kada je potrebno angažovati eksperte

S obzirom na veličinu i resurse prosečnog CERT tima, teško je očekivati da će svaki tim imati dovoljno znanja o svakom operativnom sistemu ili mrežnom protokolu. Stoga je često potrebno uspostaviti saradnju na analizi artefakata sa raznim ekspertskim grupama. S obzirom na osetljivost zadataka, ali i u zavisnosti od prirode CERT organizacije i njenih konstituenata, ovi eksperti moraju biti unapred identifikovani, i provereni sa stanovišta bezbednosti, i potrebno je preduzeti formalne mere (npr. potpisivanje ogovora o poverljivosti podataka sa ekspertskom ogranizacijom) pre nego što se uđe u proces saradnje i razmene informacija.

Primera radi, postoje CERT organizacije, koje imaju saradnju na dobrovoljnoj bazi sa ekspertima iz organizacija svojih konstituenata. Dobit je obostrana – CERT organizacija dobija adekvatnu pomoć tokom analize incidenata, a angažovani eksperti imaju informacije o najnovijim izazovima i trendovima na polju bezbednosti.

7.4.2.4.3 Kada prekinuti analizu

Najbolje je unapred definisati kriterijume, do koje dubine, i koliko dugo se analiza vrši pre nego što se taj proces zaustavi i zadatak prosledi nekom drugom entitetu (delu CERT tima koji se bavi analizom artefakata kao posebnim servisom, ili nekoj spoljnoj ekspertskoj organizaciji). Te granice mogu biti jednostavno određene na bazi veličine CERT tima i vremena koje im stoji na raspolaganju za ovakve aktivnosti, ili u zavisnosti od kompleksnosti samog incidenta ili artefakta koji se ispituje.

7.4.2.5 Analiza softverskog okruženja

Često nije dovoljno analizirati samo maliciozni kod ili log fajlove, već je jednako značajno proučiti i okruženje u kojem su pronađeni tragovi aktivnosti napadača, kako bi se sklopili svi delovi „mozaika“ i stekao uvid u širi kontekst dešavanja u napadnutom sistemu. Najčešće je uspeh napada određen upravo softverskim okruženjem, tj. karakteristikama napadnutog sistema.

Operativni sistem se sastoji od desetina aktivnih programa i komponenata, kao i stotina programa koji su u pozadini i pokreću se po potrebi. Fajl sistemi su obično jako kompleksni, sa pravima pristupa koja su dodeljena određenim korisnicima i grupama na gotovo „slučajnoj“ bazi.

Skripte malicioznog koda je ponekad lako analizirati jer same govore šta im je cilj, mada ponekad mogu sadržati i slučajne sekvence događaja, ili biti napisane na način koji je teško razumljiv.

Sa druge strane, izvršni fajlovi malicioznog koda su teži za analizu, tj. mogu se analizirati i razumeti njihovo delovanje samo kada se pokrenu na nekom sistemu. U tom slučaju potrebno je imati na raspolaganju laboratorijsko okruženje u kojem je moguće napraviti repliku napadnutog sistema i aktivirati maliciozni kod.

Zapravo, analiza artefakata je toliko povezana sa analizom softverskog okruženja, da jedna bez druge nemaju mnogo smisla. Otuda se preslikavaju i pravila koja su već navedena u vezi sa analizom artefakata:

- ko god da se bavi analizom artefakata (konstituenti, CERT, spoljnji eksperti), treba da se pobrine i za analizu softverskog okruženja u kojem se napad dogodio,
- preuzimanje i analiza artefakata podrazumeva i preslikavanje originalnog softverskog okruženja u kojem se incident desio. Poželjno je da se testovi izvode na istim operativnim sistemima, sa istim verzijama i nivoima „zakrpa“, sa istim konfiguracionim fajlovima, i slično. Naravno, najbolje bi bilo izvesti testove na originalnom okruženju, ali je to neprihvatljivo jer konstituenti imaju potrebu da se u najkraćem mogućem roku oporave od incidenta i nastave normalno poslovanje. Ponekad je, međutim, i to moguće, na primer ako se radi o akademskom okruženju, u kojem postoji, i lako je dostupno, brojno tehničko osoblje sa odgovarajućim nivoom stručnosti, gde je moguće u kratkom roku napraviti izolovano test okruženje, tj. gde postoji interesovanje za samu ovu aktivnost i njene rezultate.

Ponekad analiza artefakata i pripadajućeg softverskog okruženja može otkriti neke poznate ranjivosti sistema, i tada se žrtvi napada pomaže sa odgovarajućim savetom, a u slučaju većeg broja žrtava napada, šalje se i obaveštenje o tom događaju širom zajednice konstituenata. Sa druge strane, može se desiti da se analizom otkriju do tada nepoznate ranjivosti sistema, za koje još ne postoji rešenje, tj. „zakrpa“. U tom slučaju analizu problema treba proslediti timu u okviru CERT organizacije, koji se ovim poslovima bavi kao zasebnim servisom, ili eksternim saradnicima ili organizacijama sa kojima postoji saradnja na ovim poslovima. U idealnom slučaju novootkrivena ranjivost će u najkraćem roku biti sanirana, i o tome se obaveštavaju konstituenti čiji su sistemi napadnuti, kao i sve ostale zainteresovane strane.

7.4.2.6 Analiza mreže povezanih incidenata

Napredni napadači obično preko Interneta uspostavljaju čitavu mrežu konekcija, koristeći skup ranjivosti koji im omogućava da dobiju pristup brojnim sistemima, a zatim te kompromitovane sisteme koriste za ostvarivanje napada na druge sisteme. Kreiranje ovakve kompleksne mreže konekcija otežava detektovanje izvora napada, tj. otkrivanje identiteta napadača. Samo u slučaju da se otkrije „centar“ ovakvog napada (što bi na primer mogao biti prvi u lancu kompromitovanih sistema koje napadač koristi), može postojati mogućnost da se uđe u trag napadaču.

Lociranje napadača je proces kojem treba pristupiti sa izuzetnom pažnjom, jer je moguće da tokom tog procesa napadač i istražitelj istovremeno imaju pristup istim sistemima. Pri tome napadač obično ima pristup sa najvišim privilegijama (na primer *root* nalog na UNIX serveru ...), i može biti u mogućnosti da detektuje prisustvo istražitelja na sistemu, ili da sabotira njegove aktivnosti.

Analiza mreže povezanih incidenata je od izuzetne važnosti za uspešnu odbranu od napadača. Što su jasnije mreža konekcija i operacije koje napadač izvodi lakše je izvesti protivmere, i sprečiti da se incident proširi na druge sisteme, i na kraju moguće je locirati i uhvatiti napadača. Tokom izvođenja ove analize, potrebno je utvrditi i pratiti veze, tj. „otisak“ napadača, koji se pojavljuje kao trag napadača u log fajlovima napadnutih sistema.

7.4.2.6.1 Utvrđivanje veza u log fajlovima

Log fajlove, ili njihove delove koji su u vezi sa napadom, treba pažljivo analizirati, i treba istražiti svaku konekciju koja se sa posmatranog sistema pravi ka drugim sistemima. To obično znači da je po potrebi neophodno uključiti konstituente ili druge CERT organizacije u analizu, dajući im na uvid delove log fajlova koji su za njih relevantni. Štaviše, savetuje se da se u ovu analizu obavezno uključe i druge CERT organizacije, i da se sa njima dele informacije o načinu na koji napadač izvodi svoje aktivnosti, kako bi oni mogli na vreme da ih prepoznaju i deluju proaktivno na prevenciji novih napada. Ovo treba činiti sa svakim novim tragom koji se tokom analize incidenta otkrije, bez obzira na vreme i resurse koje takav događaj zahteva od CERT timova.

7.4.2.6.2 Utvrđivanje „otiska“ napadača

Tokom analize log fajlova potrebno je uložiti napor da se izoluje „otisak“ napadača, koji može da se uporedi sa drugim ranije otkrivenim potpisima. Pod „otiskom“ se podrazumeva način na koji napadač izvodi svoje aktivnosti, skripte koje koristi, lozinke koje koristi da pristupi sistemima koje napada, programi, tj. ranjivosti koje najčešće napada, kao i

imena fajlova ili direktorijuma koje najčešće koristi, a u kojima smešta svoje fajlove ili alate za napad na sistem.

Vođenje evidencije o ovim otiscima olakšava razumevanje aktivnosti napadača. Ukoliko se u sistemu pronađu instance koje nisu u skladu sa utvrđenim otiskom napadača, onda se može raditi o tome da postoji više njih koji simultano napadaju sistem, bilo slučajno ili organizovano.

7.4.3 Vođenje evidencije o incidentima

Tokom životnog ciklusa svakog incidenta, veoma je važno evidentirati sve informacije koje se odnose na incident, sa različitim nivoima detalja. Ovime se olakšava organizovanje informacija i efikasnije rešavanje incidenata. Evidentiranje informacija na logičan i organizovan način daje uvid u istoriju svih aktivnosti u delegiranju poslova i preduzetih koraka koji su doveli do razrešenja incidenta. Ova evidencija može da se koristi i za kreiranje raznih statistika i izveštaja koji su korisni u okviru funkcija servisa za upravljanje incidentima, ili funkcijama i procedurama nekih drugih servisa (kao što su merenje kvaliteta servisa, izveštavanje rukovodilaca CERT timova ili konstituenata, merenje angažovanja osoblja CERT tima, i slično).

Nivo detalja evidencije varira od tima do tima, zavisno od specifičnosti njihovih organizacija, nivoa servisa za upravljanje incidentima koji pružaju, kao i dubine analize koja se preduzima. Dobra praksa je da se za svaki incident evidentira minimalno sledeći skup informacija, dat u tabeli 7.2.

U zavisnosti od svojih individualnih politika, timovi mogu čuvati informacije o incidentima u svom sistemu za evidenciju u kraćem vremenskom periodu, dok je to još uvek neophodno, npr. tokom nekoliko nedelja po zatvaranju incidenta radi prikupljanja statističkih informacija. Međutim, običaj je da se podaci čuvaju malo duže od toga u slučaju da postoji mogućnost da se isti incident ponovo aktivira. Ponekad postoje zahtevi da se podaci čuvaju dok god traju istražni ili sudski postupak koji je iniciran nekim incidentom.

7.5 PROCES IZDAVANJA OBAVEŠTENJA

Kao što je ranije već pomenuto, zadatak procesa izdavanja obaveštenja je izdavanje informacija u različitim formatima, u skladu sa potrebama konstituenata. Smisao izdavanja obaveštenja varira od razmene informacija o tekućim incidentima i pretnjama, kao i koracima koje treba preduzeti da bi se od njih zaštitili, do prerađenih informacija o aktuelnim trendovima na temu obima i prirode napada koji su prijavljeni CERT timu u nedavnoj prošlosti. Kada su u pitanju CERT timovi koji pružaju širi spektar različitih servisa, izdavanje obaveštenja se može posmatrati kao poseban servis, i kao takav on može da pruža mnogo više informacija koje se dobijaju na bazi drugih implementiranih servisa, kao što su servisi za analizu artefakata ili istraživanje ranjivosti sistema.

Od kada postoje CERT organizacije izdavanje obaveštenja konstituentima CERT tima smatra se delom svakodnevnog posla CERT tima, bilo da se sprovodi kao poseban servis, ili kao deo servisa za upravljanje incidentima. Međutim, kao što je ranije pomenuto, proces izdavanja obaveštenja je opciona delatnost, s obzirom da nije kritična sa stanovišta osnovnog servisa za upravljanje incidentima. Glavni cilj ove funkcije je da se konstituentima proslede informacije koje će im pomoći u zaštiti njihovih sistema, ili da bi se pronašli tragovi potencijalnog napada davanjem informacija o mogućim, tekućim ili nedavnim pretnjama.

Dodatno, sugerišu se metode za prevenciju, otkrivanje ili oporavak od incidenata. Kada se objavljuju informacije u vezi sa napadom određenog tipa, treba obezbediti da je nivo informacija koje se otkrivaju dovoljan da konstituenti razumeju prirodu napada i mogu da provere da li su postali žrtve tog napada, ali ne toliko detaljne da bi mogle da se upotrebe kao uputstvo za sprovođenje napada. Ovo je jedan od najvećih izazova za funkciju izdavanja obaveštenja.

Tabela 7.2: Evidencija informacija o incidentima

INFORMACIJA KOJA SE EVIDENTIRA	**OPIS**
Jedinstveni indentifikator incidenta u okviru lokalnog CERT-a	CERT tim po prijemu prijave incidenta treba da mu dodeli jedinstveni identifikator, koji se zatim koristi za evidentiranje svih informacija i akcija koje se povodom tog incidenta preduzimaju
Jedinstveni identifikator posmatranog incidenta dodeljen od drugih CERT-ova	U slučaju da je incident već evidentiran od strane drugih CERT organizacija treba evidentirati informaciju o tome kako bi se u kasnijim fazama razrešenja incidenta olakšala komunikacija i razmena informacija sa drugim CERT organizacijama.
Ključne reči ili kategorizacija	Ovo je informacija kojom se karakteriše incident, i olakšava uspostavljanje veza između različitih incidenata. Ova informacija može da se menja tokom životnog ciklusa incidenta, u zavisnosti od novih informacija do kojih se dolazi tokom analize incidenta.
Kontakt informacije	Imena, brojevi telefona, adrese elektronske pošte i druge kontakt informacije svih strana koje su uključene u incident. Ove informacije treba da sadrže i podatke o preferiranim metodama enkripcije i pridružene ključeve.
Politike	Polise ili napomene pravne prirode kojima se utvrđuje način postupanja tokom rešavanja incidenta.
Prioritet	Oznaka prioriteta incidenta u skladu sa šemom prioritetizacije CERT organizacije. Moguće je da se prioritet incidenta menja tokom njegovog životnog ciklusa.
Drugi materijali	Lokacije na kojima su smešteni materijali o incidentu (kao što su log fajlovi ili štampani materijal).
Istorija incidenta	Evidencija svih poruka elektronske pošte, ili detalji telefonskih razgovora i faks poruka koji su u vezi sa incidentom.
Status	Trenutni status incidenta.
Akcije	Lista prošlih, trenutnih i budućih akcija koje treba preduzeti u svrhu razrešenja incidenta. Svaka akcija treba da bude delegirana tačno određenom članu CERT tima. U slučaju da je to moguće, svaka akcija treba da ima evidentiran trenutak izvršenja, ili rok za izvršenje.
Koordinator incidenta	CERT tim može po potrebi da imenuje člana tima koji je zadužen za koordinaciju aktivnosti na razrešenju incidenta. Ovo je važno radi uspostavljanja centralne tačke za razmenu informacija, u cilju kreiranja šire slike incidenta i efikasnijeg razrešenja.
Parametri kvaliteta servisa	Informacije koje mogu pomoći u merenju kvaliteta pruženog servisa. Referenciranje na obaveze preuzete deklarisanim nivoom podrške mogu uticati na pristup CERT tima u rešavanju incidenta.
Tekstualni opis	Opis u slobodnoj formi svih aspekata incidenta koji nisu evidentirani ni u jednom od prethodnih polja.

7.5.1 Tipovi obaveštenja

Obaveštenja mogu imati mnogo različitih formi, od onih koja pružaju kratkoročne informacije u vezi sa specifičnim tipovima tekućih aktivnosti, do dugoročnih informacija opšte prirode kojima se podiže svest o informatičkoj bezbednosti. Svaki od ovih tipova obaveštenja imaju svoje prednosti i mane.

7.5.1.1 Najave

Najave obično imaju formu kratke poruke, u slučaju kada detaljne informacije još uvek nisu dostupne. Svrha najava je da se konstituenti i drugi entiteti informišu o nečemu što će verovatno postati važno u vrlo bliskoj budućnosti, i one imaju brojne dobre strane. Prvo, CERT tim na ovaj način može proaktivno da upozori i informiše svoje konstituente o potencijalnoj pretnji. Drugo, sami konstituenti mogu već i pre toga imati neka saznanja ili probleme koji su u vezi sa najavom, o čemu mogu da podele više informacija sa svojim CERT timom. Treće, čak i ako primaocima najave u datom trenutku nije jasan njen sadržaj, može im biti od pomoći ako kasnije primete dešavanja na koja se ona odnosi, i shvate značaj informacije koju su ranije dobili.

Međutim, jedan od nedostataka ovakve vrste informacija je da se one tokom vremena mogu promeniti, tako da je preporučljivo da najave u okviru svog teksta sadrže i iskazano odricanje od odgovornosti, kako bi se jasno napomenulo da je neka informacija nepotvrđena ili može biti na nivou špekulacije.

7.5.1.2 Upozorenja

Upozorenja su kratkoročne objave o kritičnim dešavanjima koja sadrže hitne informacije o nedavnim napadima, uspešnim upadima u sisteme, ili novootkrivenim ranjivostima sistema. Događaj koji je tema upozorenja može već biti detaljno opisan sa svim neophodnim informacijama, ali se ponekad može desiti da se upozorenje dopuni novim informacijama.

7.5.1.3 Saveti

Saveti su jedan od najčešćih tipova obaveštenja koje izdaju CERT organizacije. Oni daju srednjoročne i dugoročne informacije o problemima i rešenjima koja su pogodna za podizanje svesti o informacionoj bezbednosti i sprečavanje incidenata. Oni obično sadrže informacije o novootkrivenim ranjivostima sistema, ali mogu sadržati i informacije o aktivnostima napadača. Saveti su najčešće proizvod kvalitetnih istraživanja i analiza i sadrže ključne tehničke detalje o „zakrpama“ i rešenjima u slučaju pojave određenih bezbednosnih incidenata. U najvećem broju slučajeva oni su usmereni na tehničko osoblje, kao što su administratori sistema ili mreža, mada ponekad mogu sadržati i dodatne informacije koje su interesantne i za širu publiku.

7.5.1.4 Kratka obaveštenja

Slično kao i saveti, ovo su dokumenta koja sadrže srednjoročne i dugoročne informacije, ali u kraćoj formi biltena, sa manje tehničkih detalja, i namenjena su široj populaciji. Ona mogu sadržati informacije edukativne prirode, koje mogu biti od koristi

netehničkom osoblju koje ima interesovanja za pitanja informacione bezbednosti. Često su namenjena obaveštavanju rukovodstava organizacija, pravnih službi, ili novinara.

7.5.1.5 Smernice

Smernice mogu biti opširni dokumenti koji sadrže niz koraka koji nekoga, ko je upoznat sa osnovnim konceptima informacione bezbednosti, mogu provesti kroz proces proširivanja znanja i svakodnevne prakse na temu informacione bezbednosti.

7.5.1.6 Tehničke procedure

Tehničke procedure su još opširnije od smernica, sa više tehničkih detalja namenjenih ekspertima, i često se tiču usko definisane tehničke problematike.

7.5.2 Prethodna razmatranja

Definisanje skupa tipova obaveštenja je samo prvi korak u okviru sveobuhvatnog procesa izdavanja obaveštenja. Postoji niz faktora koje treba uzeti u obzir pre izdavanja konkretnog obaveštenja, i oni idu od toga koji kriterijum je okidač za izdavanje obaveštenja, do toga na koji način će biti distribuirana.

7.5.2.1 Kriterijumi za izdavanje obaveštenja

Potrebno je uspostaviti kriterijume kojima se utvrđuje koji su to okidači koji pokreću proces izdavanja svakog od različitih tipova obaveštenja. Oni mogu biti bilo šta, od informacija koje se primaju od drugih CERT timova, do naglog porasta broja incidenata koje je CERT tim registrovao. Očigledno, da bi uspostavljeni kriterijumi imali smisla potrebno je konstantno voditi evidenciju o pristiglim informacijama. Najčešće je izvor informacija sam CERT tim, na bazi aktivnosti koje sam sprovodi, ili informacija koje dobija od konstituenata, ili u vidu obaveštenja koje dobija od drugih CERT timova.

7.5.2.2 Kriterijumi za kategorizaciju

Korisno je uspostaviti kriterijume koji pomažu u kategorizaciji materijala koji treba da budu predmet obaveštavanja, kako bi tip obaveštenja odgovarao tipu informacije koja se deli. Ovaj zadatak nije toliko težak u slučaju da se kriterijumi baziraju na izvorima informacija, ali može biti teži ako se baziraju na tipu sadržaja.

Primera radi, ukoliko informacije pristižu sa javnih servisa za obaveštavanje, one se mogu pretočiti u najave, ali svakako ne u savete, osim u slučaju da se njihov sadržaj proveri i verifikuje kroz neku vrstu analize u okviru CERT tima (kategorizacija na bazi izvora informacije). Slično tome, ukoliko se neka CERT organizacija generalno ne bavi računarskim virusima, ogroman porast broja incidenata sa virusima neće izazvati izdavanje saveta ili smernica, ali može da da bude signal CERT organizaciji da izda upozorenje ili najavu (kategorizacija na bazi sadržaja informacija).

Kada se radi kategorizacija na bazi sadržaja obaveštenja, treba imati u vidu i ciljanu publiku kojoj je obaveštenje namenjeno.

Primera radi, u slučaju otkrivanja velikog bezbednosnog propusta u nekom protokolu, ili široko zastupljenom softveru, mogu se objaviti vrlo detaljni tehnički saveti namenjeni

iskusnim sistem administratorima, a ne širokoj publici. Sa druge strane, u slučaju otkrivanja bezbednosnih propusta u nekom Internet pretraživaču, treba objaviti opis problema sa manje tehničkih detalja u vidu kratkog obaveštenja koje je namenjeno široj publici.

7.5.2.3 Prioritetizacija

Nekoliko (manje ili više subjektivnih) faktora utiče na utisak o važnosti svakog pojedinačnog obaveštenja. Dodeli objektivnih prioriteta obaveštenjima treba pristupiti sa pažnjom, kako na osnovu tipa objave, tako i na bazi informacija koje obaveštenja sadrže. CERT organizacija mora da koristi odgovarajući tip obaveštenja da bi odgovarajuće informacije plasirao odgovarajućoj publici.

Primera radi, ranije su CERT organizacije imale samo jedan način na koji su javno objavljivale informacije za svoje konstituente, i to je bila forma saveta. Savetima su se konstituenti upućivali na ono na šta treba da „obrate pažnju“. Ovaj način je jedno vreme smatran efikasnim, međutim, ispostavilo se da nisu sve informacije podjednako važne, tj. da neke moraju imati veći prioritet od drugih. Korišćenje samo jednog tipa objave informacija, u okruženju u kojem postoji jako puno različitih tipova događaja i informacija, zahteva postojanje i drugih ranije navedenih šema obaveštavanja, koje mogu imati različite prioritete.

7.5.2.4 Selekcija informacija za obaveštavanje

U skladu sa politikama i procedurama CERT organizacije koje se tiču objavljivanja informacija, informacije koje CERT želi da objavi u formi obaveštenja, moraju biti selektovane, tj. „prečišćene“ do određenog nivoa, u zavisnosti od toga da li se objavljuju javno, ili samo interno u okviru CERT organizacije. Da bi se ovaj proces odvijao bez problema potrebno je prethodno uspostaviti jasna pravila za prečišćavanje informacija.

Primera radi, jedno od očiglednih pravila za selekciju informacija koje se objavljuju može biti to da one nikada ne sadrže podatke o konkretnim pojedincima, konstituentima ili lokacijama. Drugo slično pravilo je to da se informacije koje se dobiju od drugih CERT timova ne mogu objaviti bez odgovarajuće dozvole tih timova.

7.5.2.5 Kanali distribucije obaveštenja

U zavisnoti od tipa obaveštenja, potrebno je uzeti u obzir različite faktore pre nego što se odabere kanal za njihovu distribuciju:

- Osetljivost informacija – Da li je odabrani kanal za distribuciju informacija dovoljno bezbedan ?
- Publika/konstituenti kojima se obraćamo – Da li je odabrani kanal adekvatan da se dopre do svih ciljanih konstituenata ?
- Brzina – Da li će odabranim kanalom informacije stići do korisnika dovoljno brzo ?
- Troškovi – Da li će distribucija obaveštenja doneti odgovarajuće rezultate, da isplati utrošene resurse i vreme u kreiranju obaveštenja ?

7.5.3 Životni vek obaveštenja

Pošto se donese odluka o kriterijumima za izdavanje obaveštenja, i stilu njihovog prezentovanja, sledeći korak je da se definišu procesi i procedure za upravljanje kreiranjem

obaveštenja (tipovi, forme, stil, i slično). U životnom veku svakog obaveštenja može se generalno prepoznati pet faza koje su opisane u tekstu koji sledi.

7.5.3.1 Iniciranje obaveštenja

Kada se identifikuju informacije koje je moguće objaviti u nekoj formi (npr. tokom procesa analize nekog incidenta) potrebno je utvrditi da li su te informacije u skladu sa kriterijumima opisanim u poglavlju 7.5.2, ili su u nekom drugom smislu dovoljno važne da bi ih trebalo objaviti u formi obaveštenja. Zatim je potrebno odrediti tip obaveštenja, tip sadržaja, kao i ciljanu publiku kojoj je obaveštenje namenjeno. Korisno je i alocirati neki identifikator obaveštenja u sistemu za evidenciju koji CERT organizacija koristi, kako bi se lakše pratio razvoj i objava obaveštenja.

Prioritet, ili važnost teme koja se pokriva, tip obaveštenja, tip sadržaja, kao i ciljana publika određuju sledeće važne parametre obaveštenja:

- stil obaveštenja i nivo detalja koje obaveštenje sadrži,
- mere za prečišćavanje informacija koje će biti objavljene, i
- kanali distribucije koji će se koristiti.

Dodatno, drugi faktori koje treba uzeti u obzir odnose se na vremenski okvir za obaveštavanje, interne resurse koji su u tom smislu neophodni, odgovornost za preuzeti zadatak. Naravno, postoji i faktor saradnje sa drugim entitetima na ovom poslu, kao što je razmena informacija sa drugim CERT organizacijama radi poboljšanja kvaliteta obaveštenja, ili sinhronizacije u njihovom objavljivanju.

7.5.3.2 Interna prioritetizacija obaveštenja

Ovo je faza na koju se treba stalno vraćati u procesu izrade obaveštenja. Moguće je da timovi u nekom trenutku imaju nekoliko paralelnih aktivnosti na kreiranju obaveštenja (u različitim fazama razvoja), i pri tome su obaveštenja, koja još uvek nisu objavljena, prioritetizovana na bazi predefinisanih kriterijuma, i to u trenutku kada je započet rad na kreiranju obaveštenja. Međutim, neka obaveštenja mogu imati veći prioritet, u smislu hitnosti, i ona moraju dobiti prednost u odnosu na ostala obaveštenja koja su u tom trenutku u izradi. Primera radi, obaveštenja koja daju uopštene statističke informacije mogu se smatrati najmanje važnim, tj. moguće je vreme njihovog objavljivanja prolongirati ukoliko se u međuvremenu pojave druge bitnije informacije čije je objavljivanje hitno. U ovakvim slučajevima najbolje je prioritetizaciju vršiti na bazi ozbiljnosti problematike na koju se obaveštenje odnosi, kao i broj i tip konstituenata kojima je obaveštenje namenjeno.

7.5.3.3 Kreiranje obaveštenja

Ova faza se odnosi na tehnički opis i samo sastavljanje teksta obaveštenja. Većina CERT timova ima standardizovanu formu za različite tipove obaveštenja, na kojima se baziraju njihov izgled i sadržaj. Može se kreirati i radna verzija obaveštenja koja se prosleđuje na internu, ili limitiranu eksternu proveru, kako bi se dobili detaljni komentari od strane eksperata koji nisu deo CERT organizacije koja izdaje obaveštenje. Pri tome, treba navesti restrikciju da sadržaj obaveštenja nije spreman za dalju distribuciju dok to ne učini sama CERT organizacija na zvaničan način. Da bi se u ovom procesu sadržaj obaveštenja zaštitio od napada ili prevremene objave potrebno je da radni dokument bude enkriptovan i digitalno potpisan.

7.5.3.4 Finalna priprema

Pre same objave treba rešiti i neke tehničke probleme, kao što je generisanje kriptografskih parametara samog obaveštenja, ili objekata na koje se ono odnosi. Međutim, većina problema koji postoje u ovoj fazi su netehničke prirode, i odnose se na način predstavljanja sadržaja (datumi, zaglavlja, komentari, priznanja, odricanje odgovornosti ...). Pre izdavanja obaveštenja CERT tim treba da proveri da li su sve reference u okviru dokumenta validne i dostupne.

Još jedna stvar koju teba uzeti u obzir je to da li je potrebno ponuditi distribuiranje obaveštenja unapred, za neke privilegovane kategorije, kao što su prijateljske CERT organizacije, ili mediji sa kojima CERT organizacija sarađuje. Time se ovim organizacijama daje mogućnost da se pripreme na reakcije javnosti ili konstituenata u odnosu na problematiku koja je tema obaveštenja.

Članovi CERT tima koji se bave trijažom incidenata, ili drugim funkcijama servisa za upravljanje incidentima, treba da budu u stanju da prime povratnu informaciju, ili daju adekvatan odgovor konstituentima, koji se obrate CERT timu reagujući na primljeno obaveštenje. Zato je potrebno da većina članova CERT tima bude do detalja u toku sa informacijama koje čine sadržaj obaveštenja.

Na kraju, svako objavljeno obaveštenje treba da ima eksterni evidencioni identifikator, koji se obično kreira na bazi tipa obaveštenja. Zatim je potrebno dokument obaveštenja digitalno potpisati i zaštititi od neovlašćene izmene sadržaja.

7.5.3.5 Distribucija obaveštenja

Ova aktivnost se odnosi na aktivnosti u distribuciji obaveštenja, korišćenjem mehanizama za zadati tip obaveštenja. Ovo može da uključuje postavljanje obaveštenja na odgovarajuće servere CERT tima, kao što su ftp ili web server, ili distribuciju preko drugih mehanizama kao što su: elektronska pošta, automatizovano slanje fax poruka, ili putem medija.

7.6 PROCES DAVANJA POVRATNIH INFORMACIJA

Glavni cilj većine CERT organizacija je razrešavanje bezbednosnih incidenata i davanje podrške konstituentima radi oporavka od posledica ovih incidenata. Ukoliko je CERT organizacija u tome efikasna do nje će stizati i drugi zahtevi i prijave problema, koje se ponekad čak i ne moraju ticati CERT organizacije, ili servisa za upravljanje incidentima koji ona pruža. Na žalost, ignorisanje ovakvih zahteva i prijava, čak i kada nisu u opisu delovanja CERT organizacije, može loše uticati na reputaciju tima, i na odnos koji konstituenti imaju prema njemu. Zbog toga je u interesu svakog CERT tima da obezbedi odgovarajući nivo povratnih informacija, bez obzira na to ko im se obraća i sa kojim povodom.

Sa druge strane, iz perspektive dobijenih informacija, tj. tipova zahteva sa kojim se konstituenti ili drugi entiteti obraćaju CERT organizaciji, moguće je steći uvid u stanje njihovih trenutnih potreba. Davanje povratnih informacija kao rezultat ima bolju isporuku servisa koje CERT tim pruža, ali i uspostavljanje adekvatnih očekivanja koje konstituenti treba da imaju prema svojoj CERT organizaciji. CERT organizacija treba da teži da da odgovor na bilo kakav zahtev koji do nje stigne, makar to bio i odgovor tipa „ne možemo

odgovoriti na vaš zahtev, jer je to van okvira servisa koje pružamo“, ili da konstituente uputi na druge izvore informacija.

Primera radi, ukoliko CERT tim ne odgovori na pitanja koja mu se upute, može se steći utisak da je tim nije na raspolaganju svojim konstituentima, ili je nesposoban da pomogne, ili čak i gore, da je arogantan, neinformisan i loše vođen. Da bi se izbegla ovakva percepcija tima, tim treba barem da izda izjavu o svrsi svog postojanja, i zbog čega nije u prilici da pruži dalje informacije na temu postavljenog pitanja (ukoliko tematika nije u okviru poslova i servisa koje tim pruža).

Zahtevi ili pitanja koja uobičajeno stižu na adresu CERT tima mogu se generalno podeliti u četiri kategorije:

- Opšti zahtevi na temu informacione bezbednosti - Ovakvi zahtevi uglavnom se odnose na dobijanje informacija kojima se može proaktivno pomoći u izbegavanju bezbednosnih incidenata, ili o tome na koji način je moguće stupiti u kontakt sa CERT organizacijom u slučaju da se ipak dogodi bezbednosni incident. S obzirom da se CERT timovi u opštem slučaju bave bezbednosnim incidentima, oni sigurno mogu pomoći u dobijanju ovakvih informacija. Otuda se čini prirodnim da ljudi upućuju CERT timovima ovakva pitanja ili zahteve. CERT timovi bi trebali, kada god je to moguće, da učestvuju u razmeni informacija i proaktivno deluju na sprečavanju bezbednosnih incidenata i podizanju svesti o informacionoj bezbednosti, kako svojih konstituenata tako i šire zajednice.
- Zahtevi od strane medija - Ovi zahtevi se odnose na upite koji stižu od medija koji traže informacije radi izveštavanja javnosti na opšte teme informacione bezbednosti, ili u vezi sa nekim bezbednosnim incidentima ili objavama koje stižu od CERT organizacija. Kada god je to moguće CERT timovi treba da izađu u susret zahtevima medija, ali obazrivo i u skladu sa svojim politikama o deljenju informacija.
- Ostali zahtevi i pitanja - Postoji čitav niz različitih pitanja ili zahteva koje konstituenti mogu uputiti svojoj CERT organizaciji, a na koje tim ima potrebu da odgovori. Primera radi, može se od CERT organizacije zahtevati da delegira govornika na skupovima o informacionoj bezbednosti, ili se može tražiti dozvola od CERT timova da se u edukativne svrhe koriste njihovi istraživački radovi ili drugi autorski materijali. Ispunjenje ovakvih zahteva doprinosi podizanju svesti o delovanju CERT tima i njegovoj dobroj slici u javnosti. Takođe, u ovu opštu kategoriju može se svrstati i izdavanje godišnjih izveštaja CERT organizacija, iako se to više tiče proaktivnog davanja informacija, nego odgovaranja na nečiji zahtev.
- Zahtevi van okvira delovanja CERT-a - Ovi zahtevi nemaju dodirnih tačaka sa oblastima delovanja CERT organizacije, ali kao što je već napomenuto, čak i u takvim situacijama treba dati nekakvu povratnu informaciju, radije nego da se takvi zahtevi ignorišu.

7.6.1 Životni ciklus povratnih informacija

CERT tim može odlučiti da vodi evidenciju o svakom od različitih tipova zahteva, sa različitim tipovima identifikatora. Ili mogu voditi evidenciju o svim zahtevima sa jedinstvenim tipom identifikatora, i da zatim označe različite tipove zahteva, prema prirodi odgovora koji je dat na svaki od tih zahteva. Dakle, zahtevi imaju životni ciklus koji je sličan

životnom ciklusu bezbednosnih incidenata, osim što za njih nije uobičajeno da se drže u otvorenom statusu dugo posle davanja inicijalnog odgovora od strane CERT tima, iako se ponekad za neka od pitanja može razviti i diskusija.

7.6.2 Odgovori na najčešće postavljena pitanja i druge opšte objave

Ponekad se svaki zahtev ili pitanje može tretirati individualno, ali CERT timovi obično nisu u prilici da izdvoje resurse za ovaj posao, jer on može biti vremenski jako zahtevan. Najčešće timovi imaju unapred pripremljena dokumenta, na primer u vidu objave pripremljenih odgovora na najčešće postavljena pitanja. Ovakav dokument daje odgovore na neka opšta pitanja o CERT timu, detaljima servisa za upravljanje incidentima koji tim pruža, ili može ukazivati na način kako može da se pristupi dokumentaciji koja se odnosi na specifične potrebe konstituenata. Jednom kada se ovakva dokumenta pripreme, na većinu pitanja se može odgovoriti jednostavnim slanjem uputstva kako da se dođe do dokumenata u kojima je sve već opisano. Čak se i u slučaju zahteva koji su van opsega delovanja CERT tima može na ovaj način poslati poruka da se na takve zahteve ne mogu očekivati odgovori.

Primera radi, novoformirana CERT organizacija može u inicijalnoj fazi da vodi evidenciju o pitanjima i zahtevima sa kojima joj se konstituetni obraćaju, i da na bazi toga izradi svoju bazu odgovora na najčešće postavljena pitanja, kako bi se u budućnosti lakše nosila sa takvim poslom. Naravno, vremenom se ova baza može proširivati i objaviti na Internet stranici CERT tima.

Kada je u pitanju interakcija sa medijima, CERT tim se može osloniti na usluge odgovarajuće službe svoje krovne organizacije, ili takav posao može delegirati članu tima koji ima iskustva u saradnji sa medijima. U svakom slučaju, jednom kada tim uspostavi politiku odnosa sa medijima, svi zahtevi ovog tipa moraju se tretirati u skladu sa tom politikom.

7.6.3 Organizacija procesa davanja povratnih informacija

Ukoliko postoje standardni odgovori na različite tipove zahteva, onda je moguće da se i osoblje bez dubokog tehničkog znanja uključi u proces davanja povratnih informacija u okviru ovog procesa. Alternativa može biti da se podnosilac zahteva uputi na druge izvore informacija, kao što su arhive tehničkih uputstava koje su dostupne na Internetu, bilo da su objavljene od strane drugih CERT timova, ili eksternih tehničkih eksperata.

Radi bolje i konzistentne reakcije svih članova tima na postavljene zahteve, može biti korisno izgraditi i internu bazu odgovora na najčešće postavljena pitanja, kojom se članovima tima daju uputstva i opisi procedura u vezi sa odgovorima na različite zahteve konstituenata ili drugih entiteta. Ovakav dokument trebalo bi sa sadrži i detalje o tome kako se vrši prioritetizacija zahteva. Primera radi, zahtevi koji stižu od finansijera mogu imati najviši prioritet, a odmah za njima mogu biti zahtevi konstituenata. Pored toga, tim može doneti odluku da se prioritetizacija vrši prema sadržaju zahteva, a ne prema izvoru koji ga je uputio. Takođe, interna baza odgovora na najčešće postavljena pitanja može biti jako korisna u procesu obuke novih članova CERT tima.

7.7 PROCES SARADNJE

Tokom životnog ciklusa bezbednosnog incidenta, većina aktivnosti koje CERT tim sprovodi uključuje interakciju, tj. saradnju sa drugim entitetima. S obzirom na važnost i

posledice koje takva saradnja može imati, potrebno je veoma pažljivo izabrati organizacije sa kojima se sprovodi saradnja. Tokom većine interakcija, tj. tokom komunikacije i razmene informacija, potrebno je obezbediti autentifikaciju i očuvati poverljivost informacija.

7.7.1 Tačke kontakta

Tokom trajanja bilo kog incidetna kontakti se uspostavljaju po potrebi. Koliko je važno inicirati proces razmene informacija, još važnije je pronaći odgovarajuću osobu, ili organizaciju, koja će na bazi dobijenih informacija na najbolji način doprineti razrešenju bezbednosnog incidenta. Otuda je potrebno da CERT organizacije stalno rade na izgradnji kontakata i dobrih odnosa sa drugim entitetima, sa ciljem da se izgradi mreža poverenja koja doprinosi efikasnom procesu razrešenja incidenata.

U najširem smislu, kontakti se mogu podeliti u dve kategorije – one koji imaju veze sa bezbednosnim incidentima, i one koji to nisu.

7.7.1.1 Kontakti u vezi sa bezbednosnim incidentima

Ovo su kontakti koje CERT organizacija mora da ostvaruje tokom procesa razrešenja nekog konkretnog bezbednosnog incidenta. To mogu biti kontakti unutar organizacije koja je žrtva bezbednosnog incidenta, ili sa eksternim organizacijama koje mogu pružiti pomoć u njegovom razrešenju. Primeri ovakvih kontakta su:

- rukovodstvo organizacije,
- finansijeri,
- drugi sektori u okviru organizacije,
- administratori sistema i računarskih mreža,
- osoblje zaduženo za informacionu bezbednost,
- konsultanti za pravna pitanja, ili pravne službe,
- služba interne revizije,
- mrežni operativni centar, i
- mrežni informativni centar.

U velikim organizacijama može postojati unapred određena inicijalna tačka kontakta kojoj se CERT organizacija obraća u vezi sa bezbednosnim incidentom koji je prijavljen na toj lokaciji. Međutim, jako je važno da se posle toga CERT organizacija uputi na kontakt sa odgovarajućom službom ili osobama, sa kojima dalje može da sprovodi neophodne aktivnosti. Bez mogućnosti da se ostvari direktan kontakt sa rukovodstvom organizacije ili odgovarajućim službama, može doći do gubitka vremena dragocenog za razrešenje incidenta, ili umanjenje njegovih posledica.

7.7.1.2 Kontakti koji nisu u vezi sa posmatranim incidentom

Ovi kontakti omogućavaju CERT timovima da dobiju dodatne informacije koje im pomažu u pružanju servisa, da olakšaju njihovo operativno delovanje, ili da dolaze do informacija od eksperata za određene tipove bezbednosnih incidenata. Primeri ovakvih kontakata su:

- IT osoblje na lokacijama konstituenata,
- kontakti drugih službi na lokacijama konstituenata (sektor fizičkog obezbeđenja, ljudskih resursa, i slično),

- provajderi Internet servisa,
- druge CERT organizacije,
- istražni ili pravosudni organi,
- proizvođači IT opreme,
- eksperti za pitanja informatičke bezbednosti, i
- mediji.

Kao što je ranije pomenuto, postoji jako dobar razlog da CERT organizacija održava više različitih vrsta kontakata sa svojim konstituentima, a to je potencijalna potreba za eskalacijom. Uobičajeno je da se tokom rešavanja incidenta komunicira samo sa jednom službom u okviru organizacije konstituenta, a dodatni kontakti sa rukovodstvom su neophodni kada je očigledno da incident može imati šire posledice po poslovanje, ili je potrebna istovremena saradnja sa više sektora u okviru organizacije konstituenta.

7.7.1.3 Pronalaženje kontakata

Pronalaženje odgovarajućih kontakata u okviru organizacije konstituenta nije uvek jednostavan zadatak. U situacijama koje nisu kritične mogu se koristiti javno dostupni resursi, kao što su kontakt informacije na Internet stranici organizacije. Međutim, kada je na bazi kontakta sa konstituentom potrebno doneti odgovarajuće odluke, korišćenje pogrešnog kontakta može dovesti do curenja kritičnih informacija. Ovime se, takođe, demonstrira manjak kontrole i pažnje na strani CERT organizacije, što nije dobro za njenu reputaciju.

Da bi se očuvalo poverenje konstituenata u svoju CERT organizaciju potrebno je posvetiti veliku pažnju identifikovanju i korišćenju adekvatnih kontakata. Ukoliko se koriste javno dostupne kontakt informacije, koje kao takve mogu biti krivotvorene, potrebno je verifikovati ih pre uspostavljanja kontakta. U svakom slučaju, najbolje je kontakt informacije preuzeti unapred, od samih konstituenata, tj. njihovih rukovodilaca ili ovlašćenih službi.

7.7.1.4 Održavanje kontakata

Iako izgleda kao jednostavan zadatak, u realnosti održavanje liste kontakata u ažurnom stanju može biti veći izazov nego je inicijalno formirati. Kontakt informacije, u nekom svom delu, mogu postati zastarele kada neki ljudi napuste organizaciju, ili su raspoređeni na drugo radno mesto, ili im se prosto promeni fizička lokacija na kojoj rade i npr. broj telefona koji koriste. Uvek je moguće tražiti od konstituenata da pošalju informaciju o ovakvim događajima, tj. promeni kontakt informacija, ali se u realnosti to retko dešava. Za kontakte koji nisu od kritičnog značaja ovo ne mora biti tako veliki problem, tj. oni se ažuriraju u trenutku kada nove informacije dopru do CERT organizacije, na bilo koji način. Međutim, za kritične kontakte se preporučuje redovna periodična provera njihove ažurnosti (jednom u toku tromesečja, na pola godine ili na godinu dana ...) kako bi se baza ovakvih kontakata održavala u što ažurnijem stanju.

Primera radi, postoje CERT organizacije koje od svojih konstituenata zahtevaju da odrede kontakt osobu za pitanja bezbednosti, ali i da kreiraju generičku adresu elektronske pošte, koja bi se koristila za komunikaciju sa CERT organizacijom. Upravljanje tim nalogom prepušta se lokalnim administratorima, i oni treba da vode računa da se ta pošta uvek preusmerava na osobu, ili više njih, koji su u tom trenutku zaduženi za poslove informacione bezbednosti.

7.7.2 Autentifikacija

Autentifikacija je izuzetno važan aspekt prilikom komunikacije sa drugim entitetima, van CERT organizacije. Ovaj termin se obično odnosi na to da je potrebno potvrditi da je osoba sa kojom se komunicira zaista ta za koju se predstavlja. Korišćenje savremenih sredstava komunikcije ovaj posao još više otežava, tj. daje se na značaju procesu autentifikacije. Razmeni informacija nikako ne treba pristupati pre autentifikacije učesnika u komunikaciji, i potvrde da je osoba sa druge strane autorizovana za pristup tim informacijama. Pri tome, pri razmeni informacija potrebno je voditi evidenciju o svakom kontaktu, ili izvoru informacija.

Dakle, pre nego što dođe do razmene informacija, osim identiteta osobe sa druge strane, potrebno je utvrditi i njenu „podobnost“, tj. da li je ona autorizovana da prima informacije, ili sprovodi akcije na osnovu dobijenih informacija. Primera radi, tokom trajanja nekog incidenta CERT organizacija može da pokuša da kontaktira rukovodioca organizacije koja je meta napada. Ukoliko je on nedostupan, tj. njen ili njegov asistent preuzme vezu, ta osoba može biti autentifikovana, tj. može se utvrditi i potvrditi njen identitet i uloga u okviru organizacije konstituenta, ali je to i dalje ne čini podobnom da joj se saopšte informacije koje su namenjene njenom rukovodiocu. Nekada je prosto pogodnije da se sačeka dok onaj kome je informacija originalno namenjena ne postane dostupan da je primi.

Moguća je i obratna situacija, da visoki rukovodilac u okviru neke organizacije kontaktira CERT tim i zahteva sprovođenje raznih akcija po pitanju pojave nekog incidenta. Međutim, ukoliko ta osoba nije registrovana kod CERT-a kao tačka kontakta za pitanja informacione bezbednosti za datu organizaciju, takva osoba može se uputiti da se obrati svom kolegi u okviru organizacije koji to jeste, kako bi se zahtevi uputili na odgovarajući način.

Ukoliko se ne uspostave i ne poštuju ovakve procedure vrlo se lako može desiti da CERT tim, ili zajednica njegovih konstituenata, postanu žrtve napada takozvanog društvenog inženjeringa.

7.7.2.1 Društveni inženjering

Društveni inženjering je fraza koja se uobičajeno koristi da označi situaciju u kojoj se neko (tj. napadač) lažno predstavlja, kako bi prevario drugu osobu ili organizaciju, tj. naveo je na neku aktivnost koja inače ne bi bila moguća, u slučaju poznavanja pravog identiteta. Klasičan primer društvenog inženjeringa bi bio kada bi se neko lažno predstavio kao direktor kompanije i naredio službi obezbeđenja da mu dozvoli pristup prostorijama kompanije. Može zvučati čudno, ali je istinito, da uporni zahtevi ovog tipa (u formi „psihološkog“ napada na osoblje organizacije) u određenom broju slučajeva mogu uroditi plodom. Najčešće se prepoznaju dva osnovna tipa ovog napada:

- Lažni pozivi od strane medija - Kada predstavnici medija pretpostavljaju, ili imaju informaciju da je u toku neki veliki bezbednosni incident, oni mogu pokušati da dođu do informacija od CERT tima na način da ne otkrivaju svoj pravi identitet, nego se predstavljaju kao jedna od žrtava. Tada članovi tima, u želji da pomognu žrtvi napada, mogu da otkriju neke informacije koje u regularnoj situaciji ne bi javno objavljivali.
- Lažni pozivi od strane napadača - Društveni inženjering je dobro poznata i primenjena metoda među napadačima. Ukoliko napadač pretpostavi da je CERT tim otkrio njegove aktivnosti, može se desiti da uputi poziv CERT-u, lažno se predstavljajući i sa ciljem da utvrdi da li je njegova aktivnost detektovana.

Postoje i drugi pristupi ovoj vrsti napada, npr. kada se ljudi navode da aktiviraju maliciozni softver otvaranjem fajlova koje dobijaju preko elektronske pošte, ili se navode da pristupe zaraženim Internet stranicama.

7.7.2.2 Tehničke mogućnosti i ograničenja

Kada se govori o načinima autentifikacije u telefonskoj komunikaciji, moderni telekomunikacioni sistemi omogućavaju funkciju identifikacije poziva, kada je moguće imati uvid u broj telefona sa kojeg stiže poziv.

Takođe, i drugi vidovi elektronskih komunikacija imaju mehanizme kojima se omogućava provera i verifikacija nečijeg identiteta. Jedna od najpoznatijih metoda autentifikacije u današnjim mrežama su digitalni potpisi, kao što su oni koji se koriste u obezbeđivanju servisa elektronske pošte, tj. PGP i S/MIME.

Primera radi, da bi autentifikovala odlazne poruke svoje elektronske pošte, CERT organizacija može svaku prepisku zaštiti digitalnim potpisom na bazi PGP-a. Pri tome svako ko primi ovakvu poruku, i pri tome je to njegova odgovornost, može da proveri ovaj digitalni potpis koristeći javni ključ CERT organizacije koji mu je dostupan.

Važno je napomenuti da digitalni potpisi sa pridruženim metodama enkripcije mogu omogućiti visok nivo autentifikacije, ali i zaštitu od curenja informacija i drugih napada. Naravno, važno je razumeti i ograničenja ovih mehanizama, i koristiti svaki mehanizam u okvirima tih ograničenja, a sve nedostatke treba nadomestiti organizovanim pristupom pitanjima bezbednosti.

7.7.2.3 Baze podataka

Još jedna oblast u delovanju CERT timova u kojoj se koriste pomoćni alati su baze podataka, i to posebno one koje sadrže kontakt podatke konstituenata. S obzirom na važnost ovih baza podataka za proces interakcije sa konstituentima, veoma je važno da se one zaštite na odgovarajući način. Ukoliko bi napadači mogli da pristupe ovim bazama podataka mogli bi da manipulišu podacima koji se u njima nalaze i da ih menjaju prema svojim potrebama, a pri tome bi se ti podaci i dalje smatrali validnim.

Slični problemi postoje i kada se koriste javni izvori informacija, gde su mogućnosti za manipulaciju čak i veće, a samim tim je i nivo poverenja koje CERT organizacija može imati u takve podatke niži.

Primera radi, DNS sistem i *Whois* baze podataka su dva često korišćena „kataloga“ na Internetu, i vrlo često se koriste da se uspostavi kontakt sa žrtvom napada, kada nijedan pouzdaniji mehanizam pronalaženja kontakta nije na raspolaganju. Ali, s obzirom da je moguće napasti i manipulisati DNS sistemima, ovako dobijene javne informacije ne mogu se smatrati pouzdanima. Osim sumnje u autentičnost informacija, moguće je dovesti u pitanje i integritet tih podataka, jer je primera radi, *Whois* baza često neažurna i sadrži pogrešne podatke. U najgorem slučaju, korišćenje kontakata koji se dobiju na ovaj način može dovesti do curenja informacija ka pogrešnim osobama ili organizacijama.

Kada je u pitanju katalog CERT organizacija na tlu Evrope, ovu bazu održava organizacija *Trusted Introducer*. Njihov servis podrazumeva evidenciju i ažuriranje podataka CERT organizacija u *Whois* bazi podataka. Time se omogućava i pronalažanje nadležnih CERT organizacija na bazi IP adresa.

7.7.2.4 Anonimne informacije

Poseban aspekt komunikacije čini odgovor na pitanje kako CERT tim treba da se odnosi prema anonimnim prijavama, ili prijavama koje se ne mogu valjano autentifikovati. U svakom slučaju, anonimnom sagovorniku ne treba davati nikakve poverljive informacije. Međutim, ukoliko se desi da na taj način tim dođe do neke nove informacije koja može biti od koristi u razrešavanju incidenata, onda je treba pažljivo analizirati i doneti odluku o tome da li je validna. U slučaju da ne postoji mogućnost da se informacija verifikuje, onda je treba kao takvu i označiti, kao i to da potiče od anonimnog izvora. Međutim, iz bezbednosnih razloga, svako upozorenje, bilo da ono dolazi od anonimnog izvora, ili ga je uputio neko koga je moguće autentifikovati, treba proveriti.

7.7.3 Obezbeđivanje komunikacija

Autentifikacija izvora važnih informacija nije jedini aspekt u bezbednom upravljanju informacijama. Jednako je važno primeniti i bezbednosne mehanizme neophodne za zaštitu informacija tokom njihovog prenosa kroz računarske mreže. Ovo se ne odnosi samo na telekomunikacione mreže (telefonski servis, Internet, računarske mreže...), već i na tradicionalne načine za prenos informacija, kao što su kurirske službe, ili pošta, koje su, takođe, osetljive na napade i gubitak informacija.

Na isti način na koji kriptografski mehanizmi pomažu u autentifikaciji, mogu da pomognu i u očuvanju poverljivosti podataka. U svakoj situaciji kada se koriste kriptografski mehanizmi, glavni zadatak je upravljanje ključevima, kako sa stanovišta politika njihovog korišćenja, tako i sa stanovišta operativnih procedura.

Kada su u pitanju telekomunikacioni servisi, često je potrebno koristiti dodatnu opremu za enkripciju, jer poverljivost podataka baš i nije podrazumevana karakteristika u okvirima standardnih telekomunikacionih servisa.

7.7.4 Posebna razmatranja

Kada se ulazi u saradnju i razmenu informacija sa korisnicima, jedna od prvih stvari koja treba da bude definisana u politikama i procedurama CERT organizacije je nivo servisa koji je sposobna ili voljna da isporuči različitim stranama. Ovo može uključivati detalje kao što su vreme odziva na prijavu incidenta, ili specifične forme za razmenu informacija. Na ovaj način se raspoloživi resursi raspoređuju na odgovarajuće zadatke, i po potrebi se vrši prioritetizacija.

Kada je u pitanju saradnja sa spoljnim entitetima, CERT timovi se mogu naći u različitim situacijama, a neki od osnovnih tipova interakcija i tipova spoljnjih organizacija sa kojima CERT timovi sarađuju dati su u narednom tekstu.

7.7.4.1 Konstituenti

Primarni cilj CERT timova jeste da pomažu svojim konstituentima. Kada je u pitanju proces razmene informacija postoji i dodatna potreba da se uspostave različite vrste kontakata sa konstituentom, čak i kada se radi o samo jednoj njegovoj lokaciji. Naravno, ukoliko jedna osoba na lokaciji konstituenta pokriva više različitih uloga koje su relevantne sa stanovišta bezbednosnih incidenata, onda CERT tim ima samo taj jedan kontakt.

Takođe, s obzirom da je u procesu razrešenja incidenata često potrebno i donošenje nekih odluka (na primer da se o nekom događaju obaveste istražni ili pravosudni organi), potrebno je ustanoviti i procedure za eskalaciju, sa kontaktima za svaku pojedinačnu fazu eskalacije. Primera radi, tehnički detalji o incidentu na nekoj lokaciji prosleđuju se administratorima IT sistema ili mreže tog konstituenta, ali se neke informacije moraju proslediti i rukovodiocima te organizacije. Takođe, ukoliko je konstituent o tekućem incidentu već obavestio i istražne i pravosudne organe, onda takvu informaciju treba podeliti i sa drugim entitetima, jer to može uticati na način donošenja odluka u vezi sa incidentom.

Tokom procesa definisanja politika i procedura CERT tim mora da se pobrine o tome da spreči da jedan događaj na lokaciji jednog konstituenta iscrpi sve njegove resurse, osim ukoliko ne postoji procena tima da su aktivnosti povodom takvog incidenta od izuzetne važnosti i da im mora dati prioritet u odnosu na sve druge poslove. Tokom perioda kada CERT tim funkcioniše sa smanjenim resursima (kada je osoblje tima na godišnjim odmorima, obukama, konferencijama...) mora postojati šema prioritetizacije poslova i distribucije aktivnosti na raspoložive članove tima.

Politike CERT tima koje su dokumentovane i javno dostupne omogućavaju konstituentima da razumeju ograničenja sa kojima se CERT organizacije suočavaju, ali čak i tada treba preduzimati korake da se konstituenti obaveštavaju o specifičnim situacijama kada CERT tim funkcioniše sa umanjenim kapacitetima. Time se na odgovarajući način uspostavljaju očekivanja konstituenata, koji bi u takvim situacijama trebalo da imaju više razumevanja za ograničenja svog CERT tima.

U zavisnosti od broja konstituenata, i broja različitih servisa koje CERT tim pruža, dobra opcija je i da postoji prethodna registracija konstituenata. Naravno, ovo je realno i moguće ukoliko broj konstituenata nije previše veliki, i ako je ta brojka relativno stabilna. U takvim slučajevima se od konstituenata očekuje da tokom registracije ostave podatke o svojim kontaktima, ali i da im se predoče restrikcije u pogledu razmene informacija, ili bezbednosne mere (bezbednost sredstava komunikacije) tokom razmene informacija.

7.7.4.2 Druge CERT organizacije

Pored direktnog kontakta sa konstituentima, najvažniji partneri za saradnju sa CERT timovima su njihove kolege iz drugih CERT timova. Direktna pomoć i razmena informacija između CERT timova su izuzetno važni u procesu razrešenja incidenata, s obzirom da je u današnje vreme izuzetno retko da su incidenti izolovani na mrežu ili sistem samo jednog konstituenta, tj. CERT organizacije koja ga opslužuje.

Svi CERT timovi imaju koristi od saradnje i razmene informacija jer im to pomaže u ispunjavanju njihovih obaveza i poboljšanju kvaliteta servisa koji pružaju. Međutim, razmena informacija sama po sebi nije tako jednostavan zadatak. Pre svega, obim saradnje i razmene poverljivih informacija koji je neki CERT tim spreman da sprovede zavisi od postojećeg nivoa poverenja koje CERT organizacije između sebe imaju. Ponekad u tom smislu može pomoći ako postoje pisani ugovori između CERT organizacija o saradnji i razmeni poverljivih informacija.

Izgradnja poverenja između CERT organizacija koje žele da uspostave efikasnu saradnju je težak i dugotrajan proces. Jedan od bitnih koraka u tom smeru je međusobno upoznavanje. Timovi treba da razmene posete i da pokušaju da što bolje razumeju ciljeve, procedure i politike druge strane. To pomaže timovima da naprave realnu procenu o obimu i dubini saradnje koja može da se postigne i koja je svrsishodna za obe strane. Najčešće se saradnja započinje na manje kompleksnim poslovima sa minimalnim rizicima.

Mogući tipovi podrške između CERT timova opisani su u tabeli 7.3, dok su različiti aspekti prilikom razmene i korišćenja informacija opisani su u tabeli 7.4.

Postoje i drugi aspekti saradnje među različitim CERT timovima, koji su u bližoj vezi sa njihovim operativnim procedurama.

7.7.4.2.1 Obavezne informacije

Postoje neke informacije u vezi sa incidentima koje su kritične i neophodne CERT timu da bi mogao da efikasno da se bavi njihovim razrešavanjem. Ukoliko inicijalna prijava incidenta ne sadrži ove informacije onda će postojati kašnjenje u razrešenju incidenta, sve dok CERT tim ne dobije sve neophodne informacije. Ovo kašnjenje u nekim situacijama može biti značajan faktor, ukoliko se radi o prijavama problema iz različitih vremenskih zona, ili je incident takve prirode da ne trpi kašnjenje u razrešavanju. Da bi CERT timovi bili sigurni da će jedni drugima prosleđivati kompletne podatke, može se unapred dogovoriti forma ili dokument za razmenu informacija.

Tabela 7.3: Mogući tipovi podrške među CERT timovima

TIP PODRŠKE	**OPIS**
Edukacija/Treninzi	Ovo se može odnositi na širok spektar pomoći, od „formiranja novog CERT tima“, do tehničkih tutorijala na temu boljeg razumevanja bezbednosnih incidenata.
Pokrivanje podrške van radnog vremena	Ukoliko jedan CERT tim, shodno svojim resursima, pruža podršku samo tokom radnog vremena, ugovorom o saradnji sa drugim CERT timom, koji ima radno vreme 24/7, može se definisati podrška drugog tima u prijemu prijava incidenata van radnog vremena.
Tehnička ekspertiza	Odnosi se na dobijanje odgovora na tehnička pitanja i razmenu znanja među timovima.
Saradnja u rešavanju incidenata	Ukoliko postoji problem koji je suviše zahtevan za resurse samo jednog tima, može se više timova udružiti u njegovom rešavanju.
Dobijanje drugog mišljenja	Tokom bavljenja nekom vrstom problema, može se desiti da članovi tima izgube fokus za objektivno sagledavanje problema. Da bi se izbegle negativne posledice u ovakvim slučajevima, može se zahtevati od drugog tima da da svoje mišljenje o problemu, ili ponuđenom rešenju, pre nego što se ono javno distribuira.
Tačka kontakta za druge timove ili eksperte	Ukoliko je nekom timu potreban pouzdan kontakt sa nekim od konstituenata, tim se o tome može raspitati kod drugih timova ili eksperata.

Tabela 7.4: Aspekti razmene i korišćenja informacija

ASPEKT	**OPIS**
Poverljivost/Tajnost	Poverljivost informacija mora biti očuvana bez obzira na činjenicu da ih je neophodno deliti između više različitih timova. Ovo se odnosi na prenos podataka, njihov čuvanje i upotrebu. Eventualna nesmotrenost bilo kog člana bilo kog tima može da dovede u pitanje očuvanje tajnosti informacija.
Pravilno korišćenje informacija	Dok god neka informacija pripada nekom timu, da bi ostali timovi dobili pristup toj informaciji oni se moraju povinovati svim restrikcijama i pravilima korišćenja koje je izvorni tim uspostavio u pogledu te informacije. Često se u tom smislu između različitih CERT organizacija potpisuju i ugovori o očuvanju poverljivosti podataka.
Objavljivanje informacija	S obzirom da se može desiti da se u nekom trenutku informacije distribuiraju u javnost, sve restrikcije u pogledu objavljivanja informacija treba napomenuti unapred. Ponekad je to ograničenje samo vremenskog tipa.
Izjava zahvalnosti	Ukoliko neki tim koristi informacije koje je prikupio, analizirao i objavio neki drugi tim, onda tom timu treba iskazati odgovarajuću zahvalnost.

7.7.4.2.2 Preuzimanje inicijative

Tokom saradnje na razrešavanju incidenta uobičajeno je da neki od timova preuzme inicijativu, jer je potrebno obezbediti koordinaciju između timova, da se resursi ne bi uzaludno trošili (da različiti timovi ne rade isti posao, ili dostavljaju iste informacije, i sl.). Najčešće ulogu lidera preuzima tim koji je prvi dobio prijavu incidenta, ili u datom trenutku može da mu posveti najviše svojih resursa. Naravno, i ovi aspekti se mogu unapred urediti potpisivanjem odgovarajućih ugovora o saradnji između CERT organizacija.

7.7.4.3 Ostale organizacije

Kada se uspostavlja CERT tim i kada se alociraju resursi i odgovornosti, važno je razumeti da će tim dobijati informacije i zahteve i van kruga svojih uobičajenih konstituenata, na koje će morati na neki način da odgovori. U najjednostavnijem slučaju to može biti i samo upućivanje podnosioca zahteva na odgovarajuću adresu kojoj može da se obrati. Da bi mogla da odgovara na ovakve zahteve CERT organizacija treba unapred da pripremi neophodne informacije, i da uspostavi odgovarajuće procedure.

U svakoj situaciji kada se CERT timu obrati neko ko je konstituent drugog CERT tima, treba ga uputiti na odgovarajući CERT tim, ili taj CERT tim treba obavestiti da njegov konstituent ima problem. Ukoliko konstituent tom prilikom insistira na potpunoj poverljivosti onda ga svakako treba u startu usmeriti na odgovarajući CERT tim, i objasniti prednosti takvog postupka. Krajnji cilj je da konstituent od trenutka prijave incidenta dobije odgovarajući tretman, tj. da se proces razrešenja incidenta što više skrati.

7.7.4.4 Krovne organizacije

CERT timovi se često formiraju u okviru drugih većih organizacija, koje u tom slučaju imaju ulogu krovne organizacije CERT tima, u smislu rukovođenja CERT timom, ili finansiranja njegovih aktivnosti. Krovna organizacija CERT tima, kao i bilo koji drugi konstituent, može biti korisnik servisa CERT tima, tj. da koristi servise upravljanja incidentima, konsultantske usluge, ili usluge edukacije. Odnos CERT tima prema krovnoj organizaciji je od izuzetne važnosti, jer će u većini slučajeva prijave incidenata koje dolaze od krovne organizacije imati prioritet u odnosu na prijave drugih konstituenata.

7.7.4.5 Istražni i pravosudni organi

U svakoj situaciji kada se prijavljeni incident odnosi na kriminalne radnje, neophodna je saradnja i sa državnim istražnim i pravosudnim organima, jer oni u takvim situacijama očekuju da dobiju informacije o prirodi samog incidenta, tehničkim aspektima incidenta, lokacijama na kojima je incident zabeležen i kontaktima na tim lokacijama, kao i informacije o eventualno preduzetim aktivnostima na razrešenju incidenta i njegovim posledicama.

Izazov sa kojim se u takvoj situaciji suočava CERT tim je da balansira između potrebe da održi poverljivost informacija, što je njihova obaveza prema konstituentima, a da istovremeno ostvari efikasnu saradnju na razmeni informacija sa istražnim i pravosudnim organima. U tom smislu CERT tim mora da definiše politike saradnje sa istražnim i pravosudnim organima kojima se opisuje tip i obim informacija koje može da im dostavi. Naravno, mogu postojati i situacije kada je CERT organizacija pod zakonskom obavezom da podeli informacije sa istražnim i pravosudnim organima. U takvim uslovima, politike i procedure CERT organizacije moraju jasno da definišu okolnosti pod kojima se vrši razmena informacija.

Da bi se obezbedila dobra saradnja sa istražnim i pravosudnim organima mora se uspostaviti obostrano poštovanje i razumevanje za okolnosti u kojima ove organizacije funkcionišu. U tom smislu je jako korisno da CERT tim u što ranijoj fazi uspostavljanja svog rada definiše odgovarajuće odnose sa istražnim i pravosudnim organima.

Politikama CERT tima mora se definisati ko je odgovoran za komunikaciju sa istražnim i pravosudnim organima. Ovo se odnosi i na slučaj kontakta sa inostranim istražnim i pravosudnim organima. Zapravo, komunikaciju sa istražnim organima drugih zemalja treba preusmeriti na istražne i pravosudne organe države u kojoj CERT organizacija funkcioniše, i to preko unapred određenih kontakata.

Jedna od dobrih strana saradnje sa istražnim i pravosudnim organima je razmena informacija kojima se podiže svest unutar tih organizacija o tome koji su tipovi aktivnosti kojima se bavi CERT organizacija, tj. koji su tipovi prijava incidenata koje ona dobija. S obzirom da CERT timovi imaju saznanja iz prve ruke, ne samo o kriminalnim aktivnostima, već i o bezbednosnim incidentima koji se ne moraju smatrati kriminalom, oni mogu značajno pomoći istražnim i pravosudnim organima u stvaranju šire slike o stanju informacione bezbednosti u svojoj državi. Istražni i pravosudni organi sa svoje strane, u meri u kojoj je to moguće, tj. u okvirima zakona, mogu CERT timovima davati povratne informacije koje im mogu koristiti u aktivnostima na razrešavanju prijavljenih incidenata.

7.7.4.6 Mediji

S obzirom da mediji imaju značajnu ulogu u kreiranju javnog mnjenja, svaki CERT tim treba da ima razrađene politike i procedure saradnje sa medijima. Ciljevi ove saradnje su da se, u meri u kojoj je to moguće, javnost izveštava o aktivnostima CERT organizacije i podiže svest o važnosti teme informacione bezbednosti.

Mediji imaju svoje ciljeve i razloge zbog kojih traže informacije na temu bezbednosnih incidenata. Oni su često u suprotnosti sa ciljevima i procedurama CERT organizacija, koje zbog toga najčešće nisu raspoložene da daju sve informacije koje su medijima interesantne. Stoga je potrebno da CERT tim imenuje osobu zaduženu za kontakt sa medijima, i ta osoba mora biti na odgovarajući način edukovana, tj. mora da bude svesna koje su najčešće situacije i izazovi pred kojima će se naći tokom kontakta sa predstavnicima medija, i na koji način treba da se ophodi u takvim situacijama.

7.8 PROCES UPRAVLJANJA INFORMACIJAMA

Upravljanje incidentima je uvek u vezi sa upravljanjem informacijama. Informacije su uvek ključ, bez obzira da li se odnose na lokaciju, proizvod, novu ranjivost, napad koji je u toku, ili lozinke.

Informacije je prvo potrebno prikupiti i evidentirati u sistemu za vođenje evidencije o bezbednosnim incidentima. Svaka informacija mora da se sačuva i zaštiti za sve vreme tokom kojeg je relevantna za CERT organizaciju. Da bi se olakšalo upravljanje informacijama potrebno je dodeliti im identifikator, u zavisnosti od tipa informacije i njene poverljivosti. Pre nego što se pređe na obradu informacija potrebno je da se odradi i njihova prioritetizacija, kako bi se obezbedilo da se prvo obrađuju najbitnije informacije. Nakon što se informacije pregledaju i analiziraju, pojedinačne informacije, ili skup pojedinih delova različitih informacija, mogu se objaviti kako bi se dale smernice ili podrška zainteresovanim stranama, najčešće konstituentima CERT tima koji su prijavili bezbednosne incidente.

7.8.1 Prikupljanje informacija

Veliki deo informacija kojima upravlja CERT tim dolaze do njega direktno od konstituenata, ali često postoji i potreba da se informacije prikupljaju na druge načine, npr. proaktivnom pretragom na Internetu, ili iz drugih izvora (tehnološki izveštaji, analize, novosti, izveštaji eksperata, i slično).

Pre prikupljanja informacija preporučuje se da se ustanove politike i odrgovarajuće procedure kojima se određuje:

- koja vrsta izvora informacija je prihvatljiva,
- na koji način se sprovodi kontrola kvaliteta informacija, i
- kako da se prepoznaju greške, propusti ili nepreciznosti u podacima.

Ukoliko se informacije akivno prikupljaju one mogu da dolaze iz sledeća dva tipa izvora:

- Otvoreni izvori informacija - U ove informacije spada bilo koja vrsta javno dostupnih informacija. To mogu biti tradicionalni servisi kao što su novinski bilteni, mejling liste ili pretraživanje na Internetu.

- Razmena informacija sa drugim entitetima - S obzirom da druge organizacije ili pojedinci mogu raspolagati informacijama koje su interesantne za CERT timove, razmena informacija sa ovim entitetima može biti korisna za CERT tim. Glavni problem u tom smislu je prepoznati ko poseduje neke vrste informacija, i kako uspostaviti saradnju na bazi poverenja, kako bi razmena informacija bila moguća.

S obzirom da se informacije koje su dostupne CERT timu mogu menjati tokom vremena, politike i procedure prikupljanja informacija treba često preispitivati i verifikovati kako bi se obezbedilo da se uvek prikupe najsvežije i najbitnije informacije.

Kao što je ranije već pomenuto u poglavlju 7.3 („Proces trijaže“), dolazne informacije prvo moraju da prođu kroz proces trijaže. Kako bi se stimulisalo dostavljanje informacija u vezi sa bezbednosnim incidentima ili ranjivostima sistema, potrebno je dati konstituentima i adekvatnu podršku u tom smislu, na primer u vidu formulara za prijavu incidenata. Ove forme bi trebalo da sadrže i kontakt informacije, kao što su broj telefona i adresa elektronske pošte CERT tima, putem kojih je moguće dostaviti druge tipove informacija ili prijave incidenata.

Standardizacija politika i procedura za prikupljanje informacija pomaže CERT timovima da informacije prikupljaju u ustaljenom formatu. Kada se standardizuje format, onda su i druge akcije sa informacijama, kao štu su čuvanje, verifikacija, kategorizacija i prioritetizacija mnogo lakše za sprovođenje.

7.8.2 Verifikacija informacija

Pre nego što neka informacija počne da se koristi potrebno je da se na neki način verifikuje. Aspekti procesa verifikacije su sledeći:

- Izvor informacije - Faktori koji su u vezi sa izvorom informacija su znanje, iskustvo, uloga i funkcija lica, ili organizacije, koja dostavlja informaciju. Izvor informacije suštinski određuje način na koji će se ona obraditi i koristiti. Ukoliko prijava nekog događaja dolazi od izvora u koji postoji poverenje, utoliko će i dalje postupanje biti lakše.
- Sadržaj informacije - Kada se ima uvid u sadržaj neke informacije, postavlja se pitanje da li je ona tačna, ili je očigledno pogrešna sa ciljem da zavara dalju analizu događaja. Prisustvo ili odsustvo tehničke korektnosti u sadržaju informacije utiče na njenu dalju obradu i korišćenje.
- Distribucija informacije - Ovaj aspekt se odnosi na kanal koji je korišćen za prenos informacije, i moguće uticaje na autentičnost tako dobijenih informacija. Naravno, ne uzima se na isti način u razmatranje informacija koja je stigla sa digitalnim potpisom koji se može verifikovati, i informacija koja stiže u vidu anonimne prijave putem telefonskog poziva ili tradicionalnom poštom.

7.8.3 Kategorizacija informacija

Informacije koje pristižu u CERT organizaciju moraju na neki način biti kategorizovane. Sve informacije koje pristižu u CERT prolaže kroz proces trijaže, što olakšava njihovu inicijalnu kategorizaciju. Kategorizacija informacija je obično u uskoj vezi sa prioritetizacijom, ali je ipak treba posmatrati kao odvojenu i nezavisnu aktivnost.

Kategorija u koju se neka informacija svrsta kasnije utiče na način na koji se sa njom postupa (kako se čuva, razmenjuje, uništava...). U svakom slučaju, bezbednost svih informacija u okviru CERT organizacije mora biti na najvišem nivou.

Čak i ukoliko eksplicitna kategorizacija ne postoji, osoba koja pregleda informacije koje pristižu će na bazi nekakve svoje percepcije davati različit značaj informacijama u koje ima uvid. S obzirom da je takva percepcija individualna, moraju postojati jasne i precizne procedure kako bi se proces kategorizacije standardizovao.

Mnoge CERT organizacije imaju poseban proces ili proceduru za upravljanje kontakt informacijama, koji se razlikuje od procedura za upravljanje informacijama u vezi sa bezbednosnim incidentima. Kontakti (ljudi i organizacija) se obično strogo čuvaju, čak i od drugih partnerskih organizacija. Neki timovi kontakt informacije čak tretiraju kao posebnu kategoriju.

Kategorizacija se najčešće bazira na samom sadržaju informacije. Nekada se kategorija utvrđuje tokom same interakcije sa dostavljačem informacije, a nekada se „nasleđuje“ od organizacije koja je informaciju dostavila (npr. partnerska CERT organizacija dostavlja informaciju koja je već klasifikovana prema njihovim pricedurama).

Ponekad je potrebno da se informacije (logički) podele na manje delove, npr. iz log fajla nekog incidenta potrebno je ukoniti imena sistema ili mrežne adrese, pre nego što se ostatak informacije podeli sa drugima.

7.8.4 Čuvanje informacija

Jedan od najvažnijih aspekata čuvanja informacija (bilo da su one u pisanom obliku, ili se čuvaju u informacionom sistemu) je njihova bezbednost. Ukoliko nema bezbednosti informacija, CERT tim ne može uspešno da štiti interese svojih konstituenata, u smislu poverljivosti podataka kojima raspolaže.

Pitanje bezbednosti je naročito važno ukoliko se sve informacije čuvaju na jednom mestu, u vidu centralne baze podataka. U tom slučaju, takva baza podataka ima veću vrednost nego suma pojedinačnih informacija koje se u njoj nalaze. Iz istog razloga iz kojeg sve prikupljene informacije daju prednosti CERT timu (da im pomognu da izgrade širu sliku informacione bezbednosti), one mogu da budu i njihova slabost. Na primer, ukoliko CERT tim usled lošeg rukovanja informacijama objavi neku manju količinu informacija (npr. nesmotreno se pošalje elektronska pošta na neželjene adrese), to ne mora biti veliki problem. Ali, ukoliko procuri velika količina prethodno prikupljenih informacija (koje nisu „prečišćene“, tj. sadrže konkretne podatke o konstituentima ili njihovim lokacijama), koje se tiču nekog konkretnog incidenta, to može pogubno da utiče na reputaciju CERT tima.

CERT organizacije su jako privlačne za razne vrste napadača. Očigledan je njihov interes da upadima u sisteme, i dobijanjem pristupa poverljivim informacijama, diskredituju CERT organizacije i izbace ih iz daljeg poslovanja. Postoje i drugi motivi za napade na sisteme CERT organizacija, a neki od njih su da napadač uvidom u informacije CERT-a može da stekne sliku o tipovima incidenata koji se prijavljuju CERT timu, slabostima sistema konstituenata koje je moguće iskoristiti za napade, kao i da utvrdi da li je neka od njegovih aktivnosti zabeležena i da li je pod istragom.

Jedan od dobrih pristupa čuvanju informacija je korišćenje više logički organizovanih baza podataka. Cilj je da informacije budu dostupne, da se lako koriste, lako menjaju, i da postoji fleksibilnost za podršku različitim tipovima servisa koje CERT tim pruža. Na koji god način da se čuvaju informacije, potrebno je obezbediti pristup sledećim podacima:

- kontaktima,

- preduzetim aktivnostima (ili onima koje će biti preduzete),
- incidentima (informacija o trenutnim aktivnostima i statusu incidenta, sa redovnim ažuriranjem tokom procesa razrešavanja incidenta),
- uočenim ranjivostima sistema i odgovarajućim zakrpama,
- artefaktima (skripte, alati, fajlovi ...), i
- log fajlovi i drugi podaci u vezi sa incidentima.

7.8.5 Prečišćavanje i uništavanje informacija

Prečišćavanje i uništavanje informacija je izuzetno važna karika u procesu upravljanja informacijama. Ovo je naročito važno za CERT organizacije koje često dolaze u kontakt sa poverljivim informacijama, koje se ponekad tiču velikih grupa ljudi ili organizacija. Kao što je već naznačeno u odeljku o kategorizaciji informacija, u zavisnosti od osetljivosti informacija, osetljive informacije određenih kategorija je potrebno prečistiti i uništiti na odgovarajući i konzistentan način.

Informacije se vrlo često prečišćavaju da bi se sprečio gubitak poverljivih delova informacija, a da pri tome ne postoji gubitak u korisnosti tako tretiranih informacija. Primera radi, log fajlovi koji sadrže tragove pristupa nekim sistemima, često u sebi nose informacije o korisničkim imenima i lozinkama naloga preko kojih je moguće pristupiti nekim sistemima. Pre nego što se ovakvi fajlovi pošalju drugim entitetima na uvid ili analizu, poželjno je odstraniti informaciju o lozinkama koje se koriste za pristup sistemima. Time sadržaj log fajlova ne gubi na značaju, a istovremeno se štite poverljive informacije konstituenta.

Takođe, u poverljive informacije mogu da se svrstaju i informacije o kontaktima ili lokacijama konstituenata, kao i informacije o incidentima koje se mogu direktno povezati sa konkretnim konstituentima ili njihovim lokacijama. CERT timovima je jako važno da imaju i čuvaju ovakve informacije, ali je to istovremeno i potencijalno opasno za njihove konstituente. Primera radi, može se desiti da istražni ili pravosudni organi zahtevaju od CERT tima da im dostavi informacije o nekom specifičnom incidentu, tj. konstituentu. U takvim slučajevima, pogodno bi bilo da CERT tim može da preda samo informacije u vezi sa navedenim incidentom, i nijednu drugu informaciju koja bi dovela u vezu tog konstituenta sa nekim drugim incidentima. Time se povećava poverenje konstituenata u svoj CERT tim. Naravno, ovo mora biti podržano tehničkim merama, tj. načinom na koji CERT tim organizuje i čuva informacije u vezi sa pojedinačnim incidentima ili konstituentima.

Da bi se sprečilo curenje informacija tokom vremena, CERT tim može da odluči da se, posle nekog unapred određenog vremena, čuvaju samo prečišćene informacije, ili presek informacija u vidu statističkih podataka, ili tehnoloških smernica. U ovom slučaju tim mora da investira i puno vremena u to da uništi sve informacije koje više nisu potrebne (a da pri tome na bazi tih informacija prvo napravi statističke izveštaje...). Ovo je naročito teško kada postoje rezervne kopije informacija koje, takođe, treba prečistiti, iako je cilj takvih kopija da se informacije čuvaju na duži rok.

7.8.6 Kriterijumi za prioritetizaciju

Iako se mnogi tipovi incidenata mogu smatrati „kritičnim“, ili „ozbiljnim“, čak i u okviru ovih individualnih kategorija, CERT timovi moraju da dodeljuju odgovarajuće

prioritete kako bi se znalo koji se incident prvi obrađuje. Ozbiljnost incidenta može da zavisi od brojnih faktora, a prioritet se može tokom vremena i promeniti u svetlu nekih novih informacija. Dakle, prioritetizacija tekućih incidenata nije lak zadatak, a može se čak i smatrati jako dinamičnom aktivnošću.

Postoje različite šeme za odabir najvažnijeg incidenta, ili za rangiranje nekoliko paralelnih incidenata:

- resursi CERT tima koje je potrebno angažovati,
- uticaj na konstituente,
- tip incidenta,
- obim i štetnost incidenta, i
- cilj ili izvor napada.

Naravno, potrebno je ovakvim šemama pridružiti i odgovarajući nivo fleksibilnosti. Na primer, može se nekom incidentu dodeliti neki podrazumevani inicijalni prioritet do trenutka dok mu se na bazi nekih novih informacija ne dodeli odgovarajući prioritet. Sve politike koje se tiču procesa prioritetizacije moraju se često proveravati u praksi i revidirati na način da se prilagođavaju realnim dešavanjima, i trendovima i potrebama konstituenata na polju informacione bezbednosti.

Primera radi, nekada se smatralo da je kompromitovanje *root* naloga na sistemima konstituenata incident najvišeg prioriteta. Međutim, vremenom, sa porastom Internet mreže i servisa, kao i usled promene misija CERT timova, neki drugi tipovi incidenata dobili su viši prioritet. U opštem slučaju to su bezbednosni incidenti kod kojih može postojati opasnost po život ljudi, napadi na kritičnu informacionu infrastrukturu ili Internet infrastrukturu, obimni i automatizovani napadi na mreže ili sisteme velikih grupa konstituenata, razvijanje novih tipova napada ili eksploatacija novih ranjivosti sistema širokih razmera, i slično.

Od prioriteta koji je dodeljen nekom incidentu zavisi i način na koji će biti tretiran. Primera radi, potrebno je da na inicijalnoj prioritetizaciji incidenata rade iskusni članovi tima koji će onda biti u stanju da razrešavanje incidenata delegiraju odgovarajućim članovima tima. U tom slučaju, incident koji je prepoznat kao „lakši“ biće dodeljen nekom od novijih članova tima, sa manje iskustva, a oni koji su ozbiljniji i zahtevaju veću ekspertizu biće preusmereni na iskusne članove tima.

Kao što je već rečeno, prioritet incidenta se tokom vremena može menjati u svetlu novih dobijenih informacija. O bilo kakvoj promeni prioriteta incidenta potrebno je obavestiti sve zainteresovane strane, jer to može imati uticaj na njihove dalje postupke po pitanju incidenta, bilo da se prioritet snižava ili povećava.

S obzirom da se svi timovi u nekom trenutku suočavaju sa limitiranim resursima, mogu postojati situacije u kojima CERT tim ne može da odgovori na sve prijave incidenata. U nekim retkim slučajevima moguće je preusmeriti ih na neki drugi CERT tim. U svakom slučaju, kada jedan CERT tim u datom trenutku nema resursa da se bavi prijavljenim incidentom on o tome mora da obavesti svog konstituenta, koji je taj incident prijavio. Nedostatak ovakve komunikacije, tj. ostavljanje konstituenta bez bilo kakvog odgovora, može dovesti do štete po reputaciju CERT tima i smanjenog poverenja konstituenata.

U kreiranju opštih kriterijuma prioritetizacije, CERT timovi obično koriste kombinacije različitih šema prioritetizacije. Obično se osnovna prioritetizacija vrši po jednoj šemi, a zatim se nad tako dobijenim kategorijama vrši „fina“ prioritetizacija po nekoj drugoj šemi. Naravno, svaka šema prioritetizacije ima svojih dobrih i loših strana, i o tome treba stalno razmišljati i argumentovati svoje izbore jer će uvek biti konstituenata koji smatraju da njihovi problemi moraju imati veći prioritet od drugih. U nastavku su opisane neke od mogućih šema prioritetizacije.

7.8.6.1 Prioritetizacija po meti ili izvoru napada

Kada se vrši prioritetizacija bazirana na meti napada, prioritet se dodeljuje na bazi uloge, misije, ili važnosti napadnute lokacije ili sistema. Za CERT organizaciju, koja ima svoju zajednicu konstituenata, najvažnije je ukoliko su mete napada organizacije iz te zajednice. Ukoliko se napad dešava simultano na više organizacija u okviru zajednice konstituenata, CERT organizacija mora biti u stanju da i tada izvrši prioritetizaciju. Prioritetizacija se tada može izvršiti na osnovu vrste podataka koje meta ima u svom posedu, uloge koju ima u sistemima ključne informacione infrastrukture, ili na osnovu nekog drugog faktora.

Kada su u pitanju izvori napada, pravi izvor napada nije uvek moguće utvrditi, jer napadač može da krije originalni izvor svojih aktivnosti. Obično napadači imaju na raspolaganju čitavu mrežu povezanih sistema preko kojih vrše napade. Rezultat toga je da CERT tim kao informaciju o izvoru napada obično ima lokaciju ili sistem koji je iskorišćen da se sa njega izvrši napad, što može biti neka druga lokacija koja je i sama žrtva napada. Prioritetizacija se i u ovom slučaju vrši dodeljivanjem prioriteta na bazi moguće vrste izvora napada, tj. percepcije pretnji koje oni mogu izazvati.

7.8.6.2 Prioritetizacija po tipu i obimu štetnosti incidenta

Obim štete ili gubitaka koji su posledica nekog bezbednosnog incidenta je ponekad teško odrediti. Ne samo da je teško prikupiti podatke o eventualnoj šteti, već je teško i proceniti štetu sa nekom velikom tačnošću. Na procenu štete utiču lično iskustvo onoga ko učestvuje u proceni, tačnost dolaznih izveštaja, kao i tip informacija koje su uopšte dostupne CERT timu. CERT timovi koji imaju direktan autoritet nad svojim konstituentima lakše dolaze do tačnih podataka i mogu dati precizniju procenu štete. Otuda se ova šema prioritetizacije češće koristi među timovima koji imaju veći stepen autoriteta nad svojim konstituentima.

7.8.6.3 Prioritetizacija po tipu incidenta

Koristeći se ovim kriterijumom, poznati tipovi incidenata se rangiraju u zavisnosti od njihovog sveukupnog uticaja sa tehničkog aspekta. Rezultat ovakve vrste prioritetizacije može biti da ima previše incidenata koji su označeni sa najvišim prioritetom. Pri tome, ako se posmatraju samo tehnički aspekti incidenta, oni ne moraju biti od ključnog interesa osim ako se ne otkrije da se radi o nekom novom, ili neuobičajenom tipu napada ili ranjivosti sistema. Rezultat toga je da se ova šema prioritetizacije najčešće koristi u kombinaciji sa nekim drugim šemama prioritetizacije.

7.8.6.4 Prioritetizacija davanja povratnih informacija

Zahtevi za dobijanjem povratnih informacija se u opštem smislu mogu tretirati potpuno nezavisno od prijava bezbednosnih incidenata. Obično je princip da se zahtevi opslužuju po redosledu prijema, mada i u ovim slučajevima može doći do potrebe da se poslovi prioritetizuju, usled zauzetosti tima drugim aktivnostima, ili usled nekih drugih razloga. Jedan od metoda prioritetizacije u ovom slučaju može biti u zavisnosti od toga ko je lice ili organizacija koja traži povratnu informaciju. Što je pozicija te osobe ili organizacije viša, odnosno bitnija sa stanovišta funkcionisanja i misije CERT organizacije, to je prioritet koji se daje njihovim zahtevima viši.

7.8.7 Kriterijumi za eskalaciju

Proces eskalacije se obično meša sa procesom prioritetizacije. Iako se podrazumevaju slične aktivnosti, eskalacije se odnose na podizanje važnosti neke aktivnosti bez obzira na prioritet koji ona ima. Eskalacija uvek podrazumeva da postoji bar jedan nivo rukovodstva koji se mora umešati u proces radi potrebe donošenja odluka. Ukoliko dolazi do eskalacije po pitanju jedne ili više aktivnosti CERT tima, to može biti znak da je tim pod većim pritiskom posla nego inače.

Kriterijumi za eskalaciju, tj. procesi, procedure i smernice koje su im pridružene, moraju biti unapred definisane, kako bi se mogle koristiti u odgovarajućim situacijama. I u ovom slučaju potrebno je stalno nadgledati te procedure i prilagođavati ih trenutnim potrebama konstituenata, kao i novim trendovima na polju informacione bezbednosti. Isti kriterijumi eskalacije mogu se primeniti na sve servise koje pruža CERT organizacija, uključujući i servis za upravljanje incidentima.

Primera radi, ukoliko se desi bezbednosni incident koji je u početku izolovan, a kasnije počinje nekontrolisano da se širi na sve veći broj konstituenata, može se desiti da se iscrpe resursi CERT organizacije, tj. da ona bude „zatrpana“ prijavama incidenata. Jedan od mogućih ishoda eskalacije je da rukovodstvo CERT organizacije, ili krovna organizcija koja finansira CERT tim, odluči da investira u dodatno osoblje kako bi se CERT tim izborio sa novonastalom situacijom.

7.8.7.1 Eskalacija individualnih incidenata

Kada su u pitanju individualni incidenti uvek se može desiti potreba za eskalacijom, bez obzira na prioritet incidenta. Obično je to rezultat situacije u kojoj onaj ko se bavi posmatranim incidentom nije u stanju da se izbori sa jednim ili više aspekata tog incidenta. U tom slučaju potrebna je dodatna podrška na razrešenju incidenta, ili nadzor rukovodioca kojim bi se obezbedila preraspodela posla među članovima tima, kako bi se uspešno odgovorilo na eskalirani incident. Kako se incident razvija, i nove informacije stižu do CERT tima, može postati jasno da osoba kojoj je dodeljen zadatak da se bavi nekim incidentom nema potreban nivo tehničkog znanja da se sa time izbori, i onda je potrebna eskalacija. Razlozi eskalacije incidenata su po svojoj prirodi slični onima koji dovode do njihove prioritetizacije.

Uobičajeni kriterijumi za eskalaciju individualnih incidenata mogu biti:

- broj lokacija i sistema koji su napadnuti,
- tip podataka koji je u riziku od gubitaka ili neovlašćenog pristupa,
- ozbiljnost napada,
- status napada,
- izvor ili meta napada,
- uticaj na integritet infrastrukture, ili cena oporavka,
- napad na „prividno“ bezbedne sisteme,
- uvid šire javnosti u incident,
- nova metoda napada koja se koristi,
- prekidi u komunikacijama, i
- tehničke mogućnosti, znanje i stručnost osoblja CERT tima.

Nekada se kao kriterijum za eskalaciju postavlja i prosta potreba da se rukovodstvo organizacije obavesti o neobičnim, ili potencijalno važnim dešavanjima.

Takođe, u situacijama kada je u pitanju reputacija CERT tima, o tome treba obavestiti rukovodstvo CERT-a. Primera radi, može se desiti problem u komunikaciji izazvan (osnovanim ili neosnovanim) nezadovoljstvom konstituenata. Konstituenti mogu biti nezadovoljni načinom na koji se tretiraju incidenti, bilo tehnički ili proceduralno, ili mogu imati problema u komunikaciji sa nekim od članova CERT tima, i to je situacija koja zahteva eskalaciju kod rukovodilaca CERT tima.

Može se desiti i da aktivnosti CERT tima budu ograničene zbog nedovoljne količine informacija kojima raspolažu o nekom incidentu. U normalnim situacijama CERT tim nastavlja da se bavi incidentom u svetlu informacija koje su mu dostupne, ali može biti i situacija kada su neke zaista kritične informacije neophodne. Ukoliko tim ima osnova da veruje da takve informacije postoje, ali neki drugi entitet ne želi da ih prosledi CERT timu, to može biti razlog za eskalaciju, kako bi se našao neki način da se do kritičnih informacija dođe. Eskalacija u ovom slučaju može biti u vidu posete članova CERT tima organizaciji koja je žrtva ili izvor bezbednosnog incidenta, ali nije voljna da razmeni informacije, kako bi se ostvarila neposredna komunikacija i objasnila situacija, kao i eventualne posledice ili sankcije, ukoliko ta organizacija ne sarađuje na razrešenju incidenta sa CERT timom.

7.8.7.2 Eskalacija višestrukih incidenata

Sa stanovišta servisa za upravljanje incidentima, kriterijumi za eskalaciju incidenata moraju da uzimaju u obzir i dodatne faktore, kao što su nivo poslova i obaveza kojima je CERT tim u datom trenutku zauzet, potreba da ispuni svoju misiju, potreba da se utvrdi kako se neki incident uklapa u širu sliku informacione bezbednosti, ili potreba za dodatnim resursima ili članovima CERT tima.

Postoje situacije kada do CERT tima pristiže više prijava incidenata nego što je tim u stanju da obradi, ili bar ne u predviđenom vremenskom roku. Nekada se do ovakvih situacija dolazi postepenim porastom broja prijavljenih incidenata, a nekada je to iznenadna pojava, kao posledica masovnih i iznenadnih napada na sisteme konstituenata. U svakom slučaju, smisao eskalacije je da se tim osposobi da na adekvatan način izađe na kraj sa ovakvim situacijama.

Svaki tim na svoj način sprovodi akcije koje su rezultat eskalacije. Mogućnosti idu od toga da se uposle dodatni resursi (da se produži radno vreme članova tima, ili da se angažuju drugi timovi ili eksperti radi pomoći u kriznim situacijama), do toga da se smanji nivo nekih nekritičnih servisa koje tim pruža. Pomoć drugih eksperata ili timova može biti i u tome da se preuzme posao komunikacije sa konstituentima, ili objavljivanje dokumenata i informacija, kao i druge vrste administrativne podrške, kako bi se članovima tima omogućilo da se fokusiraju na razrešenje kritičnih incidenata.

Kada CERT tim eskalira neki incident tako što traži pomoć drugih timova i organizacija, onda se to mora činiti prema unapred ustanovljenim procedurama i smernicama za dobijanje takve vrste pomoći. O tome se mora unapred diskutovati sa osobljem i organizacijama koje bi trebalo da pruže pomoć, jer oni moraju biti osposobljeni i voljni da pomognu kada god je to potrebno. Podrazumeva se da sa takvim organizacijama postoje i unapred dogovoreni kontakti i metode na uspostavljanju sistema podrške. U tom slučaju članovi CERT tima mogu da se fokusiraju na tekuće incidente, umesto da se bave obukom tima ili pojedinaca koji treba da im pomognu. Potencijalni resursi koji mogu biti od pomoći CERT timu su:

- zaposleni u okviru CERT tima raspoređeni na druge poslove,
- drugi zaposleni u okviru krovne organizacije, koji nisu članovi CERT tima,

- drugi CERT timovi, eksperti, ili eksterni konsultanti, i
- konstituenti ili dobrovoljci.

CERT timovi se mogu naći u situaciji da zbog nedostatka resursa moraju da obore nivo nekih servisa kako bi eskalirani incidenti dobili adekvatan tretman. Primera radi, ukoliko je zadatak da se u najkraćem roku zaustavi neki napad, ili da se sistemi konstituenta u što kraćem roku vrate u funkcionalno stanje, to za posledicu može imati da se ne posveti dovoljna pažnja uzroku incidenta, metodi napada, identifikovanju napadača, i sličnim detaljima kojima bi se CERT tim u normalnoj situaciji detaljno bavio. Zbog toga se gubi mogućnost da se stekne uvid u širu sliku incidenta, a to je važno naročito u slučajevima eskalacija, kada je postojanje šire slike od velikog interesa, kako za CERT tim, tako i za njegove konstituente. Čak i u kritičnim situacijama, kada su resursi ograničeni, od značaja je da se ulože dodatni napori da se istraže svi aspekti nekog incidenta sa dovoljno detalja, koji bi omogućili širi uvid u aktivnosti napadača.

Naravno, kada je CERT tim suočen sa radom u kritičnom režimu usled povećanja obima posla, važno je da se vrati u režim normalnog funkcionisanja u što kraćem roku. Potrebno je ustanoviti jasne kriterijume o tome kada se može smatrati da je neka krizna situacija okončana. Time se omogućava da se umanji nivo pritiska na CERT tim, da se njegovi članovi pregrupišu, da se redefinišu prioriteti i da se svi vrate svom uobičajenom poslu i redovnim zadacima koji su možda bili suspendovani tokom trajanja krizne situacije.

7.8.8 Objavljivanje informacija

Da bi jedan CERT tim uopšte mogao da funkcioniše, podrazumeva se da mora da razmenjuje, tj. objavljuje informacije. Međutim, ukoliko se ovaj proces odvija na neodgovarajući način, ovakva aktivnost može da dovede do gašenja, tj. prestanka rada CERT tima. Da bi se sprečilo neodgovarajuće (pogrešno ili neovlašćeno) objavljivanje informacija, sve informacije se moraju objavljivati, ili razmenjivati, strogo u skladu sa odgovarajućim politikama tima koje su na snazi za ovu oblast.

Postoje različiti razlozi zbog kojih je neophodno objaviti ili razmeniti neke informacije, kao i različite grupe, ili organizacije kojima su namenjene. Proces razmene informacija je različit, i zavisi od grupe kojoj je namenjena, i načina na koji će je koristiti. U nastavku su dati primeri različitih grupa korisnika koji mogu primiti informaciju, i razlozi zbog kojih im se informacije dostavljaju:

- drugi CERT timovi se obaveštavaju o novoj ranjivosti sistema koja je uočena,
- drugi CERT timovi sa kojima se sarađuje na analizi i razrešavanju incidenata,
- konstituenti, tj. njihove lokacije koje su meta ili izvor napada,
- rukovodstva CERT timova radi slanja statističkih izveštaja,
- grupe za upravljanje bezbednosnim rizicima, radi pomoći u planiranju bezbednosne infrastrukture,
- krovne organizacije ili finansijeri, da bi se opravdali troškovi aktivnosti CERT timova,
- istražni ili pravosudni organi, na njihove zahteve povodom istraga koje se sprovode,
- vladine organizacije, radi izveštavanja.

Potreba da se objavljuju informacije može biti i potreba zahteva, ili prijava incidenata, od strane konstituenata. Takođe, to može biti rezultat događaja koje upućuju CERT tim na određene aktivnosti, kao što je objavljivanje upozorenja ili preporuka. Politike objavljivanja

informacija moraju da uzmu u obzir okolnosti koje se odnose na razlog, ali i način na koji će se objaviti neka informacija.

Primera radi, kada god je u toku bezbednosni incident, tj. napad širokih razmera, CERT tim će radije o tome obavestiti sve svoje konstituente, nego da obavesti samo one za koje je potvrđeno da su žrtva napada. Ponekad se izvori takvog napada, a često ni konkretne mete napada, ne mogu sa sigurnošću identifikovati. Međutim, ponekad postoji opravdanje da se objavi izvor napada. Primer za to je kada je saznanje o izvoru napada ključno za njegovo zaustavljanje, ali konstituent, čiji su sistemi na nekoj od njegovih lokacija izvor napada, nije voljan da sprovede korektivne akcije. Ukoliko u tom trenutku CERT tim nema dovoljno resursa da na drugi način umanji ili spreči štetu od napada, tim može odabrati da o napadu koji je u toku objavi što je moguće više informacija (uključujući i preventivne i reaktivne mere), i prepusti konstituentima da se u što većoj meri sami izbore sa nastalom situacijom. Cilj slanja informacija svim konstituentima u ovakvim situacijama je da se obaveste administratori sistema i mreža, ali i korisnici generalno, da obrate pažnju i prijave svaku sumnjivu aktivnost, koja bi inače mogla proći neprimećeno.

U procesu definisanja politika o informacijama treba imati minimalistički pristup. U najvećem broj interakcija i razmena podataka nije neophodno objaviti čitav skup informacija, jer je najčešće samo njihov deo relevantan za one kojima se informacije upućuju. Prema tome, politike treba da razlikuju skup „najnužnijih“ informacija koje se uobičajeno objavljuju, i potpuno objavljivanje svih poznatih informacija o nekom događaju, u izuzetnom slučaju kada za to postoji potreba i opravdanje.

Primera radi, ukoliko jedan CERT tim ustupi artefakte nekog incidenta drugom timu radi analize, nije neophodno dati i informaciju o konstituentu, ili lokaciji, sa koje su artefakti prikupljeni (naravno, ovo nije problem ukoliko ne postoji razlog za diskreciju, ili je izvor neki javni entitet na Internetu). Ukoliko su tom drugom timu potrebne dodatne informacije radi analize artefakta, on ih može tražiti od prvog tima, i u slučaju da su razlozi opravdani, prvi CERT tim će kontaktirati svog konstituenta, objasniti situaciju, i tražiti dozvolu da razmeni i neophodne dodatne informacije. Najčešće će konstituent dozvoliti razmenu dodatnih informacija, ali važno je obavestiti ga i tražiti dozvolu. Dobra praksa je da svaki CERT tim unapred zatraži dozvolu od svojih konstituenata za razmenu različitih vrsta informacija sa drugim CERT timovima (uključujući i identitet, tj. kontakt informacije konstituenta koji je žrtva bezbednosnog incidenta), kako bi se ovaj proces ubrzao u situacijama kada je to ključno za efikasno razrešavanje incidenata.

Pitanja privatnosti, tj. poverljivosti informacija o kontaktima konstituenata, ili informacija o tome da je neko postao žrtva bezbednosnog incidenta, su očigledno jako osetljiva. U tom smislu CERT organizacija mora da vodi računa i o odredbama lokalnog zakonodavstva kada definiše svoje politike na ovu temu.

Izrada statističkih izveštaja o trendovima je jedan od najinteresantnijih servisa koje CERT timovi mogu da ponude, mimo uobičajenog servisa za upravljanje incidentima. Zahvaljujući svojoj specifičnoj ulozi, CERT timovi su u stanju da:

- izgrade širu sliku o stanju informacione bezbednosti svojih konstituenata,
- obezbede neophodne informacije za krovne organizacije i finansijere,
- omoguće bolje servise za svoje konstituente, i
- utiču na podizanje svesti o informacionoj bezbednosti.

Deo misije svakog CERT tima je da prikupljene informacije iskoristi na najbolji način u službi interesa svojih konstituenata. Važno je da CERT tim razmotri koje će informacije da prikuplja, i da strateški planira na koji način će te informacije da koristi, kome će da ih distribuira, i kakve će politike pri tome da primenjuje. Primera radi, često se zahteva od CERT

timova da redovno objavljuju statističke izveštaje, a na njima je da odluče šta ti izveštaji mogu da obuhvate, i u kojoj formi će biti prezentovani.

Još jedna stvar o kojoj treba voditi računa u vezi sa razmenom informacija je standardizacija i unifikacija, s obzirom da se čitava CERT organizacija ogleda kroz ovaj proces koji je vidljiv njihovim konstituentima i široj javnosti. Način na koji se informacije distribuiraju mora biti konzistentan tokom vremena, kako bi izveštaji mogli da se upoređuju. Dodatno, standardizacijom se utvrđuje i „korporativni identitet" CERT organizacije. Detalji o kojima u tom smislu treba voditi računa su sledeći:

- format teksta, bez obzira da li se tekst distribuira preko elektronske pošte, ili Internet prezentacije (zaglavlja, logo, fontovi ...),
- autentifikacija dokumenata preko digitalnih potpisa, i
- smernice za sadržaj i stil obraćanja.

8. TROŠKOVI REALIZACIJE I FUNKCIONISANJA NACIONALNOG CERT-A

8.1 MODEL FINANSIRANJA CERT ORGANIZACIJE - OPŠTE

Kada Nacionalna CERT organizacija odabere osnovne servise koji će biti implementirani, sledeći korak će biti razmatranje modela finansiranja, tj. koji će servisi, ili neki njihovi aspekti, istovremeno biti efikasni i isplativi.

U idealnom slučaju model finansiranja bi morao biti prilagođen potrebama konstituenata, ali u realnosti, protfolio servisa koji će biti implementirani mora se prilagoditi budžetu koji je na raspolaganju CERT organizaciji. Dakle, potrebno je od početka razmišljati o finansijskim pitanjima, tj. uzeti u razmatranje sve troškove, kao i potencijalne izvore prihoda.

8.1.1 Troškovni model

Dva glavna faktora koji utiču na troškove CERT organizacije su utvrđivanje radnog vremena CERT tima, kao i broj i kvalitet osoblja koje će biti angažovano na mestu članova CERT tima. U tom smislu, potrebno je doneti odluku o tome da li tehnička podrška, i odgovor na prijavljene incidente, moraju biti dostupni u režimu 24/7, ili će se ovi servisi isporučivati samo u toku redovnog radnog vremena.

U zavisnosti od zacrtane dostupnosti organizacije, i tehničke opremljenosti, tj. mogućnosti da se posao obavlja na daljinu (npr. od kuće), moguće je organizovati aktivna ili pasivna dežurstva van radnog vremena.

Scenario o kojem vredi razmisliti je da se i reaktivni i proaktivni servisi isporučuju tokom regularnog radnog vremena, a da se van njega obezbeđuje samo ograničen skup servisa (na primer slučaj velikih incidenata ili vanrednih događaja, koje bi pokrivao član CERT tima koji je u tom trenutku na dežurstvu).

Druga opcija je da se ispita mogućnost međunarodne saradnje sa drugim CERT timovima. Već postoje dobri primeri saradnje po principu podele po vremenskim zonama. Na primer, saradnja između timova u Evropi i Americi pokazala se kao korisna, u smislu mogućnosti da ovi timovi dele svoje kapacitete na efikasan način. Postoje i CERT timovi u okviru velikih multinacionalnih kompanija, koje imaju svoje ispostave u različitim vremenskim zonama širom sveta, i koje isporučuju svoje servise u režimu 24/7 na način da se nedovršeni posao prosleđuje timu u sledećoj vremenskoj zoni. Ovime se smanjuju troškovi,

jer svaki tim je angažovan samo tokom redovnog radnog vremena, a istovremeno se postiže da su servisi dostupni svuda u svetu tokom bilo kojeg doba dana ili noći.

Takođe, treba napomenuti da o potrebi da se servisi isporučuju u režimu 24/7 treba dobro prodiskutovati i sa samim konstituentima CERT organizacije. Slanje upozorenja ili alarma tokom noći nema mnogo smisla ukoliko će ih primalac pročitati tek sledećeg jutra. Postoji tanka, ali vidljiva razlika između „potrebe za servisom" i „želje za servisom", i kada se uzima u razmatranje radno vreme CERT organizacije naročito treba voditi računa o ovome, jer od usvojenog radnog vremena bitno zavisi i brojno stanje članova CERT tima, a samim tim i prostor i infrastruktura neophodni za njihov rad, što sve bitno utiče na troškove rada CERT organizacije.

8.1.2 Model prihoda

Kada se procene troškovi poslovanja CERT organizacije, potrebno je definisati i moguće modele finansiranja, tj. ostvarivanja prihoda, sa ciljem da se omogući normalno funkcionisanje organizacije. Postoji nekoliko mogućih scenarija koje treba razmotriti:

- Korišćenje postojećih resursa - Ukoliko se CERT organizacija formira u okviru neke nadređene organizacije treba proceniti mogućnost da CERT tim koristi i neke resurse te organizacije. Na primer, moguće je da u okviru IT službe krovne organizacije postoje ljudi sa potrebnim nivoom stručnosti koji mogu da potpomognu rad CERT organizacije u početnoj fazi njenog uspostavljanja, ili da obezbeđuju podršku za CERT tim na *ad-hoc* bazi (npr, stručnjaci pravne i ekonomske struke).
- Naplata članarine - Postoji i mogućnost da se servisi „prodaju" konstituentima, i to naplatom godišnje ili kvartalne članarine, tj. pretplate na servise. Takođe, mogu se implementirati i dodatni komercijalni servisi, kao što su konsultantske usluge, ili revizije stanja informacione bezbednosti, koji bi se posebno naplaćivali. Druga opcija je da se servisi za interne konstituente ne naplaćuju, a da se za eksterne obezbeđuju na komercijalnoj osnovi. Još jedna ideja može biti da se savetodavni i informativni bilteni objavljuju na javnom Internet portalu CERT organizacije, s tim da se formira i sekcija dostupna „samo članovima", koja bi sadržala potpunije i konkretnije informacije za te posebne grupe konstituenata.Ono što se u praksi pokazalo je da „pretplaćivanje" na servise CERT timova ima vrlo ograničen učinak u obezbeđivanju dovoljnih finansijskih sredstava za potrebe CERT organizacija, naročito u početnoj fazi njihovog rada. Primera radi, postoje fiksni osnovni troškovi za potrebe uspostavljanja CERT organizacije (za članove tima, njihovu opremu, poslovni prostor, ...), koji moraju biti plaćeni unapred. Finansiranje ovih troškova prodajom servisa CERT organizacije je veoma teško i potrebna je zaista detaljna finansijska analiza kako bi se pronašla tačka isplativosti u ovakvom scenariju.
- Subvencije - Još jedna mogućnost za finansiranje CERT organizacija koju treba uzeti u obzir je apliciranje za projektne subvencije koje vrlo često obezbeđuje država, tj. njeni organi, jer u današnje vreme mnoge države u svojim fondovima (odnosno budžetima) imaju sredstva koja su namenjena projektima u oblasti informacione bezbednosti. Stoga je potrebno kontaktirati odgovarajuća Ministarstva i istražiti ovu mogućnost.

Naravno, način prihodovanja CERT organizacije je najčešće mešavina svih pomenutih opcija.

8.2 FINANSIJSKI TOK I FAZE REALIZACIJE

Donošenjem Zakona o informacionoj bezbednosti Republike Srbije, RATEL je dobio zadatak da formira Nacionalni CERT. U prethodnim glavama ovog projekta detaljno su opisane funkcije i zadaci Nacionalnog CERT-a. Na osnovu navedenih funkcija i zadataka, predložen je plan realizacije Nacionalnog CERT-a. Prema tom planu, realizacija Nacionalnog CERT-a je podeljena u pet faza, po godinama realizacije.

Prve godine je potrebno zaposliti dirketora, sekretara/icu i 3 inženjera. Osnovni zadaci ove prve grupe zaposlenih u CERT-u su sledeći:

- formiranje Nacionalnog CERT-a,
- nabavka jednog putničkog vozila za potrebe Nacionalnog CERT-a,
- pronalaženje adekvatnog prostora za smeštaj opreme i boravak zaposlenih,
- prilagođavanje prostora specifičnoj funkciji Nacionalnog CERT-a,
- nabavka kompletne opreme za funkcionisanje Nacionalnog CERT-a,
- instalacija i stavljanje u funkciju nabavljenje opreme,
- osnovna obuka zaposlenih vezano za poslove Nacionalnog CERT-a,
- specifikacija zahteva za izradu namenskog informacionog sistema za prijem i obradu prijava bezbednosnih incidenata,
- realizacija komunikacija infrastrukture za povezivanje lokacije *data* centra sa lokacijom Nacionalnog CERT-a,
- povezivanje mreže Nacionalnog CERT-a na Internet,
- sertifikacija jednog zaposlenog (CISSP - *Certified Information Systems Security Professional* sertifikat),
- izrada *web* prezentacije Nacionalnog CERT-a i integracija sa informacionim sistemom za prijem i obradu prijava o bezbednosnim incidentima, i
- obezbeđenje korišćenja baze podataka sa do sada poznatim vrstama kompromitacije IKT sistema i načinima odbrane i zaštite IKT sistema, u cilju što bržeg funkcionalnog početka rada Nacionalnog CERT-a.

Do kraja prve godine predviđeno je da Nacionalni CERT bude formiran i da počne sa osnovnim radom u smislu pružanja osnovnih servisa samo tokom radnog vremena. Van radnog vremena zaposleni će biti na pasivnom dežurstvu (tzv. „dežurstvo od kuće"). Finansijskim planom predviđeno je da se za kapitalna ulaganja potroši 304.126 € tokom prve godine rada, dok su operativni troškovi predviđeni u iznosu od 213.652 €. Detaljna specifikacija troškova po godinama i po stavkama za kapitalna ulaganja data je u tabeli 8.1, a za operativne troškove u tabeli 8.2.

Početkom druge godine predviđeno je dalje povećanje broja zaposlenih, u skladu sa planom i dinamikom zapošljavanja. Početkom druge godine predviđeno je zapošljavanje još tri inženjera i jednog marketing stručnjaka. Tokom druge godine predviđene su sledeće aktivnosti:

- nabavka preostale opreme i komunikacionih linkova za povezivanje *data* centra i poslovnog prostora Nacionalnog CERT-a redundantnim linkom,
- nabavka preostale opreme (rutera i servera) koja treba da obezbedi redundantnost za osnovne servise Nacionalnog CERT-a,
- nabavka opreme i softvera (operativni sistem za računare, antivirusni softver, *office* alati) za novozaposlene,

- završetak radova na razvoju i implementaciji informacionog sistema za prijem i obradu bezbednosnih incidenata,
- nabavka preostalog softvera (aplikacija za *Netflow collector*, digitalnih sertifikata za nove zaposlene) potrebnog za ispravno funkcionisanje Nacionalnog CERT-a,
- završavanje osnovnih kurseva za obuku novozaposlenih,
- nastavak obuke zaposlenih koju su zaposleni tokom prve godine rada, i
- sertifikacija jednog zaposlenog (CISSP sertifikat).

Finansijskim planom predviđeno je da se tokom druge godine rada Nacionalnog CERT-a za kapitalna ulaganja potroši 119.831 €, dok su operativni troškovi predviđeni u iznosu od 375.963 €.

Početkom treće godine predviđeno je da se zaposle dva nova inženjera. Tokom treće godine predviđene su sledeće nabavke:

- nabavka opreme za formiranje laboratorije CERT-a za potrebe istraživanja i analize bezbednosnih incidenata,
- nabavka potrebne opreme za rad novozaposlenih (računar, mobilni i fiksni telefon),
- nabavka adekvatnog sofvera potrebnog za rad zaposlenih u Nacionalnom CERT-u,
- nabavka još jednog putničkog vozila za potrebe Nacionalnog CERT-a,
- nastavak školovanja i obuke novozaposlenih i zaposlenih u prethodnom periodu,
- sertifikacija za 5 zaposlenih (CCFP - *Certified Cyber Forensics Professional* sertifikat),
- sertifikacija jednog zaposlenog (CISSP sertifikat), i
- akreditacija Nacionalnog CERT-a kod međunarodnih institucija.

Finansijskim planom predviđeno je da se tokom treće godine rada Nacionalnog CERT-a za kapitalna ulaganja potroši 220.887 €, dok su operativni troškovi predviđeni u iznosu od 431.585 €.

Početkom četvrte godine predviđeno je zapošljavanje preostala 3 inženjera čime će Nacionalni CERT dostići predviđeni broj zaposlenih. Po završetku obuke novozaposlenih steći će se uslovi da Nacionalni CERT počne sa radom po principu 24x7x365. Tokom četvrte godine predviđene su sledeće nabavke:

- nabavka potrebne opreme za rad novozaposlenih (računar, mobilni i fiksni telefon),
- nabavka adekvatnog sofvera potrebnog za rad zaposlenih u Nacionalnom CERT-u (operativni sistem za računare, antivirusni softver, *office* alati, alati za analizu mrežnog saobraćaja),
- nastavak školovanja i obuke novozaposlenih i zaposlenih od ranije,
- sertifikacija za 5 zaposlenih (SSCP - *Systems Security Certified Practitioner* sertifikat), i
- sertifikacija jednog zaposlenog (CISSP sertifikat).

Finansijskim planom predviđeno je da se tokom četvrte godine rada Nacionalnog CERT-a za kapitalna ulaganja potroši 189.360 €, dok su operativni troškovi predviđeni u iznosu od 521.337 €.

Tokom pete godine predviđene su sledeće nabavke:

- zamena računarske i tehničke opreme kojoj je istekao amortizacioni period,
- nastavak školovanja i obuke zaposlenih,
- sertifikacija za 5 zaposlenih (CCFP sertifikat),
- sertifikacija jednog zaposlenog (CISSP sertifikat), i
- sertifikacija Nacionalnog CERT-a kod međunarodnih institucija.

Finansijskim planom predviđeno je da se tokom pete godine rada Nacionalnog CERT-a za kapitalna ulaganja potroši 236.387 €, dok su operativni troškovi predviđeni u iznosu od 521.337 €.

Realizacijom prethodno opisanog finansijskog plana i navedenih zadataka, Nacionalni CERT će posle pet godina biti u potpunosti osposobljen za obavljanje svih funkcija koje su predviđene i opisane u prethodnim glavama ovog projekta.

Tabela 8.1: Pregled kapitalnih troškova (CAPEX) po stavkama za period od pet godina

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
1	Internet ruter (2 komada) – minimalno 3 x 1000BaseT ili 1000BaseX interfejsa, podrška za BGPv4, dovoljno RAM memorije da može da prihvati 3 pune BGP tabele rutiranja, interni *firewall* za potrebe zaštite samog rutera od nedozvoljenog pristupa, sa podrškom za sledeće protokole: BGPv4, MP-BPG, IPv4 i IPv6 rutiranje, SSHv2, SNMPv3, NTP, Netflow.	45.000 €					45.000 €
2	Ruter/*layer* 3 *switch* za povezivanje lokacije u RATEL-u sa udaljenim *data* centrom (2 komada) – uređaj sa minimalno 4 x 1000BaseX interfejsima i sa integrisanom *firewall* funkcionalnošću, sa podrškom za sledeće protokole: OSPFv2 i OSPFv3, IPv4 i IPv6 rutiranje, SNMPv3, SSHv2, NTP, Netflow.	13.500 €	13.500 €				27.000 €
3	*Firewall* (2 komada) – uređaj sa minimalno 5 x 1000BaseT interfejsima, sposobni da rade *load balancing* saobraćaja u *active/active* režimu. Zadatak ovog *firewall* uređaja je zaštita mreže od upada sa Interneta, interna kontrola pristupa zaštićenim serverima u serverskoj mreži i u DMZ-u i terminiranje VPN tunela udaljenih korisnika.	6.600 €					6.600 €

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
4	*Workgroup switch* (6 komada) – namena ovih *Ethernet switch*-eva je povezivanje komunikacione opreme, servera i radnih stanica; minimalno 24 x 10/1000BaseT interfejsima, upravljivi, podrška za sledeće protokole: SSHv2, SNMPv3, LACP, Rapid STP, IEEE 802.1x, Radius, *Port-based* VLAN, BPDU *Guard, port autonegotiation, Automatic media-dependent interface crossover*, IGMP *snooping* v1 i v2, *Switch Port Analyzer*, *Remote Switch Port Analyzer*, NTP *synchronization*. 6595 eura po komadu bez PDV-a.	39.570 €					39.570 €
5	Serveri za informacioni sistem na kojima će se čuvati podaci o incidentima (2 komada).	7.000 €					7.000 €
6	Serveri za *mail* podsistem (3 fizicka servera). – *Mail* sistem se sastoji od dva *mail servera* čiji je zadatak prijem i distribucija *e-mail* poruka, dva servera za anti-spam i anti-virus proveru svih poruka i jednog servera na kome će se nalaziti sami nalozi korisnika.	6.300 €	3.500 €				9.800 €
7	Server za DNS servis (1 komad).	2.200 €					2.200 €
8	Server za *web* portal (2 komada). – Na ovom serveru treba da se nalazi *web* stranica CERT-a sa portalom za prijem prijava o sigurnosnim incidentima. Zbog važnosti ovog servisa, ovaj server mora da bude udvojen.	7.600 €					7.600 €

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
9	Oprema za laboratorijski LAN: serveri (2 komada), radne stanice (3 komada), *ethernet switch* (24 x 100/1000BaseT, upravljivi), laptop računar (3 komada), mobilni telefon sa iOS operativnim sistemom (1 komad), mobilni telefon sa Android operativnim sistemom (1 komad), mobilni telefon sa Windows Phone operativnim sistemom (1 komad).			12.200 €			12.200 €
10	Radne stanice za zaposlene i telefonski aparati	4.500 €	3.600 €	1.800 €	7.200 €	3.600 €	20.700 €
11	Štampači (4 komada).	600 €	600 €				1.200 €
12	Nabavka mobilnih telefona za svakodnevni rad zaposlenih (n komada - zavisno od broja novozaposlenih).	2.500 €	2.000 €	1.000 €	4.000 €	2.000 €	11.500 €
13	Fax aparat (1 komad).	300 €					300 €
14	Televizor (1 komad) – za praćenje aktuelnih događanja.	800 €					800 €
15	Video projektor (1 komad) – za prezentacije.	800 €				800 €	1.600 €
16	Kola za odlazak na teren.	17.000 €		17.000 €			34.000 €
17	Dve optičke veze – *setup fee.*	500 €	500 €				1.000 €
18	Linkovi ka dva nezavisna ISP-a – *setup fee*.	500 €	500 €				1.000 €

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
19	Direktne telefonske linije (5 komada) – *setup fee*.	200 €	200 €	100 €			500 €
20	Izgradnja lokalne računarske mreže u poslovnom prostoru - pasivni deo.	3.000 €					3.000 €
21	Preuređenje prostorija u poslovnom prostoru za potrebe CERT-a.	15.000 €					15.000 €
22	Zakup rek ormana u *data* centru – *setup fee*.	200 €					200 €
23	Operativni sistemi za radne stanice (Windows).	1.053 €	842 €	421 €	632 €	0 €	2.947 €
24	Anti-virusni softver.	218 €	327 €	362 €	482 €	427 €	1.816 €
25	MS Office + Project Pro + Visio Pro	6.456 €	777 €	389 €	2,026 €	0 €	9.649 €
26	Izrada namenskih aplikacija za funkcionisanje CERT-a.	10.000 €	10.000 €				20.000 €
27	Nabavka aplikacije za *Netflow collector*		5.000 €				5.000 €
28	Nabavka prava pristupa bazi podataka sa do sada poznatim vrstama kompromitacije IKT sistema i načinima odbrane i zaštite IKT sistema	86.600 €					86.600 €
29	Izrada *web* prezentacije CERT-a.	5.000 €	.				5.000 €
30	*WebSite-Watcher Business Edition* – 6 licenci.	494 €					494 €

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
31	Digitalni sertifikati za web sajt i *e-mail* komunikaciju.	2.335 €	135 €	165 €	2.470 €	210 €	5.315 €
32	Troškovi školovanja administratora i analitičara. – cena jednog kursa kod SANS-a je 5620 US$ + troškovi boravka, suma 7.000US$ = 6350€ (https://www.sans.org/ondemand/courses/all/).	6.350 €	25.400 €	25.400 €	38.100 €	38.100 €	133.350 €
33	Troškovi TRANSITS 1 kursa (750 eura po osobi) + prevoz	5.600 €	9.800 €	2.800 €	4.200 €		22.400 €
34	Troškovi TRANSITS 2 kursa (1100 eura po osobi) + smeštaj i prevoz		6.800 €	5.100 €	3.400 €	5.100 €	20.400 €
35	CISSP Exam*	6.350 €	6.350 €	6.350 €	6.350 €	6.350 €	31.750 €
36	CCFP Exam**			37.800 €		31.500 €	69.300 €
37	SSCP Exam***				30.500 €	18.300 €	48.800 €
38	Troškovi akreditacije CERT-a			50.000 €			50.000 €
39	Troškovi sertifikacije CERT-a					50.000 €	50.000 €
40	Ostali kursevi		30.000 €	60.000 €	90.000 €	80.000 €	260.000 €
	Ukupno:	304.126 €	119.831 €	220.887 €	189.360 €	236.387 €	**1.070.591 €**

* - CISSP® - *Certified Information Systems Security Professional*
**- CCFP - *Certified Cyber Forensics Professional*
*** - SSCP® - *Systems Security Certified Practitioner*

Tabela 8.2: Pregled operativnih troškova (OPEX) po stavkama za period od pet godinama

R. br.	Naziv	1. godina	2. godina	3. godina	4. godina	5. godina	Ukupno
1	Plaćanje mesečnog zakupa rek ormana u *data* centru.	700 €	700 €	700 €	700 €	700 €	3.500 €
2	Plaćanje mesečnog zakupa optičkih linkova između poslovnog prostora i udaljenog *data* centra (11 km i 18 km).	1.301 €	3.431 €	3.431 €	3.431 €	3.431 €	15.024 €
3	Plaćanje telefonskih računa.	300 €	400 €	500 €	700 €	700 €	2.600 €
4	Plaćanje mesečnih računa za korišćenje Internet linkova (2 x 100Mb/s simetrično).	2.072 €	2.072 €	2.072 €	1.400 €	1.400 €	9.016 €
5	Plaćanje godišnje naknade za korišćenje adresnog prostora i AS broja.	100 €	100 €	100 €	100 €	100 €	500 €
6	Plaćanje mesečnih troškova korišćenja prostora u poslovnom prostoru – cena 25 eura po kvadratu, 100 kvadratnih metara.	2.500 €	2.500 €	2.500 €	2.500 €	2.500 €	12.500 €
7	Plaćanje mesečne nadoknade za pristup bazi podataka sa do sada poznatim vrstama kompromitacije IKT sistema i načinima odbrane i zaštite IKT sistema.	41.022 €	82.044 €	82.044 €	82.044 €	82.044 €	369.198 €
8	Troškovi plata zaposlenih.	148.657 €	240.716 €	296.239 €	371.463 €	371.463 €	1.428.537 €
9	Troškovi odlaska zaposlenih na konferencije u cilju usavršavanja i povezivanja sa drugim CERT organizacijama – 3.000€ po konferenciji po učesniku.	6.000 €	18.000 €	18.000 €	18.000 €	18.000 €	78.000 €
10	Troškovi marketinga.	5.000 €	20.000 €	20.000 €	20.000 €	20.000 €	85.000 €
11	Troškovi održavanja akreditacije.				15.000 €	15.000 €	30.000 €
12	Tekući troškovi poslovanja.	6.000 €	6.000 €	6.000 €	6.000 €	6.000 €	30.000 €
	Ukupno:	**213.652 €**	**375.963 €**	**431.585 €**	**521.337 €**	**521.337 €**	**2.063.875 €**

8.3 POVRAĆAJ INVESTICIJE U INFORMACIONU BEZBEDNOST

8.3.1 Uvod

Kao i sve druge organizacije, i CERT organizacije moraju da mere svoju isplativost, kako bi opravdale sredstva koja se u njih ulažu, i obezbedile ubedljive argumente za dobijanje svakog narednog budžeta. Međutim, CERT organizacije često imaju poteškoće da precizno izmere efekte i troškove svojih aktivnosti na polju informacione bezbednosti. Razlog za ovo je taj što investicija u bezbednost nije nešto što donosi profit, već sprečava gubitke. Otuda se postavlja pitanje koja je to odgovarajuća suma koju jedna organizacija treba da investira u svoju informacionu bezbednost?

Da bi se dobio odgovor na ovo pitanje potrebno je kreirati neke bazične alate i iskoristiti najbolju praksu kako bi se izračunao „povraćaj investicije u informacionu bezbednost" (*Return on Security Investment – ROSI*), što bi bilo analogno pojmu „povraćaja investicije" (*Return on Investment – ROI*) u klasičnoj ekonomskoj praksi. Ovaj parametar onda može da se iskoristi kao valjan argument kojim se opravdavaju troškovi i dodeljuju budžetska sredstva organizacijama koje se bave informacionom bezbednošću.

Iako su metode za određivanje *ROSI* parametra relativno jednostavne, u njihovoj primeni u stvarnom svetu treba uzeti u obzir i činjenicu da postoji generalna tendencija da se potcenjuju troškovi prouzrokovani bezbednosnim incidentima, a taj „trošak incidenta" je ključni faktor u izračunavanju *ROSI*.

Ipak, kada su u pitanju CERT organizacije, a s obzirom na njihovu raznovrsnost, načine finansiranja i kapacitete delovanja, proračun povraćaja investicije mora da ide dalje od izračunavanja samo *ROSI* parametra. Zapravo, procena isplativosti CERT organizacije mora uzeti u obzir i razne korisne akcije koje CERT organizacije sprovode na polju detektovanja i upravljanja bezbednosnim incidentima, otklanjanja posledica tih incidenata, ili njihovog ranog i efikasnog suzbijanja, kao i edukacije u cilju sprečavanja pojave bezbednosnih incidenata. Pri tome, što pre se incident razreši, to su troškovi u vezi sa incidentom manji. Samim tim, profitabilnost CERT organizacija treba posmatrati u svetlu razlike u troškovima razrešavanja incidenata u slučaju kada postoji pomoć CERT organizacije u njihovom razrešavanju, u odnosu na situaciju kada pomoći CERT organizacije nema.

8.3.2 Potreba za izračunavanjem *ROSI*

8.3.2.1 Povraćaj investicije (ROI)

U svakom javnom ili privatom preduzeću, svaka investicija mora biti opravdana, a njeni efekti se ocenjuju tokom vremena. U svetu finansija ova ocena se naziva „povraćaj investicije" (eng. *Return on Investment – ROI*), ili „stopa povraćaja". *ROI* se izračunava po formuli (8.1), pri čemu je *Gain from investment* – zarada od investicije, a *Cost of investment* – troškovi investicije:

$$ROI = \frac{Gain\ from\ investment - Cost\ of\ investment}{Cost\ of\ investment} \qquad (8.1)$$

Primer izračunavanja *ROI*: Jovana želi da se bavi prodajom limunade tokom leta. Potreban joj je novac da započne posao, i Petar joj daje 200 EUR. Za uzvrat, Jovana pristaje da sa Petrom podeli 50% svoje zarade. Na kraju leta, Jovana završava posao sa 1000 EUR zarade i predaje Petru njegovih 500 EUR. U Petrovom slučaju, povraćaj investicije se izračunava kao:

$$ROI = \frac{500 - 200}{200} = 150\% \tag{8.2}$$

8.3.2.2 Povraćaj investicije u informacionu bezbednost (ROSI)

Koncept izračunavanja *ROI* primenljiv je za svaku vrstu investicije, i informaciona bezbednost nije u tome izuzetak, jer rukovodioci koji donose odluke žele da znaju kakav je uticaj informacione bezbednosti na celinu poslovanja. Da bi znali koliko treba da potroše na informacionu bezbednost, potrebno je da znaju koliki trošak i štetu po njihovo poslovanje nosi nedostatak informacione bezbednosti i koja su rešenja u tom smislu najisplativija.

Kada se *ROI* koncept primeni na informacionu bezbednost, izračunavanje *ROSI* može pružiti kvantitativne odgovore na bazična finansijska pitanja:

- Da li preduzeće previše investira u informacionu bezbednost?
- Koliki finansijski uticaj na produktivnost može imati nedostatak informacione bezbednosti?
- Koliko je uopšte potrebno investirati u informacionu bezbednost?
- Da li postojeća bezbednosna struktura ili proizvod daje nekakav efekat?

Klasičan finansijski pristup pri računanju *ROI* nije odgovarajući kada su u pitanju parametri informacione bezbednosti, jer informaciona bezbednost nije investicija koja sama po sebi donosi profit. Informaciona bezbednost se više tiče smanjenja i sprečavanja gubitaka. Drugim rečima, kada se investira u informacionu bezbednost ne očekuju se finansijski prinosi, već se očekuje da se smanje rizici koji prete imovini preduzeća. Ovakvim pristupom, kvantitativna procena *ROSI* se dobija proračunom koliki su gubici sprečeni investicijom u informacionu bezbednost.

8.3.2.3 Metodologija za izračunavanje ROSI

Kao što je već rečeno, procena bezbednosne investicije uključuje procenu koliko se uštedi na potencijalnim gubicima zahvaljujući investiciji u bezbednost. Dakle, novčana vrednost investicije mora se uporediti sa novčanom vrednošću smanjenja rizika. Ova novčana vrednost rizika može se odrediti kvantitativnom procenom rizika.

8.3.2.3.1 Osnovni koncepti procene rizika

Kvantitativna procena rizika određuje se na bazi procene nekoliko komponenata rizika. Definišu se sledeći pojmovi:

- očekivani trošak pojedinačnog gubitka (*Single Loss Expectancy – SLE*),
- godišnja učestalost događaja (*Annual Rate of Occurrence – ARO*), i
- očekivani gubici na godišnjem nivou (*Annual Loss Expectancy – ALE*).

SLE je očekivana suma novca koja će se izgubiti u slučaju pojave bezbednosnog incidenta. U ovom pristupu, *SLE* se može posmatrati kao ukupni trošak incidenta u slučaju njegovog pojedinačnog pojavljivanja.

S obzirom na specifičnu prirodu informacionih incidenata, najkompleksnije je odrediti sve entitete na koje je neki bezbednosni incident imao uticaja. Na primer, ukradeni laptop ne nosi sa sobom samo trošak njegove zamene novim uređajem, već isto tako utiče i na gubitak produktivnosti, gubitak reputacije, troškove IT podrške, gubitak podataka, a moguće čak i troškove u vezi sa intelektualnom svojinom. Dakle, ukupna procena troška mora uključivati trošak direktnih gubitaka (npr. vreme nedostupnosti Internet sajta, zamenu hardvera, nemogućnost normalnog rada, oporavak od gubitka podataka...), kao i troškove indirektnih gubitaka (vreme potrošeno na razrešenje incidenta, gubitak reputacije, uticaj na sliku preduzeća u javnosti, „curenje“ poverljivih podataka ka konkurenciji...).

Ne postoje univerzalne vrednosti za *SLE*. Šta će se uključiti u kalkulaciju *SLE* nekog događaja zavisi od poslovnih ciljeva preduzeća, kulturoloških vrednosti i postojećih mera informacione bezbednosti. Primera radi, jedno preduzeće može proceniti *SLE* izgubljenog laptopa samo na vrednost samog uređaja (npr. 2 000 EUR), dok neko drugo preduzeće koje barata osetljivim i poverljivim informacijama može proceniti ovaj gubitak i na 100 000 EUR, jer takav događaj može imati uticaja na njihov imidž, ugovore koje imaju sa svojim klijentima, ili njihove konkurentske prednosti.

Iako se *SLE* može procenjivati na različite načine, sama *ROSI* kalkulacija često uključuje poređenje različitih *SLE*, pa treba biti konzistentan u načinu njihove procene.

ARO je mera verovatnoće da će se bezbednosni incident desiti u toku perioda od jedne godine. Naravno, i ovaj parametar je samo procena i može zavisiti od brojnih faktora: npr. *ARO* u slučaju poplave zavisi od geografskih faktora, *ARO* gubitka diska može da zavisi od temperature pod kojom disk radi, *ARO* krađe zavisi od lokacije neke imovine, i tako dalje. Pored toga, *ARO* zavisi i od primenjenih mera zaštite – *ARO* za uspešan napad malicioznim softverom značajno će se smanjiti ako u organizaciji počne da se koristi efikasno anti-virusno rešenje.

ALE je parametar koji se odnosi na novčanu vrednost gubitaka koji se mogu očekivati na bazi posmatranog rizika za posmatrani sistem, i izračunava se kao:

$$ALE = ARO * SLE \tag{8.3}$$

8.3.2.4 Izračunavanje ROSI

Izračunavanje *ROSI* kombinuje kvantitativnu procenu rizika, i troškove implementacije bezbednosnog rešenja kojim se taj rizik smanjuje. Na kraju, upoređuje se *ALE* sa očekivanim uštedama zahvaljujući zaštitnim merama. Analogno definiciji *ROI*, *ROSI* se izračunava na osnovu formule (8.4), gde je *Monetary loss reduction* – ušteda, a *Cost of solution* – trošak bezbednosnog rešenja:

$$ROSI = \frac{Monetary\ loss\ reduction - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \tag{8.4}$$

Implementiranje efikasnog bezbednosnog rešenja smanjuje *ALE*, tj. što je rešenje efikasnije, to je *ALE* manji. Navedeno umanjenje novčanog gubitka, tj. ušteda, može se definisati kao razlika *ALE* bez primene bezbednosnog rešenja i modifikovanog *ALE* (*mALE*), u slučaju primene nekog bezbednosnog rešenja:

$$ROSI = \frac{ALE - mALE - Cost\ of\ the\ solution}{Cost\ of\ the\ solution} \tag{8.5}$$

Isto to se može izraziti i kroz „faktor ublažavanja" *ALE*, tj. *mitigation ratio*, u slučaju primene bezbednosnog rešenja:

$$ROSI = \frac{ALE * mitigation\ ratio - Cost\ of\ solution}{Cost\ of\ solution} \tag{8.6}$$

Primer izračunavanja ROSI: neka kompanija razmatra investiciju u anti-virusno rešenje. Svake godine ta kompanija beleži pet napada računarskih virusa (*ARO* = 5). Procena je da svaki napad generiše troškove od oko 15 000 EUR, kroz gubitak podataka i pad produktivnosti (*SLE* = 15 000). Očekuje se da anti-virusno rešenje blokira 80% napada (*mitigation ratio = 80%*), i njegova cena je 25 000 EUR godišnje (15 000 EUR iznose godišnji troškovi licenci, i dodatnih 10 000 EUR za instalaciju, održavanje, trening, i sl.).

Povraćaj ove investicije u bezbednost se obračunava kao:

$$ROSI = \frac{(5 * 15000) * 0.8 - 25000}{25000} = 140\% \tag{8.7}$$

Prema ovoj kalkulaciji, anti-virusno rešenje koje je predmet ovog razmatranja bilo bi isplativo.

Na kraju treba reći da se *ROSI* kalkulacija zasniva na tri promenljive: očekivanih potencijalnih gubitaka (*ALE*), očekivanog faktora ublažavanja rizika, i cene bezbednosnog rešenja. I dok je cenu bezbednosnog rešenja lakše predvideti, tj. odrediti, druge dve promenljive su samo procenjene vrednosti, što celoj *ROSI* kalkulaciji daje aproksimativni karakter.

8.3.3 Ograničenja *ROSI* kalkulacije

Procena količine novca koja će se uštedeti izbegavanjem gubitaka koji se možda nikada neće ni dogoditi je komplikovan zadatak, koji u realnom svetu zahteva više angažovanja nego što bi bila samo pravolinijska primena nekakve formule za izračunavanje.

8.3.3.1 Mane proračuna

ROSI kalkulacija je rezultat mnogih aproksimacija. Trošak izazvan napadom na informacionu bezbednost, kao i godišnja učestalost ovakvih događaja su teško predvidljivi, i dobijeni rezultati se mogu veoma razlikovati u zavisnosti od okruženja, tj. sredine. Ove aproksimacije se često temelje na načinu percepcije rizika, a samom *ROSI* kalkulacijom je

moguće lako manipulisati u zavisnosti od toga čije interese treba zadovoljiti. Drugim rečima, ona više može da posluži da bi se opravdala neka odluka, nego što daje realnu osnovu za njeno donošenje.

Stoga je tačnost statističkih podataka koji se koriste u kalkulaciji od ključne važnosti. Međutim, do egzaktnih podataka o bezbednosnim incidentima nije lako doći, jer kompanije često odbijaju da daju podatke o bezbednosnim incidentima i napadima koje su eventualno pretrpele.

Zato je često bolje procenu bazirati na nekim istorijskim podacima o incidentima u okviru neke kompanije, nego se samo oslanjati na podatke vendora, uopštenih izveštaja, ili studija informacione bezbednosti. Primera radi, ukoliko je web sajt kompanije u poslednjih 5 godina bio meta napada 6 puta, onda u kalkulaciji treba koristiti vrednost *ARO* = 6/5, jer je to tačnije od bilo koje druge pretpostavljene vrednosti, iz bilo kojeg drugog dokumenta ili studije.

8.3.3.2 Gordon & Loeb model

Lawrence Gordon i *Martin Loeb* su ekonomisti sa Univerziteta Merilend, čija je studija, objavljena 2002. godine, pod nazivom „Ekonomija investicija u informacionu bezbednost“ izuzetno poznata i veoma često citirana.

U svojoj studiji autori tvrde da, nasuprot osnovnim načelima procene rizika, imovina koja ima veću vrednost ne mora uvek imati veću korist od velike investicije u njenu zaštitu. Optimalna investicija u informacionu bezbednost ne mora se uvek uvećati proporcionalno sa povećanjima ranjivosti sistema, tj. postoji tačka posle koje kompanije više nemaju interesa da značajno podižu ulaganje u informacionu bezbednost.

Prema ovoj studiji, „optimalna suma koju treba potrošiti na informacionu bezbednost nikada ne prelazi 37% očekivanih gubitaka koji bi se mogli desiti u slučaju bezbednosnog incidenta (i obično je mnogo manja od 37%)”.

Naravno, postoje i druge studije koje dovode u pitanje ove zaključke, i dokazuju da ne postoji fiksni procenat ili suma investicije u informacionu bezbednost. Time se samo podvlači da je *ROSI* kalkulacija aproksimativnog karaktera, ali i da rezultate treba uvek pažljivo analizirati jer mogu da posluže kao dobra vodilja za proračun investicije u informacionu bezbednost.

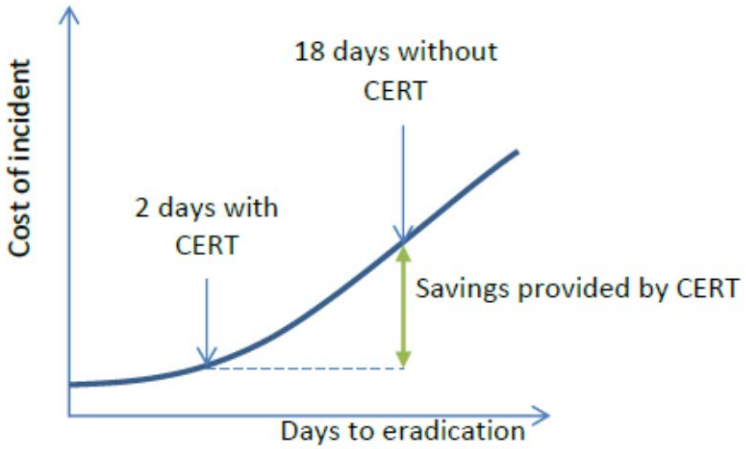
8.3.4 Procena isplativosti CERT organizacije

CERT organizacije koje svoje usluge pružaju interno, unutar sopstvene krovne organizacije, su neprofitne organizacije. Njihov cilj nije da zarađuju novac i ostvaruju profit, već da sprečavaju gubitke, tako što će se sprečavati pojava bezbednosnih incidenata, ali i omogućavati brz i efikasan oporavak za slučaj da se oni dese. Otuda se isplativost CERT organizacije mora posmatrati kao investicija u informacionu bezbednost, pri čemu se povraćaj te investicije ogleda kroz smanjenje gubitaka koji se na taj način sprečavaju.

Pri tome, proceni isplativosti treba pristupati činjenično, tj. *ALE* je najčešće lakše izračunati na bazi istorijskih podataka. Otuda, procena isplativosti CERT organizacije može se aproksimirati procenom razlike u troškovima koji su nastali kao posledica bezbednosnih incidenata, u situacijama kada nije postojala CERT organizacija koja bi se bavila razrešavanjem incidenata, i onda kada ona postoji.

Rezultati raznih studija i istraživanja pokazuju da troškovi bezbednosnih incidenata mogu da rastu u zavisnosti od dužine trajanja razrešenja incidenta. Po pravilu, što se ranije

neki bezbednosni incident ili napad detektuje, to su troškovi oporavka manji. U zavisnosti od tipa incidenta, troškovi mogu da rastu eksponencijalno tokom vremena. Otuda se ušteda u vremenu razrešenja incidenta, koja se postiže zahvaljujući postojanju CERT organizacije koja je u tome angažovana, može smatrati finansijskom uštedom, u smislu smanjenja štete i smanjenja vremena nedostupnosti informacionih servisa (grafički prikaz dat je na slici 8.1). Takođe, ukupne uštede koje omogućava CERT organizacija mogu se posmatrati kao suma svih ušteda koje se postižu kod njenih konstituenata.



Slika 8.1: Ušteda u vremenu i troškovima razrešenja bezbednosnih incidenata

Naravno, da bi se izračunale neto uštede u slučaju postojanja CERT organizacije, potrebno je od ukupne sume svih ušteda oduzeti troškove koje generiše sama CERT organizacija u svom poslovanju. U te troškove spadaju razni administrativni i materijalni troškovi (oprema, radni prostor, ljudstvo, obuke, i slično).

S obzirom da je izračunavanje *ROSI* i procena isplativosti CERT organizacija, generalno, komplikovana tema, postoje i razne radne grupe i forumi u kojima se radi na razmeni iskustava u pogledu interne organizacije CERT-ova i povećanju njihove isplativosti. Primera radi, jedna od tih radnih grupa je i *Metrics SIG*, u okviru organizacije FIRST, koja se bavi temama procene troškova bezbednosnih incidenata i povraćaja investicija u informacionu bezbednost. Rezultati ovih istraživanja i analiza treba da pomognu CERT organizacijama u proceni njihove isplativosti.

Takođe, postoje brojne studije koje pokazuju međusobnu zavisnost brzine i kvaliteta reagovanja na bezbednosne incidente, i troškova, tj. gubitaka, koji nastaju kao posledica tih incidenata. U poglavlju koje sledi prikazani su rezultati jedne takve studije, koja se odnosi na analizu troškova (i raznih parametara koji na njih utiču) za slučaj bezbednosnih incidenata koji uključuju gubitak podataka. Time se ukazuje na važnost postojanja bezbednosnih struktura, kao što su CERT organizacije, i njihove međusobne saradnje na očuvanju informacione bezbednosti.

8.3.4.1 Analiza slučaja – gubitak podataka

Kompanija IBM i *Ponemon* institut sproveli su istraživanje i u junu 2016. godine objavili rezultate studije na temu gubitaka poverljivih informacija i poslovnih podataka – „*2016 Cost of Data Breach Study: Global Analysis*“. Ova globalna studija je obuhvatila 383 kompanije iz 12 zemalja (SAD, Velika Britanija, Nemačka, Australija, Francuska, Brazil, Japan, Italija, Indija, arapski region - Ujedinjeni Arapski Emirati i Saudijska Arabija, Kanada i Južna Afrika).

Cilj ovog istraživanja je da se kvantifikuje ekonomski uticaj gubitka podataka, i procene trendovi troškova u vezi sa ovim incidentima tokom vremena. Dobro razumevanje troškova usled gubitka podataka, i ključnih uzroka pojave ovih troškova, može puno pomoći organizacijama da odrede odgovarajući nivo investicija i resursa, koji su potrebni radi prevencije ovakvih bezbednosnih incidenata, i smanjenja njihovih posledica.

Šta se podrazumeva pod „gubitkom podataka“? Pod ovim se podrazumeva gubitak ličnih podataka nekog pojedinca (u kombinaciji sa njegovim zdravstvenim, ili finansijskim podacima, kao što su npr. detalji kreditne kartice i sl.), u elektronskoj ili papirnoj formi. Ovom studijom su identifikovana tri glavna uzroka gubitka podataka:

- maliciozni napad na informacioni sistem,
- kvar na informacionom sistemu i
- ljudska greška.

Troškovi gubitka podataka mogu varirati u zavisnosti od jednog od ova tri uzroka, ali i stanja bezbednosne zaštite u datom trenutku.

Šta se podrazumeva pod „kompromitovanim podatkom“? Pod ovim se podrazumeva informacija koja identifikuje nekog pojedinca čiji podaci su izgubljeni ili ukradeni tokom bezbednosnog incidenta. Primeri mogu uključivati bezbednosne incidente sa bazama podataka trgovačkih kompanija, koje sadrže lične podatke pojedinaca, u kombinaciji sa podacima njihovih kreditnih kartica, kao i druge lične podatke. Ili to mogu biti podaci iz baza podataka zdravstvenih organizacija, koji sadrže lične podatke nekog pacijenta i informacije o metodi i sredstvu plaćanja zdravstvenog osiguranja ili zdravstvenih intervencija. Prema rezultatima istraživanja prosečni trošak gubitka ovakvog podatka je 158$.

Kako se proračunava trošak gubitka podataka? Da bi se izračunao prosečni trošak gubitka podataka, potrebno je prikupiti podatke o direktnim i indirektnim troškovima sa kojim su organizacije suočene usled gubitka podataka. Direktni troškovi uključuju troškove angažovanja stručnjaka za digitalnu forenziku, i druge vrste podrške, radi razrešenja bezbednosnog incidenta. Indirektni troškovi uključuju istražne radnje i komunikaciju u samoj kompaniji, kao i iznos gubitaka koji su posledica gubitka klijenata i lošije poslovne reputacije u budućnosti.

Prosečne vrednosti troškova do kojih se došlo u ovom istraživanju ne uključuju drastične primere gubitka podataka (kao što je npr. bio bezbednosni incident kompanije Sony, kada su hakeri neovlašćeno preuzeli više od 25GB podataka, sa raznih servera u mreži ove kompanije, koji su sadržali na desetine hiljada zapisa ličnih podataka zaposlenih i poslovnih saradnika kompanije, ali i ogromnu količinu drugih poverljivih poslovnih podataka...), jer to nisu tipični primeri incidenata koji se dešavaju većini organizacija. Da bi se održala reprezentativnost podataka na globalnom nivou, u analizu su uključeni primeri gubitka podataka koji su uključivali između 3 000 i 100 000 kopromitovanih podataka pojedinaca.

S obzirom da se ovakva istraživanja rade već duži niz godina, uočeno je postojanje nekoliko globalnih trendova:

- Od vremena izvođenja prve ovakve studije, pa do danas, prosečni trošak gubitka podataka nije se značajnije menjao. To znači da ovakva vrsta troška predstavlja stalno potencijalno opterećenje za organizacije, koje moraju biti spremne da se suoče sa bezbednosnim incidentima, i rade na njihovom sprečavanju.
- Najveća finansijska posledica po organizacije koje su suočene sa problemom gubitka podataka je gubitak poslovnih prilika zbog ugrožene reputacije. Posle ovakvih bezbednosnih incidenata kompanije moraju da ulože dodatne napore i sredstva kako bi

povratile poverenje svojih klijenata, i smanjile dugoročne nepovoljne finansijske efekte.

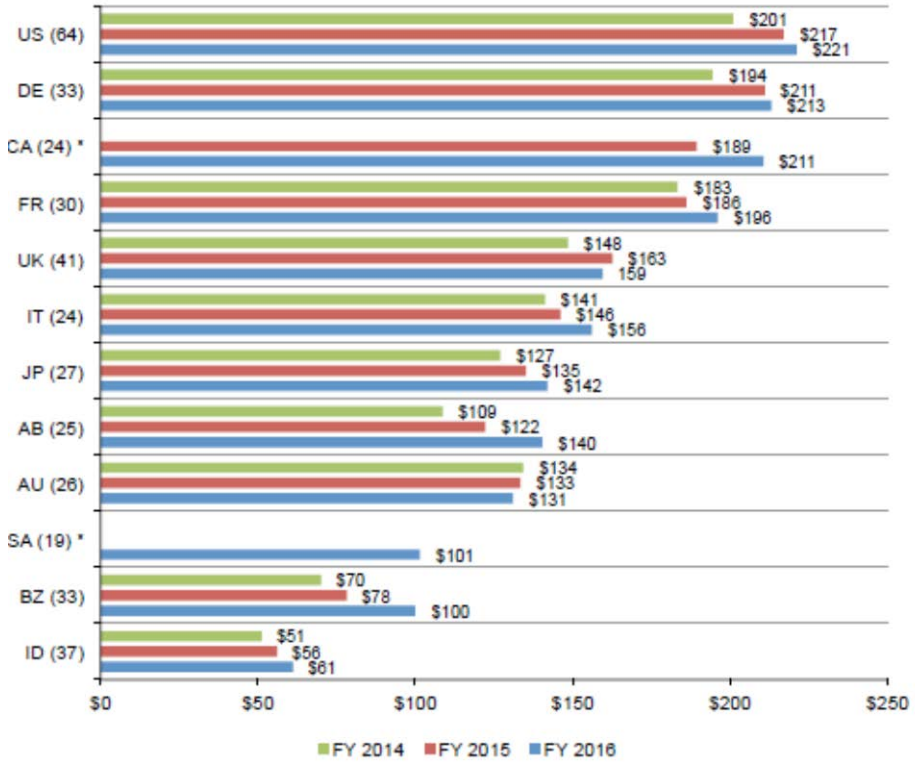
- Najveći broj bezbednosnih incidenata sa gubitkom podataka su posledica malicioznih i kriminalnih napada na informacione sisteme. Takođe, za otkrivanje i razrešenje ovakvih vrsta incidenata potrebno je i najviše vremena. Rezultat toga je da je i trošak ovakvih bezbednosnih incidenata najveći.
- Kompanije su prepoznale da, što je duže vreme koje prođe pre nego što se gubitak podataka otkrije i spreči, to je i trošak bezbednosnog incidenta veći. Iz toga proističu i veća ulaganja u bezbednosnu tehnologiju i ekspertizu unutar samih kompanija, kako bi se sprečili bezbednosni incidenti i kako bi se smanjilo vreme njihovog razrešenja ako do njih ipak dođe.
- Grane poslovanja koje su podložne intenzivnijoj regulaciji, kao što su zdravstvena zaštita, ili finansijske usluge, imaju najveći prosečni trošak gubitka podataka, zbog visokih kazni i gubitka poverenja klijenata kojima su izložene usled ovakvih bezbednosnih incidenata.
- Poboljšanja u procesu upravljanja podacima smanjuju troškove gubitka podataka. Postojanje planova za upravljanje incidentima, uspostavljanje bezbednosne strukture u okviru kompanije, obuka zaposlenih, i kontinuirano podizanje njihove svesti o značaju informacione bezbednosti doprinose smanjenju finansijskih gubitaka usled bezbednosnih incidenata.
- Investiranje u određene mehanizme za zaštitu od gubitka podataka, kao što su enkripcija podataka, i zaštita računarske opreme zaposlenih anti-virusnim softverom, su izuzetno značajni u sprečavanju gubitka podataka, i smanjenju troškova koji su sa tim u vezi.

Ovi trendovi ukazuju da je potreban kontinuirani rad na poboljšanju bezbednosti informacionih sistema, kao i uspostavljanju CERT organizacija i međunarodne saradnje, jer je to dobar način za smanjenje troškova koji nastaju kao posledica bezbednosnih incidenata, i skraćivanje vremena koje je potrebno za oporavak od finansijskih i drugih posledica bezbednosnih incidenata.

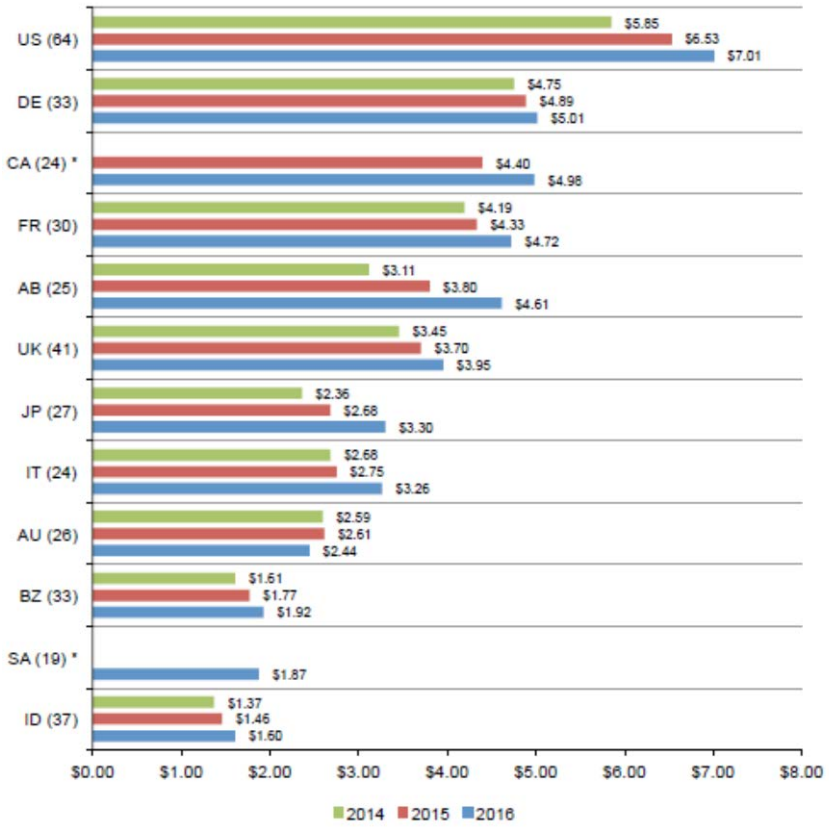
Neki od konkretnih podataka do kojih se došlo u studiji iz 2016, godine su sledeći:

- Najveći prosečni trošak gubitka podataka (za pojednica, prema definiciji datoj u prethodnom tekstu) je 221$ u SAD, tj. 213$ u Nemačkoj. Najniži prosečni trošak je u Brazilu (100$), i Indiji (61$). Ukupni prosečni trošak gubitka podataka na nivou organizacije je najveći u SAD (7.01 miliona $) i Nemačkoj (5.01 milion $). Najmanji prosečni trošak organizacija je u Indiji (1.6 miliona $). Trošak gubitka podataka, u zemljama koje su obuhvaćene studijom, na bazi pojedinačnih podataka, prikazan je na slici 8.2, a na nivou organizacija na slici 8.3.
- Trošak gubitka podataka varira u zavisnosti od grane poslovanja. Globalni prosek za trošak gubitka podataka je 158$ (na bazi pojednica čiji su podaci izgubljeni ili ukradeni). Međutim, kod zdravstvenih ustanova ovaj trošak se procenjuje na 355$, a kod obrazovnih ustanova je oko 246$. Najniži prosečni trošak je u poslovanjima transportnih kompanija (129$), istraživačkih ustanova (112$), i u javnom sektoru (80$). Raspodela troška gubitka podataka po granama poslovanja prikazana je na slici 8.4.

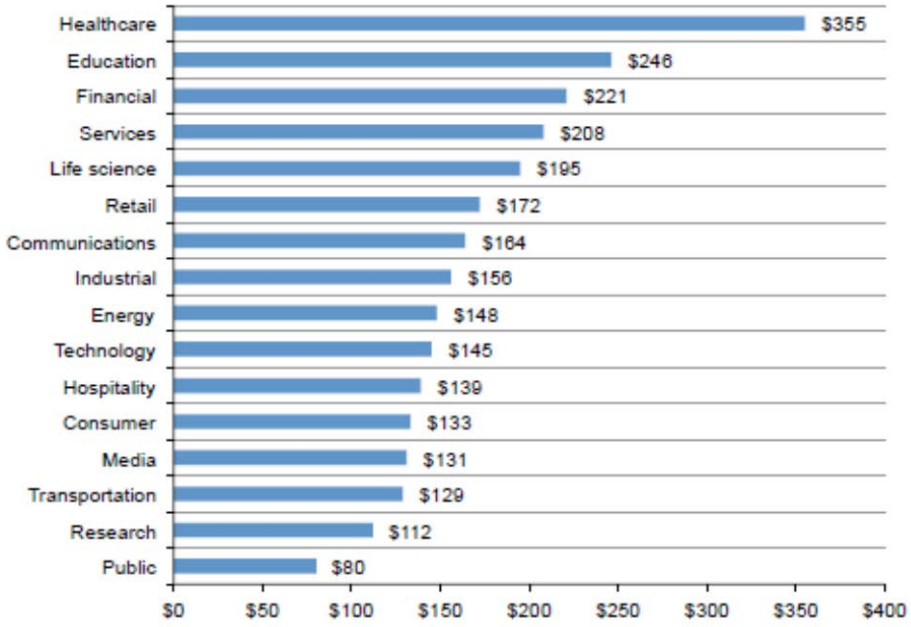
- Hakerski napadi su najčešći uzrok gubitka podataka. Prema rezultatima studije, 48% slučajeva gubitaka podataka posledica su malicioznih napada na informacione sistema. Prosečni trošak razrešenja ovakvog tipa bezbednosnog incidenta, po pojedinačnom kompromitovanom podatku, je procenjen na 170$. U poređenju sa tim, trošak gubitka podatka u slučaju kvarova na elementima informacionih sistema je 138$, a usled ljudske greške ili nepažnje je 133$. Prikaz raspodele bezbednosnih incidenata koji su uzrok gubitka podataka prikazan je slici 8.5, a raspodela troškova za razrešenje takvih incidenata na slici 8.6.



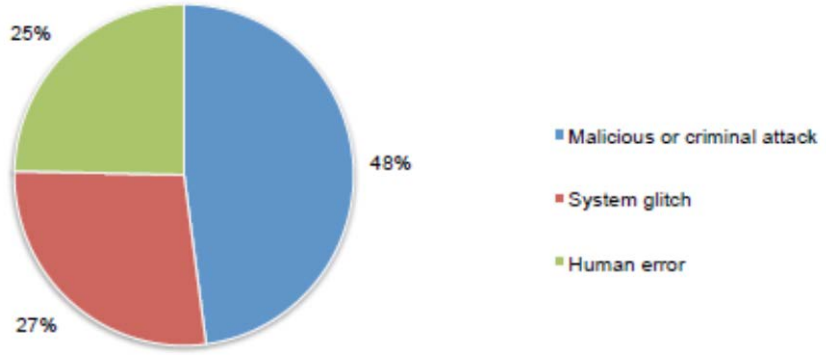
Slika 8.2: Prosečni trošak gubitka podataka za pojedinačne podatke



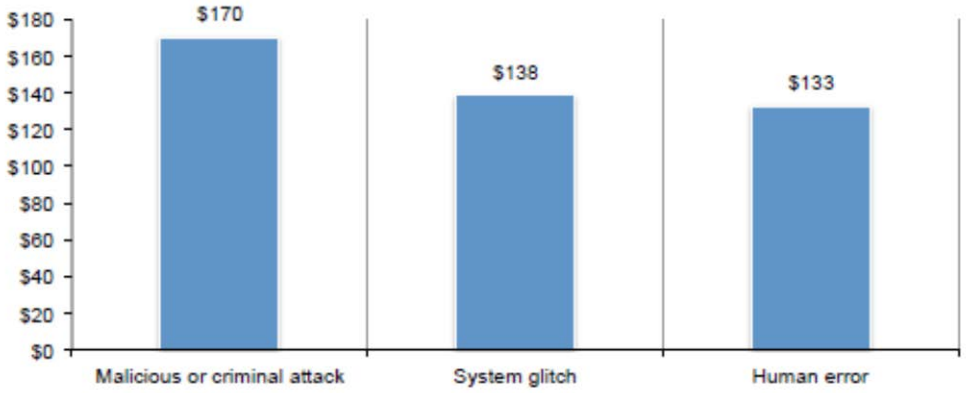
Slika 8.3: Prosečni ukupni trošak na nivou organizacija (u milionima $)



Slika 8.4: Trošak gubitka podataka po granama poslovanja

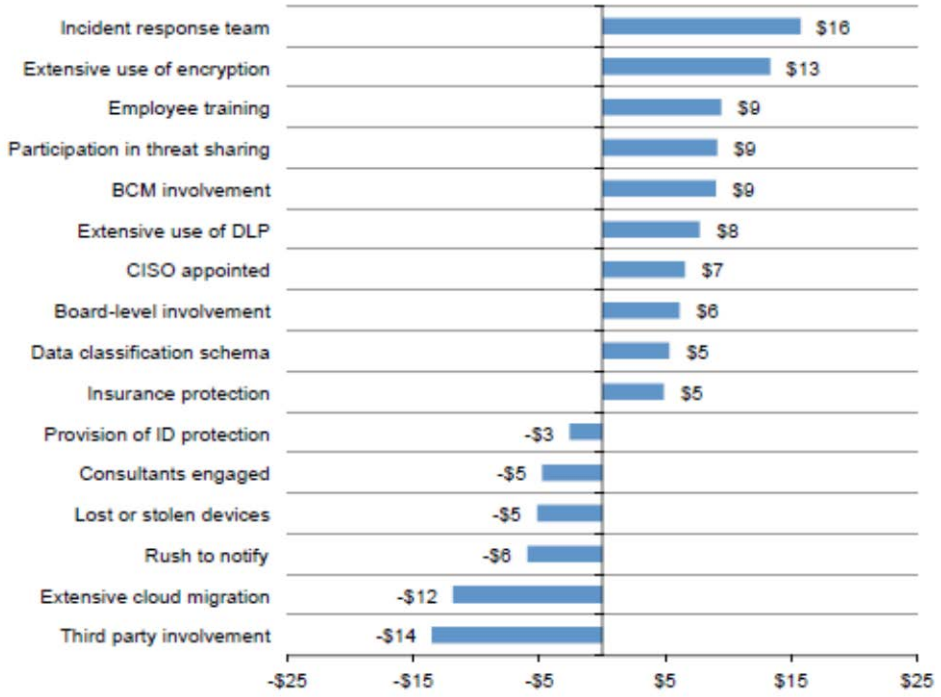


Slika 8.5: Raspodela tipova uzroka gubitka podataka



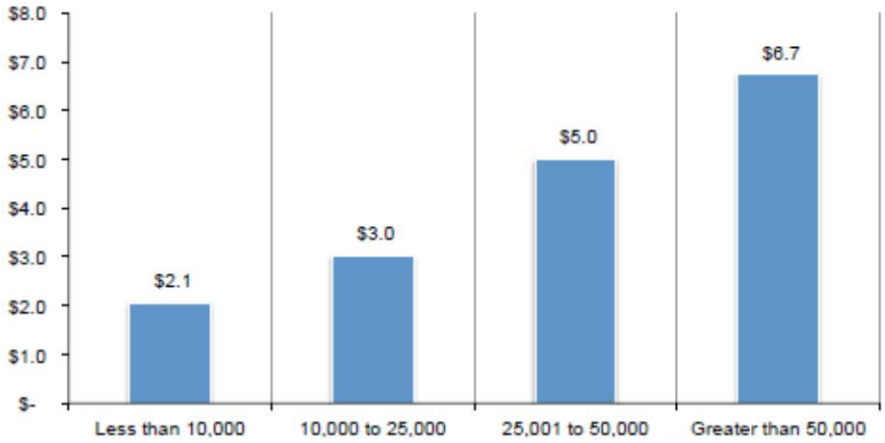
Slika 8.6: Raspodela troškova razrešenja incidenata gubitka podatka prema tipu bezbednosnog incidenta

Uspostavljanje CERT organizacija, i primena mehanizama za zaštitu podataka, kao što je enkripcija, smanjuju troškove koji su posledica bezbednosnih incidenata sa gubitkom podataka. Primera radi, postojanje bezbednosnih struktura, kao što su CERT timovi, smanjuje trošak gubitka podataka za 16$ po pojedinačnom kompromitovanom podatku. Sa druge strane, angažovanje eksternih konsultanata na razrešenju ovih incidenata povećava taj trošak za 5$. Uticaj različitih faktora na trošak gubitka pojedinačnog podatka prikazan je na slici 8.7.



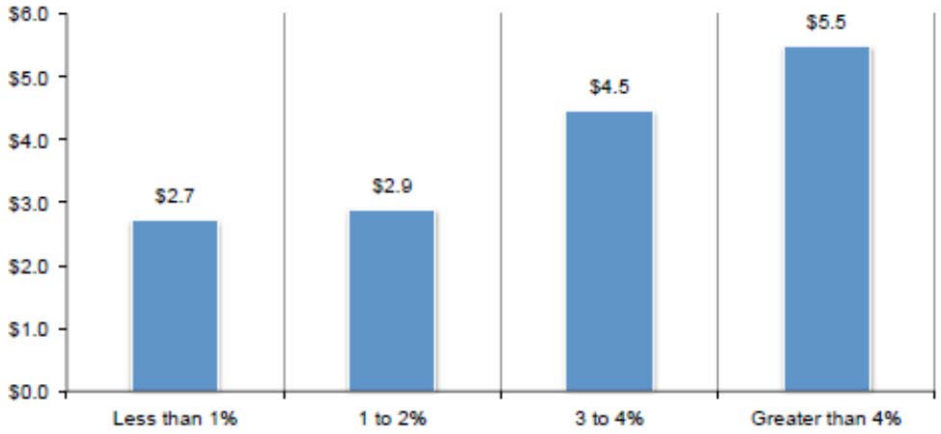
Slika 8.7: Uticaj različitih faktora na trošak gubitka pojedinačnog podatka

Kao što se iz prethodnog izlaganja već može zaključiti, rezultati analize pokazuju da postoji direktna veza između ukupnog troška gubitka podataka i količine pojedinačnih podataka koji su kompromitovani, tj. izgubljeni. Raspodela troškova gubitka podataka, u odnosu na količinu pojedinačnih izgubljenih podataka prikazana je na slici 8.8 (ukupni trošak je prikazan u milionima $).



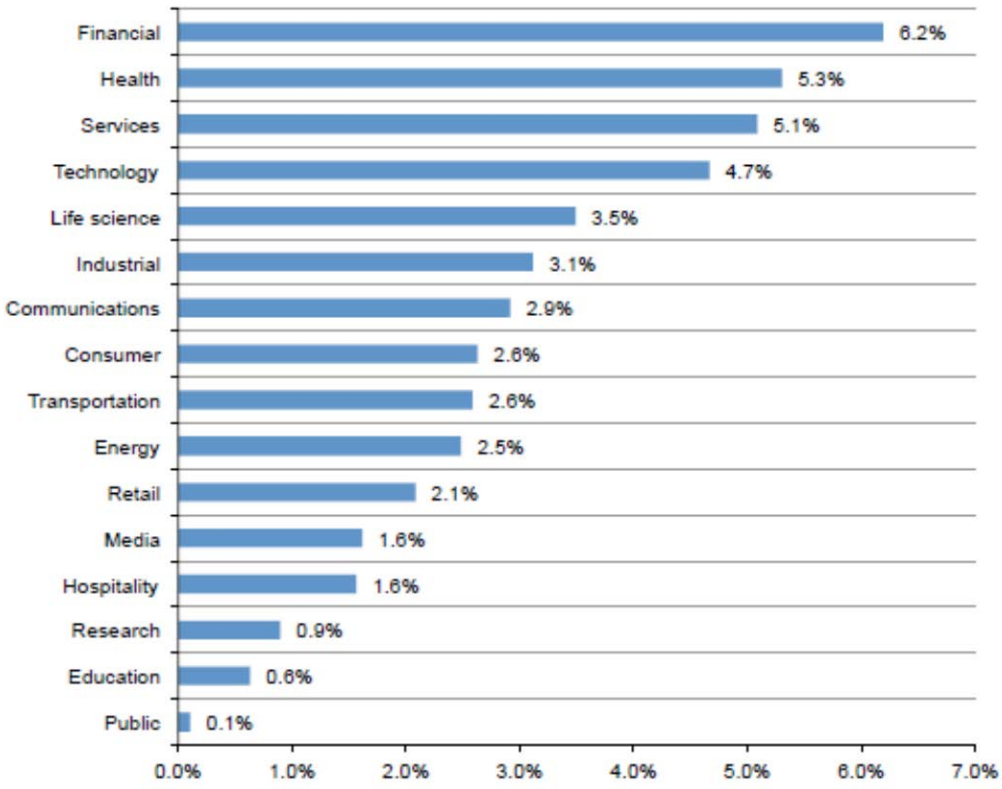
Slika 8.8: Raspodela troškova gubitka podataka (u milionima $)
u odnosu na količinu izgubljenih podataka

Gubitak podataka rezultira u gubitku poverenja klijenata, što povećava trošak gubitka podataka. Raspodela troškova gubitka podataka (u milionima $), u odnosu na procenat gubitka klijenata, koji je posledica ovog tipa bezbednosnog incidenta prikazana je na slici 8.9.



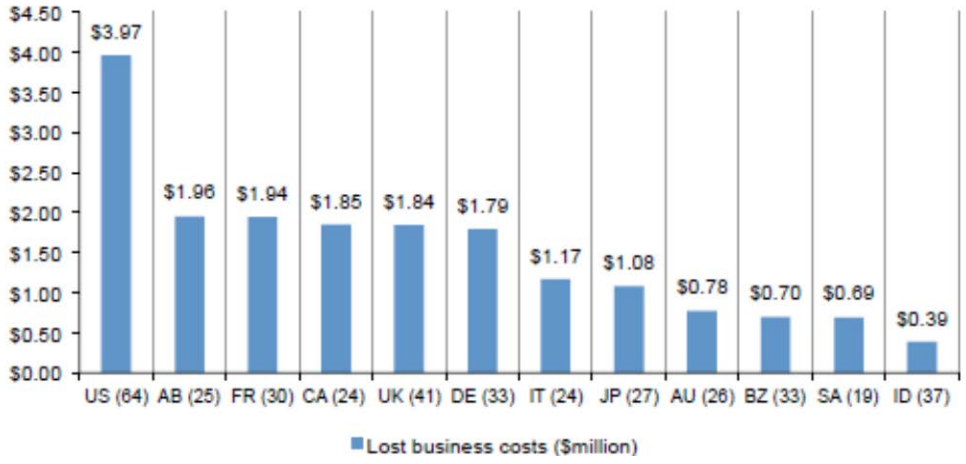
Slika 8.9: Raspodela troškova gubitka podataka (u milionima $)
u odnosu na procenat gubitka klijenata

Kao što je već pomenuto, pojedine oblasti poslovanja su osetljivije na ovaj tip incidenata. Raspodela procentualnog gubitka klijenata po oblastima poslovanja prikazana je na slici 8.10.



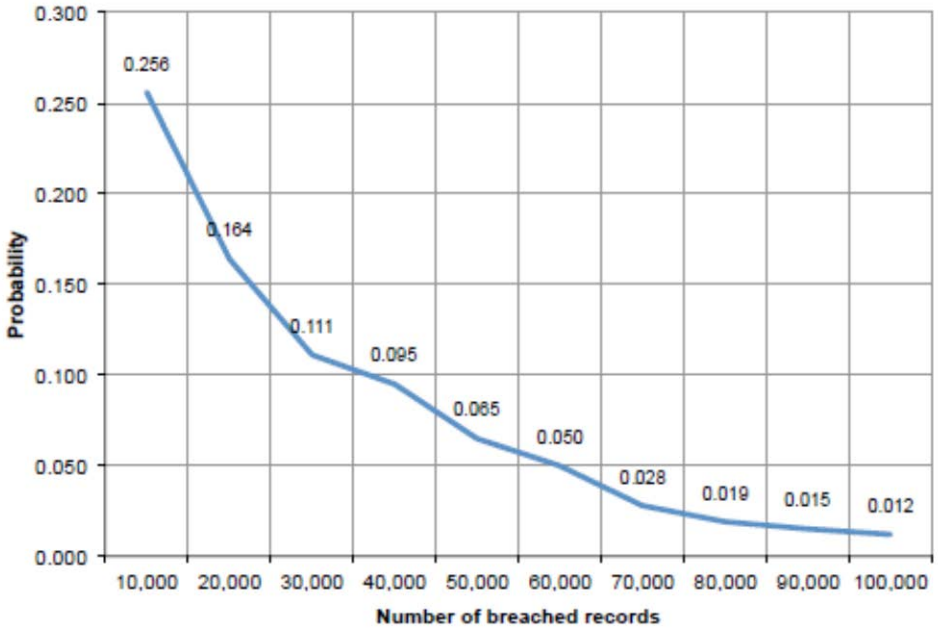
Slika 8.10: Raspodela procentualnog gubitka klijenata po oblastima poslovanja

Komponenta troška gubitka podataka (u milionima $), koja se odnosi na propuštene poslovne prilike koje su posledica ovog tipa bezbednosnog incidenta, po zemljama koje su obuhvaćene istraživanjem, prikazana je na slici 8.11.



Slika 8.11: Komponenta troška koja se odnosi na propuštene poslovne prilike (u milionima $)

Jedan od ciljeva istraživanja bio je i da se utvrdi (na bazi subjektivnog osećaja ispitanika) kolika je verovatnoća pojavljivanja bezbednosnog incidenta gubitka podataka u naredna 24 meseca. Na slici 8.12 prikazana je verovatnoća pojavljivanja incidenta gubitka podataka, u odnosu na količinu izgubljenih podataka. Sa slike 8.12 se vidi da ta verovatnoća opada sa porastom razmera incidenta, ali je izuzetno velika za incidente manjih razmera (oko 26%).



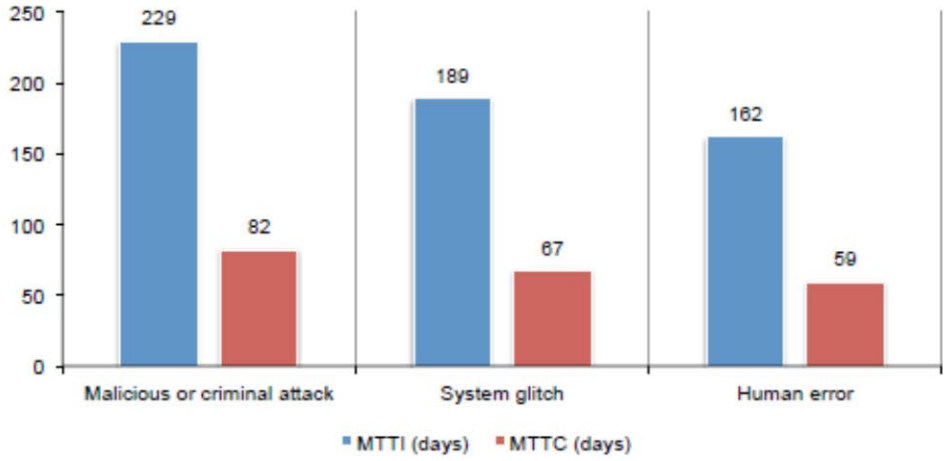
Slika 8.12: Verovatnoća pojavljivanja incidenta gubitka podataka u odnosu na količinu izgubljenih podataka

U ranijem izlaganju na temu izračunavanja *ROI* za CERT organizacije, više puta je napomenuto da je glavni dobitak u postojanju ovakvih organizacija u skraćivanju vremena otkrivanja i razrešenja bezbednosnih incidenata. U tom smislu, u okviru navedene studije, ispitani su uticaji dva parametra na troškove incidenta gubitka podataka: srednje vreme otkrivanja incidenta (MTTI – *Mean Time to Identify*), i srednje vreme razrešenja incidenta (MTTC – *Mean Time to Contain*). MTTI pomaže organizacijama da predvide vreme koje je

potrebno da se otkrije bezbednosni incident gubitka podataka, a MTTC predstavlja vreme koje je potrebno da se ovakav incident razreši, i odliv podataka prekine.

Prema rezultatima navedene studije, na bazi uzorka od 383 kompanije koje su bile predmet istraživanja, procenjeni MTTI je iznosio oko 201 dan, tj. kretao se u rasponu od 20 do 569 dana, a procenjeni MTTC je iznosio oko 70 dana, tj. kretao se u rasponu od 11 do 126 dana.

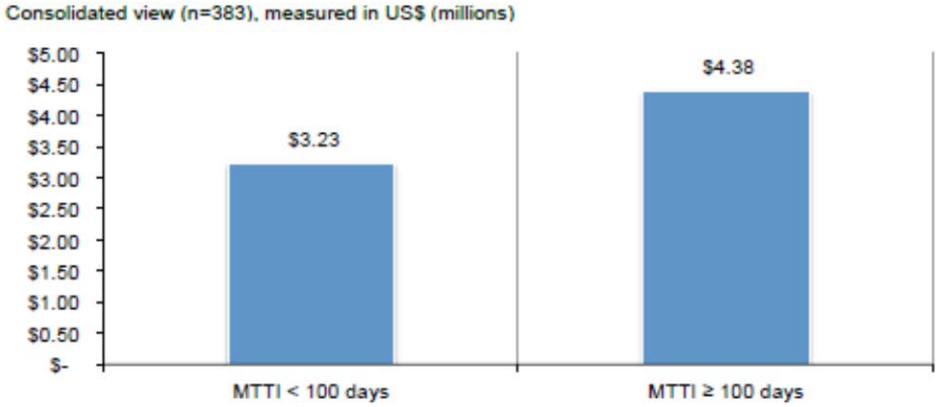
Na slici 8.13 prikazana je raspodela MTTI i MTTC u odnosu na uzrok bezbednosnog incidenta gubitka podataka, koja jasno ukazuje na potrebu postojanja bezbednosnih struktura, tj. CERT organizacija, koje se bave sprečavanjem malicioznih napada, i razrešavanjem bezbednosnih incidenata.



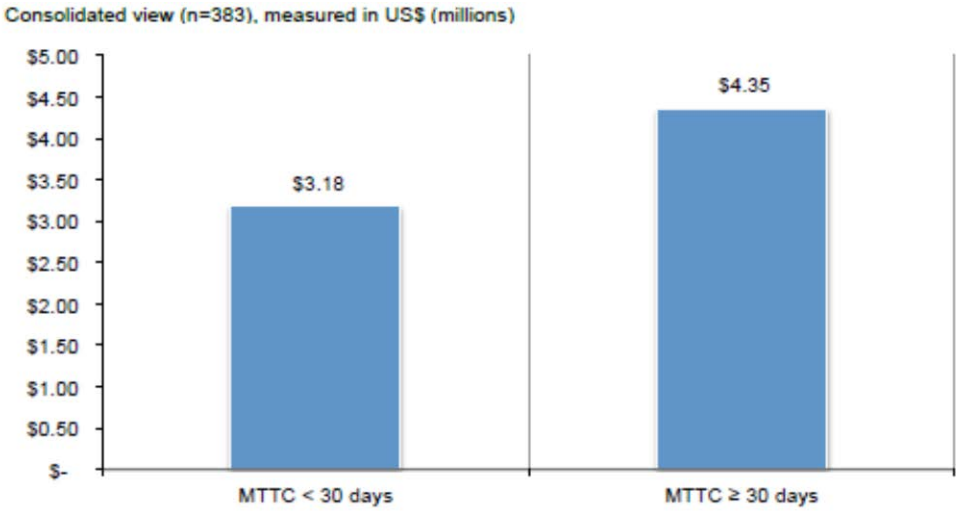
Slika 8.13: Raspodela MTTI i MTTC u odnosu na uzrok bezbednosnog incidenta gubitka podataka

Na slici 8.14 prikazana je međuzavisnost ukupnog troška bezbednosnog incidenta gubitka podataka i MTTI parametra. Ova međuzavisnot ukazuje na to da neuspeh u brzom otkrivanju gubitka podataka dovodi do povećanja troškova ovog bezbednosnog incidenta, a samim tim potvrđuje potrebu za postojanjem CERT organizacija koje ovo vreme, a samim tim i troškove, smanjuju.

Slično ovome, na slici 8.15 prikazana je međuzavisnost ukupnog troška bezbednosnog incidenta gubitka podataka i MTTC parametra, koja ukazuje da neuspeh u brzom razrešenju ovakvih bezbednosnih incidenata, takođe, dovodi do povećanja troškova incidenata.



Slika 8.14: Međuzavisnost ukupnog troška bezbednosnog incidenta gubitka podataka i MTTI parametra (u milionima $)



Slika 8.15: Međuzavisnost ukupnog troška bezbednosnog incidenta gubitka podataka i MTTC parametra (u milionima $)

8.3.5 Zaključak

Kao što se iz prethodnog izlaganja može zaključiti, izračunavanje povraćaja investicije u informacionu bezbednost, čiji je jedan segment i investicija u formiranje CERT tima, je izuzetno složen problem. Postoje dva osnovna razloga za ovo: 1) investicija u informacionu bezbednost sama po sebi ne donosi dobit, i 2) kalkulacija troškova bezbednosnih incidenata je složen proces koji je često podložan i „subjektivnim“ procenama. Zapravo, pojam „dobiti“ se u ovom kontekstu odnosi na sprečavanje, tj. smanjenje finansijskih gubitaka, kroz proces zaštite informacione bezbednosti.

Čak i kada su u pitanju CERT organizacije koje su posvećene bezbednosti neke konkretne poslovne organizacije, sa konkretnim zadacima i relativno merljivim učinkom, teško je govoriti o egzaktnoj proceni povraćaja investicije u takve CERT timove.

Još je teže baviti se ovom analizom kada su u pitanju nacionalne CERT organizacije, s obzirom na njihovu prirodu, tj. njihovu ulogu i opis njihovih poslova. Statistički podaci i procene, koje proističu iz raznih istraživanja i studija, definitivno ukazuju na postojanje korelacije između postojanja bezbednosnih mehanizama, gde značajnu ulogu imaju i nacionalne CERT organizacije, i smanjenja troškova koji su posledica bezbednosnih incidenata. Međutim, teško je na bazi takvih podataka dati konkretnu kvantitativnu procenu povraćaja investicije u nacionalnu CERT organizaciju.

Međutim, ono što definitivno može dati konkretniji odgovor na ovo pitanje, jesu podaci i iskustvo koje će sama Nacionalna CERT organizacija, koja je predmet ove studije, steći tokom vremena. S obzirom da je Nacionalni CERT „sabirni centar“ za podatke o bezbednosnim incidentima na svojoj teritoriji, posle određenog perioda rada (od nekoliko godina), na bazi istorijskih podataka o bezbednosnim incidentima i njihovim posledicama, Nacionalni CERT će biti u prilici da proceni efekte svoga delovanja među konstituentima kojima pruža svoje servise. Naravno, to će biti i prilika za osnivača Nacionalne CERT organizacije da proceni isplativost ove investicije.

Svakako, još jedan teško merljiv, ali nesporno bitan doprinos Nacionalnih CERT organizacija, jeste u njihovoj ulozi u edukaciji i podizanju šire društvene svesti o važnosti zaštite informacione bezbednosti, što je jedan od bitnih motiva uspostavljanja ovakvih organizacija.

9. AKCIONI PLAN ZA USPOSTAVLJANJE NACIONALNOG CERT-A

Akcioni plan za uspostavljanje Nacionalnog CERT-a obuhvata skup tema, aktivnosti i ciljeva na uspostavljanju operativne i efikasne Nacionalne CERT organizacije, koja će biti u stanju da ispuni svoje obaveze, u skladu sa odredbama Zakona o informacionoj bezbednosti Republike Srbije, i generalnim očekivanjima koja se postavljaju pred ovakve organizacije.

Akcionim planom, koji je predstavljen u tabeli 9.1, predviđeni su i vremenski okviri za aktivnosti koje je neophodno sprovesti u cilju uspostavljanja Nacionalnog CERT-a. Pri tome, s obzirom na obim aktivnosti u prvoj godini rada na ovom zadatku, skup aktivnosti i ciljeva tokom prve godine je grupisan po kvartalima. Po isteku prve godine, očekuje se početak operativnog delovanja Nacionalne CERT organizacije. Nakon toga, predviđen je ulazak u nešto stabilniji period rada, sa ograničenim skupom aktivnosti koje se sprovode, pa je i vremenski plan aktivnosti od početka druge godine, pa do kraja pete godine, predstavljen na godišnjem nivou.

Akcioni plan definiše i učesnike koji doprinose sprovođenju aktivnosti i postizanju ciljeva koji su predmet akcionog plana za uspostavljanje Nacionalnog CERT-a. To je, pre svega, agencija RATEL, kao krovna organizacija, čija je zakonska obaveza da formira Nacionalnu CERT organizaciju, i obezbedi podršku odgovarajućih službi (u tabeli 9.1 predstavljeni kao „podrška“), u okvirima organizacionog modela o kojem je bilo reči u glavi 6. Takođe, svoju ulogu u formiranju Nacionalnog CERT-a, ali i definisanju njegovih aktivnosti, obaveza i ovlašćenja, ima i Ministarstvo trgovine, turizma i telekomunikacija (u tabeli 9.1 predstavljeno kao „MTTT“) koje po odredbama Zakona o informacionoj bezbednosti ima ulogu Nadležnog organa. Kao takvo, ono treba da vrši nadzor nad radom Nacionalnog CERT-a u vršenju poslova poverenih Zakonom. Naravno, najveći teret aktivnosti iz ovog akcionog plana na sebe će preuzeti direktor Nacionalne CERT organizacije, kao i sami članovi CERT organizacije, tj. inženjeri iz njenog tehničkog dela (u tabeli 9.1 predstavljeni kao „CERT tim“), uz pomoć saradnika za marketing i komunikacije (u tabeli 9.1 predstavljeni kao „marketing“).

Iako među učesnicima u sprovođenju ovog akcionog plana nisu predstavljeni kao poseban entitet, važnu ulogu u stvaranju i efikasnom radu Nacionalne CERT organizacije imaju i konstituenti, tj. korisnici njenih servisa, bez čijeg angažovanja i saradnje funkcionisanje bilo koje CERT organizacije, pa ni Nacionalnog CERT-a nije moguće.

Što se tiče materijalnih resursa, tj. budžeta za sprovođenje aktivnosti na uspostavljanju Nacionalnog CERT-a, ti detalji su već predstavljeni u prethodnim glavama, i o njima neće ponovo biti reči u tabeli akcionog plana.

Tabela 9.1: Akcioni plan za uspostavljanje Nacionalnog CERT-a

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
1	Donošenje odluke i akata o formiranju nacionalne CERT organizacije.	1. kvartal	RATEL
2	Imenovanje direktora i odabir poslovnog sekretara.	1. kvartal	RATEL
3	Definisanje poslovne podrške za potrebe CERT tima u okviru krovne organizacije.	1. kvartal	RATEL i Direktor CERT-a
4	Definisanje misije, nadležnosti i ovlašćenja nacionalne CERT organizacije.	1. kvartal	RATEL i Direktor CERT-a
5	Definisanje konstituenata nacionalne CERT organizacije.	1. kvartal	RATEL i Direktor CERT-a
6	Definisanje odnosa sa Nadležnim organom (MTTT).	1. kvartal	RATEL, Direktor CERT-a, MTTT
7	Donošenje odluke o načinu finansiranja.	1. kvartal	RATEL i Direktor CERT-a
8	Odabir i uređenje poslovnog prostora.	1. kvartal	RATEL i Direktor CERT-a
9	Odabir lokacije *data* centra.	1. kvartal	Direktor CERT-a
10	Definisanje kriterijuma za radna mesta u tehničkom delu organizacije.	1. kvartal	Direktor CERT-a
11	Uvođenje poslovne podrške iz krovne organizacije (ekonomista, pravnik) u nova zaduženja u vezi sa CERT-om.	1. kvartal	RATEL i Direktor CERT-a
12	Pokretanje konkursa za zapošljavanje i prijem inženjera (2 operativna inženjera i 1 inženjer analitičar).	1. kvartal	RATEL i Direktor CERT-a
13	Odabir i nabavka računarske opreme za potrebe zaposlenih.	2. kvartal	CERT tim + podrška
14	Odabir i nabavka opreme za infrastrukturno opremanje poslovnog prostora (LAN mreža, fiksna i mobilna telefonija ...).	2. kvartal	CERT tim + podrška
15	Odabir i nabavka opreme za infrastrukturno opremanje *data* centra (DMZ mreža, Internet ruteri, DMZ serveri (DNS, WEB, email, NTP...)).	2. kvartal	CERT tim + podrška
16	Nabavka linkova za povezivanje sa *data* centrom.	2. kvartal	CERT tim + podrška
17	Nabavka Internet linkova na lokaciji *data* centra.	2. kvartal	CERT tim + podrška

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
18	Uspostavljanje kontakta sa LIR-om (*Local Internet Registry*) radi dodele ASN-a (*Autonomous System Number*) i IP adresnog prostora za potrebe CERT organizacije.	2. kvartal	CERT tim
19	Infrastrukturno opremanje poslovnog prostora (instalacija opreme po isporuci).	2. kvartal	CERT tim
20	Infrastrukturno opremanje *data* centra (instalacija opreme po isporuci).	2. kvartal	CERT tim
21	Podizanje svih infrastrukturnih servisa (LAN, DMZ, WAN, Internet) - CERT organizacija je vidljiva na mreži i sposobna za različite vidove komunikacije.	2. kvartal	CERT tim
22	Uspostavljanje kontakta sa međunarodnim organizacijama (ENISA, FIRST, TF CSIRT), predstavljanje tima i budućih namera u izgradnji nacionalne CERT organizacije.	3. kvartal	CERT tim
23	Ispitivanje mogućnosti i procedura prijema u članstvo međunarodnih organizacija.	3. kvartal	CERT tim
24	Zahtev ENISA-i za pomoć u procesu uspostavljanja Nacionalnog CERT-a.	3. kvartal	CERT tim
25	Posete drugim nacionalnim CERT organizacijama radi sklapanja poznanstava i prikupljanja iskustava.	3. kvartal	CERT tim
26	Evaluacija različitih sistema za evidenciju i upravljanje incidentima.	3. kvartal	CERT tim
27	Evaluacija eksternih izvora informacija o bezbednosnim incidentima radi eventualne pretplate na neki od dostupnih servisa za obaveštavanje.	3. kvartal	CERT tim
28	Inicijalna obuka članova CERT tima (npr. TRANSITS I kurs).	3. kvartal	CERT tim
29	Definisanje osnovnih servisa koji će se pružati konstituentima.	3. kvartal	CERT tim
30	Definisanje osnovnih politika, procesa i procedura u funkcionisanju CERT organizacije.	3. kvartal	CERT tim

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
31	Inicijalni sastanci sa važnijim konstituentima radi upoznavanja i upućivanja u servise nacionalne CERT organizacije i modele i načine buduće saradnje i komunikacije.	3. kvartal	CERT tim
32	Odabir sistema za evidenciju i upravljanje incidentima, nabavka odgovarajućeg hardvera i softvera.	4. kvartal	CERT tim + podrška
33	Nabavka linkova za povezivanje sa MTTT.	4. kvartal	CERT tim + podrška
34	Instalacija svih sistema za upravljanje incidentima, uz omogućavanje pristupa MTTT-u.	4. kvartal	CERT tim
35	Nabavka eksternih izvora informacija o bezbednosnim incidentima radi eventualne pretplate na neki od dostupnih servisa za obaveštavanje.	4. kvartal	CERT tim
36	Obuka osoblja CERT tima i MTTT-a za rad sistemu za evidenciju i upravljanje incidentima.	4. kvartal	CERT tim
37	Odabir pilot konstituenata kojima se servis pruža u testnom režimu.	4. kvartal	CERT tim
38	Testiranje svih procesa, procedura i IT sistema na primeru saradnje sa pilot konstituentima.	4. kvartal	CERT tim
39	Testiranje procesa saradnje sa međunarodnim organizacijama i drugim CERT timovima na razmeni informacija i razrešavanju bezbednosnih incidenata.	4. kvartal	CERT tim
40	Učešće na domaćim i međunarodnim skupovima na kojima se promoviše uspostavljanje novog Nacionalnog CERT tima.	4. kvartal	CERT tim
41	Početak operativnog rada sa konstituentima.	2. godina	CERT tim
42	Članstvo u međunarodnim organizacijama i saradnja sa nacionalnim CERT-ovima drugih zemalja u razrešenju incidenata.	2. godina	CERT tim
43	Prijem novih članova CERT tima (još 2 operativna inženjera i 1 inženjer analitičar).	2. godina	RATEL, Direktor CERT-a + podrška

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
44	Prelazak u režim radnog vremena 24/7 uz pasivno dežurstvo u noćnoj/trećoj smeni.	2. godina	CERT tim
45	Prijem stručnjaka za marketing i komunikacije, radi promovisanja aktivnosti Nacionalne CERT organizacije i odnosa sa javnošću.	2. godina	RATEL, Direktor CERT-a + podrška
46	Inicijalna obuka (interna i eksterna) novih članova CERT tima, upoznavanje sa politikama, procesima i procedurama organizacije.	2. godina	CERT tim
47	Napredniji nivo obuke za stare članove tima, na temu analize ranjivosti sistema, analize artefakata, i opštih poslova informacione bezbednosti. Sticanje sertifikata.	2. godina	CERT tim
48	Aktivno učešće na domaćim i javnim skupovima.	2. godina	CERT tim + marketing
49	Dodavanje novih servisa obaveštavanja i alarmiranja.	2. godina	CERT tim
50	Evaluacija alata za analizu ranjivosti sistema, i analizu artefakata.	2. godina	CERT tim
51	Nastavak aktivnosti na detaljnom dokumentovanju svih servisa, politika, procesa i procedura u okviru CERT organizacije.	2. godina	CERT tim + podrška
52	Ulaganje napora na postizanje konzistentnosti i dobrih rezultata u radu CERT tima.	2. godina	CERT tim
53	Nastavak operativnog rada sa konstituentima.	3. godina	CERT tim
54	Proširenje saradnje sa međunarodnim organizacijama i nacionalnim CERT-ovima drugih zemalja u razrešenju incidenata.	3. godina	CERT tim
55	Prijem novih članova CERT tima (još 1 operativni inženjer i 1 inženjer analitičar).	3. godina	RATEL, Direktor CERT-a + podrška
56	Inicijalna obuka (interna i eksterna) novih članova CERT tima, upoznavanje sa politikama, procesima i procedurama organizacije.	3. godina	CERT tim
57	Napredniji nivo obuke za stare članove tima, na temu analize ranjivosti sistema, analize artefakata, i opštih poslova informacione bezbednosti. Sticanje sertifikata.	3. godina	CERT tim

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
58	Aktivno učešće na domaćim i javnim skupovima.	3. godina	CERT tim + marketing
59	Dodavanje novih servisa obaveštavanja i alarmiranja.	3. godina	CERT tim
60	Primena alata za analizu ranjivosti sistema, i analizu artefakata.	3. godina	CERT tim
61	Nastavak aktivnosti na detaljnom dokumentovanju svih servisa, politika, procesa i procedura u okviru CERT organizacije radi procesa akreditacije.	3. godina	CERT tim + marketing + podrška
62	Proces akreditacije kod međunarodnih organizacija.	3. godina	CERT tim + marketing + podrška
63	Nastavak operativnog rada sa konstituentima.	4. godina	CERT tim
64	Proširenje saradnje sa međunarodnim organizacijama i nacionalnim CERT-ovima drugih zemalja u razrešenju incidenata.	4. godina	CERT tim
65	Prijem novih članova CERT tima (još 3 operativna inženjera).	4. godina	RATEL, Direktor CERT-a + podrška
66	Inicijalna obuka (interna i eksterna) novih članova CERT tima, upoznavanje sa politikama, procesima i procedurama organizacije.	4. godina	CERT tim
67	Napredniji nivo obuke za stare članove tima, na temu analize ranjivosti sistema, analize artefakata, i opštih poslova informacione bezbednosti. Sticanje sertifikata.	4. godina	CERT tim
68	Aktivno učešće na domaćim i javnim skupovima.	4. godina	CERT tim + marketing
69	Nastavak aktivnosti na detaljnom dokumentovanju svih servisa, politika, procesa i procedura u okviru CERT organizacije radi pripreme procesa sertifikacije.	4. godina	CERT tim + marketing + podrška
70	Prelazak u potpuni režim rada 24/7.	4. godina	CERT tim + marketing
71	Nastavak operativnog rada sa konstituentima.	5. godina	CERT tim
72	Proširenje saradnje sa međunarodnim organizacijama i nacionalnim CERT-ovima drugih zemalja u razrešenju incidenata.	5. godina	CERT tim

REDNI BROJ	TEMA-AKTIVNOST-CILJ	VREMENSKI OKVIR	SPROVODI
73	Napredniji nivo obuke za stare članove tima, na temu analize ranjivosti sistema, analize artefakata, i opštih poslova informacione bezbednosti. Sticanje sertifikata.	5. godina	CERT tim
74	Kreiranje portfolija servisa koji bi bili pružani na komercijalnim osnovama.	5. godina	CERT tim + marketing + podrška
75	Aktivno učešće na domaćim i javnim skupovima.	5. godina	CERT tim + marketing
76	Nastavak aktivnosti na detaljnom dokumentovanju svih servisa, politika, procesa i procedura u okviru CERT organizacije radi pripreme procesa sertifikacije.	5. godina	CERT tim + marketing + podrška
77	Proces sertifikacije kod međunarodnih organizacija.	5. godina	CERT tim + marketing + podrška

10. PREGLED POTENCIJALNIH MODALITETA FINANSIRANJA PROJEKTA IZGRADNJE NACIONALNOG CENTRA ZA PREVENCIJU RIZIKA U INFORMACIONO-KOMUNIKACIONIM TEHNOLOGIJAMA

Početkom 2016. godine Srbija je usvojila Zakon o informacionoj bezbednosti, koji, uz postojeći zakonski okvir koji implementira odredbe Konvencije iz Budimpešte Saveta Evrope o borbi protiv sajber-kriminala, uspostavlja osnovni pravni okvir u ovoj oblasti. Usvajanje Zakona o informacionoj bezbednosti predviđeno je i u okviru pristupnih pregovora Srbije sa EU, Nacionalnim programom za usvajanje pravnih tekovina Evropske unije (NPAA) od 2014-2018 godine, ali i Strategijom razvoja informacionog društva u Republici Srbiji do 2020. godine.

Sam po sebi, usvojeni Zakon je važan korak za Srbiju, a izgradnja Nacionalnog CERT-a predstavlja jedan od njegovih najvažnijih aktivnosti u praćenju nacionalnih i međunarodnih koraka u prevenciji rizika u IK tehnologijama.

Učešće na međunarodnoj sceni svakoj državi, osim međunarodnih obaveza, donosi i određene mogućnosti. U tom smislu, Srbija, kao zemlja kandidat za članstvo u Evropskoj uniji ima pristup nekim fondovima koji se efikasno mogu koristiti, kako u inicijalnoj fazi izgradnje tako i u narednim fazama operativnog rada Nacionalnog CERT-a.

U nastavku će biti opisane najvažnije mogućnosti korišćenja evropskih fondova od značaja za razmatrani Projekat izgradnje Nacionalnog CERT-a.

10.1 PREGLED TIPOVA MEĐUNARODNE FINANSIJSKE POMOĆI U RELEVANTNOJ OBLASTI PREVENCIJE RIZIKA

Međunarodna zajednica počela je da pruža pomoć Republici Srbiji u većoj meri krajem 2000. godine. U inicijalnoj fazi donatorska pomoć je imala humanitarni karakter, ali je od 2003. godine poprimila karakter razvojne pomoći za podršku strukturnim/pravnim reformama, kao i za izgradnju administrativnih i institucionalnih kapaciteta. Izraz "međunarodna pomoć" može imati oblik humanitarne pomoći, ali je najčešće termin koji se

odnosi na razvojnu pomoć. Međunarodna pomoć obuhvata podršku bilateralnih i multilateralnih donatora, uz pomoć međunarodnih finansijskih institucija (MFI). Podrška MFI uglavnom se obezbeđuje u vidu bespovratnih sredstava i koncesionih (tzv. "mekih") zajmova sa određenim povoljnostima.

Za odgovarajući projekat za koji se traži finansijska podrška, svakako je od interesa da se ostvari pomoć u vidu bespovratnih sredstava, ali treba uzeti u obzir da preduslovi koje treba ispuniti poseduju specifičan karakter u zavisnosti od razvojnog programa.

Za projekat koji pretenduje da dobije bespovratnu međunarodnu pomoć bitno je da u samom inicijalnom strateškom dizajnu i kreiranju predloga pokaže dobre izglede da će moći da zadovolji svih pet kriterijuma ocene potencijala projekta za razvojnu pomoć u koje spadaju:

(i) relevantnost,
(ii) delotvornost,
(iii) efikasnost,
(iv) uticaj na odgovarajući razmatrani sektor i definisani domen, i
(v) kao najvažniji kriterijum - održivost.

Posebno je važno naglasiti da trendovi međunarodne pomoći postaju usmereni ka podršci strukturnim reformama i održivom društveno-ekonomskom razvoju. Dodatno, očekuje se da će se ukupan iznos međunarodne pomoći smanjivati, a da će najveći izvori bespovratne pomoći predstavljati projekti koji uključuju prekograničnu saradnju, saradnju zemalja Zapadnog Balkana i sl.

Sa aspekta domena prevencije rizika u domenu IKT, Republika Srbija se kao i ostale zemlje Zapadnog Balkana, prvenstveno oslanja na regulativu, aktivnosti, standarde i preporuke Evropske Unije, što ujedno predstavlja i deo procesa pridruživanja.

Dodatno, zemljama Zapadnog Balkana u domenu bezbednosti informacija i prevencije od rizika u IKTu značajnu pomoć pružaju i sledeće međunarodne institucije:

- Savet Evrope **CoE** (*Council of Europe*),
- Organizacija za pružanje sigurnosti i saradnje u Evropi O**SE** (*Organisation for Security and Cooperation in Europe*),
- Program Ujedinjenih nacija za razvoj - **UNDP** (*United Nations Development Programme*),
- Severno-antlantski pakt - **NATO** (*North Atlantic Treaty Organisation*), i
- Međunarodna unija za telekomunikacije - **ITU** (*International Telecommunication Union).*

Svaka od ovih međunarodnih oranizacija posvećena je nekom svom specifičnom cilju, ali postoji i puno zajedničkih aspekata zaštite informacija i prevencije od rizika u IKT tehnologijama u kojima se ove organizacije preklapaju.

U tom smislu, Srbija, kao zemlja kandidat za članstvo u Evropskoj uniji ima pristup mnogim fondovima EU o kojima će u nastavku biti reči. Osim toga, Evropska unija pruža i mogućnosti korišćenja resursa iz drugih instrumenata i programa kroz koje zemlja korisnik može da obezbedi podršku za razvoj informacione bezbednosti u smislu razvoja CERTova i nacionalnih strategija informacione bezbednosti, kao i podizanja svesti u društvu o ovom pitanju.

Dodatno, Srbija ima pristup resursima koje pruža NATO program Nauka za mir i bezbednosti mogućnost korišćenja podrške Alijanse kroz formiranje konkretnih ciljeva saradnje u okviru Individualnog akcionog plana partnerstva koji se usaglašava na dve godine. Osim toga, Srbija ima pristup i programima u okviru NATO koncepta Pametne odbrane, koji su usmereni na oblast sajber odbrane.

Takođe, Srbija je i članica Međunarodne unije za telekomunikacije koja, u saradnji sa Međunarodnim multilateralnim partnerstvom protiv sajber pretnji (*International Multilateral Partnership Against Cyber Threats, IMPACT*) pruža podršku zemljama članicama ITUa u aktivnostima poput sprovođenja nacionalne procene i analize rizika u oblasti informacione bezbednosti, razvoja nacionalnih strategija informacione bezbednosti i uspostavljanja nacionalnih CERTova. RATEL Agencija je već bila uključena u ovakav proram u razmenama znanja.

U nastavku će biti predstavljen pregled najvažnijih fondova EU, a kojima je u osnovi strateški cilj podizanja nivoa bezbednosti u sajber prostoru i prevencija rizika u IKT tehnologijama na globalnom nivoa, i koji bi potencijalno mogli predstavljati projekte ili fondove kojima bi se izgradnja Nacionalnog CERT-a Republike Srbije mogla pridružiti.

10.2 INSTRUMENTI FINANSIJSKE POMOĆI EVROPSKE UNIJE I SAVETA EVROPE

Učešće na međunarodnoj sceni svakoj državi, osim međunarodnih obaveza, donosi i određene mogućnosti. U tom smislu, Srbija, kao zemlja kandidat za članstvo u Evropskoj uniji ima pristup nekim fondovima EU od kojih su najvažniji **fond za istraživanje i inovacije Horizont 2020**, **kao i Instrument za predpristupnu pomoć (IPA II instrument**). Osim toga, Evropska unija pruža i mogućnosti korišćenja resursa iz drugih instrumenata i programa kroz koje zemlja korisnik može da obezbedi podršku za razvoj informacione bezbednosti u smislu razvoja CERTova i nacionalnih strategija informacione bezbednosti, kao i podizanja svesti u društvu o ovom pitanju.

10.2.1 IPA II FOND (*Instrument for Pre-Accession Assistance*)

IPA FOND (*Instrument for Pre-Accession Assistance*) je instrument za pretpristupnu pomoć koji je namenjen pružanju podrške zemljama kandidatima, kao i potencijalnim kandidatima za članstvo u EU.

Prioriteti ovog programa su pružanje pomoći zemljama korisnika u ispunjavanju političkih, ekonomskih i drugih kriterijuma koji se odnose na usvajanje pravnih tekovina EU, izgradnju administrativnih kapaciteta i jačanje pravosuđa, kao i pomoć zemljama u procesu priprema za korišćenje strukturnih i kohezionih fondova EU nakon pristupanja Evropskoj uniji.

Pomoć treba da pruži podršku zemljama kandidatima, kao i potencijalnim kandidatima, u njihovim naporima jačanja demokratskih institucija i vladavine prava, reformi državne uprave, reformi privrede, poštovanju ljudskih i manjinskih prava, promociji jednakosti

između polova, jačanju civilnog društva, unapređenju regionalne saradnje, dostizanju održivog razvoja.

Sredstva iz IPA se mogu koristiti u osnovi na četiri načina:

- Kao **„tehnička pomoć“,** što obično uključuje angažovanje eksperata, konsultanata, koji onda pružaju usluge našim institucijama.
- Kroz **„tvining“** (*twinning*), što znači uparivanje, kada se jedna domaća institucija, npr. Odeljenje za zaštitu potrošača poveže sa institucijom sličnog tipa iz neke od država članica Evropske unije, i sprovodi projekat zajedno sa njom koji se tiče prenošenja znanja, iskustava, pružanja pomoći na usklađivanju propisa, itd.
- Kao **„investicioni projekti“,** koji uglavnom uključuju nabavku opreme, izvođenje radova, sprovođenje finansijskih aranžmana sa drugim finansijskim institucijama. Da bi se usvojio ovakav jedan projekat, neophodno je pripremiti odgovarajuću projektnu dokumentaciju, npr. studiju izvodljivosti, finansijske i ekonomske analize, procenu uticaja na životnu sredinu, dozvole, itd.
- Kao **„grantovi“,** koji predstavljaju dodelu sredstava za finansiranje posebnih projekata civilnog društva, lokalne samouprave, agencija, itd. Obično funkcionišu tako što se raspiše poziv za prikupljanje projekata, gde ovlašćeni predlagači pripremaju predloge projekata u odgovarajućem formatu.

Najveći i najznačajniji korisnici su vladine institucije, jer one donose i primenjuju najveći deo reformskih zakona i propisa. Samim tim, ovlašćeni predlagači za predlaganje projekata tokom procesa programiranja su ministarstva, posebne organizacije i službe Vlade, Narodna skupština, Narodna banka Srbije. Isto tako, deo sredstava se izdvaja i za lokalnu samoupravu i organizacije civilnog društva, koje su pored Vlade najvažniji akteri i partneri u procesu evropske integracije. Iz tog razloga ovlašćeni predlagači su u obavezi da obezbede koordinaciju i konsultacije u procesu programiranja IPA sa svim zainteresovanim stranama (tzv. princip partnerstva). Što se tiče privatnih preduzeća, iako ne mogu biti predlagači projekata, mogu biti korisnici raznih programa obuke za mala i srednja preduzeća, npr. o tome kako da sprovode donete propise. Ona mogu biti korisnici manjih grantova za ulaganja u oblastima koje su označene kao razvojni cilj u samom predlogu projekta - npr. ulaganja u projekte korišćenja obnovljivih izvora energije, ili tome slično.

Jednom kada zemlja postane članica Evropske nije, ona više neće koristiti IPA sredstva, već sredstva koja se koriste kroz regionalnu politiku EU, a to su strukturni fondovi i kohezioni fond EU. Ta sredstva su po obimu mnogo veća, ali se njihova „implementacija“ isključivo zasniva na principima decentralizovanog sistema upravljanja. U periodu kada je za sve države koje koriste IPA sredstva (2007. – 2013. godine) izdvojeno 11,5 milijardi evra, kroz strukturne fondove i kohezioni fond za države članice izvojeno je oko 350 milijardi evra.

IPA fond u periodu 2007-2013 (IPA I)

IPA fond je inicijalno uspostavljen Uredbom Evropskog saveta br. 1085/2016 od 17. jula 2006. godine i danas je poznatiji kao IPA koja je važila za period od 2007. do 2013.godine.

U inicijalnom trenutku nastajanja IPA je objedinila pet pretpristupnih instrumenata koje su zemlje zapadnog Balkana koristile pre 2007. godine: PHARE, SAPARD, ISPA, CARDS, i pretpristupni instrument za Tursku. U periodu od 2000. do 2006. godine Republika Srbija je koristila sredstva CARDS programa u iznosu od oko 1,2 milijardi evra.

Ukupna finansijska vrednost za sve zemlje korisnice IPA u periodu 2007.-2013. godine iznosila je 11.468 milijardi evra, od čega je za Srbiju zaključno sa 2013. godinom iz IPA fonda izdvojeno približno 1.4 milijarde evra.

IPA II fond u periodu 2014-2020

Nova IPA II regulativa usvojena je uredbom Evropskog parlamenta i Evropskog saveta br. 231/2014 od 11. marta 2014. godine. Ova uredba dopunjena je Uredbom o zajedničkom sprovođenju br. 236/2014, koja predstavlja skup pojednostavljenih i usaglašenih pravila i procedura za sprovođenje svih akcionih instrumenata EU, kao i Uredbom o sprovođenju IPA II br. 447/2014 koju je Evropska komisija usvojila 2. maja 2014. godine. Na taj način, Evropska komisija je uspostavila jedinstveni instriment za predpristupnu pomoć zemljama u procesu evropskih integracija za budžetski period od 2014. do 2020. godine. Zemlje korisnice IPA II fonda u razmatranom periodu su: Albanija, Bosna i Hercegovina, BJR Makedonija, Island, Kosovo (bez naznake zvaničnog priznavanja samostalnosti), Crna Gora, Srbija i Turska.

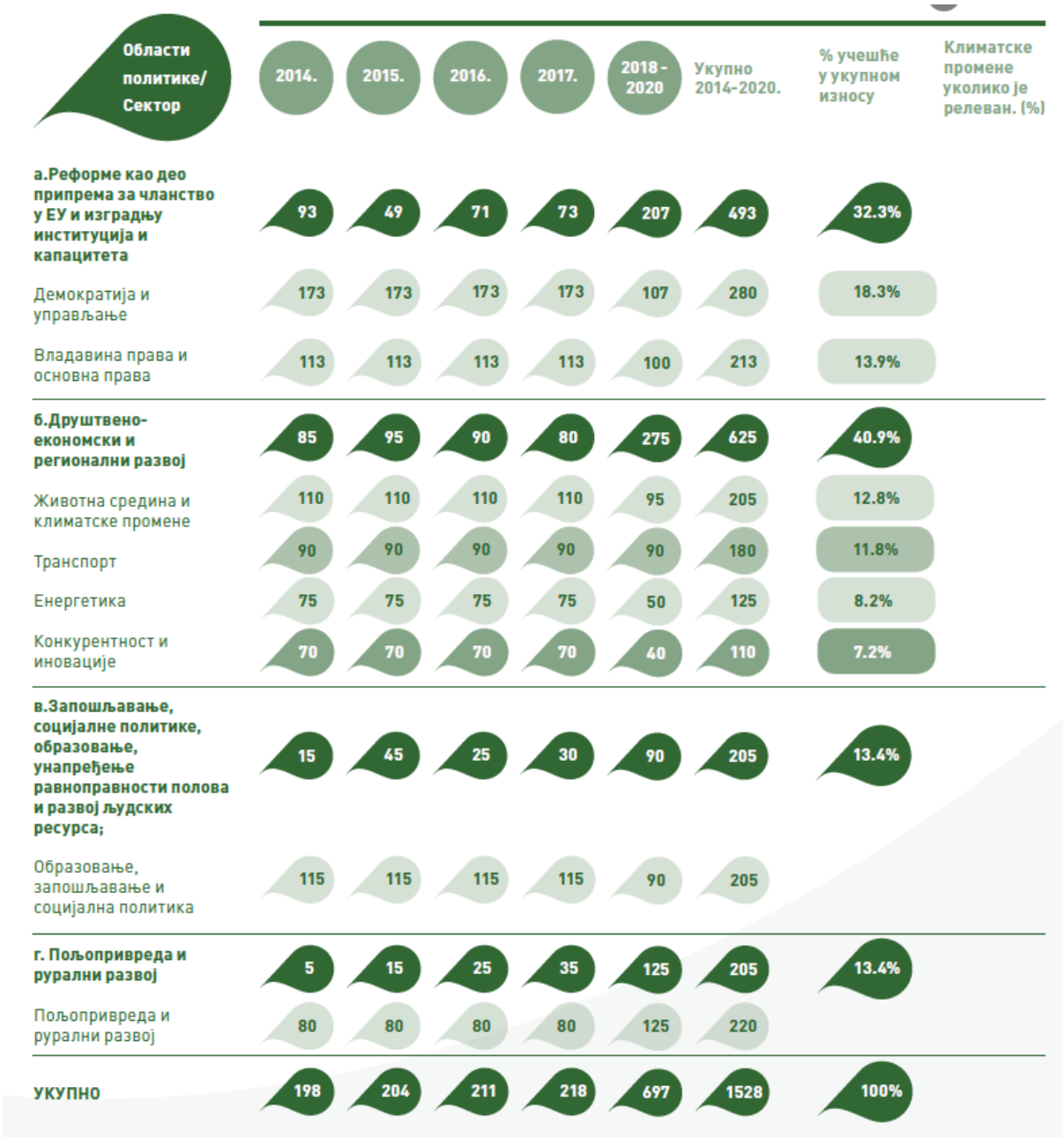
Ukupan budžet IPA za period 2014.-2020. iznosi 11,668 milijardi evra, pri čemu je iznos namenjen za Republiku Srbiju 1,67 milijardi evra. Podrška EU za navedeni period usklađena je sa potrebama procesa pristupanja i strategijom proširenja, a baziraće se na podršci nacionalnim reformskim procesima i pomoći drugih donatora i međunarodnih finansijskih institucija. Na osnovu specifičnih potreba proizišlih iz procesa skrininga u kasnijem toku pregovora, podrška će se suštinski zasnivati na strategijama i akcionim planovima usvojenim u okviru pregovaračkog procesa, iako može biti upotrebljena i za nepredviđene prioritetne potrebe relevantne za pregovore. Kroz IPA će biti nastavljeno kofinansiranje učešća Republike Srbije u programima EU.

U novom budžetskom periodu promenjena je struktura programa IPA II, koji sada umesto pet komponenti koje su bile karakteristične za IPA I sadrži tzv. Oblasti politike (*Policy areas*). Oblasti politike su po sadržaju veoma slične komponentama IPA I. Konkretno, Oblasti politike u okviru IPA II su:

- Reforme kao deo priprema za članstvo u EU i izgradnju institucija i kapaciteta.
- Društveno-ekonomski i regionalni razvoj.
- Zapošljavanje, socijalna politika, obrazovanje, unapređenje ravnopravnosti polova i razvoj ljudskih resursa.
- Poljoprivreda i ruralni razvoj.
- Regionalna i teritorijalna saradnja.

Najvažnija novina koju donosi IPA II instrument jeste strateški fokus na određene segmente investiranja koji se definišu za svaku od zemalja kao nacionalni prioriteti. Promena je proizašla iz shvatanja Evropske komisije i ostalih aktera u procesu primene IPA fondova da dosadašnja praksa finansiranja pojedinačnih projekata usmerenih na zadovoljenje različitih prioriteta nije dala očekivane rezultate. Zbog toga, u procesu planiranja korišćenja sredstava IPA II fondova primenjivaće se sektorski pristup. Na taj način se sredstva pretpristupne pomoći usmeravaju na manji broj strateških sektora, koje zajednički identifikuju EU i zemlje korisnice pomoći.

Slika 10.1 u potpunosti prikazuje raspodelu fonda od ukupno 1,67 milijarde evra namenjenih Republici Srbiji, po prikazanim oblastima politike i odgovarajućim sektorima.



Области политике/ Сектор	2014.	2015.	2016.	2017.	2018 - 2020	Укупно 2014-2020.	% учешће у укупном износу	Климатске промене уколико је релеван. (%)
а.Реформе као део припрема за чланство у ЕУ и изградњу институција и капацитета	93	49	71	73	207	493	32.3%	
Демократија и управљање	173	173	173	173	107	280	18.3%	
Владавина права и основна права	113	113	113	113	100	213	13.9%	
б.Друштвено-економски и регионални развој	85	95	90	80	275	625	40.9%	
Животна средина и климатске промене	110	110	110	110	95	205	12.8%	
Транспорт	90	90	90	90	90	180	11.8%	
Енергетика	75	75	75	75	50	125	8.2%	
Конкурентност и иновације	70	70	70	70	40	110	7.2%	
в.Запошљавање, социјалне политике, образовање, унапређење равноправности полова и развој људских ресурса;	15	45	25	30	90	205	13.4%	
Образовање, запошљавање и социјална политика	115	115	115	115	90	205		
г. Пољопривреда и рурални развој	5	15	25	35	125	205	13.4%	
Пољопривреда и рурални развој	80	80	80	80	125	220		
УКУПНО	198	204	211	218	697	1528	100%	

Slika 10.1 - Indikativna raspodela IPA II fonda za Republiku Srbiju po oblastima politike i relevantnim sektorima

Proces programiranja IPA II pomoći za Projekat izgradnje Nacionalnog CERT-a

Kao kandidat za članstvo u EU, Republika Srbija je od aprila 2014. godine dobila akreditaciju za samostalno korišćenje IPA fondova EU. U cilju efikasnog i efektivnog korišćenja IPA fondova, sve zemlje korisnice, uključujući i Srbiju, imenovale su nacionalne koordinatore za IPA (NIPAC), koji su odgovorni za koordinaciju, planiranje i praćenje pomoći EU u svim IPA komponentama. Poslove Tehničkog sekretarijata nacionalnog

koordinatora za IPA obavlja Kancelarija za evropske integracije (http://www.seio.gov.rs i http://www.seio.gov.rs/kontakt/kontakt.631.html).

Da bi razmatrani projekat izgradnje Nacionalnog CERT-a bio finansiran iz IPA II sredstava neophodno je da bude adekvatno priključen procesu **Programiranja IPA II.**

Proces Programiranja IPA II predstavlja složen proces identifikacije potreba, odnosno prioritetnih ciljeva unutar pojedinačnih sektora, definisanje aktivnosti, procedura, kao i vremenskih rokova u postupku pripreme i selekcije predloga projekata koji treba da doprinesu realizaciji utvrđenih ciljeva. Ovaj postupak se odvija kroz sveobuhvatan konsultativni proces u koji su aktivno uključeni svi ovlašćeni predlagači projekata, Evropska komisija, bilateralni i multilateralni donatori, predstavnici organizacija građanskog društva, kao i jedinice lokalne samouprave. Proces programiranja podrazumeva učešće svih navedenih aktera i pripremu velikog broja dokumenata raspoređenih u tri faze:

1**) Faza procesa identifikovanja dugoročnih i srednjoročnih sektorskih ciljeva**: Navedena faza je obavljena pre početka IPA II budžetskog perioda (u periodu 2012.–2014. godine) i obuhvata zadatak Srbije kao države korisnice da obezbedi odgovarajući strateški okvir koji će predstavljati osnovu za pripremu Strateškog dokumenta. U slučaju Republike Srbije takav ključni nacionalni dokument je NAD. Drugi strateški dokument je „Potrebe Republike Srbije za međunarodnom pomoći u periodu 2014.– 2017. godine, sa projekcijama do 2020. godine".

2) **Faza prioritizacije dugoročnih i srednjoročnih sektorskih ciljeva** u vidu formulisanja određenih sektorskih mera: Navedena faza obuhvata izradu sektorskih planskih dokumenata (*Strategic Planning Document* - SPD) za svaki od utvrđenih sektora. Sektorski planski dokumenti se pripremaju za period 2014.–2017. godine, nakon toga za period 2017.–2020. godine, i definišu sektorske prioritete i akcije za njihovo sprovođenje. Pored toga, sektorski planski dokumenti definišu i institucionalni okvir za programiranje i sprovođenje projekata i indikativne alokacije sredstava. Ova faza se sprovodi godinu dana pre početka IPA budžetskog ciklusa i prve godine budžetskog ciklusa (2013.–2014. godina) i zatim se ponavlja na polovini budžetskog perioda (2017.–2018. godina).

3) **Faza operacionalizacije srednjoročnih sektorskih mera** u vidu pripreme predloga projekata za finansiranje iz godišnje alokacije: Navedena faza obuhvata pripremu predloga projekata (tzv. Akcionih dokumenata - AD) za finansiranje iz godišnje alokacije. Formulacija predloga projekata se vrši na sektorskoj osnovi, pri čemu su ključni partneri ovlašćeni predlagači projekata, odnosno, ministarstva i posebne organizacije osnovane Zakonom o ministarstvima, službe Vlade, Narodna banka Srbije i Narodna skupština. Ministarstva su u obavezi da obezbede koordinaciju i konsultacije sa svim zainteresovanim stranama (organizacijama, institucijama, javnim preduzećima, organizacijama civilnog društva) u okviru njihove nadležnosti, kao i da formalno odobre predloge projekata koje iniciraju zainteresovane strane. Faza formulacije predloga projekata obično počinje početkom kalendarske godine i traje do kraja iste kalendarske godine. Bitno je napomenuti da formulacija nacrta predloga projekata u tekućoj programskoj godini obuhvata projekte čiji se početak realizacije očekuje tokom naredne dve godine.

Vremenski aspekt procesa programiranja može se sagledati na slici 10.2

2012	2013	2014	2015	2016	2017	2018	2019	2020
Indikativni strateški dokument za Srbiju								
	Sektorski dokumenti				Sektorski dokumenti			
		Akcio-ni dok.	Ak-cioni dok.	Ak-cioni dok.	Ak-cioni dok.	Ak-cioni dok.	Ak-cioni dok.	Ak-cioni dok.
	CBC Operativni programi							
	IPARD program[13]							

Slika 10.2 – Kalendar programiranja IPA II pretpristupne pomoći i plan generisanja odgovarajućih IPA programskih dokumenata

Pored Kancelarije za evropske integracije i odgovarajućih nacionalnih kontakt centara (NIPAC), koji su odgovorni za koordinaciju, planiranje i praćenje pomoći EU u svim IPA komponentama važnu ulogu imaju **Ovlašćeni predlagači projekata.**

Ovlašćeni predlagači projekata su resorna ministarstva i posebne organizacije, službe Vlade, Narodna skupština i Narodna banka Srbije. Uloga ovlašćenih predlagača projekata, prevashodno, preko svojih predstavnika u sektorskim radnim grupama, usmerena je na utvrđivanje prioriteta za finansiranje iz IPA fondova u ciklusu programiranja, formulisanje nacrta predloga projekata u zahtevanom formatu, njihovo unošenje u informacioni sistem za koordinaciju razvojne pomoći u Republici Srbiji (ISDAKON IS10 http://www.evropa.gov.rs/Evropa/PublicSite/index.aspx), aktivno učešće na konsultativnim sektorskim sastancima, kao i obezbeđivanje koordinacije i uključivanja svih relevantnih institucija u okviru svojih nadležnosti u procesu programiranja.

Proces uključivanja agencije RATEL za potrebe realizacije projekta izgradnje Nacionalnog CERT-a potencijalno bi podrazumevao niz sledećih aktivnosti:

1. Definisanje sektorske grupe IPA II pretpristupne pomoći i tipa projekta kojima bi po svojim karakteristikama razmatrani Projekat izgradnje Nacionalnog CERT-a najviše odgovarao.
2. Kontaktiranje odgovarajućih NIPAC nacionalnih koordinatora, resornih ministarstava i relevantnih sektorskih grupa u cilju daljeg rada na pripremi relevantnih IPA II programskih dokumenata (SPD dokumenta za novi ciklus 2017.-2020. godine i odgovarajućih jednogodišnjih Akcionih dokumenata), tj. definisanje plana aktivnosti u skladu sa odabranim tipom IPA II projekata i procedurama koje su svojstvene apliciranju u odabranom sektorskom domenu.
3. Rad na definisanju nacrta projekta u zahtevanom formatu, njihovo unošenje u ISDAKON IS10 i sprovođenja ostalih aktivnosti programiranja.

Izbor odgovarajuće IPA II grupe programa za razmatrani Projekat izgradnje Nacionalnog CERT-a

Regulatorna agencija za elektronske komunikacije i poštanske usluge svakako predstavlja nezavisnu regulatornu agenciju koja je aktivna u procesu pridruživanje Evropskoj Uniji i uključena je u procedure usklađivanja zakona i praksi sa pravilima Evropske Unije. RATEL ima pravo da učestvuje u svim tipovima prethodno opisanih projekata.

Sa aspekta konkretnog projekta, na osnovu izložene tipologije projekata podobnih za buduća IPA II finansiranja, važno je napomenuti da je uslov da sam cilj projekta bude neprofitabilan, što je jednoznačno potvrđeno u prethodnim poglavljima ove studije.

Po svojoj tematici, potencijal projekta za izgradnju mreže Nacionalnog CERT-a može se prepoznati u:

a. Posebnoj sektorskoj grupi IPA II infrastrukturnih projekata (II grupa) iz oblasti politike " Reforme kao deo priprema za članstvo u EU i izgradnju institucija i kapaciteta" sa posebnom namenom za borbu protiv sajber kriminala, i
b. Grupi programa **prekogranične i transnacionalne saradnje (*Multicountry* IPA II).**

Cilj IPA (Multy-country IPA) fonda je da u određenim sektorima jača regionalnu saradnju, omogući učešće svake zemlje regiona, ali i da smanji ukupne troškove zbog obima i fokusiranih ciljeva. Jedan od prioriteta ovog EU programa je borba protiv organizovanog kriminala, a u okviru ovog priroteta i borba protiv sajber kriminala. Ovde se EU oslonila na kapacitete Saveta Evrope, koji je na području Zapadnog Balkana u u okviru gore pomenute Višekorisničke IPA-e implementirao projekte:

- **CyberCrime@IPA** „Regionalna saradnja u oblasti krivičnog prava: jačanje kapaciteta u borbi protiv sajber kriminala“ u periodu 2010-2013: **(**http://www.coe.int/en/web/cybercrime/cybercrime-ip**),** a korisnice ovog programa bile su Albanija, BiH, Hrvatska, Crna Gora, Makedonija, Srbija, Turska i Kosovo. Cilj projekta bilo je jačanje kapaciteta sudskih organa krivičnog prava da efektivno sarađuju protiv sajber kriminala na bazi Budimpeštanske konvencije o sajber kriminalu i ostalih standarda. Ukupno gledano, u okviru ovog projekta napredak je zabeležen po svim preporukama, ali pre svega u podizanju svesti, jačanju saradnje između javnog i privatnog sektora u ovoj oblasti, kao i u jačanju regionalne i međunarodne saradnje u borbi protiv sajber kriminala.
- **iPROCEEDS (2016-2019)** projekat čija je implementacija u toku **(**http://www.coe.int/en/web/cybercrime/iproceeds**).** Projekat iPROCEEDS ima za cilj jačanje kapaciteta državnih organa u regionu IPA da traže, zaplene i oduzmu prihode ostvarene putem sajber kriminala, kao i da spreče pranje novca na Internetu.

Obe grupe istaknutih projekata poseduju određene potencijale za uključivanje RATEL agencije u njihove okvire i time obezbeđivanje određenih izvora finansiranja za razmatrani Projekat izgradnje Nacionalnog CERT-a.

10.2.2 OSMI PROGRAMSKI OKVIR ZA ISTRAŽIVANJE I INOVACIJE HORIZON 2020

Horizont 2020 (*Horizon 2020 - The EU Framework Programme for Research and Innovation*) predstavlja po obimu najveći ikada programski okvir Evropske unije za finansiranje programa istraživanja i inovacija sa skoro 80 milijardi evra raspoloživih sredstava. Planirani iznos će se rasporediti na mnogobrojne programe tokom vremenskog prozora od 7 godina (2014 do 2020). Osnovna ideja i cilj Horizont 2020 programa je da na globalnom nivou podrži istraživački razvoj (*European Research Area*) i obezbedi komercijalizaciju i iskorišćenje najprosperitetnijih ideja, kao i da podstakne globalnu konkurentnost. Horizont 2020 je osmi po redu okvir finansiranja programa koji sprovodi Evropska Komisija kao izvršno telo Evropske unije i nastavlja se na sedmi okvir FP7 (*Seventh Framework Program*) iz perioda 2007.-2013. godine.

Horizont 2020 poseduje veliku političku podršku evropskih lidera i Članica Evropskog parlamenta jer se smatra pokretačem globalnog ekonomskog razvoja i stvaranja prostora za nova radna mesta. Postignut je konsenzus da je istraživanje ujedno ulaganje u budućnost i kao takvo stavljeno je u primarne inicijative Evrope na putu ka inteligentnom i održivom razvoju društva. Posebni fokus Horizont 2020 programa usmeren je na najnovija naučna rešenja i njihovu inovativnost, razvoj industrije i rešavanje društvenih izazova budućeg doba.

Horizont 2020 je otvoren za sve učesnike, ali se poseban akcenat stavlja na partnerstva realizovana na međunarodnom nivou, spajanju istraživačkih institucija, kao i privatnog i javnog sektora. U programu učestvuju sve zemlje Evropske unije kao i 14 dodatnih pridruženih članica među kojima je i Republika Srbija. Švajcarska je delimično pridružena zemlja.

Struktura programa je napravljena tako da obuhvata tri glavne oblasti istraživanja koje se još nazivaju i "stubovi" programa**:**

- ***Izuzetnost u nauci "Excellent Science"*** **-** odnosno oblast najsavremenijih naučnih dostignuća. Programi iz ove oblasti se koncentrišu na ulaganje u timove naučnika i istraživača u cilju podrške i ubrzavanja razvoja najsavremenijih naučnih dostignuća. Ukupni budžet programa iz ove oblasti od 24 milijarde evra se raspoređuje na:
    - 13 milijardi evra dodeljenih od strane Evropske komisije za istraživanje timovima naučnika i istraživača za razvoj aplikacija,
    - 2,7 milijardi evra za buduće tehnologije u nastajanju FET (*Future Emerging Technologies*),
    - 6,1 milijardi evra za programe mobilnosti istraživača MSCA (Marie *Sklodowska-Curie Action*), i edukacije istraživača na svim stupnjevima razvoja njihove karijere i
    - 2,5 milijardi evra za programe razvoja evropske istraživačke infrastrukture.
- ***Liderstvo u industriji "Industrial Leadership"*** **-** odnosno oblast najsavremenijih industrijskih dostignuća. Programi iz ove oblasti se koncentrišu na ulaganje u industriju u skladu sa strategijama Unije za Evropu 2020 i Inovacije. Ukupni

budžet programa iz ove oblasti od 14 milijardi evra se raspoređuje na šest potprograma vođstva u razvoju industrijskih tehnologija "*Leadership in Enabling and Industrial Technologies*":

- Informaciono-komunikacione tehnologije,
- Nanotehnologije,
- Napredne vrste materijala,
- Napredne tehnike proizvodnje i procesiranja,
- Biotehnologija i
- Svemir.

Programi iz oblasti upravljanja industrijom moraju biti usklađeni sa tehnološkim platformama Evrope (ETP - *European technology platforms)* i odgovarajućim agendama strateškog razvoja. Poseban podstrek daje se razvoju malih i srednjih preduzeća.

- ***Društveni izazovi "Societal Challenges"*** - odnosno oblast ulaganja u potencijalna rešenja za predstojeće društvene i ekonomske probleme. Ukupni budžet programa iz ove oblasti se raspoređuje na sedam potprograma:
  - 7,5 milijardi evra dodeljenih programima iz oblasti zdravstva,
  - 3,8 milijardi evra dodeljenih programima iz oblasti bioekonomije, hrane, vode i šumarstva,
  - 5,9 milijardi evra dodeljenih programima iz oblasti energetike,
  - 6,3 milijardi evra dodeljenih programima iz oblasti saobraćaja,
  - 3,1 milijardi evra dodeljenih programima iz oblasti akcija usmerenih na klimatske promene, životne sredine, efikasnosti resursa i sirovina,
  - 1,3 milijardi evra dodeljenih programima iz oblasti Evropskog društva,
  - 1,3 milijardi evra dodeljenih programima iz oblasti sigurnosti,
  - 0,8 milijardi evra dodeljenih programima iz oblasti podsticanja širenja naučne izuzetnosti i učešća "*Spreading excellence and widening participatio*n" i
  - 0,5 milijardi evra dodeljenih programima iz oblasti primene naučnih dostignuća za dobrobit društva "*Science with and for society* ".

Horizont 2020 primenjuje agilnu administrativnu strukturu u procesu izbora projekata koje treba podržati, na taj način što za svaku oblast redovno generiše pozive (*Horizon 2020 Calls*) na apliciranje sa specifičnim opisom i sadržajem, odnosni izazovima i ciljevima, koje potencijalni projekat treba da ispuni.

Pozivi za projekte vezane za sajber bezbednost grupisani su u najvećoj meri u okviru **oblasti Društveni izazovi, podoblast Bezbedna društva** – čuvajući slobodu i bezbednost Evrope i njenih građana. Od ukupno pet poziva za projekte u okviru ove podoblasti, dva su relevantna za sajber bezbednost:

- **Zaštita kritične infrastrukture** (koja se bavi temama koje povezuju fizičku i sajber bezbednost KI), i

- **Digitalna bezbednost** koja prati sajber bezbednost malih i srednjih preduzeća, lokalnih administracija i individua, zatim ekonomija sajber bezbednosti, saradnja na nivou EU i međunarodni dijalog o istraživanjima i inovacijama u oblasti sajber bezbednosti i privatnosti. U ovu oblast spadaju i kriptografija, pitanja naprednih pretnji u oblasti sajber bezbednosti i aktera tih pretnji, kao i veoma važna privatnost, zaštita podataka, digitalni identiteti.

Srbija se uključila u u program Horizont 2020 1. jula 2014. godine. Ministarstvo nauke, prosvete i tehnološkog razvoja je nadležno da pruži podršku za sve programske blokove i teme Horizona 2020 kroz uspostavljenu mrežu nacionalnih kontakt osoba. Horizont 2020 nacionalne kontak tačke (NCP - *National Contact Points*) odgovorne su da institucijama Republike Srbije pomognu u svim koracima: izboru relevantne Horizont 2020 oblasti, obezbeđivanju treninga i pomoći u pisanju predloga projekta, administrativnim i pravnim procedurama i dostavljanju relevantnih dokumenata i formulara, kao i u procesu traženja partnera. Osim toga, Srbija je formirala stručnu radnu grupu „Horizon 2020“, i postavila Centar za promociju nauke kao instituciju koja će se baviti promocijom ovog važnog programa. S tim u vezi, Centar organizuje program Horizont četvrtkom, kojim se svakog četvrtka ovaj program promoviše zainteresovanoj stručnoj javnosti i građanima. 11. februara 2015. godine program Horizont četvrtkom se fokusirao na IK tehnologije (H2020 i IKT. Centar za promociju nauke. http://www.cpn.rs/aktivnosti/h202-i-ict-2).

Sa tematskog aspekta, možese konstatovati da Projekat izgradnje Nacionalnog CERT-a pod vođstvom RATEL Agencije poseduje potencijal za učešće u Horizont 2020 programima. Pomenuto učešće je teže ostvariti u inicijalnoj fazi razvoja Nacionalnog CERT-a, ali se može uz dobar angažman i praćenje aktivnih poziva iz gore navedenih domena, očekivati u kasnijim fazama, kada Nacionalni CERT bude već operativan.

Opšti proces apliciranja podrazumeva izbor poziva, pronalaženje odgovarajućih partnera, generisanje relevantnog dokumenta u skladu sa pozivom, rangiranje projekta sa dodeljenim ocenama nakon revizije i potpisivanje finansijskih ugovora ukoliko se finansiranje odobri. Specifični pozivi i aktuelni projekti za svaku od odabranih oblasti mogu se naći na web stranici https://ec.europa.eu/programmes/horizon2020/en/h2020-sections-projects.

Za detaljan pristup pozivima potrebno je razmotriti dokument:

"*A guide to ICT-related activities in WP2016-17. European Comission* https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/Guide%20to%20ICT-related%20activities%20in%20WP2016-17%20".

Dodatno za efikasno iskorišćenje finansijske podrške održivosti Projekta izgradnje Nacionalnog CERT-a i njegovog angažmana u najsavrmenijim naučnim oblastima digitalne bezbednosti i zaštite IKT infrastrukture, potrebno da RATEL agencija u odgovarajućem trenutku kontaktira jedan ili više relevantnih Horizont 2020 nacionalnih kontakt autoriteta, http://ec.europa.eu/research/participants/portal/desktop/en/support/national_contact_points.html#c,contact=country/sbg/Serbia/0/1/0&function_details..function_abbr/sbg//0/1/0&+person.last_name/desc.

10.2.3 OSTALI FONDOVI EVROPSKE UNIJE ZA PREVENCIJU RIZIKA U IK TEHNOLOGIJAMA

EC Erasmus+ program

RATEL Agencija kao deo Republike Srbije takođe ima i pristup **Erasmus+** programu Evropske unije (*Erasmus+ Programme Guide. 2016. European Commission. http://ec.europa.eu/programmes/erasmusplus/sites/erasmusplus/files/files/resources/erasmus-plus-programme-guide_en.pdf*) u okviru kojeg se finansiraju aktivnosti usmerene na stvaranje „mreža znanja“ (***knowledge alliances***) među ustanovama visokog obrazovanja, kao i razvoj kapaciteta istih. Ove aktivnosti je Erasmus+ program preuzeo iz prethodnog TEMPUS programa koji je ukinut 1.1.2014. godine. U okviru pomenutog TEMPUS programa, Crna Gora je na primer, u okviru konzorcijuma visokoškolskih ustanova i organizacija iz Slovenije, Velike Britanije, Italije i Crne Gore predvođenog Univerzitetom u Mariboru u periodu 2013-2016 godine sprovodila projekat "Jačanje sajber obrazovnog sistema Crne Gore (*Enhancement of cyber educational system of Montenegro, ECESM*)" (http://ecesm.net/).

Osnovni cilj projekta bio je da „poboljša, razvije i implementira standarde, smernice i procedure u oblasti sajber bezbednosti na nacionalnom nivou u Crnoj Gori, kako bi se omogućilo stvaranje obučene i profesionalne radne snage sposobne da reaguje na dinamične e-pretnje“. Ovaj cilj sprovođen je kroz radionice, prezentacije i druge aktivnosti podizanja svesti; specijalizovane treninge za različite grupe – državnu administraciju, lokalnu administraciju, privatni sektor, operatore/vlasnike kritične infrastrukture, velika, srednja i mala preduzeća, akademske institucije itd; kreiranje akreditovanog master programa prepoznatog i potpomognutog od strane relevantne međunarodne akademske zajednice sa ciljem stvaranja visoko obrazovanih profesionalaca u oblasti sajber bezbednosti.

Na osnovu predstavljenog profila ECESM projekta i prikupljenih iskustava, može se zaključiti da bi Nacionalni CERT Republike Srbije pod nadležnošću RATEL agencije u kasnijim fazama, nakon izgradnje, mogao da ostvari jako kvalitetnu saradnju sa relevantnim i najvažnijim obrazovnim institucijama Srbije iz oblasti prevencije rizika u IKT tehnologijama i razvije kvalitetan projekat u okviru pomenutog Erasmus+ programa.

EDA programi

Evropska agencija za odbranu (*European Defence Agency, EDA*), telo Saveta EU, još jedna je EU jedinica koja se bavi razvojem kapaciteta u oblasti sajber bezbednosti. Srbija je od 2013. godine, na osnovu potpisanog Administrativnog ugovora sa ovom agencijom, u mogućnosti da učestvuje u projektima i programima ovog EU tela (https://www.eda.europa.eu/info-hub/), iako je prvi put ovu mogućnost iskoristila tek u 2016. godini odlukom da se pridruži projektu **"EU Satcom tržište"**. Sajber odbrana je jedna od prioritetnih oblasti kojima se EDA bavi, i to kroz razvoj kapaciteta, odnosno u domenu istraživanja i tehnologije.

EDA organizuje kurseve i vežbe o sajber bezbednosti i odbrani za različit nivo donosilaca odluka, kao i projekte koji se bave podizanjem svesti, razvojem istraživačke agende u oblasti sajber odbrane, detekcijom APT (*Advanced Persistent Threats*) pretnji, zaštitom informacija i kriptografijom.

Evropski fond za strateške investicije -
EFSI (*European Fund for Strategic Investments*)

Jedan od novijih ciljeva EU je da poveća svest sajber zajednice o mogućnostima finansiranja na evropskom, nacionalnom i regionalnom nivou koristeći postojeće instrumente i kanale, poput Evropske mreže preduzeća (***European Enterprise Network***). Komisija će, sa Evropskom investicionom bankom (***European Investment Bank***) i Evropskim investicionim fondom (***European Investment Fund***), istražiti načine da olakša pristup resursima, na primer, kroz stvaranje Investicione platforme za sajber bezbednost (***Cybersecurity Investment Platform***) u okviru Evropskog fonda za strateške investicije (***European Fund for Strategic Investments***, EFSI). Takođe, Komisija će istražiti mogućnost razvoja Pametne platforme za specijalizaciju u oblasti sajber bezbednosti (***Cybersecurity Smart Specialisation Platform***) u konsultaciji sa zainteresovanim državama članicama i regionima, u cilju bolje koordinacije strategija sajber bezbednosti i uspostavljanja strateške saradnje zainteresovanih strana u regionalnim ekosistemima.

EFSI je trenutno usmeren na investicije koje će pomoći jačanje ekonomije Evropske unije i država članica. Glavni cilj je mobilizacija privatnih investicija u cilju prevazilaženja postojećih rupa u finansiranju u samoj Uniji u oblastima kao što su transport, energetika i digitalna infrastruktura, edukacija i obuke, istraživanje i razvoj, informacione i komunikacione tehnologije, kao i podrška malim i srednjim preduzećima. EFSI nije samostalno telo već je formirano u okviru Grupe Evropske investicione banke.

U tom smislu, iako je usmeren na države članice EU, postoji mogućnost prekogranične saradnje u okviru EFSI programa, dok Srbija istovremeno, kao država u „regionu proširenja EU“ (enlargement region), ispunjava uslove za investicije iz Evropske investicione banke.

Prema tome, po eventualnom uspostavljanju Investicione platforme za sajber bezbednost u okviru Evropskog fonda za strateške investicije, treba istražiti mogućnosti za saradnju **Nacionalnog CERT-a RATEL Agencije** u okviru ovog programa.

11. ZAKLJUČAK

Sveopštom informatizacijom društva, pitanje informacione bezbednosti je dospelo u prvi plan. Kompromitovanje IKT sistema može u potpunosti da paralizuje moderna društva. Navedeni problem je prepoznat i u našem društvu zbog čega je donet Zakon o informacionoj bezbednosti („Službeni glasnik RS“, br. 6/2016). Članom 14 ovog Zakona predviđeno je formiranje Nacionalnog centra za prevenciju bezbednosnih rizika u IKT sistemima ili skraćeno Nacionalni CERT. Istim članom Zakona predviđeno je da Nacionalni CERT bude osnovan od strane Regulatorne agencija za elektronske komunikacije i poštanske usluge. Imajući u vidu tipove poslova koje je na osnovu zakona RATEL sprovodio u dosadašnjem radu, ali i postignuti kvalitet u izvršavanju tih poslova, jasno je da RATEL ima veliki potencijal za uspešnu realizaciju Nacionalnog CERT-a.

Osnovni zadaci Nacionalnog CERT-a su da prikuplja i razmenjuje informacije o rizicima za bezbednost IKT sistema, kao i događajima koji ugrožavaju bezbednost IKT sistema i u vezi toga obaveštava, upozorava i savetuje lica koja upravljaju IKT sistemima u Republici Srbiji, kao i javnost. Da bi odgovorio tom zadatku, Nacionalni CERT mora da ima zaposlene eksperte za oblast informacione bezbednosti. Pored prikupljanja i razmene informacija o bezbednosnim incidentima u IKT sistemima, eksperti zaposleni u Nacionalnom CERT-u će biti u mogućnosti da svojim savetima i preporukama pomognu operatorima IKT sistema od posebnog značaja. Rešenjem organizacione strukture i načina rada Nacionalnog CERT-a koje je predloženo u okviru ove studije, Nacionalni CERT treba da postane glavno mesto koncentracije znanja iz oblast informacione bezbednosti u Republici Srbiji. Nacionalni CERT treba da formira informacioni sistem koji će skupljati sve informacije o bezbednosnim incidentima, načinima njihovih prevazilaženja i prevencija. Tehnička infrastuktura Nacionalnog CERT-a treba da obezbedi da i Ministarstvo trgovine, turizma i telekomunikacija (MTTT) može da obavlja svoju funkciju, predviđenu Zakonom, u oblasti prikupljanja i obrade informacija o bezbednosnim incidentima na teritoriji Republike Srbije. Međusobni odnosi i način saradnje između MTTT, kao Nadležnog organa, i Nacionalnog CERT-a biće predmet posebnog dogovara.

Studijom predloženo rešenje predviđa da Nacionalni CERT do kraja pete godine postojanja treba da ima 14 stalno zaposlenih. Od tog broja, jedno mesto je predviđeno za direktora, jedno mesto za poslovnog sekretara i jedno mesto za stručnjaka za marketing.

Preostalih 11 mesta predviđeno je za inženjere stručnjake za oblast informacione bezbednosti. Navedena raspodela strukture zaposlenih u Nacionalnom CERT-u pokazuje jasno opredeljenje za formiranje visoko profesionalne organizacije koja treba da pruži adekvatnu stručnu pomoć iz oblasti informacione bezbednosti svim operatorima IKT sistema od posebnog značaja, kao i ostalim operatorima IKT sistema u Republici Srbiji. S obzirom da je na polju informacione bezbednosti u svetu i kod nas izražen nedostatak visoko specijalizovanog stručnog kadra, prvi petogodišnji plan predviđa veoma intenzivnu obuku svih zaposlenih u Nacionalnom CERT-u. Po završetku prvog petogodišnjeg plana, Nacionalni CERT će imati visoko specijalizovani CERT tim koji će biti u stanju da odgovori na sve probleme koji se mogu pojaviti na polju informacione bezbednosti. U prvim godinama rada Nacionalnog CERT-a, težište će biti na podizanju potrebne infrastrukture, stručnom usavršavanju zaposlenih, definisanju svih potrebnih procedura za rad i komunikaciju sa relevantnim telima u zemlji i inostranstvu. Od treće godine, Nacionalni CERT bi trebao da ima dovoljno znanja da može u potpunosti da odgovori na sve izraženije izazove u oblasti informacione bezbednosti. Tokom četvrte godine, kada broj zaposlenih bude dostigao predviđeni nivo, Nacionalni CERT će preći u režim rada 24/7 koji će obezbediti neprekidnu pomoć, na nivou cele Republike Srbije, za rešavanje potencijalnih problema iz oblasti informacione bezbednosti.

Predloženo rešenje Nacionalnog CERT-a predviđa petogodišnji budžet u iznosu nešto većem od 3.1 miliona Evra. Pri tome, treba imati u vidu da je navedeni iznos posledica činjenice da se formira veoma specifična organizacija za koju RATEL u sadašnjem trenutku nema adekvatan stručni kadar za obavljanje ove vrste posla. To praktično znači da je potrebno kupiti i realizovati kompletnu tehničku infrastrukturu Nacionalnog CERT-a i obučiti stručnjake da mogu da se uhvate u koštac sa ovom problematikom. Oblast informacione bezbednosti je jedna od najdinamičnijih oblasti modernog društva zbog čega je neophodna konstantna obuka i stručno usavršavanje stručnjaka koji se njome bave. Isti zahtev se u tom smislu postavlja i pred stručno osoblje Nacionalnog CERT-a. Treba imati u vidu da Nacionalni CERT nije zamišljen kao profitabilna organizacija. Posledica toga je da će finansiranje Nacionalnog CERT-a morati da bude rešeno kroz budžet krovne organizacije, što je u ovom slučaju RATEL. Zbog specifičnosti problema koje Nacionalni CERT treba da rešava, nije moguće formulisati povraćaj uloženih sredstava klasičnim metodama. Ako se pogleda značaj postojanja i kvalitetnog i profesionalnog rada Nacionalnog CERT-a u modernom društvu, on se svrstava u istu ravan sa vojskom, policijom i ostalim organizacijama koje obezbeđuju zaštitu i nesmetani razvoj društva. Štete koje mogu da nastanu u modernom informatičkom društvu zbog eventualne kompromitacije IKT sistema se mere milijardama Evra. Nacionalni CERT je jedna do ključnih organizacija koja treba da obezbedi prevenciju i zaštitu modernog društva od takvih neželjenih događaja. Ako se pretpostavi da profesionalno delovanje Nacionalnog CERT-a smanjuje štete po moderno društvo najmanje za 10% (a u praksi je to značajno više), jasno je da navedene uštede višestruko prevazilaze potrebni budžet za njegovo funkcionisanje.

12. LITERATURA

1. Moira J. West-Brown, Don Stikvoort, Klaus-Peter Kossakowski, Georgia Killcrece, Robin Ruefle, Mark Zajicek, „*Handbook for Computer Security Incident Response Teams*“, April 2003
2. Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek, „*State of the Practice of Computer Security Response Teams (CSIRTs)*“, October 2003
3. „*A step-by-step approach on how to set up a CSIRT*“, ENISA, 2006
4. „*Baseline Capabilities for national/governmental CERTs*“, ENISA, 2009
5. „*Baseline capabilities for national / governmental CERTs (Part 1 Operational Aspects) “*, ENISA, 2009
6. „*Baseline Capabilities of National/Governmental CERTs (Part 2 Policy Recommendations) “*, ENISA, 2010
7. „*Introduction to Return on Security Investment*“, ENISA, 2012
8. „*Deployment of Baseline Capabilities of n/g CERTs - Status Report 2012*“, ENISA, 2012
9. „*Baseline Capabilities of n/g CERTs - Updated Recommendations 2012*“, ENISA, 2012
10. „*CERT community - Recognition mechanisms and schemes*“, ENISA, 2013
11. „*National/governmental CERTs - ENISA's recommendations on baseline capabilities*“, ENISA, 2015
12. „*CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs*“, ENISA, 2016
13. ENISA interactive CERT inventory: https://www.enisa.europa.eu/topics/national-csirt-network/csirt-inventory/certs-by-country-interactive-map
14. „*Best Practices for Establishing a National CSIRT*“, Organization of American States, April 2016
15. „*National Cyber Security Strategies*“, ENISA, 2012
16. „*NIS Directive and National CERTs*“, ENISA, Feb 2016
17. Andrew Cormack, Miroslaw Maj, Dave Parker, Don Stikvoort, „*CCoP – CSIRT Code of Practice*“, Septembar 2005
18. „*Cyber Security Assesment Netherlands*“, National Cyber Security Center netherlands, 2015
19. „*Creating and Managing CSIRT*“, Carnegie Mellon University, 2008
20. „*2016 Cost of Data Breach Study: Global Analysis*“, IBM & Ponemon Institute, June 2016
21. „*Good Practice Guide for Incident Management*“, ENISA 2010
22. „*Strategies for incident response and cyber crisis cooperation*“, ENISA 2016