РАТЕЛ
РЕГУЛАТОРНА АГЕНЦИЈА ЗА
ЕЛЕКТРОНСКЕ КОМУНИКАЦИЈЕ
И ПОШТАНСКЕ УСЛУГЕ

Палмотићева 2
11103 БЕОГРАД

Студија изводљивости успостављања процедура националног ЦЕРТ-а и управљања системом за пријаву инцидента

САДРЖАЈ

Преглед табела у документу

Преглед приказа у документу

1 УВОД

1.1 Предмет и циљ студије

Студија треба да усмери руководство Националног ЦЕРТ-а у наредним корацима успоставе функционалне организације и оперативних поступака, а пре свега у препознавању, класификацији и дефинисању приоритета (потенцијалних) инцидената, система за праћење инцидената и догађаја, начинима размене података са другим равноправним ентитетима и надлежним телима те дисеминације релевантних информација и унапређивања свести о информационој безбедности и потенцијалним претњама.

Додатно, у Студији се дају и предлози за унапређење одн. препоруке за припрему формалних оквира уређивања неких од области информационе безбедности конституената одн. ИКТ система од посебног значаја у Србији.

1.2 Значај потребе одговора на инциденте

Значај правовременог и адекватног одговора на инциденте и откривање рањивости које могу бити злоупотребљене је и интуитивно јасан – могуће је брже и боље применити адекватне мере у циљу умањења потенцијалне штете. Без обзира да ли је у питању нарушавање тајности, интегритета или доступности информационих добара, у општем случају (нпр. самостални оператори ИКТ система) последице могу бити изражене губицима кроз квантитативне (новчане) и репутационе аспекте. У контексту националног нивоа, инциденти могу бити и индикатор сајбер (*cyber)* напада таквих размера, да могу значајно нарушити функционисање ИКТ система од посебног значаја на националном нивоу, па чак и представљати елемент напада стране државе на Републику Србију. Штавише, напади могу бити потенцијално тако оркестрирани да могу имати негативан утицај и на више од једне државе.

Специфичан проблем могу бити и тзв. напредне учестале претње (*Advanced Persistent Threats*, APT [1]), које карактерише циљаност, софистицираност и велика вероватноћа дуже присутности у неком ИКТ систему пре него је откривена; овакве ситуације захтевају специфичан приступ али и ургенцију у отклањању како основног узрока тако и откривању опсега и решавању последица

[1] Advanced Persistent Threat (**APT)** - Притајени и континуални *hacking* процеси, оркестрирани и усмерени на конкретан циљани ентитет - било приватни или државни. Мотив може бити како пословни тако и политички. Захтева висок степен притајености у дужем периоду. Подразумевају софистициране технике, најчешће у простављању и коришћењу злонамерног кода који ће злоупотребити рањивости у систему. Перзистентност обично подразуева спољашњи *command & control* систем који континуално надзире компромитовани ентитет и извлачи податке из или утиче на функционисање компромитованог ИКТ система.

оваквог инцидента - који примарно лежи на страни погођеног ИКТ система, али може захтевати додатну координацију тима Националног ЦЕРТ-а [2] са осталим релевантним телима.

Да би правовремени и адекватни одговор био могућ, неопходно је имати праву информацију у право време. Сталним скраћивањем овог временског оквира за реаговање, све више се уочава значај сталног:

- праћења догађаја у ИКТ системима;
- размене информација и сарадње са другим институцијама;
- истраживања и анализе доступних информација;
- давања превентивних упозорења по потреби;
- спровођења едукативних и активности подизања свести о потенцијалним претњама и ризицима.

Без адекватне координације и посвећености на поменуте активности, адекватан одговор на потенцијалне претње није могућ.

1.3 Листа послова и услуга које пружа национални ЦЕРТ у складу са Законом о информационој безбедности

Законом о информационој безбедности из 2016. [3] (у даљем тексту *Закон*) **Регулаторна агенција за електронске комуникације и поштанске услуге** (у даљем тексту *РАТЕЛ*) је одређена као

- Тело коме телекомуникациони оператори пријављују инциденте у ИКТ системима који могу да имају значајан утицај на нарушавање информационе безбедности (чл. 11);
- за обављање послова Националног ЦЕРТ-а (чл. 14).

Законодавац је Националном ЦЕРТ-у поверио

- послове координације превенције и заштите од безбедносних ризика у ИКТ системима на националном нивоу;
- прикупљање и размену информација о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система, обавештавање, упозоравање и саветовање лица која управљају ИКТ системима у Републици Србији и јавности;
- промовисање, усвајање и коришћење прописаних и стандардизованих правила за управљање и санирање ризика и инцидената, класификацију информација о ризицима и инцидентима те озбиљности истих и дефиницију формата података за размену предметних информација.

---

[2] Закон о информационој безбедноси Републике Србије („Службени гласник РС“, бр 6/16 и 94/17), у чл. 14 наводи: „Национални центар за превенцију безбедносних ризика у ИКТ системима (у даљем тексту: Национални ЦЕРТ) обавља послове координације превенције и заштите од безбедносних ризика у ИКТ системима у Републици Србији на националном нивоу. За послове Националног ЦЕРТ-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге.

[3] Закон о информационој безбедноси Републике Србије („Службени гласник РС“, бр 6/16 и 94/17)

Према члану 15 Закона о информационој безбедности:

- Национални ЦЕРТ прикупља и размењује информације о ризицима за безбедност ИКТ система, као и догађајима који угрожавају безбедност ИКТ система и у вези тога обавештава, упозорава и саветује лица која управљају ИКТ системима у Републици Србији, као и јавност, а посебно:

    1) прати стање о инцидентима на националном нивоу;

    2) пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инцидентима;

    3) реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих информација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања;

    4) континуирано израђује анализе ризика и инцидената;

    5) подиже свест 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) води евиденцију Посебних ЦЕРТ-ова.

- Национални ЦЕРТ непосредно сарађује са Надлежним органом, Посебним ЦЕРТ-овима[4] 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;

- промовише усвајање и коришћење прописаних и стандардизованих правила за:

    1) управљање и санирање ризика и инцидената;

    2) класификацију информација о ризицима и инцидентима;

    3) класификацију озбиљности инцидената и ризика;

    4) дефиницију формата и модела података за размену информација о ризицима и инцидентима и дефиницију правила по којима ће се именовати значајни системи.

У чл. 19 Закон одређује да су самостални оператори ИКТ система у обавези да формирају сопствене центре за безбедност ИКТ система ради управљања инцидентима у својим системима те да размењују информације међусобно, са националним ЦЕРТ-ом и са ЦЕРТ-ом републичких органа, а по потреби и са другим организацијама.

Према чл. 11 Закона, надлежни орган коме се упућују обавештења о инцидентима

- може наложити његово објављивање ако је инцидент од интереса за јавност;

[4] У чл. 17 Закон дефинише **Посебан ЦЕРТ** као правно лице или организациону јединицу у оквиру правног лица, које је уписано у евиденцију посебних ЦЕРТ-ова коју води Национални ЦЕРТ.

- обавештава надлежно јавно тужилаштво, односно министарство надлежно за унутрашње послове ако је инцидент везан за извршење кривичних дела која се гоне по службеној дужности;
- у случају да је инцидент повезан са нарушавањем права на заштиту података о личности, заједно са самосталним оператором ИКТ система обавештавају и Повереника за информације од јавног значаја и заштиту података о личности.

Према члану 12 Закона Национални ЦЕРТ (као надлежни орган) остварује међународну сарадњу у области безбедности ИКТ система, а нарочито пружа упозорења о ризицима и инцидентима који испуњавају најмање један од следећих услова:

1) брзо расту или имају тенденцију да постану високи ризици;
2) превазилазе или могу да превазиђу националне капацитете;
3) могу да имају негативан утицај на више од једне државе.

Према чл. 5 Закона наводи се да „у циљу остваривања сарадње и усклађеног обављања послова у функцији унапређења информационе безбедности, као и иницирања и праћења превентивних и других активности у области информационе безбедности Влада оснива Тело за координацију послова информационе безбедности (...), у чији састав улазе представници министарстава надлежних за послове информационе безбедности, одбране, унутрашњих послова, спољних послова, правде, представници служби безбедности, Канцеларије Савета за националну безбедност и заштиту тајних података, Генералног секретаријата Владе, ЦЕРТ-а републичких органа и Националног ЦЕРТ-а“.

У одлуци Владе Србије од 3.3.2016. о образовању *Тела за координацију послова информационе безбедности* стоји да је “задатак Тела за координацију (...) да остварује сарадњу између органа и усклађује обављање послова у функцији унапређења информационе безбедности, иницира и прати превентивне и друге активности у области информационе безбедности, предлаже мере за унапређење информационе безбедности у Републици Србији, даје сугестије и предлоге који се односе на припрему стратешких докумената, подзаконских аката и политика информационе безбедности у Републици Србији, и утврђује међусобну сарадњу у случају инцидената који могу да имају знатан утицај на нарушавање информационе безбедности у Републици Србији”, те да “Тело за координацију подноси извештај о свом раду Влади два пута годишње”, и да „стручну и административно-техничку подршку Телу за координацију пружа Министарство трговине, туризма и телекомуникација”.

1.4 Коментар и препоруке

Може се рећи да је Национални ЦЕРТ добио мандат да представља земљу у међународној ЦЕРТ заједници и служи као национални контакт за друге ЦЕРТ-ове и организације одн. институције које се баве информационом безбедношћу. Имајући у виду наведено, Национални ЦЕРТ служи и као тачка за пријављивање неког инцидента у случају недоумице коме се обратити, те може проследити информације одговарајућем надлежном субјекту.

Користећи приступ на који се може наићи у више релевантних извора – као нпр. *Европска агенција за безбедност мрежа и података* (*ENISA*) [5] и Универзитет *Carnegie Mellon* [6] - ове *Услуге* које су Законски дефинисане могу се систематично подвести под 3 основне категорије (из свеукупно препознатих категорија) и то као:

- **Реактивне** – фокусиране на активности након пријаве одн. извештавања о инцидентима од стране конституената или других релевантних извора претњи или напада (злонамерни код, рањивости итд.)
  - узбуњивање и обавештавање;
  - управљање инцидентом.
- **Проактивне** – с циљем да детектују догађаје и спрече нападе пре појаве последица на продукционим системима; информације које генеришу ЦЕРТ-ови и друге заједнице прослеђују се конституентима и партнерима -
  - објаве;
  - праћење техничких ресурса;
  - ширење информација о претњама.
- Оријентисане на **управљање квалитетом сервиса** – на захтев конституената у циљу прегледа и унапређења стања у области информационе безбедности; најчешће нису непосредно временски корелиране у односу на друге активности -
  - анализа ризика;
  - унапређење свести о темама из области информационе безбедности.

ENISA је у својим првим извештајима навела као основне услуге за конституенте: одзив на инциденте, узбуњивање и обавештавање, објаве. Такође, омогућено је да се конституентима и другим партнерским организацијама пружају и неке додатне и/или напредније услуге (изван основног скупа) – нпр. форензичка анализа или сл.

Екстерни сервиси захтевају и адекватне интерне процесе који ће их подржавати (нпр. у вези за управљањем инфраструктуром или ресурсима). Ови процеси морају имати адекватну пажњу како би се могло одржати али и унапређивати даље функционисање и зрелост институције као што је Национални ЦЕРТ.

Узимајући у обзир Законом додељене послове Националном ЦЕРТ-у, те препоруке ENISA-е, предлаже се да се овај *Портфолио Услуга* (тј. оперативно-техничке могућности) допуни укључивањем одн. препознавањем и ових сегмената:

- успостављање сарадње са државним и приватним сектором и олакшавање конституентима да дођу до адекватне напредније помоћи у смислу умањивања последица инцидента, анализе инцидената, артефакта, итд. (реактивна услуга) одн. активних провера стања безбедности система кроз контролисане активности откривања слабости и рањивости из перспективе потенцијалног нападача (*penetration test*) и сл. активности (проактивна услуга) - у случају да им је таква асистенција потребна и затраже је. Овим би се и заокружила „обавеза“ пружања техничке помоћи конституентима;

[5] https://www.enisa.europa.eu/topics/csirt-cert-services (март 2018.)

[6] https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf (март 2018.)

- управљање рањивостима – превасходно реактивна услуга, са одређеним аспектима и у другим сегментима; такође, пример је „уплитања“ интерног процеса који помаже пружање екстерне услуге. Редовно праћење појаве и заступљености рањивостима у сопственом окружењу омогућава правовремену припрему и дистрибуцију адекватних информација конституентима, али и широј јавности. Узимајући ове информације у обзир, те евиденцију инцидената и податке добијене праћењем неког IDS (Система за детекцију упада у мрежу) добија се додатни контекст. Такође, могу се добити значајне информације за Анализу ризика. Даље, овај контекстуални скуп информација може се искористити у припреми садржаја комуникације и сесија за унапређење свести;
- детекција упада – проактивна услуга, такође пример „уплитања“ интерног процеса који помаже пружање екстерне услуге. Коришћењем тзв. *„honeypot“* система [7] (систем и/ли ресурс као мамац) и надзором свих кључних (а пре свега изложених) тачака у мрежи помоћу IDS (Система за детекцију упада) могу се добити значајне информације о актуелним нападима (тип, динамика, трендови);
- додатни саветодавни рад са конституентима у области стандардизације и унапређења политика и мера у области информационе безбедности, те (изнимно) праксе и начела процене и управљања ризицима (законска категорија, али и потенцијално велики извор неразумевања и изложености) – управљање квалитетом сервиса.

По питању одговорности и мандата Националног ЦЕРТ-а, препоручује се додатно појашњење и прецизирање у односу на постојећи текст Закона (а који и даље остаје у духу Закона):

- Национални ЦЕРТ реагује по пријављеним или на други начин откривеним инцидентима, те прати стање о инцидентима на националном нивоу. Потребно је утврдити обавезу Националног ЦЕРТ-а да прати инцидент до његовог разрешења, одн. обавезу стране која је пријавила инцидент да оперативно сарађује са ЦЕРТ-ом - извештава о статусу значајнијих интерних активности у разрешавању инцидента, значајним променама од претходне комуникације као и о евентуалном разрешењу (затварању) инцидента у међувремену и сл.. Тело за координацију би требало, пре свега операторима ИКТ система од посебног значаја, да дефинише постојање приоритета, начина, динамике и обавештавања надлежног органа, о решавању инцидената.;
- Национални ЦЕРТ пре свега има надзорну и саветодавну улогу, док *Тело за координацију* има координациону улогу у припреми стратешких предлога. Потребно је назначити неко тело које ће активно руководити одн. којој ће се предати руковођење потенцијалном кризном–ванредном ситуацијом из области информационе (сајбер) безбедности. Да би се избегло умножавање институција, могући модалитет могао би бити формирање „кризног штаба“ при неком од постојећих ЦЕРТ-ова, при чему би се овој инситуцији додала потребна овлашћења (у ограниченом временском периоду, уз периодичну ревалидацију).

[7] *Honeypot* је информатички ресурс намерно постављен на одређени небезбедан начин да би послужио као мамац, уобичајено је да се *honeypot* користи за боље разумевање шта се дешава (или шта би се могло десити) на кључним (регуларним) системима, кроз праћење њиховог неовлашћеног или нелегалног коришћења. https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide#addsearch=honeypot (март 2018.)

- и имплицитно су јасне предности неке врсте интеграције схема пријављивања (где је то и колико могуће) и веза са активним елементима који могу управљати кризним ситуацијама на националном нивоу – а пре свега када се говори о критичним ИКТ системима. Стога је систематизација на вишем нивоу потребна, како на правном-процедуралном тако и експертском нивоу;

- узевши у обзир и публикацију о стању информационе безбедности у Републици Србији из 2016. чију је израду помогао ОЕБС [8], препорука је јасније дефинисање улоге и положаја Тела за координацију послова информационе безбедности, те даље размотрити успостављање тела или групе која би окупљала представнике релевантних институција државе, академске заједнице и приватног и цивилног сектора. Овим би се могли створити услови за успоставу модалитета сарадње кроз јавно-приватно партнерство.
  Србија у оквиру *Horizon 2020* програма EU (чија је улога спровођење даљег финансирања активности усмерених на истраживање и развој у области сајбер безбедности) има статус *повезане државе* (*associate country*); кроз овај оквир Србија има приступ и Европској организацији за сајбер безбедност *(European Cyber Security Organisation*, ECSO) те стога испуњава услов за учешће у програмима уговорног јавно-приватног партнерства EU у области сајбер безбедности;
- како Законом није одређена прецизна дефиниција озбиљности инцидента који се мора пријавити, препоручује се дефинисање критеријума (макар за први период успостављања и стабилизације функционисања Националног ЦЕРТ-а) магнитуде инцидената који се морају пријавити како би се подржали приоритети и омогућило функционисање тима.

[8] https://www.osce.org/sr/serbia/272206?download=true (март 2018.)

2 ДЕФИНИЦИЈЕ

Као референца преузимају се постојеће дефиниције из Закона о информационој безбедности Републике Србије. Додатно, преузимају се и предлажу као полазна тачка дефиниције из других извора за релевентне појмове које Закон не наводи. Такође, за одређене појмове из Закона прилажу се и допунске информације у циљу ширег сагледавања или додатног појашњења предметних појмова.

Закон у чл. 2 дефинише следеће релевантне основне појмове:

- **информационо-комуникациони систем (ИКТ систем)** [9] је технолошко-организациона целина која обухвата:
  (1) електронске комуникационе мреже у смислу закона који уређује електронске комуникације;
  (2) уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма;
  (3) податке који се похрањују, обрађују, претражују или преносе помоћу средстава из две претходно наведене ставке (1) и (2), а у сврху њиховог рада, употребе, заштите или одржавања;
- **информациона безбедност** представља скуп мера које омогућавају да подаци којима се рукује путем ИКТ система буду заштићени од неовлашћеног приступа, као и да се заштити *интегритет*, *расположивост*, *аутентичност* и *непорецивост* тих података, да би тај систем функционисао како је предвиђено, када је предвиђено и под контролом овлашћених лица;
- **тајност** је својство које значи да податак није доступан неовлашћеним лицима;
- **интегритет** значи очуваност изворног садржаја и комплетности податка;
- **расположивост** је својство које значи да је податак доступан и употребљив на захтев овлашћених лица онда када им је потребан;
- **аутентичност** је својство које значи да је могуће проверити и потврдити да је податак створио или послао онај за кога је декларисано да је ту радњу извршио;
- **непорецивост** представља способност доказивања да се догодила одређена радња или да је наступио одређени догађај, тако да га накнадно није могуће порећи;
- **ризик** значи могућност нарушавања информационе безбедности, односно могућност нарушавања *тајности*, *интегритета*, *расположивости*, *аутентичности* или *непорецивости* података или нарушавања исправног функционисања ИКТ система;

[9] Све дефиниснае под-тачке заједно чине комплетан опис одн. дефиницију (прим аут.).
Поједностављено, ИКТ систем је скуп хардвера, софтвера, података и људи који их користе, и углавном укључује неку врсту комуникационе технологије.
https://www.bbc.com/education/guides/z2c82hv/revision (март 2018.)

- **инцидент** је унутрашња или спољна околност или догађај којим се угрожава или нарушава информациона безбедност;
- **информациона добра** обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, унутрашње опште акте, процедуре и слично;

У чл. 3, Закон дефинише основна начела, међу којима и

- **начело управљања ризиком** – избор и ниво примене мера се заснива на процени ризика, потреби за превенцијом ризика и отклањања последица ризика који се остварио, укључујући све врсте ванредних околности;

Према ISO27035:2016 [10] налазимо:

- ***CYBERSECURITY* догађај** (*event*) је идентификована појава система, сервиса или стања на мрежи која индикује могућу повреду информационе безбедности, повреду или губитак контрола или претходно непознато стање које може бити релевантно у контексту информационе безбедности;
- ***CYBERSECURITY* инцидент** (*incident*) је појединачни или серија нежељених или неочекиваних инцидената (у смислу информационе безбедности) који имају значајну вероватноћу да компромитују пословну оперативност и угрозе (тј. представљају претњу по) информациону безбедност;
- **управљање** *cybersecurity* **инцидентима** (*cybersecurity incident management*) је процес откривања, извештавања, процене, одговора на, решавања и учења из искуства *cybersecurity* инцидената;

Ресурси као што је IETF RFC 2828 [11] сугеришу дефиницију у којој:

- **напад** подразумева намеру (а посебно узимајући у обзир специфични контекст, коришћени метод или технику) да се изведе (малициозна) активност која угрожава информациону безбедност;

Од других релевантних појмова, треба навести и :

- **претња :** [ISO27005 [12], ENISA[13]] догађај или околност која може проузроковати инцидент;
- **рањивост :**
  - [ISO27005] слабост која може бити искоришћена и/или злоупотребљена од стране Актера претње (*Threat Actor*) - као што је то нападач - како би извео неовлашћене активности на рачунарском систему;

---

[10] Међународни стандард који се бави процесом управљања догађајима из домена информационе бебедности, безбедносним инцидентим и рањивостима. Објављен из 2 дела : Принципи управљања инцидентима и Смернице за планирање одзива на инциденте.

[11] https://tools.ietf.org/html/rfc2828 (март 2018.)

[12] ISO/IEC, "Information technology -- Security techniques - Information security risk management" ISO/IEC FIDIS 27005:2008; стандард који даје смернице за управљање ризицима у области информационе безбедности и надграђује основне концепте изложене у ISO/IEC 27001 стандарду.

[13] https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets/at_download/fullReport (март 2018.)

- [IETF RFC 2828 [14]] грешка или слабост у дизајну, имплементацији или раду и управљању система која може бити (зло)употребљена како би се нарушила безбедносна политика система;
- [ENISA [15]] постојање слабости, дизајна или грешке у имплементацији која може довести до неочекиваних, нежељених догађаја компромитујући тако безбедност предметног рачунарског система, мреже, апликације или протокола.

- **ризик** : [ISO27005] потенцијал да одређена претња може искористити рањивост једног или групе добара и нашкодити организацији;
- **последица** (*impact*) : у контексту информационе безбедности, губитак расположивости, интегритета или тајности информације; за додатно разумевање, али и подршку управљању ризицима, требало би узети у обзир и ефекте на предметну организацију (размере, тип – финансијски, људски животи и сл.);
- **хаковање** (*hacking*) **:** активност коришћења рачунара за илегални приступ информацијама смештеним на другом рачунарском систему или ширење рачунарских вируса; пракса модификовања или мењања рачунарског софтвер-а или хардвер-а како би се постигао циљ који је изван изворне намене коју је имао творац [16];
- **CSIRT** (*Computer Security Incident Respones Team*) **:** [US-CERT [17]] конкретна организациона целина којој је додељена одговорност координације и подршке одзиву на догађаје или инциденте у домену рачунарске (информационе) безбедности; користи се као синоним за појам CERT (*Computer Emergency Response Team*);
- **SOC** (*Security Operations Centre*) **:** односи се на организацију људи, технологије и процеса којом се подиже свест и добија увид у безбедносни статус кроз мере детекције и спречавања одн. умањења потенцијалне штете од претњи по ИКТ системе; бави се ИТ инцидентима који носе потенцијалну претњу и обезбеђује да буду адекватно препознати, анализирани, истражени, пријављени и да се о њима извести; ако CSIRT није формално успостављен тада је SOC одговоран за одзив на индиценте – у супротном SOC помаже CSIRT у прикупљању свих неопходних информација потребних за адекватан одговор на претњу. [18]

---

[14] https://tools.ietf.org/html/rfc2828 (март 2018.)

[15] https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52 (март 2018.)

[16] https://dictionary.cambridge.org/dictionary/english/hacking и https://cyber.laws.com/hacking (март 2018.)

[17] https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams (март 2018.)

[18] обично интерна и преманентна функција која централизује улогу и одговорност за заштиту информационе безбедности у некој организацији одн. институцији; укључује превенцију, детекцију, управљање и одзив на инциденте, извештавање, руковођење и надзор управљањем ризика усклађеношћу са регулаторним захтевима (*governance, risk, & compliance*), и др. елементе који се односе на управљање и одбрану информационе безбедности унутар организације одн. институције.
https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide (март 2018.)
http://resources.infosecinstitute.com/structure-csirt-soc-team/ (март 2018.)

- **Конституенти :** група корисника, сајтова, мрежа или организација за које ЦЕРТ пружа своје услуге

3 КЛАСИФИКАЦИЈЕ

3.1 Класификација информација о ризицима и инцидентима

Како би стандардизовано третирање инцидената на дневном нивоу, али и размена информација о инцидентима (како са конституентима тако и са другим ЦЕРТ-овима, а потенцијално и са органима реда) била могућа, потребно је усвојити одређену "референтну" таксономију.

Таксономија је веома значајна компонента, јер не само да даје основу особи која управља инцидентом могућност да исправно интерпретира инцидент, већ и да исправно интерпретира терминологију категорисања инцидента.

Као почетна "тачка" (а сагласно ономе што сугерише – и подржава – ENISA, *Европска агенција за безбедност мрежа и података*) препоручена је референтна таксономија популаризована кроз тзв. European CSIRT Network пројекат [19] . Иста је заснована на искуству и развоју шведског ЦЕРТ тима. Разлог за ову препоруку - иако иста није скорашњег датума – је да су главне категорије тако дефинисане да се могу сматрати како практичним тако и прилично универзалним, а осим тога је већ у употреби од стране већег броја европских ЦЕРТ-ова. Ова таксономија је (у благо адаптираном облику – који је и овде препознат) препозната од стране TF-CSIRT / Trusted Introducer [20] (као eCSIRT.net таксономија инцидената)[21] .

Оригинално, таксономија је имала два нивоа – свака категорија имала је једну или више поткатегорија. Са данашње тачке гледишта, ове поткатегорије нису у потпуности актуелне; у пракси, оне су се "изгубиле", тј. обично се не сматрају делом конкретне схеме, већ су постале део описа одн. појашњења (као могући појавни облик).

---

19 https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy (март 2018)

20 **TF-CSIRT** : Радна група која промовише сарадњу и координацију између ЦЕРТ-ова у Европи и околним регијама, истовремено повезујући релевантне организације на глобалном нивоу.
https://tf-csirt.org/ (март 2018.)
Trusted Introducer : главнни инфраструктурни сервиси и посредник у повезивању свих безбедносних и тимова за одзиве на инциденте; одржава базу Европских ЦЕРТ-ова.
https://www.trusted-introducer.org/ (март 2018.)

21 https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf (март 2018)

Инцидент (класа)	Пример Инцидента (“тип”)	Опис-појашњење
Abusive Content * *Непожељни садржај*	Spam	Масовно одаслане поруке е-поште – прималац није “затражио” ту поруку и послата је као део већег скупа порука са истим садржајем.
	Harmful Speech * *Штетно обраћање*	Дискредитација или дискриминација некога (нпр. ухођење некога коришћењем сајбер медија одн. механизама, расизам, претње против једног или више појединаца)
	Children/sexual/violence/… * *Деца / сексуално / насиље*	Дечја порнографија, величање насиља…
Malicious Code * *Малициозни програмски код*	Virus	*Софтвер* који је убачен у неки систем са малициозном намером. Корисничка интеракција је најчешће потребна за активирање кода.
	Worm	
	Trojan	
	Ransomware	
	Spyware	
	Dialer	
	Rootkit	
Information Gathering * *Прикупљање информација*	*Scanning* * *Скенирање*	Напади којима се шаљу упити систему у циљу откривања слабих тачака; ово укључује и неку врсту тестирања у циљу прикупљања информација и системима, сервисима који се извршавају на њему, корисничким налозима (нпр. fingerd, DNS querying, ICMP, SMTP EXPN / RCPT, …).
	Sniffing	Праћење и снимање мрежног саобраћаја (wiretapping)
	Social engineering * *Социјалн инжењеринг*	“Извлачење” информација из људи не-техничким методама (нпр. лагање, употреба трикова, подмићивање, претње)
Intrusion Attempts * *Покушај упада*	*Exploiting known vulnerabilities* * *Искоришћавање (злоупотреба) познатих рањивости*	Покушаји да се компромитује систем или омете функционисање неког сериса злоупотребом рањивости која има свој стандардизовани идентификатор као што је ознака у CVE – заједничкој бази рањивости (нпр. buffer overflow, backdoor, cross-side scripting, итд).
	Login attempts * *Покушаји (именованог) приступа систему*	Вишеструки покушаји приступа (погађање одн. “разбијање” лозинки, примене “грубе силе” -тзв. *brute force*, …)
	New attack signature * *Нови образац напада*	Покушај злоупотребе и компромитовања кроз претходно непознате тачке експлоатације
Intrusions * *Упад*	*Privileged account compromise* * *Компромитовање налога са посебним привилегијама*	Успешно компромитовање система или апликације (сервиса). Могуће је извршити удаљеним приступом и искоришћавањем постојеће или нове рањивности, али и кроз неовлашћени локални приступ. Такође значи и “укључивање” у тзв. botnet (botnet члан пример је примарно фокусиран на јавне web сервере – за интерне станице и сервере размторити прво малициози код као категорију)
	Unprivileged account compromise * *Компромитовање налога баз посебних привилегија*	
	Application compromise * *Компромитовање апликације*	

	Bot(member)		
Availability * *Доступност (утицај)*	DoS (Denial of Service)	Овај тип напада подразумева бомбардовање система толиким бројем пакета на мрежи да функционисање постане отежано и/или успорено или систем "попусти под притиском" и престане да ради. Примери DoS су ICMP и SYN flood, Teardrop напад и mail-bombing. DDoS напади су обично базирани на DoS нападима из botnet-а, али постоји и други сценарији (као DNS Amplification напади).	
	DDoS (Distributed Denial of Service)		
	Sabotage * *Саботажа*	Треба имати у виду да се на доступност може деловати и локалним акцијама које резултирају ометањем функционалности или уништавањем информација или опреме, али могу бити и последица дејства "више силе", спонтани кварови или као резултат људске грешке – без зле намере или великог немара.	
	Outage (no malice) * *Отказивање / квар (без зле намере)*		
Information Content Security * *Безбедност (садржаја) информација*	*Unauthorised access to information* * *Неовлашћени приступ информацијама*	Било какав приступ подацима бу одобрења - може бити резултат неодговарајуће рестрикције на дељеном ресурсу (share) али и ексфилтрација података кроз злоупотребу SQL Injection.	*Поред локалне злоупотребе података и система, безбедност информација може бити угрожена и успешним компромитовањем налога или апликација. Осим тога, могући су и напади који пресрећу или приступају информацијама током преноса (wiretapping, spoofing, hijacking). Људска грешка, грешка у конфигурисању или софтвер-ска грешка такође може бити узрок.*
	Unauthorised modification of information * *Неовлашћена измена информација*	Неовлашћена манипулација подацима или измена података у датотеци, документу или бази података.	
Fraud * *Превара*	*Unauthorized use of resources* * *Неовлашћено коришћење ресурса*	Коришћење ресурса за неодобрену намену укљ. и подухвате са циљем стицања профита (нпр. коришћење е-поште за учествовање у нелегалним ланчаним или пирамидалним схемама).	
	Copyright * *Повреда ауторских права*	Продаја или инсталирање нелиценцираних копија комерцијалног софтвер-а или др. материјала под ауторско-правном заштитом (Warez)	
	Masquerade * *Маскирање*	Типови напада у којима један ентитет преузима идентитет другог у циљу стицања неке користи од тога.	
	Phishing	Маскирање одн. претварање да је у питању други ентитет како би се корисник убедио да открије своје креденцијале.	
Vulnerable * *Рањивост*	*Open for abuse* * *Отворено за напад и злоупотребу*	Отворено доступни сервиси за разрешење Интернет адреса (Open resolver), отворено доступни штампачи, рањивости које су евидентне при скенирању неким алатом за проверу рањивости, неажурне базе "потписа" вируса, итд..	
Other * *Друго*	Сви инциденти који не спадају у неку од претходних катеорија.	У случају да се појављује повећани број инцидената у овој категорији, служи као индикатор за ревидирање шеме класификације.	
Test * *Тест*	Намењено за тестирање	Намењено за тестирање	

Табела 3-1 : класификација информација о ризицима и инцидентима

Из анализе ENISA-е, може се видети и да су ове главне категорије практичне и (у овом тренутку) довољно универзалне и да је мапирање, ових главних категорија из референтне таксономије на друге таксономије у употреби, могуће [22].

Како је и споменуто, препорука је – бар у почетној фази - класификацију користити ограничавањем на примарне категорије и коришћење наведених типова-примера као елемент појашњавања при категорисању неког инцидента (а како би се избегла конфузија у комуникацији са другим организацијама). Временом информације о класификацији инцидената и дефиницијама у референтној таксономији треба консолидовати. Свака измена (наравно) треба на стандардизован начин да буде мењана уз праћење верзија.

Приликом уноса информација о одређеном инциденту у систем за пријаву инцидената (*ticketing system*), потребно је обратити пажњу да ли се инцидент једнозначно класификује или се дозвољава придруживање више категорија; иако је ово потоње теоретски могуће, треба имати у виду да може „допринети" лажној статистици у каснијим анализама – те је препорука пажљива процена „превасходне" категоризације при уносу записа о инциденту.

У ситуацијама када је повећан број инцидената те велики број особа или тимова који сарађују могуће су и различите интерпретације или превиди; последица може бити потреба за ре-категоризацијом одређених инцидената.

Неки инциденти могу бити и део шире појаве (па чак можда и узрок појаве другог инцидента, другачијег типа); у оваквим случајевима, ре-категорисање релевантних повезаних инцидената може бити потребно због одржавања веродостојности.

3.2 Класификација информација о ризицима и инцидентима у вези са тајношћу података

	Нема / Низак	Умерен	Висок	Критичан
	Није било одлива, измена или другачије врсте компромитовања информација. Све објављене информације су класификоване као јавне.	Повреда тајности над личним подацима	Повреда тајности заштићене информације (контролисана, која није јавно позната) – нпр. нарочито осетљиви лични подаци, пословне тајне, интелект. власништво, информације о заштићеној критичној инфраструктури и сл.	Повреда тајности поверљивих информација (кључне пословне тајне, државне тајне, законски дефинисани тајни подаци, и сл., креденцијали за критичне системе)

Табела 3-2 : класификација инцидената у вези са повредом тајности података

[22] Репрезентација ове таксономије (проширена за *coformity* категорију) доступна је у JSON форми на https://github.com/MISP/misp-taxonomies/blob/master/CERT-XLM/machinetag.json (март 2018)
Укључивање Comformity категорије (оријентисана на губитак сагласности са регулаторним оквирима) – која је изван номиналне референтне таксономије - у овом тренутку не би допринело унапређењу процеса управљања одн. праћења инцидената.

3.3 Категоризација напада према утицају на пословање

	Нема	Низак	Умерен	Висок	Критичан
	Организација није онемогућена да пружа сервисе својим корисницима	Организација није онемогућена да пружа сервисе својим корисницима. Могуће варијације за неке од не-критичнисх система.	Губитак критичних сервиса за неке од (подскуп) корисника система	Организација је изгубила могућност пружања критичних сервиса корисницима	Организација је изгубила могућност пружања свих критичних сервиса свим корисницима

Табела 3-3 : категоризација напада према утицају на пословање

3.4 Класификација нивоа озбиљности инцидената и ризика

Одредница	Низак	Умерен	Висок	Критичан
Дефиниција	Није очекиван или је минимални утицај на инфраструктуру / системе на националном нивоу.	Очекиван одређени утицај на инфраструктуру / системе. Могуће ометање сервиса, више локализовано него на ширем подручју, могућ утицај на хиљаде и више људи.	Очекиван значајан утицај утицај на инфраструктуру / системе. Ометање сервиса високог значаја и/или на ширем географском подручју, може погодити и стотине хиљада људи на националном нивоу.	Велика претња за сервисе ширег спектра. Системи / инфраструктура погођени до нивоа где се разматра потенцијално катастрофа. Може погодити стотине хиљада па и милионе људи. Посебно критично ако се може прелити и изван граница државе.

Табела 3-4 : класификација нивоа озбиљности инцидената

4 УНУТРАШЊА ОРГАНИЗАЦИЈА

Организациони модел Националног ЦЕРТ-а одређен је датим мандатом и сервисима. Фокус је на координирање и праћење инцидената и олакшавање целокупног процеса. Ово укључује текућу размену информација, основну анализу и могуће давање препорука за одзив на и опоравак од инцидента, као и препоруке у циљу унапређења, али и шире праћење релевантних информација и информисање конституената о трендовима и обрасцима у појави инцидената, давање раних упозорења, упућивање на корисне информације и сл. У оваквој поставци, Национални ЦЕРТ нема ауторитет над својим конституентима за непосредно решавање инцидента и/или опоравак од истог; конституенти самостално одлучују да ли ће и како применити евентуално добијене препоруке. Очекује се да кроз координациону, информативну и саветодавну улогу, Национални ЦЕРТ може допринети унапређењу информационе безбедности, као и да својом позицијом и репутацијом "допре" до различитих слојева (укљ. и руководеће) у организацијама које су конституенти.

Веома је значајно да улога, одговорности и мандат Националног ЦЕРТ-а буду јасно представљене и релевантним странама у другим државама. Неразумевање и отежани проток информација у појединим случајевима могу имати значајне последице.

Ефикасност ЦЕРТ-а као координационог центра огледа се, пре свега, кроз успешну комуникацију ка различитим нивоима у организацијама-конституентима. Као „неутрална страна" треба да синтетише информације у сумарне прегледе активности али и да затим пружи довољно детаљну анализу конституентима који немају довољно ресурса или експертизе. Логично (не само током инцидената), ЦЕРТ ће редовно комуницирати са локалним тимовима за одзив на инциденте код конституената, а поузданост и адекватност информација са обе стране кључна је за успешност и унапређење у континуитету.

У оваквим случајевима, најчешће су у питању посвећени тимови смештени на једну главну локацију са својим дефинисаним руководиоцем. Како је тешко изводљиво да тим својом експертизом покрива све потенцијално погођене платформе, пажњу треба посветити сарадњи са тимовима конституената, али и имати дефинисану и успостављену сарадњу са другим независним организацијама, у случају да је потребна њихова експертиза. Оквири овакве сарадње могу бити нпр. кроз академске институције, постојеће уговоре о сарадњи државе са релевантним организацијама, али и кроз евентуално успостављање јавно-приватног партнерства.

Питање организације и људства већ је разматрано и у оквиру Студије изводљивости изградње Националног ЦЕРТ-а [23].

[23] Студија изводљивости изградње Националног ЦЕРТ-а (Елктротехнички факултет у Београду, октобар 2016.) http://www.ratel.rs/upload/documents/Studije/Studija%20izvodljivosti%20izgradnje%20Nacionalnog%20CERT-a.pdf (март 2018.)

Консултујући и друге ресурсе [24], овде бисмо потврдили потребу за дефинисањем (поред регуларних административних) позиција и људства за тријажу и "*hotline*", анализу инцидената, подршку и одзив, координацију. Додатно, уколико су активни такви сервиси, може бити потребе за позицијама праћења и управљања рањивостима и поступање са прикупљеним артефактима.. Осим значаја адекватног покривања функције за *hotline*/тријажу/*help-desk*, не сме се заборавити на делимично преклапање улога :

- инжењера у интерној администрацији система и подршци (у својим доменима) у процесу разрешавања инцидената;
- аналитичара у редовном праћењу и анализи прикупљених записа у интерној SoC организацији и за конституенте;
- техничког тима ЦЕРТ-а (генерално) у оперативном функционисању и спровођењу обука (интерно, за конституенте, за јавност).

Да функционисање не би било угрожено, потребан је пажљив приступ дефинисању смена и ротација на дужностима како би се покрили сви задаци и функционисање 24x7x365.

У ЦЕРТ тиму који је фокусиран на координациону улогу, **тријажа** је централна функција. Кроз тријажу се пријављени инциденти (или други захтеви) сортирају, категоризују, приоретизују – дакле, омогућава иницијалну процену и припрему за даље поступке. Такође, пружа и увид у текуће стање свих пријављених активности - отворени случајеви, на чекању за даљи поступак или колико чега је пријављено. Осим дефинисања приоритета пријављених инцидената, на основу увида у стање из тријаже је могуће добити и одреднице за дефинисање приоритета свих других активности унутар ЦЕРТ организације, али и информације за припрему анализа, прегледа и извештаја.
Јасно је да како све пријаве долазе ка ЦЕРТ-у, практично је тријажа тачка контакта. Да би то било функционално, мора постојати јасно дефинисано који су начини на који се пријаве достављају (е-пошта, веб форма, тел.), шта треба одн. не треба пријављивати, шта би требало пријава да садржи, време пружања сервиса (одн. очекивани одзив), очекивани сервиси. Људство које стоји иза функције тријаже прима, категорише, и ради иницијалну приоретизацију пријава и захтева. Пријављени инциденти се затим прослеђују одговарајућем аналитичару.

[24] нпр: Organizational Models for Computer Security Incident Response Teams
(Carnegie Mellon University Software Engineering Institute; CMU/SEI-2003-HB-001)
https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf (март 2018.)

ЦЕРТ спроводи **анализу пријављених инцидената** како би се одредила природа пријављене активности, каква су средства (алати) коришћени, опсег активности и одговарајуће мере опоравка и заштите које се примењују. Како форензика и дубља анализа нису у опсегу сервиса (то може бити задатак локалног тима организације конституента), углавном сам процес неће укључивати преглед различитих артефакта или лог-записа, већ је фокус на препознавању основне стратегије напада и покушају корелације ове информације са другим активностима које су пријављене локалним тимовима.
Имајући у виду и постојеће регулаторне препоруке за операторе ИКТ система од посебног значаја шта од инцидената треба пријавити [25], очекивано је да ЦЕРТ неће добити пријаву сваког инцидента који се појави код конституената; стога је потребно праћењем и искуством на основу прикупљених информација доћи до могућности да се адекватно раде процене опсега и могућих последица испољених претњи.

Сагледавањем кроз анализу инцидената, ЦЕРТ може боље да разуме шта се дешава код конституената, идентификује трендове и методе напада, а на основу тога и да износи предлоге за унапређења у области информационе безбедности.

Како представници ЦЕРТ-а нису „присутни на лицу места" током неког инцидента, не може се говорити о оперативној подршци. Али садржај **подршке** се може прилагодити већинским потребама конституената. Неке од активности подршке:

- комуникација са конституентима и одговори на упите добијене телефонским путем или е-поштом;
- истраживање и анализа инцидената и рањивости и давање релевантне информације конституентима;
- вођење евиденције и архиве информација о инцидентима (и евентуално рањивостима), омогућавање приступа тим информацијама конституентима;
- припрема и достављање упозорења и препорука за начин одговора на и опоравак од потенцијалних претњи;
- припрема оперативних и препорука добре праксе;
- припрема активности и материјала за унапређења свести, едукацију из области информационе безбедности за конституенте и ширу јавност;
- учествовање у припреми и одржавању медија за дисеминацију информација (нпр.: е-пошта, листе за слање, главни или посебни веб сајтови, интранет).

[25] http://www.ratel.rs/upload/documents/Regulativa/Informaciona_bezbednost/Uredba%20-%20Dostavljanje%20podataka%20o%20incidentima.pdf (март 2018)

Координација је такође једна од средишњих функција. Уколико овде постоје посвећени ресурси, могуће је постићи свеобухватно праћење, бележење и дисеминацију релевантних информација. Консолидација прикупљених информација омогућава боље сагледавање и проналажење сличних напада, начина злоупотребе, трендова, образаца; потенцијално је могуће идентификовати и нове претње те припремити предлоге третмана и заштите.

Активности су углавном фокусиране на размену информација и омогућавање одн. олакшавање интеракције више учесника који су укључени у анализу и/или опоравак од текућег инцидента. Пожељно је имати могућност комуникације са експертима изван самог ЦЕРТ-а (корисничке заједнице, академска заједница, произвођачи софтвера, друге организације посвећене питањима информационе безбедности) како би се добила додатна помоћ при анализи у случају комплекснијих инцидената – где ЦЕРТ може одиграти битну улогу у повезивању са овим учесницима, али и прослеђивању информација о примењеним мерама.

НАПОМЕНА: Додатни елементи дискусије и информације релевантне за унитрашњу организацију могу се наћи и у поглављу посвећеном функционалном опису система (имајући у виду да унутрашња структура утиче и на избор алата и архитектуру).

4.1 Нацрт акта о начину управљања инцидентима од стране запослених у Националном ЦЕРТ-у

РЕЗИМЕ

Национални ЦЕРТ (формиран при РАТЕЛ) бави се прикупљањем, координацијом и разменом информација о догађајима који угрожавају безбедност ИКТ система, ризика за безбедност ИКТ система, саветовањем лица која управљају ИКТ системима у Републици Србији и јавности, као и промовисањем добре праксе и стандардизованих правила за управљање и санирање инцидената и ризика.

СВРХА

Сврха Политике управљања инцидентима јесте успостава основних правила третирања пријављених инцидената Националном ЦЕРТ-у, како би се обезбедио адекватан, примерен и равноправан третман, усаглашен са регулаторним захтевима и дорбом праксом.

ОПСЕГ

Политика се односи на све запослене у ЦЕРТ-у, прикупљене податке и повезане треће стране обухваћене активностима прикупљања, управљања и дисеминације информација о инцидентима.

Национални ЦЕРТ спроводи законом дефинисане активности и нема ауторитет да захтева спровођење одређених мера.

РЕФЕРЕНЦЕ

- Политика информационе безбедности;
- Закон о информационој безбедности Републике Србије;
- Кодекс понашања за *cyber security* тимове под окриљем TF-CSIRT / Trusted Introducer [26] (**TI TF/CSIRT CCoP**) [27] ;
- Правила за класификацију информација;
- Traffic Light Protocol (TLP) дефиниције и смернице за употребу [28];
- RFC 2350 документ;
- План континуитета пословања;
- План за опоравак од катастрофа;
- Процедура управљања инцидентима.

ПОЛИТИКА

- Национални ЦЕРТ функционише сагласно Кодексу понашања за *cyber security* тимове усвојеном под окриљем TF-CSIRT / Trusted Introducer (**TI TF/CSIRT CCoP**), и унутар Законски дефинисаног мандата;
- Национални ЦЕРТ надлежан је за инциденте у којима је бар једна од укључених страна у Републици Србији;
- Национални ЦЕРТ функционише по принципу сталне доступности (24x7x365) за своје конституенте, али и за националне и међународне партнере.
  У циљу одржавања доступности сервиса, Национални ЦЕРТ примењује релевантне организационо-техничке мере, у складу са Планом континуитета пословања, Планом опоравка од катастрофа;
- Национални ЦЕРТ спроводи активности координације одзива на инцидент и има саветодавну улогу;
- Национални ЦЕРТ не пружа директно подршку крајњим корисницима; инциденте пријављује номинована особа/тим за управљање и решавање инцидената у организицији конституента, и активности координације се спроводе у комуникацији са њима;

---

[26] **Trusted Introducer** је међународна платформа за подршку активностима центара за реаговање на угрожавање безбедности информационих система

[27] https://www.trusted-introducer.org/TI-CCoP.pdf , актуелна верзија 2.4 усвојена 21.9.2017. (март 2018)

[28] **Traffic Light Protocol (TLP)** је скуп одредница које се користе за размену информација са одговарајућим скупом примаоца, укљ. и осетљиве. Користе четири боје за означавање очекиваних ограничења размене информација коју одређује извор а примењују примаоци.
https://www.first.org/tlp/ , вер. 1 (март 2018)

- Национални ЦЕРТ је ауторизован за све (пријављене) инциденте из области информационе безбедности који се појаве или се могу појавити код конституената а захтевају координацију између више организација;
- начин управљања инцидентима дефинсан је ПРОЦЕДУРОМ УПРАВЉАЊА ИНЦИДЕНТИМА. Процес управљања инцидентима ослања се на релевантне оквире, стандарде и искуства добре праксе других ЦЕРТ-ова и релевантних организација;
- Национални ЦЕРТ пружиће адекватан одзив и ниво подршке сагласно утврђеном приоритету пријављеног инцидента; чиниоци који на ово утичу могу бити тип и озбиљност инцидента, тип и специфичности конституента, ширина домета инцидента, доступни ресурси у ЦЕРТ-у, али и др. фактори.
  Уколико није другачије одређено или процењена хитност, први одзив на пријављени инцидент може се очекивати истог дана за пријаву до 13:30 ч., односно наредног дана за пријаве после овог времена;
- све достављене информације о инцидентима третирају се као поверљиве. Информације могу бити прослеђене само у случају и обиму неопходном за помоћ у разрешавању инцидента, према регулаторним и законским одредбама или уз добијено имплицитно или експлицитно одобрење. За потребе размене информација иста може бити анонимизована;
- размена информација руководи се правилима и смерницама TLP (Traffic Light Protocol);
- комуникација мора бити аутентификована (нпр. узвратни позив или порука, лично присуство, итд.);
- примењују се мере заштите комуникације примерене класификацији информација. Осим уобичајеног садржаја који не захтева посебне мере заштите, за размену е-поштом користи се PGP [29] енрипција;
- инциденти се пријављују ЦЕРТ-у преко е-поште, веб-форме, телефона [30]. Предвиђено је да се телефон користи за изузетно хитне случајеве или пријаве ван радног времена;
  Адреса е- поште, веб форма и број телефона за пројаву инцидената треба да буду јасно приказани и доступни на Интернет страници Националног ЦЕРТ-а, уз образац који садржи све потребне релевантне податке за пријаву инцидента (и који се може користити за пријаву е-поштом или телефоном);
- веб сајт и систем за е-пошту треба да буду имплементирани према доброј пракси и заштићени од напада (anti-spam, code-verify, санитација уноса, и сл.).
  На веб сајту објављује се јавни кључ потребан за енкрипцију комуникације.
  Веб сајт треба да јасно назначи права и одговорности за коришћење сервиса и последице у случају злоупотребе.

---

[29] **PGP** (**Pretty Good Privacy**) – назив решења за енкрипцију комуникације електронскких података. **OpenPGP** је најраширенији стандард за енкрипцију електронске поште; дефинисан је у оквиру OpenPGP Радне Групе IETF као предлог стандарда по RFC 4880.
https://www.openpgp.org/about/ (март 2018.)

[30] иако веб-форма може слати податке директно ка систему за управљање инцидентима, евентуално се може имплементирати и да веб-форма генерише е-поруку форматирану за парсирање од стране система за управљање инцидентима) и на тај начин се консолидују канали комуникације

На веб сајту Националног ЦЕРТ-а доступан је RFC 2350 документ стандардизоване форме који дефинише области деловања и одговорности Националног ЦЕРТ-а.

4.2 Нацрт акта о начину поступања изван оквира редовног радног времена

Национални ЦЕРТ има дефинисану особу која је дежурна, доступна („stand-by“) на позив одн. реагује на пријаву електронским путем (е-пошта, веб-форма); систем за пријем пријава прослеђује пријаве за инциденте означене као хитне одн. критичне на уређај дежурне особе. Дежурна особа спроводи иницијалну проверу инцидента. Уколико инцидент није одбачен, ради се дефинисање приоритета. Сагласно дефинисању приоритета, узбуњује се остатак тима неопходан за процес праћења решавања инцидента. Даље се поступа сагласно стандардној процедури.

5 ПРОЦЕДУРЕ

5.1 Предлог правила по којима ће се класификовати степен утицаја инцидента на нарушавање информационе безбедности

У случају када је потребна шира перцепција (националног нивоа) изазов је успоставити систем вредновања сајбер инцидената који би промовисао конзистентност, а истовремено узео у обзир и процену ризика који носи инцидент у одговарајућем контексту. Контекст у овом случају треба да узме у обзир и ситуацију у којој је вредновање истог или сличног инцидента другачије, зависно од ИКТ система који га пријављује.

Овде се предлаже узимање у обзир принципа добре праксе из посебне публикације NIST (National Institute of Standards and Technology) 800-61r2 и прилагођеног система вредновања који користи US-CERT одн. Амерички национални центар за интеграцију сајбер безбедности и комуниникација (National Cybersecurity and Communications Integration Center) - назван NCCIC Cyber Incident Scoring System (NCISS) [31].

NCISS користи пондерисани прорачун како би се добио резултат на скали од 0-100, који се касније користи за тријажу, ескалацију и дефинисање приоритета третмана одн. (у овом случају) активности подршке и/или укључивања других тела у процес решавања и праћења инцидента. Осим тога, имајући у виду да не постоји унифицирана методологија процене ризика међу свим постојећим и будућим конституентима, овај приступ може унети део примене начела ризика у процену дефинисања приоритета инцидента.

У пракси, принцип узима у обзир одговор на питања из неколико категорија, где сваки одговор даје одређену нумеричку вредност. Свака од категорија има свој тежински коефицијент, те се вредности које су резултат ових одговора множе овим коефицијентом (кориговани резултат). Након тога се прорачун спроводи као:

$$\left[\frac{\text{(прорачунати збир коригованих вредности - сума мин. могућег збира коригованих вредности)}}{\text{(сума макс. могућег збира коригованих вредности - сума мин. могућег збира коригованих вредности)}}\right] \times 100 = I$$

Приказ 5-1 : прорачунати скор за дати инцидент

Категорије које би се узеле у обзир при процени инцидента:

[31] https://www.us-cert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf (март 2018)

- **функционални** утицај - на расположивост

  Мера текућег утицаја на угрожени ИКТ систем и организацију;

- утицај на **информацију** - на тајност или интегритет информације

  Користи се у циљу ближег описа степена и типа компромитовања или губитка информације;

- **могућност опоравка – степен и "лакоћа"**
  Процена ресурса потребних за опоравак од инцидента – од интерних, преко потребе за сарадњом и унајмљивањем других организација, до тога да нпр. у неким случајевима опоравак можда није могућ;
- **локација-тип угроженог информационог добра**
  Зависно од позиције и критичности информационог добра потенцијалне последице али и препоручене мере управљања и решавања инцидента варирају;
  Локација угроженог добра може варирати током напада одн. инцидента, те ова може бити потребно овај параметар кориговати током праћења инцидента;
- **актер-извор инцидента (напада)**
  Зависно од типа извора одн. узрока зависи варира и процена вештина и малициозности. Није ретко да не постоји довољно података за реалну процену актера;
- **сектор у коме функционише ИКТ систем (фактор међузависности)**
  У случају претходне анализе, могуће је на основу тога направити расподелу коефицијената. За неке од система критичне инфраструктуре, међутим, јасно је да могу условити и другачији обим последица. Инцијално служи као начин дистинкције између основних конституената, ИКТ система од посебног значаја, и др. ИКТ система (сагласно томе и садржај може бити промењен);
- **Потенцијал последица**
  Процена, која додатно узима у обзир како реалност ескалације тако и национални контекст у случају да угрожени сервиси буду потпуно онемогућени (дакле, исти инцидент у различитим организацијама може бити релативно другачије третиран). При процени треба узети у обзир колико је велика та организација (број корисника), колико екстерних корисника користи њихове услуге, колико је оквирна финансијска "мера" прихода или буџета и сл.
  Процена треба да буде третирана управо тако – као процена у најбољој намери и сагласно познатим параметрима али са фокусом на конкретни циљ – приоретизација инцидента.

Категорија • **АТРИБУТ**	**Коеф. кат.**	**Коеф. атриб.**	**Напомена**
Функционални утицај - на расположивост	**6**		
• НЕМА Организација није онемогућена да пружа		0	

Категорија • **АТРИБУТ**	Коеф. кат.	Коеф. атриб.	Напомена
сервисе својим корисницима			
• НИЗАК Губитак ефикасности, али сви критични сервиси и даље су доступни свим корисницима уз мање утицаја на перформансе		30	
• УМЕРЕН Губитак критичних сервиса за неке од (подскуп) корисника система		60	
• ВИСОК Организација је изгубила могућност пружања свих критичних сервиса свим корисницима		100	
Информациони утицај **- на тајност или интегритет информације**	**4**		
• НЕМА Није било одлива, измена или другачије врсте компромитовања информација		0	
• НА ИНТЕГРИТЕТ модификација или уништење (без претходног одобрења одн. овлашћења)		100	
• НА ПРИВАТНОСТ повреда тајности над личним подацима		50	
• НА ЗАШТИЋЕНО повреда тајности заштићене информације (која није јавно позната и у власништву је организације) – нпр. пословне тајне, интелектуално власништво, информације о заштићеној критичној инфраструктури и сл., нарочито осетљиви лични подаци		70	
• НА ПОВЕРЉИВО повреда тајности поверљивих информација (кључне пословне тајне, државне тајне, законски дефинисани тајни подаци, и сл.,		90	

Категорија • АТРИБУТ	Коеф. кат.	Коеф. атриб.	Напомена
креденцијали за критичне системе)			
Могућност опоравка – степен и "лакоћа"	**3**		
• НИЈЕ ПОТРЕБНО инцидент не захтева мере опоравка		0	
• УОБИЧАЈЕНО предвидљиво време опоравка, сопственим снагама са постојећим ресурсима		20	
• УЗ ПОМОЋ предвидљиво време опоравка, уз ангажовање додатних ресурса		40	
• ОТЕЖАНО није предвидљиво време опоравка, уз ангажовање додатних ресурса и помоћи споља		60	
• БЕЗ ОПОРАВКА опоравак није могућ (нпр. одлив података се већ десио)		100	
Локација-тип угроженог информационог добра	**5**		
• СТАНДАРНИ СИСТЕМ У ДМЗ [32]		25	
• СТАНДАРНИ СИСТЕМ У ИНТ. МРЕЖИ		40	
• КРИТИЧНИ СИСТЕМ У ДМЗ		65	
• КРИТИЧНИ СИСТЕМ У ИНТ. МРЕЖИ		85	
• УПРАВЉАЧКИ СИСТЕМ		100	
• НЕПОЗНАТО		50	
Актер-извор инцидента (напада)	**2**		
• НЕПОЗНАТО		50	
• HACKER		40	
• ИТЕРНИ АКТЕР		30	
• МАЛИЦИОЗНИ ИНТЕРНИ АКТЕР		70	

[32] „Демилитаризована зона", DMZ
Под-мрежа у којој се налазе и преко које се излажу „спољном свету", тј. Мрежи којој се не верује (као што је Интернет) сервиси намењени за опслуживање спљних корисника. Намена је додавање безбедносног слоја испред локалне мреже (local area network; LAN) тако да неки систем у спољашњој мрежи може приступити само оно што му је изложено из DMZ, док је остатак мреже заштићен firewall системом.

Категорија • АТРИБУТ	Коеф. кат.	Коеф. атриб.	Напомена
• APT (*advanced persistent threat*)		100	
Сектор у коме функционише ИКТ систем (апликабилност, фактор међузависности)	**3**		
• Електронске комуникације		100	
• Услуге информационог друштва		55	
• Послови у органима јавне власти		30	
• Производња, пренос и дистрибуција електричне енергије		90	
• Саобраћај (железница, ваздушни, друмски, пошта)		90	
• Производња, прерада, превоз и дистрибуција нафте, деривата и гаса		80	
• Управљање нуклеарним објектима		15	
• коришћење, управљање, заштита и унапређивање добара од општег интереса (вода, сировине, путеви, шуме, ...)		60	
• производња, промет и превоз наоружања и војна опрема		20	
• Комуналне делатности		25	
• Управљање отпадом		25	
• Здравство		35	
• Финансијске институције		35	
• Трговина, комерцијалне делатности		25	
• Друго		10	
Потенцијал последица	**5**		
• ЗАНЕМАРЉИВ		0	
• НИЗАК		25	
• УМЕРЕН		50	
• ВИСОК		75	
• КРИТЧАН		100	

Табела 5-1 : категорије за процену приоритета индицента

Сектор у коме функционише ИКТ систем (фактор међузависности) и **Потенцијал последица** су сегменти у којима се не очекује унос од стране организације која пријављује инцидент.

Приказани параметри су само пример и “слободна процена” током припреме предлога. Очекује се да исти буду прилагођени.

Узевши у обзир предлог класификације нивоа озбиљности, прорачунати Индекс за неки инцидент може се искористити за дефинисање приоритета третмана :

Приоритет	Низак	Умерен	Висок	Критичан
Граничне вредности	<35	35-60	60-85	>85

Табела 5.1:Одређивање приоритета на основу вредности индекса

ПРИМЕР: [33]

Функционални утицај	*# УМЕРЕН = 60*
Инф. Утицај	*# на ПРИВАТНОСТ = 40*
Опоравак	*# УОБИЧАЈЕН = 20*
Угрожено добро	*# КРИТИЧНИ У ДМЗ = 60*
Актер	*# ХАКЕР = 40*
Сектор организације	*# ЕЛ. КОМУНИКАЦИЈЕ = (конституент) = 100*
Последица	*# ВИСОК = 75*

Прорачунати Индекс инцидента (узевши дате параметре) = ~ 44 => Умерен

У случају да постане уочљиво да се ради о серији повезаних инцидената, укупно рангирање се руководи највишим постојећим. У случају идентификовања потенцијалне кампање, процена приоритета за кампању агрегирано би се представила наредним вишим рангом у односу на идентификоване за појединачне инциденте.

5.2 Анализа потребе за појединачним процедурама којима се уређују мере заштите ИКТ система од посебног значаја у Србији

Законом о Информационој безбедности Републике Србије прописује се да (извод):

- (члан 7) Оператор ИКТ система од посебног значаја одговара за безбедност ИКТ система и предузимање мера заштите ИКТ система (…у 28 области, којима…) се обезбеђује превенција од настанка инцидената, односно превенција и минимизација штете од

[33] Пример имплементације алата за ову намену доступан је на https://www.us-cert.gov/nciss/demo#

инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима;

- (члан 8) Оператор ИКТ система од посебног значаја дужан је да донесе Акт о безбедности ИКТ система …(којм се)… одређују (…) мере заштите, а нарочито принципи, начин и процедуре постизања и одржавања адекватног нивоа безбедности система, као и овлашћења и одговорности у вези са безбедношћу и ресурсима ИКТ система од посебног значаја…. Акт (..:) мора да буде усклађен с променама у окружењу и у самом ИКТ систему….Оператор ИКТ система (…) је дужан да (…) врши проверу усклађености примењених мера ИКТ система са Актом (…) и то најмање једном годишње и да о томе сачини извештај;
- (члан 3) Приликом планирања и примене мера заштите ИКТ система треба се руководити начелима …управљања ризиком, свеобухватне заштите, стручности и добре праксе, свести и оспособљености.

Начела и мере. одн. области које Закон наводи, иако другачије структуиране, у значајној мери произилазе из захтева добре праксе и стандарда као што је ISO/IEC 27000 фамилија стандарда [34] - а најпре ISO/IEC 27001 (који представља скуп захтева за систем управљања информационом безбедношћу - *ISMS, information security management system*). Систем управљања информационом безбедношћу подразумева систематски приступ управљању информацијама неке организације како би се очувала њена безбедност. Обухвата људе, процесе, технологију и пратеће документе у циљу управљања, надзора и провера стања. Систем упраљања информационом безбедношћу треба да очува поверљивост, интегритет и доступност информација применом процеса управљања ризицима (узимајући у обзир специфичности тј. контекст сваке поједине организације).

Поједностављено речено, управљање информационом безбедношћу бави се доношењем одлука о начину третирања ризика. Ово, међутим, мора да прати и процес одн. систем којим ће (у циљу управљања ризицима) успоставити такав оквир да се доделе одговорности на адекватан начин, те да стратегије и мере буду усклађене са кључним организационим циљевима и регулаторним захтевима - кроз усклађеност са политикама и интерним контролама; ово се обично означава као *Information Security Governance* [35].

Закон о информационој безбедности кроз поменуте чланове препознаје потребу како за имплементацијом *Information Security Management* тако и *Information Security Governance* праксе.

Претпоставка је (имајући у виду да је рок за то истекао) да је већина оператора ИКТ система донела „кровни“ Акт о безбедности ИКТ система – постављајући тако принципе и основе за даљу имплементацију мера, процедура и праксе заштите. Имајући у виду да ауторима у тренутку писања нису познати резултати прегледа имплементације мера, није могуће процењивати зрелост

[34] https://www.iso.org/isoiec-27001-information-security.html

[35] GARTNER дефинише појам *Information Security Governance* као

“Спецификација права одлучивања и оквир за препознавање и очување одговорности како би се охрарило пожељно понашање у вредновању, стварању, чувању, коришћењу, архивирању и брисању информација. Укључује процесе, роле, стандарде и метрику којима се обезбеђује ефентивна и ефикасна употреба информација у омогућавању да организација постигне своје циљеве”.

имплементације организационо-техничких мера код оператора ИКТ система од посебног значаја, као и до ког нивоа су спроведене процедуре и упутства.

Јасно је да је без дефинисаних политика, процедура, упутстава и/или усвојених стандарда теже пратити и конзистентно спровести постављене циљеве (па чак и елементе основне „безбедносне хигијене“). Самим тим је и већа могућност за грешке или немар који могу повећати изложеност организације. Законом препознате области у којима треба применити мере могу (чак и свака за себе) захтевати припрему и усвајање једне или више политика, процедура и упутстава. Садржај може значајно варирати између институција – како због специфичности сектора деловања, регулаторних захтева (националних и међународних), тако и због контекста пословне политике, културе и организације; наведено јасно индикује и спефичност нивоа и садржаја детаља који могу бити потребни. Стога не постоји једнозначан начин „пописивања“ и формализације елемената подршке имплементацији оваквих мера. Основни принципи - произашли из стандарда и оквира добре праксе – јесу основа.

У наставку је дат прилагођени образац релевантних политика и процедура, као оквир и пример за даљу припрему и имплементацију.

У циљу унапређења информационе безбедности и сагледавање реалног стања предлаже се да надлежно тело у Републици Србији размотри припрему стандардизованог оквира процене техничких ризика и унапређење управљања ризицима који би могли бити полазна тачка примарно за операторе ИКТ система од посебног значаја или барем за операторе ИКТ система који су у државном власништву одн. органе јавне власти, али (наравно) доступни и за друге операторе ИКТ система. Овакве иницијативе и пракса – ширег опсега од оних које се баве само техничким ризицима – нису непознате (као што се може видети нпр. из прегледа извештаја Европске комисије из 2012 о прегледу методологија процене ризика за заштиту критичне инфраструктуре [36]). Као пример може се навести и (иако сада изван званичне обавезне употребе) *Суплемент за процену и третман техничких ризика* из архиве *Националног центра за cyber безбедност Уједињеног краљевства* [37].

Овакав приступ би могао помоћи хармонизацију праксе, ојачати међусекторску сарадњу са центрима за хитне реакције, а са становишта Националног ЦЕРТ-а, индиректно олакшати дефинисање приоритета и третман пријављених инцидената.

У том смислу, могући начин оперативних активности – у контексту информационе безбедности - могао би бити покренут и контролисан кроз активности Тела за координацију послова информационе безбедности (чија је законски дефинисана улога „да остварује сарадњу између органа и усклађује обављање послова у функцији унапређења информационе безбедности, иницира и прати превентивне и друге активности у области информационе безбедности, предлаже мере за унапређење информационе безбедности у Републици Србији, даје сугестије и предлоге који се односе на припрему стратешких докумената, подзаконских аката и политика информационе безбедности у Републици Србији…“[38])

[36] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf (март 2018.)

[37] https://www.ncsc.gov.uk/guidance/technical-risk-assessment-and-risk-treatment-is1-2-supplement (март 2018.)

[38] http://mtt.gov.rs/vesti/obrazovano-telo-za-koordinaciju-poslova-informacione-bezbednosti/ (март 2018.)

5.3 Нацрти процедура којима се уређују мере заштите

Нацрти процедура се прилажу као посебни документи, уз овај документ:

- Политика класификације информација;
- Процедура управљања инцидентима.

5.4 План за обезбеђење континуитета пословања

Појмови, континуитет пословања (*business continuity, BC*) и опоравак од катастрофалних ситуација (*disaster recovery, DR*), често се користе да означе исти концепт. Иако тесно повезани, разлика постоји, те је битно усагласити дефиниције [39].

Континуитет пословања односи се на способност да се прилагоди изазовима, ризицима и одржи континуитет пословања. Подразумева припрему процеса и процедура које треба имплементирати како би целокупни пословни систем (пословни процеси, а пре свега критичне функције) био оперативан и након непредвиђених догађаја.

Три су основна аспекта кроз која се остварује континуитет пословања:

- висока доступност – способност као и процеси којима ће се омогућити да и поред локалних отказа (у процесима, инфраструктурним ресурсима, *хардвер*-у или *софтвер*-у) буде могућ приступ потребним ресурсима (апликацијама, подацима, …);
- континуитет операција – способност да се одржава функционисање у „редовним“ условима (нпр. да није неопходно гасити апликацију да би се радио редован *backup* или др. планске активности одржавања);
- опоравак од катастрофалних ситуација (*Disaster Recovery*) – способност поновне успоставе функционисања информационог система након таквог догађаја који потпуно уништи функционисање постојећих система (нпр. комплетно уништење локације); време и начин опоравка обично варира за одређене сервисе зависно од њихове критичности.

Из наведеног је очигледно да је *DR* део *BC* плана, фокусиран пре свега на технолошку инфрастуктуру и системе, док је *BC* има додир са скоро сваким сегментом пословних процеса, инфраструктуре и људи неког пословног система.

У наставку се сумира методолошки приступ управљању континуитетом пословања, у циљу структуирања даљих корака у пракси.

Процес управљања континуитетом пословања (*Business Continuity Management, BCM*) идеално је цикличан (затворена петља). Методолошки се представља обично кроз 3 или 4 главне фазе:

[39] https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR (март 2018.)

- фаза **Сагледавање стања** (*assess*) садржи два главна сегмента:
  - анализа;
  - процена.

  Започиње се анализом потенцијалних ризика, последица и способности да се исти отклоне или умање. Потенцијални ризици се анализирају и успоставља се профил ризика кроз:

  - пословне локације;
  - пословне функције;
  - пословне процесе.

  Последице неких догађаја се процењују узимајући у обзир финансијске губитке, изгубљену добит или могућности и репутационе аспекте.

  Следи анализа постојећих способности да се примене „заштитне“ мере, а користећи те информације прилагођава се оквир за управљање ризицима. Да би се профил ризика свеобухватније сагледао, препорука је структуирати процес кроз неки стандардизовани оквир, кроз више сегмената, нпр. [40]:

  - стратегија – потребна за обављање свакодневних активности и обезбеђивање континуираног рада;
  - организација – структуре, вештине, комуникација и одговорности запослених;
  - апликације и подаци - *софтвер* неопходан за пословну оперативност као и методи за обезбеђивање високе доступности (*High availability*) коришћени за имплементацију тог *софтвер*-а;
  - процеси – критични пословни процеси неопходни за пословање, као и ИТ процеси неопходни за целокупну функционалну оперативност;
  - технологија – системи, мрежа, као и специфична технологија за одређен делатност неопходна да се обезбеди континуални рад и *backup* апликација и података;
  - објекти и инфраструктура – за потребе DR локације у случају да је примарна уништена.

САГЛЕДАВАЊЕ СТАЊА:

- одређивање профила ризика;
- приоретизација критичних пословних процеса;
- процена и прорачун утицаја на пословање;
- процена тренутног стања и способности у пословном и ИТ домену да се третирају идентификовани ризици.

Након овога се идентификују области ризика које треба додатни аналиизирати и процењује се зрелост способности примене заштитних мера.

[40] IBM Business Resilience Framework
„Risk mitigation for business resilience“ - White paper (IBM, 2007)
https://www-935.ibm.com/services/pl/gts/html/pdf/gmw14000-usen-00.pdf (март 2018.)

- фаза **Планирање** садржи два главна корака**:**
  - дефинисање;
  - дизајн.

  У овој фази постављају се циљеви имплеметнације мера за отклањање или умањење ризика или унапређење стања кроз:

  - дефинисање опсега стратегије третмана ризика – да ли на нивоу целокупног пословног система, одређених пословних функција, пословних процеса или пословних система;
  - избор ризика који ће се третирати, укљ. и процедуралне, техничке, организационе, економске, геолошке, економске, финансијске, инфрастурктурне, друштвене, државне и из области животне средине.

  Након овога се припрема дизајн стратегије и архитектуре, узимајући у обзир:

  - пословна и финансијска оправдања и сагласност руководилаца, као и мишљења интерних и спољних ревизора;
  - спецификацију и оквир одговорности (*governance*), надлежност и политике (које се односе на мисију, дисциплину, и комуникацију);
  - дисциплине управљања системима у областима као што су управљање конфигурацијама, променама и проблемима [41];
  - физичку и логичку безбедност;
  - апликације и податке, укљ. и заштиту података, *backup*, и синхронизацију;
  - извршавање програма, укљ. извештавање, роле и одговорности, односе са јавношћу, пословну интеграцију и покретање планова;
  - управљање објектима и инфраструктуром.

  Дизајн решења дефинише циљеве и смернице, функционалне, логичке и техничке компоненте, те преглед трошкова (узевши у обзир однос добијеног и уложеног).

ПЛАНИРАЊЕ:

- одређивање циљева континуитета пословања;
- одлучивање о третману ризика:
  - прихватање;
  - трансфер;
  - припрема стратегије примена мера за третман.
- припрема плана и архитектуре која користи технологију и сервисе за постизање континуитета пословања, високе доступности и опоравка од катастрофалних ситуација.

[41] ITIL (*IT Infrastructure Library*) процеси.

- фаза Имплементација и тестирање

Улазни параметри из преходне фазе дефинишу задатке и користе се као основа за детаљнији план имплементације (с циљем заштите критичних информација и континуитета одн. опоравка пословних функција).

По завршеној имплементацији ради се валидација и тестирање. Добра пракса је да то иде кроз 2 фазе :

- декомпозиција *data* центра;
- извршавање тестног плана, који обухвата обухвата и *data* центре, ланац апликација, саме аплиакције, и компоненте.

Кроз ово се проверавају претпоставке и утврђују времена потребна за коначне стратегије опоравка, процедуре , и процесе; као елемент проналажења потенцијалних проблема у плановим за ИТ и пословни опоравак пре стварних догађаја користе се и тзв. „папирни“ (*walk-through*) тестови.

ИМПЛЕМЕНТАЦИЈА:

- Имплементација технологије и/или сервиса за континуитет и опоавак у циљу оспособљавања извршења плана континуитета
- Тестирање у циљу валидације усклађености са дефинисаним *RTO* и *RPO*

- фаза Управљање и одржавање

Након дефинисања и имплементације стратегије одржавања пословања, неопходно је успоставити централизован *governance* програм како би се обезбедило управљање, контрола и надзор ове стрегетије. Да би се контролисали негативни ризици, ова фаза укључује:

- константан процес управљања ризицима пре, за време и после насталих дођаја;
- редовно тестирање да би се обезбедила спремност за непредвиђене ситације;
- спровођење политика и процедура из governance оквира;
- обука како би се обезбедило да сви запослени знају своје улоге и одговорности;
- проакиван приступ заштити информација и података;
- тачна и прецизна комуникација у сваком тренутку;
- могућност приступа критичним инфомрмацијама када је то потребно.

ОДРЖАВАЊЕ:

- континуалан и интегрисан процес;
- тестирање, праћење и извештавање о статусу планова, архитектуре, процеса, организационе спремности;
- покретање процеса измена у случају промењених услова одн. неусклађености.

Фокус је на сталном унапређењу стратегије одговора на ризике. О свим изузецима примећеним надзором, треба правовремено известити надлежне, и истрајати на проналажењу правог узрока.

Уз овај документ, прилаже се Оквир плана континуитета пословања.

5.5 План опоравка од последица инцидента

План опоравка од инцидената у основи је покривен поступцима из Плана за континуитет пословања. Плана за континуитет пословања предвиђа критериујме који се користе за процену стратегије опоравка.

Припремом тзв. *DR* плана (у основи намењеном опоравку ИКТ сервиса) потребно је извршити адекватно мапирање пословних сервиса (функција) на ИКТ сервисе, а затим и на апликације и инфраструктурне ресурсе који те пословне сервисе подржавају. Критеријуми опоравка (RTO, RPO), као и одлуке о третирању ризика основа су за стратегију решења. Овим параметри су основа за припрему архитектуре и дизајна решења. Управо у овом сегменту се крије и одлука о начину и могућностима опоравка одн. одржавања функционалности одређених сервиса и ком контексту, те од тога ће кључно зависити и нпр. могућност активирања техничких процедура опоравка без потребе за активирањем DR плана или сл.

6 ПОСТУПАК

6.1 Анализа изводљивости различитих модела прикупљања и размене информација о ризицима за безбедност ИКТ система између Националног ЦЕРТ-а и оператора ИКТ система од посебног значаја

Адекватна и правовремена информација кључне су за напоре да се умање последице неког актуелног или будућег инцидента, односно спрече злоупотребе неких рањивости. Све је већи изазов из великог обима информација извући ону која ће заиста бити „од користи“ .

Информација – која би била од користи ЦЕРТ-у и конституентима у смислу одзива на инциденте, примена мера против могућих претњи или решавања компромитације - може се назвати „Активном информацијом” (*actionable information*) [42]. Различите организације и контекст утичу и на појам/садржај Активне информације. За национални ЦЕРТ свака пријава инцидента али и добијено упозорење са друге стране, или независно прикупљена информација може бити Активна информација, уколико се одређени сервис који је у питању налази у ИКТ систему конституента. С друге стране, за конституента нпр. информација о индикаторима и њиховом повећаном број у домаћем адресном простору која долази од стране ЦЕРТ-а може бити Активна информација.

Да би се нека информација третирала као Активна информација, сматра се да су њени основни квалитативни критеријуми (контекстуално): **релевантност**, **правовременост**, **тачност**, **комплетност**, и **могућност увоза информације**.

- да би информација била **релевантна**, мора бити применљива на окружење у домену одговорности примаоца. Са становишта националног ЦЕРТ-а могло би се рећи да је битно познавање мрежних опсега и домена конституената, како би се на одговарајући начин могле третирати одн. издвајати информације из различитих извора;
- по питању **правовремености,** у неким случајевима и пар сати може значити да нешто није више релевантно. Размена великог обима података у приближно реалном времену, међутим, била би друга крајност и могла би негативно утицати на могућности увоза података, али и захтевати додатно време за њихову обраду. Стога је потребно пронаћи одговарајући компромис између правовремености, комплетности и тачности информација. Терет проналаска баланса (али и вредности информације) лежи на обе стране – и ЦЕРТ-а и конституента;
- информација мора бити **тачна** – како би прималац могао исту „конзумирати“ без одлагања, под претпоставком да је претходно проверена и без познатих грешака. Ово је суштински комбинација вере у поузданост извора и локалног контекста примаоца. Додатни фактор је транспареност извора који се користи у прикупљању. Размена информација између укључених страна неопходна је да би се одржало поверење, али и исправиле мањкавости;
- активна информација би сама по себи требало да има значај за примаоца у контексту у коме је доступна. Али, и за оног који пружа информацију може бити проблем да потврди

[42] Actionable information for security incident response (ENISA, Nov. 2014.), https://www.enisa.europa.eu/publications/actionable-information-for-security (март 2018.)

њену **комплетност**, тј. шта је то што можда недостаје. Додатно (очекивано), обим одн. ниво детаља пружених информација може бити лимитиран из више разлога (не одавање превише интерних података, правно-регулаторна ограничења, и сл.). Стога је битно да обе стране усагласе одговарајући баланс између потребног контекста и ограничења. Одређене информације саме за себе можда немају значај, али комбиноване са другим добијају одговарајући контекст;

- неопходно је да информација може бити **увежена –** форма треба да омогући лак увоз и извлачење опажених елемената и индикатора. Овде је нагласак на форматима и преносним протоколима који се користе за размену података. Активна информација би на крају требала бити целовита и дата у формату који је јасно описује, како би је системи на страни примаоца могли примити (мање или више) аутоматизовано и искористити за даљу корелацију и придруживање другим информацијама.

Други аспект који треба размотрити, јесте тип одн. ниво детаља информација које могу бити размењене. За потребе дискусије овде се преузима преглед одн. структура коју даје ENISA [43], имајући у виду да на једноставан начин илуструје процес њиховог сажимања и помаже у индикацији елемената који у контексту релације Националног ЦЕРТ-а и конституента не доносе адекватну вредност или сувише откривају о системима конституента:

Ниво података	**Тип информације**
Подаци нижег нивоа	• записи мрежног саобраћаја; • лог записи; • узорци извршних датотека, докумената, е-порука.
Индикатори откривања догађаја	• IP адресе, DNS [44] називи, URL [45]; • вредности неких посебних поља (нпр. заглавље е-поруке); • артефакти који се односе на неки малициозни код; • специфичне секвенце догађаја ниског нивоа који имају везе са неким малициозним понашањем.
Упозорења	• рањивости, код за експлоатацију, закрпе, стање закрпа; • обрасци на нивоу хоста, сервиса, мреже или Интернета.

[43] Actionable information for security incident response (ENISA, Nov. 2014.) https://www.enisa.europa.eu/publications/actionable-information-for-security (март 2018.)

[44] DNS (Domain Name System) – базни интернет сервис, који омогућава превођење текстуалних у нумеричке ознаке и обратно. https://www.rnids.rs/lat/domeni/dns-sistem (март 2018.)

[45] URL (Uniform Resource Locator) - адреса-референца на неки web ресурс, означава његову мрежну локацију и начин (протокол) приступа, често се као синоним (упрошћено) користи web адреса. https://searchnetworking.techtarget.com/definition/URL (март 2018.)

Стратешки извештаји	• сажете анализе претњи, у текстуалном облику.

Приказ 6-1 : слојеви информација према детаљности

У општем случају, ЦЕРТ националног нивоа није у позицији да се бави свеобухватним надзором на националном нивоу; ЦЕРТ-ови са интерном конституенцијом (понекад организовани и као продужена рука неког SoC - Security Operations Centre [46]) су у другачијој су позицији. Стога је за ове потоње примеренија имплементација и прикупљање података нижег нивоа.

Надлежност Националног ЦЕРТ не укључује активно решавање инцидената „на лицу места“, па самим тим није ни посебно предвиђена дубља анализе логова, мрежног саобраћаја или др. артефакта. Стога је и потенцијални ниво аутоматизације и интеграције у размени од стране конституента ка ЦЕРТ-у делом ограничен. Очекивана је успостава специфичних режима размене података, мануелних одн. мање аутоматизованих анализа и коришћења више алата у циљу сагледавања стања у домену активности.

Подаци о инцидентима, одн. подаци добијени од конституента, само су део онога што се „слива“ у ЦЕРТ.

Део података нижег и осталих нивоа Национални ЦЕРТ може добити из интерних извора, нпр.

- колекција логова и записа о мрежним везама са сервера, *firewall* уређаја,различитих сензора, IDS, *honeypot* система,итд.;
- систем за снимање и/или анализу мрежног саобраћаја;
- имплементирањем SIEM-а или сличног система, којим се централизује скупљање података са више извора (лог записа и записа о мрежним везама); добија се бољи увид и могућност корелације, па чак и праћење неких трендова или аномалија;
- систем за препознавање и управљање рањивостима, кроз анализу доступних сервиса и и проверу статуса закрпа;
- и др.

… али (већи) део дођи ће из екстерних извора

- мрежа других *honeypot* система;
- *feed*-ови репутационих сервиса, *threat intelligence feed*-ови, информације о *hack*-ovanim системима;
- информације добијене од других ЦЕРТ-ова.

Управо ови екстерни подаци можда стављају у фокус додатну улогу ЦЕРТ-а (из перцепције конституента) као агрегационе тачке која из већег броја различитих извора комбинује информације на различитим нивоима, примењује контекстуалну филтрацију и фузију прикупљеног и потенцијално може помоћи у откривању корелација скривених у мноштву података. Уколико ЦЕРТ открије неку претњу самостално кроз аутоматизоване системе, исти могу генерисати (осим

[46] SoC (Security Operations Centre) - тимови организовани да прате, спречавају, откривају, процењују и одговарају на cybersecurity претње и инциденте.
https://www.gartner.com/newsroom/id/3815169 (март 2018.)

података нижег нивоа) и податке типа индикатора или чак упозорења, а истрага довести до различитих информација које могу бити од користи у будућности (и за конституенте). Треба рећи да је и поред евентуално високог степена аутоматизације углавном човек тај који доноси коначну одлуку о овим информацијама.

Осим наведеног, ЦЕРТ у овом случају за свог конституента практично обавља и додатну валидацију спољних извора, али и трансформацију ових података у форму коју конституенти могу конзумирати у својим системима.

Типично, конституенти од ЦЕРТ-а у оваквом сценарију користе информације типа индикатора и упозорења , као што су IP адресе и/или DNS називи *C&C* (*Command & Control*) система [47], називи или *hash* [48] вредности датотека, информације о тактици-техникама-процедурама нападача (скраћено *TTP;* то су нпр. заједнички елементи неких *phishing* кампања, циљани ресурси и сл.).

Део података које ЦЕРТ „дистрибуира“ може произаћи из реалних инцидената. У том случају од стране ЦЕРТ-а морају се предузети мере анонимизације, и то само оних елемената као што су извор података, „жртва“ напада, начин прикупљања података и било какве личне информације. Делимично је ово можда могуће имплементирати и кроз примену таквих формата, конзистентан унос и третман мета-података којима се имплементирају правила као што је то TLP, али уколико ово није доступно у потпуности, инструкције о третману информација се могу пренети и другим медијима. Национални ЦЕРТ и конституенти за овај ток информација треба да усагласе оквир којим се утврђују прецизније правила за размену информација о инцидентима.

Учешће националног ЦЕРТ-а у у различитим групама и зајединцама значајно је као елемент грађења екепртизе али и одржавања свести о актуелним дешавањима и грађењу међусобног поверења. Размена информација у овом контексту треба да иде у оба смера – од Националног ЦЕРТ-а ка конституентима и обратно.

У основи, овде се препознаје оквир потреба за имплементацијом:

- *Threat Intelligence / Threat Sharing платформе*, која би служила за прикупљање, чувањем и корелацију индикатора (компромитовања) напада, threat intelligence података, можда и информација о рањивостима те као интерфејс (за диструбуцију информација) ка конституентима; платформа мора бити довољно отворена да омогући прилагођавање стандардним форматима и механизмима за размену података;
- платформе за дискусије и размену информација/знања/искустава (портали, форуми, заједнице) ; ово може бити имплементирано нпр. према критеријумима привереног сектора или/и технички оријентисаних тема и сл., а реализација може бити и као јавна али

[47] C&C системи управљају тзв. *botnet* мрежом рачунара (често се називају и *botnet* зомбии); ова мрежа – обично инфицираних – рачунара бот командом C&C система користи се за дистрибуирање малициозног софтвер-а, неовлашћено прикупљање информација, а понекад и за оркестрацију DDoS напада. https://whatis.techtarget.com/definition/command-and-control-server-CC-server (март 2018.)

[48] Специфичним алгоритмом прорачуната вредност (тзв. *File Checksum*) која је јединствена за одређену датотеку и служи за идентификацију одн. потврду њене аутентичности; један од веома коришћених начина провере да ли је у питању малициозна датотека провером по доступним реистрима. https://blogs.cisco.com/security/malware_validation_techniques (март 2018.)

и као „приватна“ тј. заштићена платформа која је доступна само укљученим конституентима и ЦЕРТ-у;

- система за пријем инцидената од стране конституената (е-пошта, веб-сајт са припремљеном формом, препоручљиво са неком врстом сервиса подршке типа *call*-центар са интегрисаним регистром података о конституентима, другим ЦЕРТ-овима и сл., али и унутар ЦЕРТ-а).

6.2 Нацрт процедуре којом се уређује поступак пријема, обраде и реаговања на податке о инцидентима

1 **Пријава инцидента**

1.1 **Пријем пријаве инцидента**

ЦЕРТ прима пријаву преко е-поште, веб-форме, телефона[49]; тел. се користи за изузетно хитне случајеве или/и ван радног времена.

ЦЕРТ може доћи до информације и пре пријаве од стране конституента – праћењем форума, ажурних “црних листи”, сервиса за евиденцију компромитованих система, али и праћењем сопствених IDS или др. система за надзор у сопственој мрежи или периметру. Уколико ЦЕРТ примети на независним изворима потенцијално инцидентну ситуацију свог конституента, треба да контактира истог и заједнички започну процес пријаве (или одбацивања).

1.2 **Бележење инцидента (регистрација)**

Пријава се бележи у систему за управљање инцидентима; инцидент уносом добија јединствен идентификациони број “случаја” (који аутоматизовани систем за управљање инцидентима обично сами додељују). У случају комбиновања инцидената, потребно је обратити пажњу на оригинални идентификатор.

Форма тј. информације које треба да садржи пријава објављени су на сајту и доступни конституентима и широј јавности за преузимање; очекује се да се користе при пријави инцидената.

2 **Тријажа**

Фаза се састоји од 3 основне под-фазе:

- провера;
- иницијална класификација;
- додељивање.

Спровођењем тријаже долази се до приоретизације и основа за даљи прогрес праћења и разрешења инцидента - озбиљност, хитност, коме доделити и сл.

[49] иако web-форма може слати податке директно ка систему за управљање инцидентима, евентуално се може имплементирати и да web-forma генерише е-поруку форматирану за парсирање од стране система за управљање инцидентима) и на тај начин се консолидују канали комуникације

Током ове фазе, тражи се одговор на нека од основних питања [50]:

- Да ли је заиста у питању инцидент везан за повреду информационе безбедности или не?;
- Да ли је у питању основни конституент, неки други ИКТ систем од посебног значаја, "обични" ИКТ систем, појединац или др.? ;
- Колико озбиљно делује инцидент? Постоји ли могућност да се – директно или индиректно – прошире последице унутар организације ? Може ли да утиче и на друге конституенте? ;
- Да ли постоје посебни захтеви одн. околности које треб узети у обзир за третман конкретног инцидента? ;
- Коме доделити и колико ресурса може бити потребно за праћење инцидента? Да ли потенцијално може бити потребно из неког разлога укључити (и) ресурсе изван ЦЕРТ-а?.

2.1 **Провера инцидента (верификација)**

Пријава се проверава и процењује да ли је у питању заиста (релевантан) инцидент. Очекивано је да обим "небитних" пријава варира како од конституента, тако и од дефинисане и препоруке и/или праксе нивоа инцидента који треба да буду пријављени, али и поштовања ових смерница.

Спровести анализу "небитних" у односу на "битне" пријаве у циљу даљих корака за едукацију конституената и оптимизацију ресурса.

Уколико страна која пријављује инцидент излази из оквира "препознатих" конституената, одн. постоји надлежна ЦЕРТ организација, пријава може бити одбијена или евидентирана и прослеђена другој страни.

Уколико пријава индицира и захтев за сервис који излази из мандата ЦЕРТ-а, такав захтев може бити одбијен (инцидент као такав може бити на неки начин евидентиран).

За било који од наведених случајева применити одговарајући третман и послати одговор на пријаву.

Сваку пријаву стандардно прати адекватан (аутоматизовани) одговор :

- за пријаву преко е-поште и веб-форме оптимално је да то буде е-порука са потврдом пријема, следећим кораком, ев. шта се очекује од организације која је пријавила инцидент;
- уколико је пријава одбијена, одговор садржи поруку која појашњава статус и разлог одбијања, пожељно и савет како избећи овакву ситуацију.

Уколико је у питању пријава инцидента која је анонимна, или од стране за коју постоји индикација да није "поуздана", иста се обично игнорише.

2.2 **Иницијална класификација инцидента**

[50] Ова (али др. питања која се могу појавити при процени) треба да помогну у одлуци о даљем поступку – нпр: да пријава буде одбијена, само евидентирана и "прослеђена" другој страни за даље праћење/третман и сл.

Иницијална класификација спроводи се по дефинисаној шеми/таксономији. Уколико нема довољно детаља за правилну класификацију и “извлачење” адекватног закључка, контактирати конституента и тражити потребне информације, потом унети иницијалну.

— периодично (нпр. квартално) изводити прегледање инцидената; извршити по потреби ревалидацију додељених категорија и анализу претходно забележених преквалификација. Урадити сумарну анализу и резултате искористити у унапређењу процеса.

2.3 **Приоретизација**

Осим дистинкције конституената према другим организацијама, и међу конституентима је потребно направити одређену врсту категоризације, те сагласно томе и приоретизације пружених сервиса – наравно, узимајући у обзир и озбиљност самог инцидента.

Приликом приоретизације користити припремљени образац за иницијалну процену; применити изнимне промене уз одобрење одн. сагласност са надзорним органом, и информацију о корекцији додати у забелешку инцидента.

2.4 **Додељивање инцидента**

Принципи могу бити различити – иницијално се може применити принцип да особа која је примила пријаву даље прати инцидент, али - уколико је тим довољно велик и/или постоје делом специјализације за одређене типове инцидената - оптимално може бити инцидент доделити особи са одговарајућом “специјализацијом”.

3 **Праћење (разрешења) инцидента**

Спроводи се кроз цикличне фазе :

- анализа података;
- истраживање одн. потрага за мерама које могу потенцијално довести до решења;
- предлагање мера;
- (праћење статуса) примене мера;
- разрешење и опоравак.

Активности се спроводе у више циклуса до разрешења одн. затварања инцидента.

3.1 **Анализа података**

Контактирати релевантне стране укључене у инцидент – приоритетно оне које су највише угрожене.

Разменити релевантне информације о даљем току процеса праћења инцидента; уколико је могуће, пренети пар иницијалних информација/савета који могу потенцијално бити од помоћи.

Прикупити што је могуће исцрпније податке, и то :

- од стране која је пријавила инцидент – додатни контакт детаљи (по потреби), детаљнији опис инцидента, каква је перцепција класификације и озбиљности инцидента стране која пријављује, прецизније време појаве/откривања инцидента, додатни технички детаљи (оперативни систем, други софтвер, детаљи

о мрежи, антивирус, *firewall*, …), релевантне информације из SIEM [51]или *log-management* система, ...;

- прегледати базу инцидената у покушају бржег сагледавање потенцијално релевантних детаља – да ли постоји још неки инцидент који је пријављивала ова страна ? да ли постоје већ забележени инциденти оваквог типа и магнитуде?;
- претражити податке из сопствених системе за надзор – да ли се појављује нешто релевантно за пријављене адресе и системе укључене у инцидент;
- прегледати остале изворе информација – регионалне или светске базе инцидената, рањивости, упозорења и сл.;
- контактирати по потреби и друге организације (нпр.: наводна страна која је извор напада, (над)пружалац Интернет услуга, извор дигиталног садржаја, органе реда и сл.).

Проценити које податке (не)треба разматрати, одн. којим редоследом их анализирати:

- шта од прикупљеног садржи највише информација корисних за помоћ у решавању инцидента?;
- из којих извора долазе подаци? Којим изворима се више верује (системима/људима/…)?.

(По потреби), распоредити посао на тим – према експертизи и тренутном оптерећењу.

3.2 **Потрага за могућим решењима**

Размена информација и идеја са другим члановима тима.

Припремити и радити сагласно оквирном плану.

Одржавати периодичне сесије за „пресек стања“.

Размотрити да ли је класификација инцидента „једнозначна“, одн. да ли треба тражити помоћ „у другом смеру“.

3.3 **Предлог могућих мера**

Припремити скуп практичних и конкретних активности за сваку укључену страну.

Комуникација и размена информација (прилагођена учеснику).

3.4 **Праћење примене мера**

Коришћењем одговарајућих медија (е-пошта, телефон, *chat*, …) праћење извештаја о примени и резултатима примене активности и мера. Усагласити модалитет и динамику комуникације.

3.5 **(по потреби) додатна провера успешности примењених мера**

Да ли претходно угрожени систем функционише као пре појаве инцидента или отежано? Има ли неких додатних појава које се уочавају? Да ли неки други систем показује неочекивано „понашање“ након примене мера?

4 **Затварање инцидента**

[51] SIEM (Security information & Event Management) - системи који се баве праћењем и чувањем записа о доагађајима на елементима ИКТ система, корелацијом у приближно реалном времену, те упозоравањем, извештавањем и другим облицима консолидације и баратања овим записима релевантним за информациону безбедност.

4.1 **Финализација информација**

Контактирати (у циљу размене закључних информација) страну која је пријавила инцидент, али и друге стране које су биле укључене у процес праћења/решавања. Проследити кратак резиме: шта је пријављено (укљ. и класификацију по ЦЕРТ таксономији), шта је коначни резултат, додатне релевантне информације и поуке/препоруке.

4.2 **Закључна класификација инцидента**

Примена одн. задржавање оригиналне класификације или евентуална модификација према искуствима из процеса решавања инцидента. Урадити искључиво у изнимним ситуацијама.

4.3 **Архивирање инцидента**

Аутоматизован процес система за управљање инцидентима)

5 **Накнадна анализа**

На месечном нивоу спроводити анализу над изабраним инцидентима (најкомплекснији, „иновативни“, другачији од других)

5.1 **Аналитичке сесије**

Кратки преглед статистике за протекли периодичне

Посебан приказ за пар изабраних случајева

Детаљна анализа тима

Дискусија

5.2 **Предлози за унапређење**

Припрема закључака дискусије и анализе

По потреби, слање додатних информација или препорука релевантним (укљученим) странама. Размена информација са другим телима у држави и другим ЦЕРТ-овима. При размени информација ограничити се на искључиво неопходне информације које нису под регулаторним или дугим ограничењима.

6.3 Начин формирања и садржај базе знања на основу прикупљених података о инцидентима

Када се прича о управљању знањем [52], превасходно мисли се на тзв. формално знање – оно на неки начин забележено одн. опредмећено.

Општи процес управљања неким знањем оично се представља на сличан начин – кроз 3 основна корака у циклусу [53] : **Креирање**, **Чување** и **Дељење**. На ово се може (при)додати још један: **Примена знања**.

[52] Уобичајено се за знање каже да је то активна одн. примењена информација – дакле, да има контекстуалну димензију.

- креирање укључује и аквизицију података из различитих извора (унутрашњих и спољних), али и идентификацију оног што је добра пракса и потенцијално корисно у датом контексту;
- чување укључује не само смештај већ структуирање-организацију ових података (индексирање, повезивање, мапирање, класификација);
- дељење као корак ширења знања и колаборације између сарадника постиже се кроз различите методе – заједнице, интранет и екстранет, *groupware* платформе, али организацију обука и сл.;
- примена се односи на подршку доношењу одлука, решавању проблема, развоју компетенција и сарадње у тимовима.

Узевши у обзир контекст ЦЕРТ-а националног нивоа, треба имати у виду да ЦЕРТ олакшава координацију и одзив на инциденте, али да се не бави директним решавањем проблема; такође је могуће да неће све активности у процесу праћења и решавања инцидента и анализе спровести самостално (врло често конкретне информације нису у поседу самог ЦЕРТ-а).

Почетни корак у процесу унапређења „колективног знања“ ЦЕРТ-а стога је је идентификација постојећег стања (почевши од процене не-формалног знања тима), потреба, и могућег начина унапређења процеса које подржава – одн. контекстуални приступ.

Уопштено речено, намена оваквог система јесте архивирање и орагнизовање релевантних информација као што су јавно доступне информације, рањивости, релевантне информације водећих вендора, и сл. али и интерних инскустава и закључака, и то на начин који ће исте ставити људству ЦЕРТ-а на располагање (на адекватан начин). Да би систем био функционалан, неопходно је да постоји начин обележавања, индексирања и претраге, те „корелације“ ових информација. Овакав систематичан и организован приступ као додатну вредност даје и смањивање непотребног умножавања и размене информација (када то није неопходно).

Примарно, информације које би биле садржане у некој „бази знања“ треба да буду оне које би особа која је укључена у решавање неког инцидента могла искористити као референцу током анализе инцидента (нпр. стандардни кораци за процену ситуације, одговор на инцидент, ситуациони прелед, добра пракса итд.)

Гледајући „ширу слику“, може се доћи до веома комплексне структуре ове збирке.

Током постепеног грађења система стога се у пракси препоручује да први фокус буде на једноставнији приступ у циљу ефикасности: релативно једноставна база података, збирка *on-line* извора, текстуалних докумената, табела и сл. могу бити добра основа (како у контексту садржаја тако и флексибилности - узимајући у обзир доступност механизама претраге и дељења ресурса између чланова тима). Наравно, примарни и веома битан садржај јесу управо записи које тим/особа током процеса праћења инцидента оставља забележене – најчешће у самом систему за управљање инцидентима. Већина система за управљање инцидентима пружа могућност оваквог (постепеног) прављења неке врсте базе знања, али и повезивања са другим релевантим

[53] Timo Kucza: *Knowledge Management Process Model* (VTT, 2001) http://www.vtt.fi/inf/pdf/publications/2001/P455.pdf (март 2018.)

платформама. Добробит оваквог приступа јесте да је примарни алат и примарни извор или усмеривач на адекватне ресурсе који могу помоћи при решавању инцидента. Очекивано је да се након након решавања инцидента креира одн. допуни запис везан за индиент са поукама и да се исти налази у систему за управљање инцидентима. При креирању оваквог записа неопходно је сачувати пуни контекст инцидента; ово подразумева и техничке информације (нпр. детаљи о хардвер-у и софтвер-у) али и не-техничке (шта је конституент мислио да је узрок и потенцијална последица – а шта реално стање и др.), који су кораци предузети, али и унос мета-података којима се овај запис адекватно категорише и омогућава се претрага и даљи кораци у чувању, унапређивању и коришћењу знања. Приступ у коме се са креирањем записа о инциденту започиње и запис намењен бази знања практично би учинио то интегралним процесом, а вероватноћа очувања есенције контекстуалних информација овим се повећава.

Редовни прегледи након инцидента и документоване додатне поуке произашле из тог процеса такође су информације које треба систематично држати на заједничкој дељеној платформи. Редовни прегледи и анализе из којих произлазе сумарни и аналитички извештаји, осим самог прегледа стање такође дају увид у нпр. процене трендова, очекиваних ниова последица или времена потребних за решавање одређених типова инцидената и сл., те их као такве треба сматрати делом базе знања.

Размена оваквих информација и запажања са другим Националним ЦЕРТ-овима, те сарадња са асоцијацама које подржавају ЦЕРТ-ове могу ефикасно помоћи аквизицију битних знања.

Део оваквих информација, и велики обим других (екстерно аквизираних) вероватно ће бити смештен на некој платформи *Enterprise Content Management* [54] типа, преферабилно уз неки вид интеграције са интранет порталима.

Надаље, а у контексту мандата и сервиса организације каква је национални ЦЕРТ, очекује се да се постепено гради основа да се база знања обогаћује различитим (детаљнијим) информацијама која појашњавају значај и валидности индикатора, али и догађаја који претходе инцидентима; на основу праћења записа са IDS/IPS система, лог записа, копија електронских порука, али и индикатора из раличитих *threat intelligence* збирки, размене информација са сличним организацијама, записа од рањивостима и сл. Претпоставка је да се неком врстом интеграције са системима CIF [55] типа осим операционализације поступка управљања инцидентима обогаћује и процес обогаћивања забележених знања додатним нивоом детаља.

Као додатни елемент за бољи увид у трендове (као и евентуалне циклусе) и методе потенцијалних напада, предлог је да се размотри успостављање *honeypot* система - и то не само „сопственог“ већ постепено и као мрежу таквих ситема у срадњи са другим ЦЕРТ-овима у Србији и разменом информација о догађајима и индикаторима између учесника. Овакав приступ може допринети развоју активнијег модела подршке решавања инцидената – не само кроз ранији увид у догађаје,

---

[54] *Enterprise Content Management (ECM)* системим намењени су олакшавању колаборације кроз интеграцију функција управљања документима, дигиталним информационим добрима и чувања записа и омогућавајући приступ корисника овим добрима сагласно њиховим ролама и сагласно томе додељеним правима https://searchcontentmanagement.techtarget.com/definition/content-management-system-CMS (март 2018.)

[55] *Collective Intelligence Framework (CIF)* – системи који омогућавају комбиновање познатих информација о претњама из различитих извора и да се те информације користе за идентификацију (одзив на инцидент), детекцију (IDS) и примену мера; помажу парсирање, нормализацију, чување, накнадно процесирање, претраживање, дељење и припремање *threat intelligence* скупова података.

већ и кроз могућност дубљег увида у активности и обрасце напада на „мамце“. Слични (посебно припремљени) системи могу се користити и за вежбе у којима технички експерти система симулирају напад на одређени систем и на тај начин добијају увид из перспективе хакера [56] (нпр. *Capture the Flag* вежбе [57]), а искуства и резултати искористити и за припрему приручника и предлога унапређења мера заштите.

Део сазнања добјених на претходно описане начине се у прилагођеном облику може објавити и на јавно доступним рерусрсима

Део свеукупне базе знања који се понекад превиди јесте управо чињеница да постоје и она тзв. имплицитна знања (која нису формализована). Наиме, сваки члан ЦЕРТ тима вероватно има различите области експертизе које се могу користити у решавању различитих догађаја и инцидената [58]. То њихово знање може бити искоришћено уколио је познато свима у тиму „ко зна шта“ ; ово ствара једну заједничку свест о свеукупном тиму која може бити веома значајна за решавање појединих проблема. Стога је потребно у некој бази имати забележену неку врсту „мапе експертиза“ – опис компетенција појединаца унутар (али и изван) организационе структуре.

На крају, не треба заборавити да сва ова забележена знања имају свој животни циклус па и животни век; дакле, треба их прегледати, ажурирати, размењивати али и повлачити из употребе када за то дође време. Да би се ово на систематичан начин радило, потребно је одредити некога у тиму са тим специфичним задатком, (*knowledge manager*), ко ће периодично пратити стање колекција и иницирати потребне акције.

6.4 Функционални опис система преко кога се подаци о инцидентима примају и обрађују

Традиционално, ЦЕРТ има реактивну улогу: прима пријаву о инциденту да би се започео процес координације. Типична пријава инцидента може бити текстуални опис, уз неке референтне податке као нпр. детаљи о систему, у општем слуају понекад и лог записи и сл. (подаци нижег нивоа и индикатор).

Током Студије, већ је дат аргуменат да није необично да ЦЕРТ открије потенцијалне инциденте и кроз сопствени надзор (сопственим средствима). Уколико је у питању самостална детекција обично се користе аутоматизовани системи као што су *IDS* или системи за детекцију аномалија на мрежи, који генеришу податке типа индикатора (нпр. специфична TCP комуникација) или упозорења (нпр. необично понашање неких система или корисника).

---

[56] *Ethical hacking* или *penetration testing* су појмови који се односе на подухвате покушаја екплоатације неког IT система уз одобење власника како би се октриле његове рањивосити и слабости. Резлутати се користе за препоруку превентивних одн. корективних мера.
https://searchsecurity.techtarget.com/definition/ethical-hacker (март 2018.)

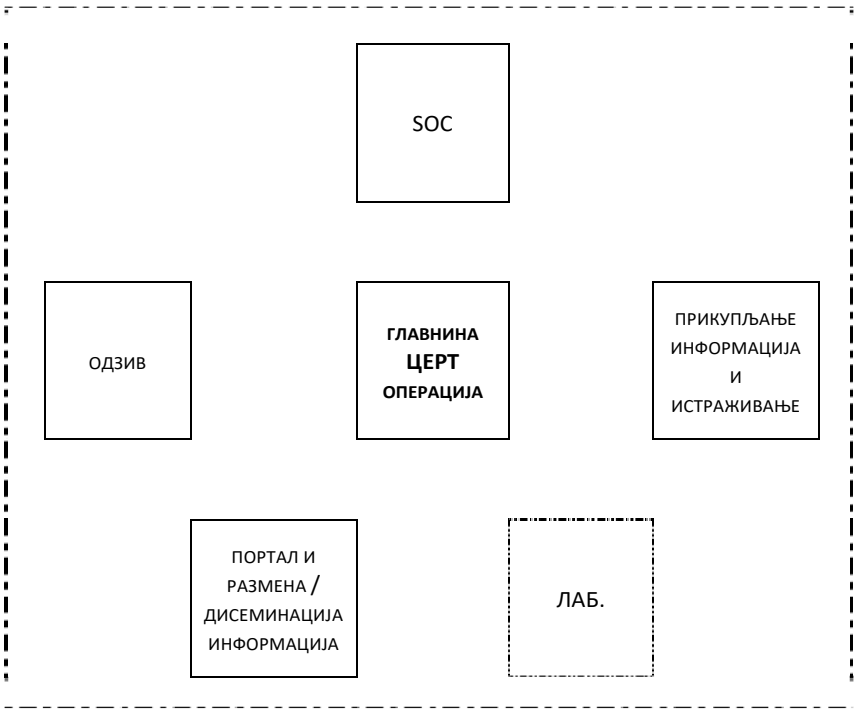
[57] Вежба за професионалце (и оне који би да то постану) из области информационе безбедности како би се видело као хакери могу „пробити“ заштиту и самим тим како се од њих одбранити. Често се изводи као такмиење.
https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it (март 2018.)

[58] https://www.incidentresponse.com/wp-content/uploads/GMU-Cybersecurity-Incident-Response-Team_social_maturity_handbook-updated_10.20.16.pdf (март 2018,)

Поменути приступ сугерише поставку у којој се унутар ЦЕРТ-а за подршку редовном функционисању успоставља нека врста *SOC* (*Security Operations Centre*), а централна функција управљања инцидентима која првенствено има интеракцију са конституентима служи и као „продужена рука“ унутарње *SOC* организације [59].

Поједностављено, основна структура ЦЕРТ-а могла би се представити као на овде датом приказу.

(ЛАБораторија је приказана као опциона, али у даљем развоју свакако има своју повезану улогу са сегментом прикупљања информација и страживања одн. верификацијом одређених налаза).



Приказ 6-2: основна структура/компоненте ЦЕРТ-а

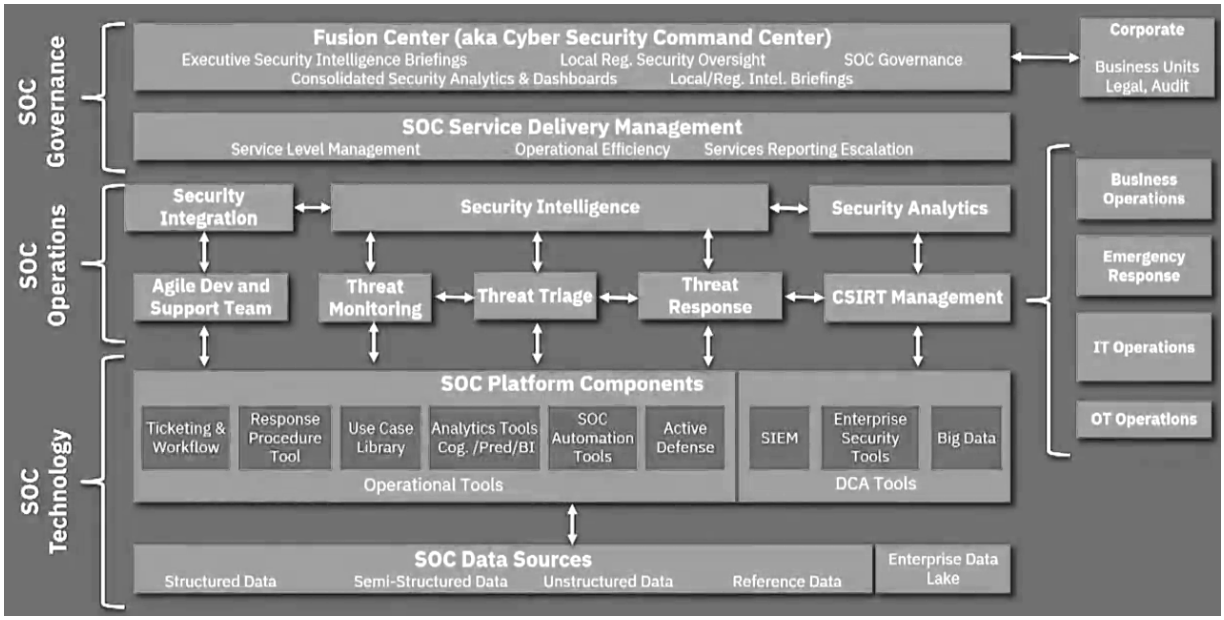
Може се уочити да је SOC овде релевантан – не само као извор информација и начин да се потенцијалне претње брже сагледају већ и као део (очекиване) добре праксе управљања информационом безбедношћу унутар Националног ЦЕРТ-а, помоћ „увежбавању“ извршавања основних задатака, и „давања примера“ другима.

(Иако фокус ове студије није на SOC), пре даље дискусије дајемо један од могућих приказа оперативног модела за SOC [60], који може послужити и као додатни аспект сагледавања групе релевантних алата и оперативних слојева и компоненти.

---

[59] в. Поглавље 2 (Дефиниције).
Ако CSIRT није формално успостављен тада је SOC одговоран за одзив на индиценте – у супротном SOC помаже CSIRT у прикупљању свих неопходних информација потребних за ефективан одговор на претњу

[60] “Security Operations Centers and the Evolution of Security Analytics” (Paul Dwyer, презентација на IBM Think 2018 форуму) https://www.ibm.com/events/think/watch/replay/113897913/ (април 2018.)

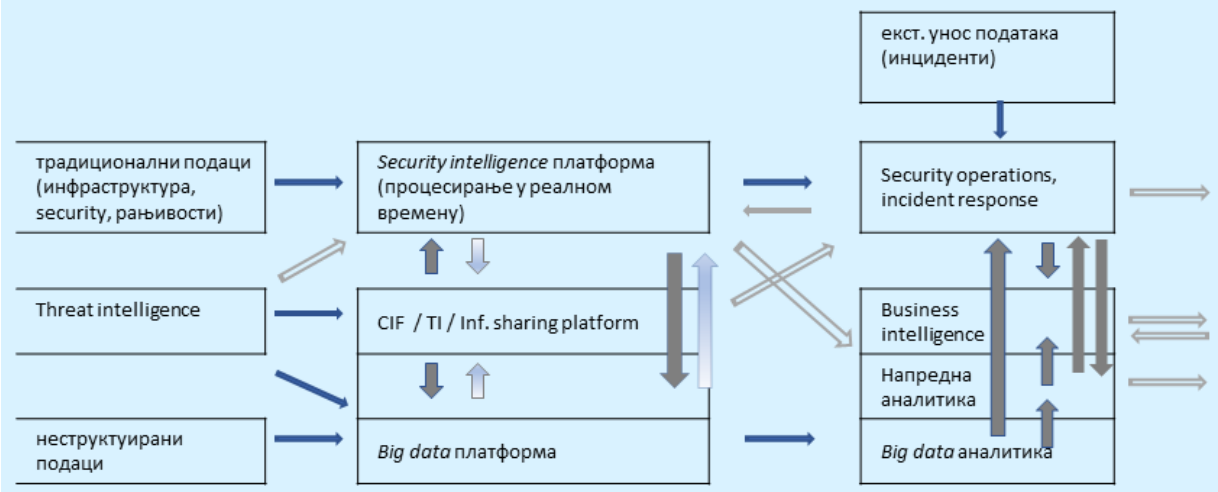


Приказ 6-3 : IBM SOC оперативни модел

Препознајемо неке кључне сегменте (који се принципијелно налазе и унутар засебног ЦЕРТ ентитета):

- улазни подаци – струкртуирани и неструктуирани;
- компоненте – оперативни и аналитички алати;
- оперативне функције – хоризонтална оперативна организација, повезаност CSIRT са функцијама који нису искључиво посвећене информационој безбедности;
- *governance* – управљање нивоом сервисима, надзор, комуникација, извештавање.

Узевши у обзир претходну дискусију, за оријентацију предлаже се приказ грубе архитектуре одн. градивних елемената за ЦЕРТ, који могу бити имплементриани у мањој или већој мери, укљ. и корекције неих од логичких токова информација. Обим и ниво имплементације у пракси зависи од мандата и планиране динамике развоја ЦЕРТ-а, али може послужити као основа за разматрање конкретних наредних корака („ куда би могли кренути „).



Претпоставка је да би се кроз свеобухватну имплементацију у будућности могло одговорити и на изазове евентуално промењене одн. активније улоге Националног ЦЕРТ-а, али и нпр. потенцијално тешње сарадње са неким од посебних ЦЕРТ-ова и сл. Главни критеријум при разматрању у планирању имплементације градивних блокова је свакако имати праву и правовремену информацију на располагању како би се могле разматрати и брзо применити адекватне мере, а алати који су на располагању ЦЕРТ-у томе треба да помогну одн. то омогуће; аналитичарима треба омогућити максимални фокус на иницдент, те стога треба имати у виду могућности минимизације мануелних активности (нпр. код претраге различитих извора, корелирања, размене информација са другим члановима тима итд.).

У наставку ће бити посвећена пажња неким од поменутих елемената.

Кренимо од централне тачке за ЦЕРТ: управљање инцидентима.

За управљање инцидентима ЦЕРТ-ови користе прилагођене *ticketing* и/или наменске *incident management* / *incident response* системе са обзиром на захтеве процеса управљања безбедносним инцидентима тј. сакупљање и обраду података специфичних за безбедносне инциденте (*incident artifacts*), интеграцију са другим техничким система, аутоматизацију одређених корака одговора на инцидент и брз и координиран рад особља задуженог за одговор на инциденте уз могућност адаптације промењеним околностима у току овог процеса. Степен имплементиране функционалности, као и избор између *open source* [61] или комерцијалних алата, варира – зависно од мандата и конституентције ЦЕРТ-а, али (утисак је) и од наслеђа.

[61] Софтвер отвореног кода; да би неки софтвер био квалификован као *open source*, мора да задовољи 10 критеријума датих на https://opensource.org/osd (март 2018.)

Неке од особина за које је препорука потражити их при избору система за управљање и одзив на инциденте:

- брзо и једноставно креирање и праћење неког инцидента до његовог разрешења. Могућност креирања везе између више инцидената;
- подесивост, уз додавање и прилагођавање metapodataka (*tag*-ova, атрибута); могућност претраге по различитим параметрима;
- припрема и измена планова (*„playbook“*) за одзив на инциденте - нпр. на основу интерних правила или добре праксе; циљ је постићи конзистентност и сммањити потребу за „нагађањем“;
- могућност колаборације како би различити учесници у својим различитим улогама могли да сарађују на адекватан начин око конкретног инцидента;
- аутоматизација у одређеном обиму (нпр. отварање или ажурирање ticket-а, прикупљање релевантних додатних података – нпр. *threat intelligence* или артефакти , итд.); циљ је омогућити дати аналитичарима више времена да се фокусирају на битне ствари;
- оркестрација процеса и у одређеном обиму резултујућих у неким корацима кроз *incident workflow* приступ;
- могућност интеграције са другим платформама и алатима кроз пулбикован API [62] и неки од стандардизованих метода (нпр. REST API [63]; JSON [64], XML, …) – нпр. ескалација инцидента кроз е-пошту, пропагација инцидената из интерног SIEM алата, могућност преузимања индикатора који би се придодали инциденту итд.;
- преглед метрике и извештавање (уз могућност извоза података за даљу анализу по потреби) како и се сагледали инциденти, процеси и резултати.

Од *open source* алата, преглед стања сугерише као релевантне два која су опстала током дужег периода (а користе их и ЦЕРТ-ови) - Request Tracker for Incident Response (RTIR) [65] и OTRS (Open source Ticket Request System) [66], те - као релевантан пројекат нешто новијег датума - TheHive [67] :

- RTIR је прављен у сарадњи са и за ЦЕРТ заједницу, те није необична његова популарност; садржи одређени *workflow*, одвојене токове за различите фазе управљања инцидентима, повезивање *ticket*-а са неким инцидентом итд., има публикован API (REST), а постоји и скуп екстензија које развија заједница;

---

62 Application Programming Interface (API) - скуп јасно дефии+нисаних правила и метода комуникације између различитих софтверских компненти. Ниво апстракције који се овим постиже омогућава и контролисану интеракцију изеђу иницијално не-повезаних или удаљених компоненти.
в. још: https://en.oxforddictionaries.com/definition/api (март 2018.)

63 REpresentational State Transfer (REST) interface - скуп *web* сервиса преко којих екст. апликације могу покупити или ажурирати неку информацију

64 Java Script Object Notation (JSON) – текстуални формат за размену података; читљив за људе, једноставан за машинско парсирање и генерисање.
https://www.json.org/ (април 2018.)

65 https://bestpractical.com/rtir/ (март 2018.)

66 https://community.otrs.com/ , https://otrs.com/ (март 2018.)

67 https://thehive-project.org/ (март 2018.)

- OTRS се веома дуго развија и користе га и велике организације; изграђен је на основу захтева ITIL. Постоји могћност аутоматизације у управљању процесима и ресурсима, за употребу у домену информационе безбедности намењен је прилагођени пакет STORM [68] као надградња OTRS основе. Фокус креатора сада је израженији на страни корпоративне примене и наплативих услуга (нпр. SaaS),[69] али и даље се објављује тзв. *community edition*;
- пројекат TheHive је резултат напора истраживача ЦЕРТ-а *Banque de France* [70], који су тиме покушали да превазиђу појединачне недостатке различитих доступних алата. Развој је започео 2014. Аутори га карактеришу као „скалабилну, *open source* и бесплатну платформу за одзив на безбедносне инциденте, направљену за оне који морају брзо реаговати и истражити инциденте“ и „3-у-1 платформа за одзив на безбедносне инциденте“. Кључни елементи које истичу јесу: симултани рад више аналитичара, уграђена *live stream* функционалност са релевантним подацима доступнм свим члановима тима, преглед и увоз догађаја из MISP или SIEM система или пријављених е-поштом, могућност припреме образаца за рад, а захваљујући тесној интеграцији са MISP (*Malware Information Sharing Platform*) [71] могућност брзог придодавања релевантних података и индикатора конкретном случају. Такође има публикован API (REST, JSON преко HTTP), уз одређен број анализатор модула (MISP search, Virustotal, Abusefinder, Outlook msg parsser, YARA, Phishtank, Maxmind…). Покушај остваривања баланса између специфичне намене, флексибилности и тесна интеграција са MISP (која олакшава увоз индикатора) је оно што разликује ово решење од других.

Као комерцијални алати у ЦЕРТ употреби могу се наћи и прилагођени стандардни *ticketing* или *service management* пакети (нпр. BMC Remedy [72], IBM Control Desk [73] , итд. У новије време тежња је ка специфчним решењима намењеним *Incident response* и *Security operations* употреби (IBM Resillient IRP [74], RSA SecOps Manager [75], и сл.).

- Resilient *incident response* платформа датира од 2011. г., а преузимањем 2016. г. је интегрисана у IBM Security портфолио. Систем је конципиран према идеји интеграције са производима трећих страна ради аутоматизације *incident response* процеса, с тим да је (очекивано,) IBM инвестирао у значајнију двосмерну интеграцију са осталим својм

---

[68] https://otrs.com/otrs-solutions/corporate-security/storm/ (март 2018.)

[69] Software as a Service, SaaS – начин испоруке одређене услуге заједно са лиценцом од стране треће стране по принципу претплате; један од основних модела испоруке *Cloud* услуга.

[70] https://github.com/TheHive-Project/TheHive/blob/master/AUTHORS (март 2018.) https://first.org/resources/papers/conf2017/TheHive-a-Scalable-Open-Source-and-Free-Incident-Response-Platform.pdf (март 2018.)

[71] http://www.misp-project.org/ (март 2018.), *open source* софтвер и платформа за размену информација о претњама, значајно подржана од стране CIRC.LU; у великој мери оригинални развој дошао је од ЦЕРТ-а белгијских оружаних снага и NATO Computer Incident Response Capability (NCIRC).

[72] http://www.bmc.com/it-solutions/remedy-itsm.html (март 2018.)

[73] https://www-01.ibm.com/software/applications/control-desk/ (март 2018.)

[74] https://www.resilientsystems.com/our-platform/ (март 2018.)

[75] https://www.rsa.com/content/dam/pdfs/5-2017/rsa-netwitness-secops-manager-ds.pdf (март 2018.)

решењима (нпр. QRadar *security intelligence* платформа).

Resilient обједињује оркестрацију *incident response*, аутоматизацију делова процеса кроз интеграције са другим системима и покривеност регулаторног сегмента кроз интегрисану базу знања. Оркестрација се реализује кроз скуп уграђених *playbook*-ова базираних на препорукама из SANS и NIST, уз могућност екстензије овог скупа прилагођеним *playbook*-овима од стране корисника, кроз интегрисан визуелни алат којим је могуће моделовати *incident response* процесе. Корисницима је омогућено да креирају и додатне скрипте за интеграцију и аутоматизацију са другим системима (SIEM, Identity системи, IDS, *endpoint security* решења, системи за управљање рањивостима итд.) – нпр. повлачење додатних релевентних информација, прослеђивање информација другим *ticketing* системима или слање предефинисане команде. Уграђене могућности извештавања омогућују праћење процеса решевања инцидента и метрике;

- RSA Netwitness SecOps Manager део је скупа решења под називом Netwitness suite. RSA NetWitness SecOps Manager је опциони модул за RSA Archer који интегрише RSA NetWitness могућности са овом платформом за урављање ризицима. Функционалности су намењене аналитичарима као помоћ у приоретизацији, истраживању и одзиву на инциденте. Главни функционални елементи фокусирани су на агрегацију упозорења, развој планова за одзив на повреде информационе безбедности (платформа садржи одређене обрасце базиране на NIST, SANS и VERIS препорукама), одржавање контакт листе и улога у тиму, документовање политика и процедура, те праћење параметара ефективности. У интегрисаној имплементиацији решења добија се доступ форензичким могућностима других модула чиме аналитичари могу прикупити одређене артефакте (подаци са диска, из меморијем мрежне конекције и сл.). Интеграција са основном платформом за управљање ризицима и вредновање информационих добара даје могућност додатног контекста за дати инцидент.

Комерцијална решења ценовно обично се диференцирају зависно од скупа имплементираних функционалности. *Open source* решења у зависности од модела употребе могу имати лиценцне трошкове или бити без истих, али бити и праћена трошковима подршке од стране вендора који та решења „ставља на тржиште “, активно развија и сертификује за одређену употребу . При избору *open source* према комерцијалном додатно је потребно посветити пажњу постизању баланса доступних ресурса за имплементацију и одржавање које захтевају, потребне експертизе, цену пакета услуге имплементације и подршке, те захтевано време за праћење и учшће у активнм заједницама (имајући у виду да је карактеристична одлика *open source* решења стални *work in progress*).

Истраживање неког инцидента може довести до различитих информација од користи за третирање неке текуће претње – како текуће тако и неке будуће. Нпр. по неком упаду, можда је могуће идентификовати адресе учесника у *botnet*-у, параметре неког *malware* малициозног кода

(hash вредност или назив датотеке, *IoC* тј. индикатор компромитације зараженог система [76]*),* па можда и начина упада (нпр. заједничке елементе *spear-phishing* кампање, који су циљани ресурси и сл.); такве информације из сопствене али и шире праксе могу бити и велике помоћи.

Платформа за размену информација о претњама (*threat information sharing*) значајна је - како за размену са трећим странама тако и као средство обогаћивања контекста инцидената. Прегледом платформи *threat sharing* платформи уочено је да је *de facto* највећу „популарност" задобио MISP, и може се рећи да је широко прихваћен. Иницијални развој започео је још 2011., а пројекат је за своје потребе 2012. прихватио и NATO. Као додатну илустрацију зашто се MISP препоручује као један од градивнх блокова треба навести да FIRST ISSIG има инстанцу (коју оперативно одржава Computer Incident Response Center Luxemburg) која је „доступна члановима за размену техничких и не-техничких информација о *malware* узорцима, нападачима и инцидентима" [77]; такође, CERT-EU користи MISP у оквиру своје *Cyber Threat Intelligence* платформе. ENISA се такође бавила анализом ове платформе у свом извештају *Detect, SHARE, Protect - Solutions for Improving Threat Data Exchange among CERTs* још новембра 2013 [78]; тада је узорак ЦЕРТ-ова националног нивоа тестирао платформу, а током радионице са европским ЦЕРТ-овима „у начелу је потврђена корисност платформе, уз позив на заједнички приступ прављењу базе инцидената ". Треба напоменути да је још 2012. SIEMENS представио могући пример имплементације платформе (оквира) за управљање *cyber threat intelligence* информацијама под називом MANTIS (Model-based Analysis of Threat Intelligence Sources framework). Намера је била да се направи могући репозиторај за *cyber threat intelligence* информације, у којем је (осим увоза и извоза) могуће и прегледање, претрага и филтрирање прикупљеног. Имплементирана је подршка за STIX/CybOX, и IODEF формате. Од 2014. нема развоја на овом пројекту, а страница посвећена пројекту упућује на MISP као платформу „која нуди све што је иницијално намеравано за MANTIS (и више") [79].

MISP је, дакле, *open source threat intelligence* платформа за размену, чување и корелацију индикатора компромитације (*Indicators of Compromise, IoC*) циљаних напада, threat intelligence информација, информација о рањивостима итд. Неке од особина које се могу сматрати значајним за ЦЕРТ:

- подаци који се уносе чувају се на структуирани начин.
  Модел података омогућује повезивање комплексних структура;
- унос података аутоматски активира корелацију која проналази сличности између догађаја - везе између атрибута и индикатора; олакшавајући тако нпр. проналазак актера који стоје иза више напада, идентификације кампања, сагледавање трендова текућих напада и сл.;
- таксономија за класификовање догађаја и додељивање *tag*-ова је подесива, а може бити локална или дељена између више MISP инстанци; такође, у старту су вћ присутне неке

[76] Било који податак који се може употребити за тражење и индентификацију потенцијално компромитованог система назива се *Indicator of Compromis* (*IoC*) ; то могу бити IP адреса, назив домена, адреса е-поште, hash вредност за неку датотеку, URL и сл.

[77] https://www.first.org/global/sigs/information-sharing/misp (април 2018.)

[78] https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs (март 2018.)

[79] https://github.com/siemens/django-mantis (април 2014.)

чешће коришћене таксономије (које подржавају класификације које користи ENISA, EUROPOL, различити CSIRT ентитети и др.);

- већи број модула за проширење функционалности платформе, те увоза и извоза података (као и документован начин развоја).

  Поред мануелног уноса, у старту су подржани увоз и извоз података у различитим форматима (поред сопственог): увоз „слободног" текста, OpenIOC, ThreatConnect CSV, итд.; извоз у форматима за употребу у *IDS* (Snort, Bro, Suricata), OpenIOC, CSV, MISP XML или JSON (за интеграцију са другим системима); такође, подржан је извоз у STIX [80] формату (укљ. STIX 2.0);

  У старту постоји подршка и за велик број *feed*-ова [81];
- публикован API (приступ платформи преко REST API);
- флексибилан графички интерфејс; могућност визуализације.

Као опција платформе за потребе асистенције аутоматизације третмана инцидената и за прикупљање, процесирање и дистрибуцију *security* feed-ова код ЦЕРТ-ова присутан је IntelMQ [82]. У конципирању пројекта кроз иницијативу Incident Handling Automation Project (IHAP) учествовало је више ЦЕРТ-ова из Европе. Главни циљ је био олакшати прикупљање и процесирање *threat intelligence* информација и тиме унапредити у ЦЕРТ-овима процес третирања инцидената.

При развоју као узор је узета AbuseHelper [83] *open source* платформа (оквир) за пријем и редистрибуцију *abuse* и *threat intelligence* feed-ова.

На располагању је већи број feed-ова [84], који су груписани према испоручиоцима.

Овај модуларан систем има интегративни слој који повезује све процесне модуле; има више функционалних модула за смештање, обогаћивање информација итд.

За управљање конфигурацијом платформе постоји графички кориснички интерфејс - IntelMQ Manager [85] (мада за напредију употребу у неким случајевима може бити потребно прибећи командној линији – `intelmqctl`).

Платформа користи JSON формат за све поруке. Подржана је интеграција са AbuseHelper и CIF (*Collective Intelligence Framework*) алатима. Комуникација са другим системима је преко HTTP RESTFUL API-а.

IntelMQ може подржати MISP у преузимању догађаја и ажурирању *tag*-ова.

Са постојеће тачке гледишта, разматрање *big data* и напредних аналитичких алата представља поглед у будућност. С друге стране, њихова имплементација није неуобичајена код ЦЕРТ-ова

---

[80] Structured Threat Information Expression, STIX – језик и формат за размену cyber threat intelligence (CTI) информација (и *de-facto* стандард у пракси за ову намену); STIX Објекти категоришу сваки део информације специфичним атрибутима. https://oasis-open.github.io/cti-documentation/stix/intro.html (април 2018.)

[81] http://www.misp-project.org/feeds/ (април 2018.)

[82] https://github.com/certtools/intelmq/tree/develop/docs (април 2018.)

[83] https://github.com/abusesa/abusehelper (април 2018.)

[84] https://github.com/certtools/intelmq/blob/develop/docs/Feeds.md (април 2018.)

[85] https://github.com/certtools/intelmq-manager (април 2018.)

одбрамбених снага или ЦЕРТ-ова који имају активнију улогу за владине одн. државне институције и сл. Ниво међусобне повезаности одн. хомогености имплементираних компоненти у пракси варира. Примарни циљ оваквих платформи је умањити елиминацију неких извора података унапред а очувати способност брзе идентификације релевантних информација из масивног мноштва („наћи иглу у пласту игала“). Као резултат могу се добити и нпр. параметри за припрему нових или корекцију постојећих дефиниција случајева одн. образаца које треба пратити (use-case), релевантни индикатори компромитације (улаз за *threat intelligence / information sharing* платформу), сумарни подаци релеванти за извештавање (улаз за *business intelligence* и алате за ивештавање) итд.

Функционални елементи оваквих решења своде се на:

- оперативна складишта података – константни увоз - или увоз по потреби - и организација података различитог типа и из различитих извора;
- анализа садржаја – трансформација података, идентификација и извлачење ентитета и веза из неструктуираних података;
- разрешавање идентита и веза – препознавање и одбацивање дупликата и откривање скривених веза кроз више различитих степени сегрегације;
- мултидимензионална аналитика;
- напредна *big data* аналитика – визуализација, анализа и претраге кроз масивни скуп података с циљем брзог приближавања резултатитма;
- гео-аналитика – интеракција са GIS [86] системима за потребе гео-просторне анализе података;
- аналитика слободног типа – упити и претраге queries према специфичним потребама одн. наменама.

Овакве платформе морају бити скалабилне али и флексибилне – како по питању обима података тако и за подршку оперативних и корисничких окружења. Платформа-оквир за унос и приступ подацима (*data access and acquisition framework*) мора бити довољно флексибилан како би корисници могли спајати скупове података, истраживати али и анализирати на централизован начин податке из више извора. Пожељно је да постоји начин да да се визуелно граде упити кроз кориснички интерфејс како би олакшао процес анализе. Интерактивни приступ подацима кроз кориснички интерфејс требало би да дозволи симултано поређење више идентификованих образаца или скупа веза; такође, очекује се могућност подешавања грануларности приказа - како детаљно тако и нпр, као хистограм у циљу откривања трендова и аномалија. Наравно, без публикованог API-а одн. начина интеракције са платформом, није могуће очекивати ни адекватну интерпоперабилност, али ни могућност екстензије фукнциоиналности.

Специфичност примене утиче на чињеницу да не постоје препозната фокусирана *open source* решења која би испунила тражене функциналности у датом обиму. Од комерцијалних решења са дужом историјом истичемо IBM i2 Enterprise Insight Analysis, Palantir Gotham platformu и SAS

[86] Gographic Information System, GIS - систем намењне прикупљању, смештању, управљању, руковању руковању анализи и презентацији географских и просторних података. https://www.nationalgeographic.org/encyclopedia/geographic-information-system-gis/ (април 2018.)

Memex из напомену да одређени вендори стављају мањи или већи акценат на cybersecurity оријентисану употребу решења.

Већ је изнета препорука имплементације неке врсте интерног SoC, што као нужног елемента сопствене праксе информационе безбедности, али и као начина одржавања свести о актуелном стању (*situational awareness*).

Неке од мера (у основи детективних) које су уобичајено имплементиране у SoC-u [87] :

- надзор система; интеграција, управљање и преглед логова и токова мрежног саобраћаја;
- корелација уочених догађаја;
- надзор и управљање рањивостима;
- праћење и имплеменација закрпа.

Савремене Security Intelligence платформе могу послужити као основа за потребне функционалности. Оне надграђују стандардна *log management* и SIEM решења унапређеним механизмима корелације, проширујући их додатним функционалностима (управљање рањивостима, надзор мржносг саобраћаја, па чак и елементи форензике), те интегришући додатне контекстуалне информације за потребе детекције у реалном времену. Овај интегративни приступ омогућава боље сагледавање догађаја у датом контексту. Security Intelligence платформе могу бити имплементиране као „хомогенија целина“, али и као колекција предефинисаних елемената и/или уз добру интеграцију више различитих компоненти. Уколико постоји могућност, препорука је фокус на интегралнија решења.

Преглед *open source* решења за SIEM функционалност сугерише да није ретка пракса да се разликује скуп могућности између решења која се нуде са подршком вендора и оних у „слободној понуди“. Нека друга решења посежу за комбинацијом више технолошких блокова како би се надградиле основне функционалности прикупљања и претраживања *log* записа и имплементирале функције аналогне корелацији, визуализација итд. При избору решења за ову платформу сугерише се консултовање извештаја специјализованих аналитичких кућа (нпр. Gartner Magic Quadrant, Forrester Wave и сл.), дефинисање мин.-базичних захтева и жељених функционалности, пре даље анализе одн. упоређивања доступних функционалности – посебно између наплативих надградњи *open source* и комерцијалних решења.

У домену детекције и управљања рањивостима, као практично једино доступно *open source* решење уочава се OpenVAS [88] (изворни развој овог софтвера у једном сегметну одвојио се у етаблирање комерцијалног алата *Nessus* [89]). Преглед искустава неколицине корисника овог алата и личних искустава консултаната сугерише више потенцијалних мањкавости: неконзистетне перформансе (кориснички интерфејс, брзина скенирања), суб-оптимално извештавање (посебно у односу на специфичне регулаторне захтеве) и др. Како је у питању област у којој је битно брзо ажурирање базе откривених рањивости, али и могућност умањивања лажних налаза, сугерише се

[87] https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide (април 2018.)

[88] http://www.openvas.org/about.html (април 2018.)

[89] https://www.tenable.com/products/nessus/nessus-professional (април 2018.)

додатнои истраживање и пажљиво балансирање између *open source* и комерцијалних решења, те могућнсти њихове интеграције са другим елементима security intelligence platforme.

Неке од особина за које је препорука потражити их при избору решења:

- прикупљање и нормализација log записа и записа мрежног саобраћаја; осим подршке за стандардне системе (серверски ОС, мрежни уређаји, IDS, firewall, итд.) , могућност имплементације подршке за нестандардне системе (изворе записа);
- корелација прикупњених записа (догађаја) – укљ. *log* и записа о мрежним конекцијама, свођење истоветних (аналогних) догађаја са различитих платформи на заједничке категорије, могућност дефинисања и праћења аномалија; повезивање више корелираних догађаја. Преферабилно постојање предефинсаних корелационих правила (како би се убразала имплементација и иста могла користи као образац за надградњу);
- контекстуална приоретизација корелираних догађаја (битност система, статус рањивости, …);
- интеграција система за управљање рањивостима; могућност приоретизације третмана рањивости руководећи се начелом управљања ризиком;
- могућност увоза *threat intelligence* информација и њиховог коришћења за детекцију и корелацију;
- графички интерфејс, прилагођен и за аналитичаре који немају програмерско знање или искуство; могућност претраге и истраживања од вишег нивоа ка детаљнијем увиду; могућност извештавања по различитим параметрима (пожељно постојање припремљених образаца на основу постојеће добре праксе и/или стандарда);
- публикован API, могућност интеграције стандардним методама (нпр. REST API, JSON) са другим системима одн. Платформама;
- доступност екстензија или документован начин за припрему и имплементацију екстензија;
- могућност надградње или проширења система без потребе одбацивања постојећег улагања.

6.5 Дефиниција формата и модела података за размену информација о ризицима и инцидентима

При дељењу информција са другим ЦЕРТ-овима, институцијама или организацијама, очекује се да део комуникације буде колико-толико аутоматизован. Размена информација била могућа, иста мора бити структуирана и описана на конзистентан начин како би била разумљива за стране које учествују у овој размени.

Као корисник, ЦЕРТ мора да се прилагоди околностима и имплементира подешавања која ће омогућити конзумацију података у датом формату. Подршка за неки нови *feed* не би требало да захтева кардиналне напоре. У случају да ипак није могуће прилагодити окружење за транспарентну подршку неком формату, увек остају опције мануелне конверзије података у подржани формат или коришћење потпуно мануелног процеса (ако не омета остатак

оперативности). Као извор, ЦЕРТ треба да води рачуна да изабрани формат и протокол буде међу шире усвојеним - стандардним – како на страни примаоца (већином) не би било значајнијих ограничавајућих фактора за прихват података.

За боље разумевање и процену информација које се размењују, може се применити сагледавање компоненти једног инцидента кроз узрочно-последични ланац - почевши од правог узрока до резултујућег ефекта [90] :

- ланац започиње нападач одн. малициозни актер који може имати различите циљеве;
- нападач започиње напад акцијама које користе методе и алате за експлоатацију постојеће рањивости у циљном систему;
- на крају, резултат напада представљају нападнути објекат и „неауторизовани резултат" напада;
- додатно, овај „ланац" може се проширити и реакцијом стране која се брани.

Дакле, информације које ЦЕРТ размењује се тичу извештавања о инцидентима, али то може укључити и и информације о рањивостима, индикаторе и сл.

Ако се разматра размена информација о инцидентима, треба имати у виду да тај скуп података обично садржи податке који се могу сматрати осетљивим, те их пре прослеђивања некој екст. страни треба „очистити" одн. анонимизирати. Обично то значи укидање било каквих приватних података, референце на оригинални извор података, али и на „жртву" напада и сл. С друге стране, ако говоримо о догађајима (*event*) исти обично не садрже осетљиве податке, те даље дељење информација о њима мањи проблем, али и њихов значај за даље анализе може бити мањи. Додавање IoC информација у извештај је свакако добродошло. Трендови су такви да се може препоручити разматрање и могућности додавања неких података вишег нивоа који додатно индицирају методе нападача (информације о тактици-техникама-процедурама нападача, *TTP*)

„Једногласно" усвојених стандарда за формате података нема; делом је разлог управо специфична намена неког алата и прилагођеност тој намени, (не постоји једно решење за све потребе).

IODEF (Incident Object Description Exchange Format) модел података поставља оквир за размену информација уобичајену између ЦЕРТ-ова или других организација а односе се на инциденте из домена информационе безбедности или индикатора компромитације. Овим форматом одн. моделом руководи се под окриљем Internet Engineering Task Force (IETF) и Managed Incident Lightweight Exchange (MILE) радне групе [91]. IODEF в. 2 публикован је под Request for Comments (RFC) 5070-bis одн. 7970 [92], као предложени стандард.

---

[90] Florian Menges & Günther Pernul : „A comparative analysis of incident reporting formats" https://www.researchgate.net/publication/320887006_A_comparative_analysis_of_incident_reporting_formats (април 2018.)

[91] https://trac.ietf.org/trac/mile/wiki/WikiStart (април 2018.)

[92] https://datatracker.ietf.org/doc/rfc7970/ (април 2018.)

Формат је базиран на XML репрезентацији. Модел података инкорпорира информације о: хостовима, мрежама и сервисима који раде на тим системима; нападима и повезаним форензиким доказима; последицама активности; неке могућности за документовање тока поступка.

Основна намера код IODEF је била стварање оквира за размену уобичајених информација о инцидентима. Према ауторима, стога је с намером формат ограничен на најчешће коришћене типове података – како би се олакшала интероперабилност за већину планираних намена без потребе за комплексним имплементацијама; такође, покушало се са балансирањем употребе слободне текстуалне форме (за описе релевантне за анализу) и структуром која дозвољава аутоматизацију процесирања о инцидентима и индикаторима. С друге стране, IODEF схема има више поља и класа које није неопходно користити за сваку размену података.

Компоненте (класе) које се користе за опис инцидента у IODEF документу су дате у табели [93].

Агр. Класа	**Опис**
IncidentID	Јединствен број у контексту ЦЕРТ-а за праћење инцидента
AlternativeID	Број за праћење инцидента који користи други ЦЕРТ (коиј није креирао докмент)
RelatedActivity	URL, ThreatActor, Campaign, IndicatorID, Confidence, Description, AdditionalData…
DetectTime	Време прве детекције инцидента
StartTime	Време почетка инцидетна
EndTime	Време завршетка инцидетна
RecoveryTime	Време када је завршен опоравак од инцидента
ReportTime	Време када је пријављен инцидент
GenerationTime	Време креирања овог записа о инциденту
Description	Слободан текстуални опис инцидента
Discovery	Како је иницдент откривен (опис, DetectionPattern – опажена специфична конфигурација)
Assessment	Последице инцидента за жртву (IncidentCategory, SystemImpact, BusinessImpact, Counter, MitigatingFactor, Confidence …)
Method	Опис TTP или слабости које је актер претње користијо током инцидента (AttackPattern, Vulnerability, Weakness)
Contact	Контакт информација за организацију и људе укључене у инцидент (име, адреса, тел., …)
EventData	Контејнер за организацију подазака који описују догађаје који сачињавају инцидент
IndicatorData	Опажене ставке које могу помоћи форензику или детекцију малициозне активности и повезани мета-подаци (Confidence, Observable, IndicatorExpression, NodeRole, AttackPhase, …)
History	Документовање кокретне акције или догађаја који се десио током третмана инцидента
AdditionalData	Механизам за екстензију модела података

[93] https://tools.ietf.org/html/rfc7970#page-20 (април 2018.)

Табела 6-1 : преглед класа унутар Incident класе у IODEF в.2

Треба забележити и да је у IODEF моделу предвиђен атрибут при Incident класи под називом „*restriction*", којим пошиљалац индицира примаоцу упутство које се односи на ограничења даљег ширења информације садржане у класи и повезаним објектима испод (процедурални и други аспекти имплементације размене информација су одвојени од самог модела података).

Постоје и дефинисане екстензије за класу IODEF документа

- екстензије за phishing пријаву . RFC5901;
- размена података о тансакционим преварама (*Transaction Fraud Data*): RFC5941;
- екстензија за даље структуирање *cybersecurity* информација (Structured Cybersecurity Information Extension) [94].

Верзија 2 донела је унапређења у односу на оригинални формат у домену репрезентације контекста нападача и нападнуте стране; донекле је олакшана одн. побољшана и могућност аутоматске обраде [95].

Као транспортни протоколи специфицирани су

- RFC6545 [96] Real-time Inter-network Defense (RID) – као основни протокол;
- RFC6546 [97] RID преко HTTP/TLS – приступ оптимизован за *peer-to-peer* оперативни модел између тесно повезаних ЦЕРТ-ова;
- Resource Oriented Lightweight Indicator Exchange (ROLIE) [98] – за размену података о инцидентима из неког репозиторија.

Јасно је да је формат је стандардизован и креиран с намером за размену информација о инцидентима. Може се рећи да задовољава захтеве циљане намене (не улазећи у шири аспект *cyber threat intelligence* употребе). Утисак аутора је да има места унапређењу документације, те да је скуп алата који подржавају имплементацију IODEF и неког од наведених протокола ограничен - па самим тим и да је у актуелном тренутку прихваћеност ограничена (чини се да такав статус није новијег доба - својевремено је и у извештају ENISA-е под називом „Standards and tools for exchange and processing of actionable information" из јануара 2015. [99] наведено да ROLIE спада у „стандарде који се више не развијају или не одржавају или их не користе нови алати", а RID у „стандарде који се не користе у пракси"). У време писања нисмо успели приступити актуелној листи интероперабилних имплементација IODEF и RID предложеној [100] на Интернет станици посвећеној

---

[94] https://datatracker.ietf.org/doc/rfc7203/?include_text=1 (април 2018.)

[95] Florian Menges & Günther Pernul : „A comparative analysis of incident reporting formats" https://www.researchgate.net/publication/320887006_A_comparative_analysis_of_incident_reporting_formats (април 2018.)

[96] https://datatracker.ietf.org/doc/rfc6545/ (април 2018.)

[97] https://datatracker.ietf.org/doc/rfc6546/ (април 2018.)

[98] https://datatracker.ietf.org/doc/draft-field-mile-rolie/ (април 2018.)

[99] https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport (април 2108.)

[100] http://siis.realmv6.org/implementations/ (мај 2018.)

овом формату [101]. С друге стране, како је у питању формат базиран на XML, публикован као RFC - предлог за стандард, отворена је могућност за засебан развој подршке у случају потребе.

Према извештају о резултатима истраживања који је приказан на конференцији WIRTSCHAFTSINFORMATIK 2017. под називом „Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives“ [102] наводи се да се већина *threat intelligence sharing* платформи ослања на стандарде као што су OpenIOC, STIX, и IODEF; закључено је да је STIX најчешће коришћени стандард и да се може сматрати *de-facto* стандардом за *threat intelligence*.

Structured Threat Information Expression (**STIX**) је језик и формат који се користи за *cyber threat intelligence* (CTI) размену [103]. Користи се за опис и међусобно повезивање широког спектра *cyber threat* информација. Омогућава размену CTI на конзистентан начин у машински читљивом облику.

Trusted Automated Exchange of Intelligence Information (**TAXII**) је протокол апликативног нивоа за размену CTI преко HTTPS. TAXII дефинише стандардни API усаглашен са зејдничким моделом размене. Специфчно је створен као транспортни механизам да подржи размену CTI репрезентованх коришћењем STIX.

Креирани 2012., ови стандарди били су под окриљем US Department of Homeland Security одн. MITRE Corp. (федералне непрофитне институције). Од 2015. су под окриљем OASIS – непрофитног конзорцијума који се бави „развојем, конверенцијом и прихватањем отворених стандарда“ [104].

STIX и TAXII су тренутно у в. 2. Модел података је значајно прерађен од в. 1. (како би се исправили уочене неконзистентности и слабости) [105]; изабрана је JSON нотација као обавезна за STIX модел података, а за TAXII је изабран HTTP REST.

У STIX в. 2 свака информација категорише се кроз STIX Објекте и попуњавање специфичних атрибута. Дефинисано је 12 STIX Доменских Објеката (SDO) [106] и 2 Релациона Објекта (SRO) [107] :

SDO

Назив објекта	**Опис**
Attack Pattern	Тип тактике-техника-процедура (TTP) коијм се описује начин како актер покушава компромитовање свог циља.
Campaign	Груписање противничког понашања да би се описао скуп малициозних активности против одређеног скупа циљева током неког периода.

[101] https://trac.ietf.org/trac/mile/wiki/WikiStart (мај 2018.)

[102] https://wi2017.ch/images/wi2017-0188.pdf (април 2018.)

[103] https://oasis-open.github.io/cti-documentation/stix/intro (април 2018.)

[104] https://www.oasis-open.org/org (април 2018.)

[105] У циљу бољег сагледавања, може се напоменути да је у в. 1 паралелно одн. заједнички постојао CybOX (Cyber Observable eXpression) језик за опис догађаја са конкретним својствима (“*things*”) и примећених информација, а STIX се налањао на CybOX када су у питању обрасци индикатора, описи инфраструктуре и параметри акција предузетих као одговор на напад (http://cyboxproject.github.io/about/); у STIX в.2, CybOX објекти су интегрисани као *Cyber Observables*.

[106] https://oasis-open.github.io/cti-documentation/stix/intro#stix-2-defines-twelve-stix-domain-objects-sdos (април 2018.)

[107] https://oasis-open.github.io/cti-documentation/stix/intro#stix-2-defines-two-stix-relationship-objects-sros (април 2018.)

Course of Action	Акција предузета да би се спречио или одговорило на напад.
Identity	Појединци, организације или групе, као и класе појединац, организација или група.
Indicator	Неки образац који може бити искоришћен за откривање сумњиве или малициозне сајбер.
Intrusion Set	Груписани скуп поступака противника и ресурси са заједничким особинама за које се сматра да их оркестиа исти актер.
Malware	Тип TTP (малициозни код или софтвер) коиј се користи за компромитовање поверљивости, интегритета или доступности података или система „жртве“.
Observed Data	За саопштавање примећених информација на систему или (нпр.IP адреса).
Report	threat intelligence скуп фокусиран на једну или више тема, као нпр. опис актера претње, malware-а, или технике напада, укљ. и контекстуалне детаље.
Threat Actor	Појединац, група или организација за које се верује да поступају са малициозним намерама.
Tool	Легитимно софтверско средство које актер претње може користити за извођење напада.
Vulnerability	Грешка у софтверу коју хакер може директно може искористити за приступ систему или мрежи.
S R O	
Назив објекта	**Опис**
Relationship	Користи се за повезивање два SDO и описивање каква је релација између њих.
Sighting	Означава претпоставку (веру) да је опажен елемент CTI (нпр. indicator, malware).

Табела 6-2 : STIX2 доменски и релациони објекти

.

SDO се може повезати графички преко SRO именованим типом релације. Унутар STIX в.2 спецификације већ постоји основни скуп именованих релација, али је такође могуће да страна која креира садржај дефинише и своје типове релација.

Значајно је што STIX спецификација подржава тј. инкорпорира тзв. *Data marking* концепт - репрезентацију ограничења, права и др. одредница како подаци могу бити коришћени и дељени (нпр. рестрикција даљег прослеђивања или захтев да се подаци чувају у енкриптованом облику и сл.). Ове ознаке специфицирају се кроз посебне marking-definition објекте; примењују се на комплетан STIX Објекат или на појединачна својства STIX Објекта кроз грануларне ознаке. Постоје два типа *marking* дефиниција: TLP (за TLP ознаке) [108] и Statement (за текст). Према доступној

[108] http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709287 (април 2018.)

документацији, постоји план да се у укључи и подршка за FIRST Information Exchange Policy (IEP) [109] у будућности одн. у некој наредној верзији (када буде дефинисана спецификација која се може употребити за аутоматску обраду) [110].

STIX *Cyber Observables* концепт конципиран је тако да документује чињенице о томе шта се десило на неком хосту или у мрежи, али не нужно ко и где, нити се бави разлогом за догађај (нпр. информација о постојећој датотеци, опаженом процесу или саобраћају на мрежи између две IP адресе могу бити забележени као *Cyber Observable data*) [111]. Нису везани за само један STIX Доменски Објекат (SDO) већ више њих, како би се добио додатни контекст за податке који их карактеришу.

Не постоји специфична веза између IODEF i STIX. Генерално је могуће увући податке из IODEF у STIX како би се приказале информације о инцидентима, али не директном транслацијом из једне у другу структуру. Имајући у виду да у STIX2 постоји тако рећи динамичка компонента одн. референце, да би се умањио губитак контекста у транслацији, потребно је обратити пажњу на поставку релација које повезују структурне објекте.

Може се рећи да STIX садржајно покрива све битне елементе за опис неког инцидента. Коришћење динамичких референци у STIX2 омогућава употребу сагласно специфичним захтевима (*use cases*), па самим тим и умањење потенцијалне недореченост или двосмислености. Ово такође омогућава и усаглашавање формата са структурама других формата – па самим тим и побољшава и могућност интероперабилности.

На страницама OASIS техничког комитета за *Cyber Threat Intelligence* (OASIS Cyber Threat Intelligence Technical Committee, CTI TC) може се наћи списак *open source* пројеката [112] и комерцијалних софтверских производа [113] који имају имплементирану подршку за STIX/TAXII; како је већ било споменуто, MISP подржава извоз података у STIX формату (XML и JSON) – укљ. и STIX 2.0 формат [114].

Изабрана JSON нотација као обавезна за STIX модел података, и HTTP REST за TAXII протокол омогућили су стандардне начине за имплементацију. Утисак је да је модел података добро документован, да се активно прати и развија, те да је скуп алата који подржавају STIX/TAXII довољно широк (што подржава и мишљење аналитичара да је у питању de facto стандард за размену *cyber threat intelligence*). Стандард је довољно широк и екстензибилан да подржи тренутне и будуће задатке.

---

[109] Оквир за ЦЕРТ-ове, заједнице и венодре за подршку иницијатива размене информација; користи четири типа политике третмана информација - Handling, Action, Sharing, Licensing (HASL). https://www.first.org/iep/ (април 2018.)

[110] http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709283 (април 2018.)

[111] http://docs.oasis-open.org/cti/stix/v2.0/cs01/part3-cyber-observable-core/stix-v2.0-cs01-part3-cyber-observable-core.html#_Toc496715360 (април 2018.)

[112] https://wiki.oasis-open.org/cti/Open%20Source%20Projects (април 2018.)

[113] https://wiki.oasis-open.org/cti/Products (април 2018.)

[114] http://www.misp-project.org/features.html (април 2018.)

6.6 Списак података које је неопходно прикупити о сваком инциденту

Два су сегмента информација које треба прикупити [115]

- током пријаве инцидента - Основне информације (особа која пријављује инцидент);
- током процеса одзива на инцидент – „Процесне информације“ (особа/тим који прати инцидент).

Оба ова скупа чине основу оног што би се могло назвати база пријављених инцидената.

Наравно, свака организација креира своју листу елемената зависно од усвојеног модела управљања инцидентима (почевши од нијанси у усвојеном значењу појма инцидент). Ипак, иако постоје одређене разлике, основни садржај се преклапа.

- основне информације;
- контакт информације ко пријављује и ко прима пријаву одн. управља инцидентом;
- назив организације која пријављује;
- привредна грана / тип организације која пријављује;
- име;
- рола (ев. и Орг. јединица);
- адреса електронске поште;
- тел. бр.;
- адреса / локација;
- детаљи о инциденту;
- хронолошке информације (преферабилно усклађено пема UTC[116]): забележени почетак, када је откривен, када је пријављен, када је решен/закључен итд. ;
- физичка локација;
- тренутни статус;
- (ако је познат) извор иницдента (хост, IP адреса, …);
- опис инцидента (шта се десило, како је откивен, и сл.);
- опис угроженог информационог добра (систем-апликција-подаци-…);
  детаљи о систему (хост, IP адреса, функција);
- (ако је познато или претпостављено) категорија инцидента, вектор напада, тип актера, индикатори…;
- фактори приоретизације: функционални утицај, информациони утицај, процена лакоће опоравка, критичност система;
- релевантне активне мере заштите (информације које дају додатни контекст озбиљности и пиоретизацији);

---

[115] NIST Special Publication 800-61r2
https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (април 2018.)

[116] **Coordinated Universal Time** – Примарни светски стандард за време према коме се регулишу сатови; унутар ганице од 1 секунде у односу на средње соларно време на географској дужини 0°; не подлеже сезонским променама. Тренутна верзија UTC дефинисана је према препорукама ITU-R TF.460-6 Међународне телекомуникације уније.

- примењене мере и акције до пријаве;
- да ли је још неко већ контактиран, и ако јесте - ко;
- остале информације;
- процесне информације;
- актуелни статус инцидента;
- сумарни опис;
- белешке о активностима праћења/управљања инцидентом;
- активности тима за надзор / управљање инцидентима;
- активности угрожене организације;
- прикупљени записи, аретефакти и сл. (ако је применљиво);
- контакт детаљи додатно укључених страна (ако је применљиво);
- коментари особе која прати инцидент;
- извор иницдента (претпостављени/утврђени);
- белешке о утицају/последицама/опоравку….

Са становишта пријаве инцидента, препоручује се да се форма структуира у складу са овим препорукама и изабраним приступом класификацији нивоа озбиљности инцидента, те тако да остави мање места за „слободну интерпретацију“; као пример можда може послужити форма за пријаву инцидента коју на страницама US-CERT [117].
Како не морају сви елементи бити попуњени при иницијалној пријави од стране конституента, то је допуну података могуће извршити при узвратном контакту ЦЕРТ-а ка конституенту, као и верификацију већ добијених података, али и допуну контекстуалних информација.

[117] https://www.us-cert.gov/forms/report (мај 2018.)

7 ПРЕВЕНТИВА

7.1 Упутство и списак савета за запослене у операторима ИКТ система о поступању на радном месту и изван радног места, а у вези са подацима и опремом

Безбедност радних станица и мобилних уређаја оператора ИКТ система

Следеће безбедносне контроле (уколико су доступне), морају бити активиране на свим радним станицама и мобилним уређајима, како би унапредиле заштиту од крађе поверљивих података.

- активирати енкрипцијску заштиту на радним станицама и мобилним уређајима - као што је описано у даљем тексту;
- активирати *hard disk* шифру за сваки диск у *BIOS* подешавању који није заштићен методом енкрипције садржаја на целом диску (*full disk encryption*) или неким другим енкрипцијским решењем на апликативном нивоу. Није неопходно периодично мењати шифру за енкрипцију *hard disk* уређаја на радним станицама и мобилним уређајима;
- подесити заштитну шифру на тастатури (екрану) коју је потребно унети након одређеног периода неактивности и приликом преласка уређаја из стања хибернације или режима приправности (*standby)*. Заштитну шифру је потребно унети на сваком активном налогу након не више од 30 минута неактивности. *Desktop* радне станице које се налазе у радним просторима са контролом приступа или који се закључавају (тако да осим особа које имају прво приступа радној станици друге не могу приступити) није неопходно заштитити шифром на тастатури/екрану.

Привремено напуштање радног простора за запослене у операторима ИКТ система

Уколико запослени ради у радном простору који није могуће закључати:

- обавезно је активирати закључавање на на тастатури (екрану) приликом одласка из радног простора (не остављати радну станицу или мобилни уређај изложеним да тек након 30 минута неактивности захтевају уношење заштитне шифре).

Радне станице и мобилни уређаји морају бити физички обезбеђени у сваком тренутку (тј. да се налазе у физички обезбеђеном простору, закључани у орману или столу или их запослени носи са собом). Уколико то није могуће, за радне станице препоручено је коришћење *cable lock* решења помоћу кога се радна станица повезује за фиксирани неки објекат.

Путовања и рад на даљину за запослене у операторима ИКТ система

Уколико то није немогуће, у сваком тренутку задржати преносни рачунар и/или мобилни уређај у свом поседу.

- приликом коришћења авио-саобраћаја не стављати преносни рачунар или мобилни уређај у пртљагу који се предаје (није у сталном поседу запосленог), тј. носити их искључиво у личном пртљагу који се уноси у кабину авиона;
- треба бити на опрезу на могућност крађе приликом проласка кроз безбедносне провере на аеродрому.

Преносни рачунар или мобилни уређај не остављати у возилу без надзора.

- уколико се ипак преносни рачунар или мобилни уређај морају неко време оставити у возилу без надзора, размотрити начин да се они адекватно заштите. Препоручено је да не буде видно изложена, те коришћење *cable lock* решења у пртљажнику или закључавање у посебним деловима возила уколико они постоје.

Уколико преносни рачунар или мобилни уређај морају остати у хотелу без надзора, исте оставити закључане у сефу.

- уколико сеф није доступан препоручује се мин. коришћење *cable lock* решења за преносне рачунаре.

Уколико запослени у операторима ИКТ система путује са поверљивим подацима који се налазе на екстерним медијима, треба применити исте мере заштите као и за преносне рачунаре и мобилне уређаје.

Уколико дође до крађе преносног рачунар , мобилног уређаја или екстерног медија (нпр. преносни екстерни *hard disk*, преносива *USB flash* меморија), запослени у операторима ИКТ система је обавезан да без одлагања пријави инцидент безбедносној служби оператора ИКТ система, а препоручљиво и свом надлежном руководиоцу.

Компјутерски вируси и остали малициозни кодови

На свакој радној станици или мобилном уређају треба да буде инсталиран и активан антивирусни програм одобрен од и у складу са правилима надлежне службе оператора ИКТ система.

Уколико се открије вирус обезбедити могућност да сваки запослени у оператору ИКТ система има могућност да пријави инцидент (*online* форма, папирни формулар) .

Антивирусни програм мора да задовољава следеће основне критеријуме.

- откривање и блокирање покушаја вирусног софтвера у реалном времену;
- периодично скенирање и откривање вирусног софтвера који се чува на радној станици или мобилном уређају;
- ажурирање датотека контроле вирусног потписа на минимално дневном нивоу;
- аутентични проверени лиценцирани или производ отвореног кода.

Security firewall

На свакој радној станици или мобилном уређају треба да буде инсталиран и активан клијентски *firewall* [118]софтвер одобрен од и у складу са правилима надлежне службе оператора ИКТ система.

Security firewall мора да задовољава следеће основне критеријуме:

- новооткривене мреже треба третирати као непознате и (по постављеном правилу) им НЕ треба веровати;
- упозорава кориснике на нове програме који захтевају приступ мрежи;
- ускраћује приступ неовлашћеним системима;
- редовно се ажурира актуелним верзијама или допунама;
- аутентични проверени лиценцирани или производ отвореног кода.

Енкрипција

A) заштита информација које се преносе преко мреже.

Информације класификоване као Поверљиве (нпр. пословни планови, интерне финансијске информације, лични подаци…), као и подаци о кредитним картицама или медицинским записима морају бити енкриптовани уколико се преносе преко Интернета;

B) заштита информација на рачунару или мобилном уређају.

Коришћење решења за енкрипцију садржаја на целом диску (*full disk encryption*) одобреног од и у складу са правилима надлежне службе оператора ИКТ система, за радне станице и мобилне уређаје

- на којима се чувају осетљиве личне информације [119], или
- на којима се чувају информације о корисницима, или
- који се износе изван физичке локације организације

Коришћење решења за енкрипцију садржаја на портабл медијима

- на којима се чувају осетљиве личне информације, или
- на којима се чувају информације о корисницима, или
- на којима се чувају информације класификоване као Поверљиве, или
- медиј (садржај) је креиран за потребе прављења резервне копије података (*backup*)

---

[118] **Firewall** – систем или софтвер који прати и контролише мрежну комуникацију. У општем случају говори се о мрежном или хост-базираном firewall-у; мрежни филтрира саобраћај између две или више (логичких) мрежа и често је посебан уређај, док је хост-базирани у ствари софтвер који се извршава на раунарском систему „домаћину“ и контролише саобраћај ка и од тог система.
https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx (март 2018.)

[119] Означавају се и као: Sensitive Personal Information (SPI), Special Category of Data (SCD) – према GDPR (General Data Protection Regulation; https://www.eugdpr.org/)

Уколико на радној станици није примењена мера енкрипције садржаја на целом диску, минимално треба да буде активирана енкрипција садржаја локалних репозиторија где се чувају подаци електронске поште, а који садрже информације класификоване као Поверљиве – укљ. и саме поруке, датотеке, и др. реплике.

Ажурирање радних станица и мобилних уређаја

A) коришћење одобреног оперативног система

На рачунарима одн. уређајима мора бити у употреби оперативни систем (као и други софтвер) типа, верзије и са примењеним закрпама који је одобрен од стране надлежне службе организације;

B) примена сервисних пакета и закрпа

Механизми за испоруку и преузимање и примену пакета за подизање софтвера на вишу верзију, већих сервисних пакета и закрпа морају бити функционални и мора им се дозволити да изврше своје програмиране активности (одлагање примене пакета може бити одложено за случај тренутне неопходности, али не више од 24 сата).

Регистрација радних станица и мобилних уређаја

Регистрација је обавезна за све радне станице и мобилне уређаје који се повезују на рачунраску мрежу организације или се користе за потребе извршавања пословне активности организације – без обзира на власништво. Регистрација се обавља преко инсталације клијентске апликације за подршку централизованом управљању радне станице или мобилног уређаја или ручно кроз за то одређене системе за управљање информационим добрима.

Заштита Поверљивих информација

Примарни захтев је да информација класификована као Поверљива мора бити заштићена од приступа или прегледа од стране особа којима то није експлицитно дозвољено у циљу извршавања свог пословног задатка (принцип need-to-know).

A) **при креирању или дистрибуцији Поверљиве информације**

потребно је исту означити адекватно, у складу са утврђеном инструкцијом;

B) **у случају приступа, процесирања или чувања Поверљивих информација**

Дозвољено је само појединцима који имају валидну пословну потребу за приступ тој информацији.

Приступ овим информацијама никада не сме бити неограничен (тј., неопходна аутентификација за приступ и/или укључивање у листе за дозволу приступа);

C) **у случају штампања Поверљивих информација**

Информације треба заштити од крађе или неовлашћеног увида. Поверљиве информације могу се штампати само

- у просторима са контролом приступа, под надзором;
- на штампачима који имају контролу пуштања штампе од стране конкретне особе, одн. директно су додељени тој особи.

Уколико овакви услови нису доступни, могуће је користити штампаче у шире доступним просторијама коије се налазе у контролисаном пословном простору организације, али Поверљиви материјал мора бити преузет у што краћем року од штампања (макс. 30 мин).

По преузимању папирне копије се третирају сагласно дефинисаним правилима Класификације информација (чување, дистрибуција, уништавање).

D) **у случају размене Поверљивих информација преко телеконференције и сл. облика комуниикације**

Бити посебно обазрив у погледу размене Поверљивих информација у случају учешћа у комуникационх форума или конференцијских сервиса са отвореним приступом. Информација сме бити саопштена само особи која је за то овлашћена.

- пре размене поверљивих информација уверити се да учесници у телеконференцији имају одговарајућа овлашћења;
- користити решења одн. медиј за телеконференцију који је претходно проверен и одобрен од стране надлежне службе у организацији.

Заштита пословних информација након што престане потреба за њима

Сви

- пословни подаци и апликације;
- клијентски подаци и апликације;
- приступне информације и лозинке

морају бити обрисани са радних станица и мобилних уређаја када више не постоји легитимна потреба за њима или истекне одобрење за приступ.

Подаци се бришу на начин, методама и средствима прописаним од стране надлежне службе у организацији.

У случају да су информације у материјаном облику, исте морају бити уништене прописаним средствима и методама (*cross-cut shredder* [120] или др. сертификовано решење, физичко уништење и сл.)

Заштита осетљивих личних информација

Личне информације које имају потенцијал значајних последица дефинисане су регулаторним и актима организације.

Одговорност при баратању осетљивим личним информацијама:

- не прикупљати нити чувати ове информације без валидне пословне потребе;
- правилно класификовати ове информације (као поверљиве) и сагласно томе их третирати;

[120] Механички уређај намењен за уништвање (сецкање) папира, али и других медија, у делове како би се отежала одн,. онемогућило њихово поновно састављање и ре-креирање изворне информаиције која на њима била смештена. Cross-cut тип сече материјал на правоугаоне или сл. делове.
Зависно од степена уситњавања медија (димензија резултујућих делова) неки стандарди дефинишу и степен безбедности (нпр. DIN 66399)
http://www.din-66399.com/index.php/en/securitylevels (март 2018.)

- осетљиве личне информације на радној станици, мобилном уређају или портабл медију за складиштење морају бити енкриптовани (сагласно описаној пракси и захтевима за Енкрипцију).
  Уколико су информације на материјалним медијима, исти морају бити смештени на сигурном месту са имплементираним рестриктивним мерама приступа (када власник информација није присутан);
- обавезно одмах пријавити ако неке од осетљивих личних информација или медија који их садрже буде изгубљен, украден или постоји сумња да је безбедност информација компромитована;
  Испратити процедуру или преоруке за пријаву инцидента (обавезно навести да је безбедност осетљивих линих података нарушена).

Правилно коришћење ресурса организације

A) при коришћењу рачунарске мреже институције:

- не сме се користити туђи идентитет нити уређај (како не би били „откривени“);
- безбедносна тестирања над системима у мрежи или „ослушкивање мреже“ (sniffing) не смеју се вршити осим ако постоји експлицитно одбрење за коришћење таквих алата и извршавање активности;
- не инсталирати софтвер или друге алате који могу повезати радну станицу са Интернетом и остати активно повезани тако да омогућавају неометани удаљени приступ (нпр. GoToMyPC, TeamViewer);
- на мрежу организације сме се повезати само рачунар или мобилни уређај који је претходно регистрован (и адекватно припремљен);
- не додавати уређаје који могу проширити мрежу организације без претходног експлицитног одобрења и налога;
- гости се не смеју повезати на интерну мрежу организације (за госте постоји одређена посебна мрежа одн. мрежни сегмент);
- мобилни уређаји да би сем смели повезати на интерну бежичну мрежу, морају
  - имати одговарајући подржани тип и верзију оперативног система;
  - бити регистровани под постојећим програмом управљања мобилним уређајима (уз спроведена адекватна подешавања).

B) при коришћењу удаљеног приступа мрежи или системима институције

- мора се користити решење за удаљени приступ које је претходно проверено и одобрено од стране надлежне службе у организацији (као нпр. Cisco AnyConnect);
- мобилни уређаји морај укористити апликацију обезбеђену од стране организације за приступ мрежи организације;
- креденцијали потребни заудаљени приступ мрежи се морају чувати, и то тако да
  - друге особе не смеју користити туђе крецденцијале;
  - креденцијали не смеју бити снимљени (било који уређај да је у питању).

C) при коришћењу јавних система и сервиса

- коришћење јавних система за приступ ресурсима унутар организације није дозвољено (ни је дозвољено ни коришћење *bootable* медија на јавном систему за приступ);
- само информације које су одобрене за јавну употребу смеју бити забележене, копиране или прослеђене неком јавном систему или сервису
  - није дозвољено пребацивање информација из организације на нечију Интернет е-пошту, календар или јавни cloud сервис за чивање података и размену датотека – осим ако то решење није експлицитно претходно одобрено за ту намену од стране надлежне службе;
  - забрањено је аутоматско прослеђивање е-поште са интерних система за е-пошту у организацији на неке екстерне адресе преко Интернета;
  - ни информације које нису поверљиве или пословно контролисане не смеју се делити изван организације, осим са особама које имају пословону потребу по принципу "*need-to-know*."

Пријава безбедносних инцидената

Безбедносни инциденти морају бити пријављени надлежном одређеном контакт центру.

Појединац не треба да покушава да самостално истражује или примењује неку акцију против потенцијалног нападача. Надлежни тим за информациону безбедност ке квалигфикован и обучен за предузимање прописаних и адекватних активности. Уколико се затражи, појединац треба да пружи потребну помоћ надлежном тиму у процесу истраживања или решавања инцидента .

8 ПРИМЕРИ СЦЕНАРИЈА

8.1 Инцидент малог утицаја

Пример инцидента малог утицаја може бити случај када се по неком каналу комуникације открије да на одређеном програмском пакету (програмски пакети могу бити стандардне апликације, различити алати, итд.) постоје сигурносни недостаци. Канали комуникације по којима се такве информације могу прикупити могу бити различити начини објаве самог произвођача програмског пакета, затим портали или блогови који покривају теме из области сигурности, итд. У том случају одговорно лице креира ticket у ticketing систему, класификује га као инцидент малог утицаја и поставља средњи приоритет на ticket-u.

Такав инцидент се затим прослеђује надлежној групи за анализу. Након анализе, уколико постоји, документује се решење и издају се одговарајућа обавештења, препоруке за решавање, отклањање или препоруке за заштиту.

8.2 Инцидент од националног утицаја

DDoS напади су све учесталија појава и углавном су великог утицаја или критичног утицаја и могу изазвати озбиљне штете на пословање и пружање услуга нападнуте стране. Овакви напади су покушаји да се нека онлајн услуга онемогући преоптерећивањем саобраћаја из више извора. Циљају широк спектар важних ресурса, од банака до веб страница вести, владиних сајтова па и комплетне националне домене и представљају велики изазов за решавање и спречавање њиховог утицаја.

Пример инцидента може бити пријава DDoS напада на националним .rs домаинима. Такав инцидент одговорно лице евидентира креирањем тицкет-а високог приоритета и прослеђује надлежној групи за анализу.

Након анализе, документује се решење и издају се одговарајућа обавештења, препоруке за решавање, отклањање или препоруке за заштиту.

8.3 Инцидент од међународног утицаја

Напади крипто црва (*cryptoworm*) су честа појава. Могу да имају међународне размере и да нанесу огромне штете, како корпорацијама, тако и појединим корисницима. Скорији пример инцидента таквог обима је био *WannaCry ransomware* који је циљано направљен за напад на рачунаре са *Microsoft Windows* оперативним ситемом. Напад се састојао у криптовању корисничких података на самом диску рачунара и тражено је од корисника да плате откуп како би њихови подаци били откључани. Експерти су јако брзо објавили обавештење да је велики број корисника платио откуп, а да подаци нису враћени. Такође, *Microsoft* је у року од два дана објавио хитну закрпу за *Windows 7 и 8.1* системе како би се спречило даље ширење црва и омогућила заштита корисничких рачунара од даље заразе и губитка података.

У оваквим случајевима предлаже се да се отвори инцидент највишег приоритета и проследи групи одговорној за анализу. Добра пракса је да се о инцидентима највишег приоритета надлежна група обавести и телефонским позивом, како се са почетком анализе кренуло у најкраћем могућем року. И у овом случају свакако треба да се креира ticket, како би цео случај био документован за

даље коришћење. Након анализе, документује се решење и издају се одговарајућа обавештења, препоруке за решавање, отклањање или препоруке за заштиту.

9 ЗАКЉУЧАК

Доношењем Закона о информационој безбедности у Републици Србији, учињени су први кораци са циљем обезбеђивања да пружаоци кључних услуга предузимају одговарајуће техничке и организационе мере за управљање ризицима којима су изложени њихови мрежни и информациони системи неопходни за редовно обављање послова. Ових Законом је утврђено да је Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ) надлежна за координацију и извршавање послова Националног центра за превенцију безбедносних ризика у ИКТ системима (Национални ЦЕРТ).

У оквиру овог научног истраживања и израде Студије изводљивости успостављања процедура Националног ЦЕРТ-а и управљања системом за пријаву инцидената процедурално су уређени начини на који Национални ЦЕРТ добија информације о инцидентима, како поступа са њима, односно врши анализу добијених података, чува обрађене информације и обавештава јавност или поједине субјекте о начину управљања и санирања ризика и инцидената. Извршена је анализа поступка пријема, обраде и реакције на информације о инцидентима, а дати су и одговарајуће нацрти процедура које ће уредити овај поступак.

Ова студија је такође дала предлог следећих класификација:

- класификације информација о ризицима и инцидентима;
- класификације информација о ризицима и инцидентима у вези са тајношћу података;
- класификације озбиљности инцидената и ризика;
- категоризације напада према утицају на пословање;
- класификације нивоа озбиљности инцидената и ризика.

Применом следећих предложених модела рада који су обрађени као посебни документи и дати у поглављу „Прилози“:

- Политика класификације информација,
- Процедура управљања инцидентима и
- Оквир плана континуитета пословања за ЦЕРТ платформу.

био би омогућен унифициран рад свих сектора друштвене заједнице који се морају удружити и радити заједно на превенцији и борби против ургожавања рада информационо-комуникационих система.

10 ПРИЛОЗИ

10.1 Речник стручних израза и скраћеница

- ИКТ систем - информационо-комуникациони систем, 10;
- APT - Advanced Persistent Threats, 3;
- ЦЕРТ - Национални центар за превенцију безбедносних ризика у ИКТ системима, 4;
- РАТЕЛ - Регулаторна агенција за електронске комуникације и поштанске услуге;
- ENISA - The European Union Agency for Network and Information Security, 7;
- ОЕБС – Организација за европску безбедност и сарадњу;
- ECSO - European Cyber Security Organisation;
- EU – European Union;
- IDS – Intrusion Detection System;
- ICMP - Internet Control Messaging Protocol;
- SMTP - Simple Mail Transfer Protocol;
- EXPN/RCPT – Expiration / Recipient;
- DNS - Domain Name System;
- SQL - Structured Query Language;
- SYN – Synchronize;
- CVE - Common Vulnerabilities and Exposures;
- SoC - Security operation Center, 12;
- TF-CSIRT - Task Force Computer Security Incident Response Teams, 23;
- TI – Trusted Introducer, 23;
- CcoP – Code of Practice, 23;
- TLP - Traffic Light Protocol, 23;
- NIST - National Institute of Standards and Technology;
- US-CERT - United States Computer Emergency Readiness Team;
- NCCIC - National Cybersecurity and Communications Integration Center, 26;
- NCISS - Cyber Incident Scoring System, 26;
- PGP – Pretty Good Privacy, 24;
- DMZ - Demilitarized Zone
- APT - Advanced Persistent Thread;
- ISO/IEC - International Organization for Standardization/International Electrotechnical Commission , 32;
- ISMS - Information Security Management System, 32;
- BC - Business Continuity;
- DR - Disaster Recovery, 34;
- BCM - Business Continuity Management, 34;
- ITIL - IT Infrastructure Library;

- RTO - Recovery Time Objective;
- RPO - Recovery Point Objective;
- IP - Internet Protocol;
- SoC - Security Operations Centre, 41;
- IPS - Intrusion Detection System;
- SIEM - Security Information and Event Management, 46;
- TTP - Tactics, Techniques and Procedures;
- CIF - Collective Intelligence Framework;
- DoS - Denial of Service;
- DDos - Distributed Denial of Service;
- REST API - Representational State Transfer, 54;
- API - Application Programming Interface, 54;
- JSON - JavaScript Object Notation, 54;
- XML - eXtensible Markup Language, 54;
- RTIR - Request Tracker for Incident Response, 54;
- OTRS - Open source Ticket Request System, 54;
- SaaS - Software as a Service, 55;
- MISP - Malware Information Sharing Platform, 55;
- HTTP - Hypertext Transfer Protocol;
- HTTPS – HTTP Secure;
- IoC - Indicator of Compromis, 57;
- C&C - Command & Control;
- MANTIS - Model-based Analysis of Threat Intelligence Sources framework;
- CybOX - Cyber Observable Expression;
- CSV - Comma-Separated Values;
- STIX - Structured Threat Information eXpression, 58;
- IHAP - Incident Handling Automation Project;
- CIF - Collective Intelligence Framework;
- GIS - Geographic Information System, 59;
- NATO - North Atlantic Treaty Organization;
- IODEF - Incident Object Description Exchange Format, 62;
- IETF - Internet Engineering Task Force;
- MILE - Managed Incident Lightweight Exchange;
- RFC - Request for Comments;
- RID - Real-time Inter-network Defense;
- ROLIE - Resource Oriented Lightweight Indicator Exchange, 64;
- TAXII - Trusted Automated Exchange of Intelligence Information, 65;
- OASIS - Organization for the Advancement of Structured Information Standards, 65;
- SDO - STIX Data Objects, 65;
- SRO – STIX Relation Objects, 65;

- IEP - Information Exchange Policy;
- CTI TC - Cyber Threat Intelligence Technical Committee;
- BIOS - Basic Input/Output System.

10.2 Речник страних речи и израза

- cyber – информациони;
- command & control – командни и контролни;
- event – догађај;
- incident – инцидент;
- penetration test –покушај експлоатације неког IT система уз одобење власника како би се октриле његове рањивосити и слабости;
- CYBERSECURITY – информациона безбедност;
- honeypot, 7;
- impact, 10;
- hacking, 12;
- Computer Security Incident Respones, 12;
- Security Operations Centre, 12;
- network – мрежа;
- abusive content – непожељни садржај;
- malicious code – малициозни програмски код;
- information gathering – прикупљање информација;
- intrusion attempt – покушај упада;
- intrusion – упад;
- availibilty – доступност (утицај);
- information content security – безбедност садржаја информација;
- fraud – превара;
- vulnerable – рањивост;
- other – остало;
- test – тест;
- ticketing - евидентирање;
- spam, 15;
- harmful speech, 15;
- children – деца;
- sexual – сексуално;
- violence – насиље;
- virus - малициозни софтвер;
- worm - црв (врста компјутерског вируса који стети систему и сакривен је);
- trojan - тројанац (врста компјутерског вируса који је најчешће сакривен у неком фајлу);
- ransomware - малициозни софтвер који закључава систем док се не плати откупнина лицима која су га закључала;

- spyware - малициозни софтвер који шаље информације о систему на којем се налази;
- dialer - малициозни софтвер који сам обавља телефонске позиве правећи огроман рачун кориснику;
- rootkit - малициозни софтвер који омогућава приступ деловима компјутерског система којима не може свако да има приступ;
- scanning, 15;
- sniffing, 15;
- social engineering, 15;
- exploiting known vulnerabilites, 15;
- fingerd – обележавање;
- DNS querying - промена веб адреса у циљу приступања лажним сајтовима;
- wiretapping – прислушкивање;
- buffer overflow - пребукирање система захтевима које не може да обради;
- cross-side scripting – врста рањивости компјуерског система;
- backdoor - искоришћавање рупа у систему у циљу приступања истом;
- login attempts, 15;
- brute force - покушај приступа систему непрекидним логовањем са више милионским варијацијама лозике;
- new attack signature, 15;
- privileged account compromise – компромитовање налога са посебним привилегијама;
- unprivileged account compromise – компромитовање налога без посебних привилегија;
- application compromise – компромитовање апликације;
- bot - софтвер који има улогу опонашања човека;
- ICMP flood - позивање сервера простим захтевима који не може да обради;
- SYN flood - врста DoS малициозног програма;
- Teardrop - слање пакета из више мањих поруку које сервер не може да састави и на тај начин пуни своју меморију;
- mail-bombing - слање велике количине електронске поште која нема никаву вредност или значење и на тај начин пуни меморију;
- DNS amplification - огроман број захтева упућен некој DNS адреси;
- sabotage – саботажа;
- outage (no malice) – отказивање / квар (без зле намере);
- unathorised access to information – неовлашћени приступ информацијама;
- unathorised modification of information – неовлашћена манипулација подацима или измена података у датотеци, документу или бази података;
- unauthorized use of resources – неовлашћено коришћење ресурса;
- spoofing - претварање да си неко други;
- hijacking - неовлашћено узимање;
- copyright – повреда ауторских права;
- Warez - пиратски софтвер;

- masquerade – маскирање;
- phishing, 16;
- open for abuse – отворено за напад и злоупотребу;
- Open resolver – отворено доступни сервиси за разрешавање интернет (DNS) адреса;
- hotline – сервис који је увек доступан за пријављивање ицидената или злоупотребе;
- help-desk – сервис на којем можемо наћи информације које су нам потребне;
- anti-spam – софтвер који онемогућава пријем незељене и непотребне поште или информација;
- code-verify – добро оптимизован и лако читљив код;
- stand-by – особа или сервис који је увек доступна;
- Information Security Governance, 32;
- backup - израда копије података оригиналног извора за случај да се извор оштети или изгуби;
- high availability – висока доступност;
- governance – одговорност;
- data – подаци;
- actionable information, 32;
- firewall - безбедносни слој података који филтрира податке који долазе са интернета
- threat intelligence feed - подаци о претњама који долазе од извора који немају везе са постојећим информационим системом;
- hash, 42;
- call - позив;
- log-management - белезење понашања софтвера;
- chat - могућност инстант слања и примања порука;
- groupware - софтвер који омогућава људима да раде заједно иако нису на физички истим локацијама;
- Enterprise Content Management, 49;
- Capture the Flag, 50;
- knowledge manager - особа која манипулише прикупљеним подацимаopen source, 50;
- incident tracking – праћење инцидената;
- incident response – одговор на инцидент;
- tag – ознака;
- playbook – правилник;
- ticket – број генерисан од стране сервера, у сврху атуентификације клијента;
- incident workflow – ток инцидента;
- community eddition – издање за заједницу;
- live stream – пренос уживо;
- service management – управљање сервисима;
- security operations – сигурносне операције;
- spear-phishing – врста напада преко е-поште;

- threat information sharing – размена информација о претњама;
- de-facto – чињенично;
- endpoint security – крајња сигурност;
- work in progress – рад у току;
- big data – велика количина података;
- use-case – случај коришћења;
- queries – упити;
- data access and acquisition framework – платформа-оквир за унос и приступ подацима;
- situational awareness - свест о актуелном стању;
- peer-to-peer – врста архитектуре система, таква да су њени чиниоци међусобно равноправни;
- data marking – означавање података;
- marking-definition – дефиниција означавања;
- Cyber Observables – информациона надгледања;
- hard disc – тврди диск;
- full disk encryption – потпуна енкрипција диска;
- cable loc – омогућава кружну заштиту;
- online – на мрежи;
- need-to-know – морати знати;
- cross-cut shredder, 74;
- bootable – самопокрећући;
- cloud – облак;
- browser – претраживач;
- cryptoworm – крипто црв.

10.3 Политика класификације информација

Политика класификације информација се прилаже као посебан документ.

10.4 Процедура управљања инцидентима

Процедура управљања инцидентима се прилаже као посебан документ.

10.5 Оквир плана континуитета пословања

Оквир плана континуитета пословања се прилаже као посебан документ.

11 ЛИТЕРАТУРА

- Службени гласник РС, бр 6/16 и 94/17
- https://www.enisa.europa.eu/topics/csirt-cert-services
- https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
- https://www.sans.edu/cyber-research/security-laboratory/article/honeypots-guide#addsearch=honeypot
- https://www.osce.org/sr/serbia/272206?download=true
- https://www.bbc.com/education/guides/z2c82hv/revision
- ISO27035:2016 - Принципи управљања инцидентима
- ISO27035:2016 - Смернице за планирање одзива на инциденте
- https://tools.ietf.org/html/rfc2828
- Information technology -- Security techniques - Information security risk management ISO/IEC FIDIS 27005:2008
- https://www.enisa.europa.eu/publications/technical-guideline-on-threats-and-assets/at_download/fullReport
- https://tools.ietf.org/html/rfc2828
- https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary#G52
- https://dictionary.cambridge.org/dictionary/english/hacking и https://cyber.laws.com/hacking (март 2018.)
- https://www.us-cert.gov/bsi/articles/best-practices/incident-management/defining-computer-security-incident-response-teams
- https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide
- http://resources.infosecinstitute.com/structure-csirt-soc-team/
- https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy
- https://tf-csirt.org/
- https://www.trusted-introducer.org/
- https://www.trusted-introducer.org/Incident-Classification-Taxonomy.pdf
- https://github.com/MISP/misp-taxonomies/blob/master/CERT-XLM/machinetag.json
- http://www.ratel.rs/upload/documents/Studije/Studija%20izvodljivosti%20izgradnje%20Nacionalnog%20CERT-a.pdf
- https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14099.pdf
- http://www.ratel.rs/upload/documents/Regulativa/Informaciona_bezbednost/Uredba%20-%20Dostavljanje%20podataka%20o%20incidentima.pdf
- https://www.trusted-introducer.org/TI-CCoP.pdf
- https://www.first.org/tlp/
- https://www.openpgp.org/about/
- https://www.us-cert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf

- https://www.us-cert.gov/nciss/demo
- https://www.iso.org/isoiec-27001-information-security.html
- https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/ra_ver2_en.pdf
- https://www.ncsc.gov.uk/guidance/technical-risk-assessment-and-risk-treatment-is1-2-supplement
- http://mtt.gov.rs/vesti/obrazovano-telo-za-koordinaciju-poslova-informacione-bezbednosti/ (март 2018.)
- https://searchdisasterrecovery.techtarget.com/definition/Business-Continuity-and-Disaster-Recovery-BCDR
- Risk mitigation for business resilience - White paper (IBM, 2007)
- https://www-935.ibm.com/services/pl/gts/html/pdf/gmw14000-usen-00.pdf (март 2018.)
- https://www.enisa.europa.eu/publications/actionable-information-for-security
- https://www.enisa.europa.eu/publications/actionable-information-for-security
- https://www.rnids.rs/lat/domeni/dns-sistem
- https://searchnetworking.techtarget.com/definition/URL
- https://www.gartner.com/newsroom/id/3815169
- https://whatis.techtarget.com/definition/command-and-control-server-CC-server
- https://blogs.cisco.com/security/malware_validation_techniques (март 2018.)
- Knowledge Management Process Model (VTT, 2001) - Timo Kucza
- http://www.vtt.fi/inf/pdf/publications/2001/P455.pdf (март 2018.)
- https://searchcontentmanagement.techtarget.com/definition/content-management-system-CMS
- https://searchsecurity.techtarget.com/definition/ethical-hacker
- https://blogs.cisco.com/perspectives/cyber-security-capture-the-flag-ctf-what-is-it
- https://www.incidentresponse.com/wp-content/uploads/GMU-Cybersecurity-Incident-Response-Team_social_maturity_handbook-updated_10.20.16.pdf(март 2018)
- https://www.ibm.com/events/think/watch/replay/113897913/
- https://opensource.org/osd
- https://en.oxforddictionaries.com/definition/api (март 2018.)
- https://www.json.org/ (април 2018.)
- https://bestpractical.com/rtir/ (март 2018.)
- https://community.otrs.com/
- https://otrs.com/ (март 2018.)
- https://thehive-project.org/ (март 2018.)
- https://otrs.com/otrs-solutions/corporate-security/storm/ (март 2018.)
- https://github.com/TheHive-Project/TheHive/blob/master/AUTHORS
- https://first.org/resources/papers/conf2017/TheHive-a-Scalable-Open-Source-and-Free-Incident-Response-Platform.pdf (март 2018.)
- http://www.misp-project.org/ (март 2018.)
- http://www.bmc.com/it-solutions/remedy-itsm.html

- https://www-01.ibm.com/software/applications/control-desk/
- https://www.resilientsystems.com/our-platform/
- https://www.rsa.com/content/dam/pdfs/5-2017/rsa-netwitness-secops-manager-ds.pdf
- https://www.first.org/global/sigs/information-sharing/misp (април 2018.)
- https://www.enisa.europa.eu/publications/detect-share-protect-solutions-for-improving-threat-data-exchange-among-certs (март 2018.)
- https://github.com/siemens/django-mantis (април 2014.)
- https://oasis-open.github.io/cti-documentation/stix/intro.html (април 2018.)
- http://www.misp-project.org/feeds/ (април 2018.)
- https://github.com/certtools/intelmq/tree/develop/docs (април 2018.)
- https://github.com/abusesa/abusehelper (април 2018.)
- https://github.com/certtools/intelmq/blob/develop/docs/Feeds.md (април 2018.)
- https://github.com/certtools/intelmq-manager (април 2018.)
- https://www.nationalgeographic.org/encyclopedia/geographic-information-system-gis/ (април 2018.)
- https://www.ncsc.gov.uk/guidance/security-operations-centre-soc-buyers-guide(април 2018.)
- http://www.openvas.org/about.html
- https://www.tenable.com/products/nessus/nessus-professional(април 2018.)
- https://www.researchgate.net/publication/320887006_A_comparative_analysis_of_incident_reporting_formats (април 2018.)
- https://trac.ietf.org/trac/mile/wiki/WikiStart (април 2018.)
- https://datatracker.ietf.org/doc/rfc7970/ (април 2018.)
- https://tools.ietf.org/html/rfc7970#page-20 (април 2018.)
- https://datatracker.ietf.org/doc/rfc7203/?include_text=1 (април 2018.)
- Florian Menges & Günther Pernul : „A comparative analysis of incident reporting formats“ https://www.researchgate.net/publication/320887006_A_comparative_analysis_of_incident_reporting_formats (април 2018.)
- https://datatracker.ietf.org/doc/rfc6545/ (април 2018.)
- https://datatracker.ietf.org/doc/rfc6546/ (април 2018.)
- https://datatracker.ietf.org/doc/draft-field-mile-rolie/ (април 2018.)
- https://www.enisa.europa.eu/publications/standards-and-tools-for-exchange-and-processing-of-actionable-information/at_download/fullReport (април 2108.)
- http://siis.realmv6.org/implementations/ (maj 2018.)
- https://trac.ietf.org/trac/mile/wiki/WikiStart (maj 2018.)
- https://wi2017.ch/images/wi2017-0188.pdf (април 2018.)
- https://oasis-open.github.io/cti-documentation/stix/intro (април 2018.)
- https://www.oasis-open.org/org (април 2018.)
- http://cyboxproject.github.io/about/
- https://oasis-open.github.io/cti-documentation/stix/intro#stix-2-defines-twelve-stix-domain-objects-sdos (април 2018.)

- https://oasis-open.github.io/cti-documentation/stix/intro#stix-2-defines-two-stix-relationship-objects-sros (април 2018.)
- http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709287 (април 2018.)
- https://www.first.org/iep/
- http://docs.oasis-open.org/cti/stix/v2.0/cs01/part1-stix-core/stix-v2.0-cs01-part1-stix-core.html#_Toc496709283 (април 2018.)
- http://docs.oasis-open.org/cti/stix/v2.0/cs01/part3-cyber-observable-core/stix-v2.0-cs01-part3-cyber-observable-core.html#_Toc496715360 (април 2018.)
- https://wiki.oasis-open.org/cti/Open%20Source%20Projects (април 2018.)
- https://wiki.oasis-open.org/cti/Products (април 2018.)
- http://www.misp-project.org/features.html (април 2018.)
- NIST Special Publication 800-61r2 - https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf (април 2018.)
- https://www.us-cert.gov/forms/report (maj 2018.)
- https://www.microsoft.com/en-us/safety/pc-security/firewalls-whatis.aspx (март 2018.)
- https://www.eugdpr.org/
- http://www.din-66399.com/index.php/en/securitylevels (март 2018.)