ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ИЗВЕШТАЈ
О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

УПРАВЉАЊЕ ИНЦИДЕНТИМА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

Број: 400-392/2022-03/10
Београд, 16. децембар 2022. године

НЕДОСТАТАК АДЕКВАТНЕ РАЗМЕНЕ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА СЛАБИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ, МОЖЕ ДОВЕСТИ ДО ЕСКАЛАЦИЈЕ И ТРАЈНОГ ГУБИТКА ИНФОРМАЦИОНЕ ИМОВИНЕ

Државна ревизорска институција је уочила недостатке у управљању информационом безбедношћу код руковалаца ИКТ система од посебног значаја, посебно код органа јавне управе. Влада Републике Србије је донела Стратегије и прописе којима је успостављен Национални CERT са посебним CERT-овима, самостални CERT-ови, CERT у органима власти и CERT академске мреже Републике Србије. Они прикупљају и размењују информације о могућим ризицима и инцидентима, затим обавештавају, упозоравају и саветују лица која управљају ИКТ системима, као и јавност Републике Србије да предузму активности како би предупредили настанак штете и спречили ширење негативних последица по информациону имовину.

Неразумевање ових питања, низак ниво свести о припадности једном систему и друштву, избегавање пријављивања, мали број пријављених инцидената CERT-у, као и други недостаци у примени Закона о информационој безбедности намећу потребу унапређења ове области, посебно у заштити критичне информационе инфраструктуре (даље КИИ) која је од виталног значаја за опстанак друштва у критичним и кризним ситуацијама.

Управљање инцидентима је потреба и обавеза свих оператора ИКТ система без обзира на сложеност, али обим имплементираних мера заштите треба прилагодити њиховом значају/критичности за функционисање друшта и државе у целини. Пријава инцидента и боље реаговање на њихово решавање када имамо ограничене ресурсе није могућа без доброг планирања и утврђивања листе приоритета. Јачање свести о значају информационе безбедности у свим њеним аспектима о већој видљивости у јавном и интернет простору јачаће њену отпорност и укупну информациону безбедност критичне информационе инфраструктуре.

Јединствени систем за управљање инцидентима мора да омогући непосредно објављивање информација о инцидентима одмах по пријави, као и хитно обавештавање оператора који имају исте рањивости, као и целокупне јавности, како би свако могао предузети превентивне мере и активности на спречавању ескалације проблема. Хронични недостатак ИТ стручњака на инспекцијским пословима, на пословима информационе заштите у јавној управи, може решавати овлашћивањем и ангажовањем правних и физичких лица тј. ИТ стручњака из области информационе безбедности. Разменом информација о инцидентима свих делова државног система и синхоризованим деловањем на примени мера заштите оснажиће се њена укупна отпорност и штитиће се информациона имовина од потенцијалне штете и губитака.

Препоруке

Државна ревизорска институција дала је препоруке Министарству трговине, туризма и телекомуникација да:

- успоставе листу приоритета ИКТ СоПЗ према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре.
- да у сарадњи са другим надлежним организацијама утврде стварне потребе за обукама, стручним усавршавањем, редовним обавештавањем, као и друге активности намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом у циљу јачања свести о значају информационе безбедности и превентивним мерама заштите.
- измене страницу на сајту МТТТ и преусмере кориснике на Национални CERT и апликацију за пријављивање на домену cert.rs, и пропишу ту обавезност за све CERT-ове за које су надлежни.
- изврше категоризацију оператора ИКТ система по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора.
- да у сарадњи са надлежним органима прикупе податке о технолошким решењима оператора ИКТ СоПЗ, обезбеде систем за аутоматизовано обавештавање између CERT-ова и партнера, обезбеде имплементацију и примену.
- обезбеде механизам објављивања аларма по пријави инцидента, означавањем врсте инцидента, нивоа опасности, анонимизоване податке о технолошким решењима погођених ИКТ СоПЗ као и могућим плановима реаговања на исте.
- да коришћењем одговарајућих извора прибаве све неопходне податке како би могли да оцене ИТ ризике, пропишу нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите.
- да се применом дефинисаних критеријума изврши адекватна процена ризика за избор надзираних субјеката.
- успоставе систем колегијалног прегледа од стране овлашћених лица која су компетентна за утврђивање могућих рањивости код оператора ИКТ СоПЗ.

Садржај

Скраћенице и термини

У прегледу су дате скраћенице које су коришћене у извештају:

Пун назив	**Скраћеница**
Закон о информационој безбедности	ЗИБ
Министарство трговине, туризма и телекомуникација	МТТТ
Јединствени систем за пријем обавештења о инцидентима	ЈСПОИ
Информационо-комуникациони систем	ИКТ систем
ИКТ систем од посебног значаја	ИКТ СоПЗ
Оператор ИКТ система од посебног значаја	Оператор ИКТ СоПЗ
Информациони систем	ИС
Информационе технологије	ИТ
Критична информациона инфраструктура (ИКТ системи од посебног значаја)	КИИ
Тим за реаговање на рачунарске безбедносне инциденте (енг. Computer Security Incident Response Team)	CSIRT
Тим за реаговање на интернет инциденте (енг. Cyber Incident Response Team)	CIRT
Тим за реаговање на ванредне инциденте (енг. Computer Emergency Response Team)	CERT

I Резиме и препоруке

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Управљање инцидентима у ИКТ системима од посебног значаја“. Ревизијом је обухваћено Министарство трговине, туризма и телекомуникација као ресорно Министарство за област информационе безбедности српског друштва и државе.

Влада Републике Србије је донела Стратегије и прописе у вези информационе безбедности којима је успостављен Национални CERT са посебним CERT-овима, самосталним CERT-овима, CERT у органима власти и CERT академске мреже Републике Србије. Они прикупљају и размењују информације о могућим ризицима и инцидентима, затим обавештавају, упозоравају и саветују лица која управљају ИКТ системима, као и јавност Републике Србије да предузму активности како би предупредили настанак штете и спречили ширење негативних последица по информациону имовину.

Неразумевање ових питања, низак ниво свести о припадности једном систему и друштву, избегавање пријављивања инцидената, мали број пријављених инцидената CERT-у као и други недостаци у примени Закона о информационој безбедности намећу потребу унапређења ове области, посебно у заштити критичне информационе инфраструктуре (даље КИИ) која је од виталног значаја за опстанак друштва у критичним и кризним ситуацијама.Разменом информација о инцидентима свих делова државног система и синхоризованим деловањем на примени мера заштите оснажиће се њена укупна отпорност и штитиће се информациона имовина од потенцијалне штете и губитака.

Након спроведене ревизије закључили смо да:

Услед недостатка адекватне размене информација о инцидентима слаби укупна информациона безбедност критичне инфраструктуре, посебно ИКТ система од посебног значаја, онемогућавајући јачање укупне сајбер безбедности што излаже информациону имовину ризику од оштећења и могућег трајног губитка.

Наведено смо утврдили на основу закључака, које износимо у наставку, а закључци су донети на основу налаза, који су приказани испод сваког закључка.

ЗАКЉУЧАК 1: Јачање сајбер отпорности и укупне информационе безбедности КИИ није могуће без утврђивања листе приоритета ИКТ СоПЗ, јачања свести о значају информационе безбедности у свим њеним аспектима и веће видљивости у јавном и интернет простору.

- Налаз 1.1: Без утврђивања листе приоритета ИКТ СоПЗ према степену критичности, није било могуће планирати ангажовање постојећих CERT тимова за умањење последица инцидената као и успоставити ефикасан ток опоравака критичне информационе инфраструктуре;
- Налаз 1.2: Јачање свести о значају информационе безбедности без планирања које се заснива на стварним потребама за обукама, стручним усавршавањем, редовним информисањем, као и другим активностима, намењеним крајњим корисницима, запосленима на ИТ пословима и операторима које управљају КИИ, слаби отпорност целокупног друштва на будуће инциденте.;
- Налаз 1.3: Недовољна видљивост важности CERT-ова у јавности и различити садржаји на интернет локацијама CERT-ова за пријављивање инцидената стварају конфузију код

лица који пријављују инцидент и доводе до неадекватног и неблаговременог реаговања учесника у систему заштите критичне информационе имовине.

ЗАКЉУЧАК 2: Процес управљања инцидентима ИКТ СоПЗ не препознаје организациону сложеност, величину и критичност оператора за ефикасну имплементацију мера заштите, технолошка решења која користе оператори и потребу непосредног објављивања информација о инцидентима који су у току, што умањује постојеће позитивне ефекте на оснаживању сајбер отпорности.

- Налаз 2.1: Без извршене категоризације оператора ИКТ СоПЗ по величини и критичности, нису се могле дефинисати минималне/обавезне мере заштите према категоријама чиме се смањује ефикасност прописаних мера за умањење ИТ ризика;
- Налаз 2.2: Недовољно познавање технолошких решења која користе оператори онемогућило је благовремено обавештавање оператора са истим рањивостима и тиме је повећало могуће последице и утицај инцидената на ИТ ризике критичне информационе инфраструктуре;
- Налаз 2.3: Непостојање механизма непосредног објављивања аларма по пријави инцидента, док информација има значај за предузимање превентивних мера заштите у спречавању ескалирања претње по информациону имовину, повећало је рањивост система заштите критичне информационе инфраструктуре.

ЗАКЉУЧАК 3: Постојећи контролни и инспекцијски механизам не обезбеђује адекватну надзорну функцију Министарства, стварајући ризик да инциденти ескалирају и угрозе информациону имовину критичне инфраструктуре.

- Налаз 3.1: МТТТ је израдило страницу на званичној интернет презентацији намењену упису, а то је било недовољно да оператори изврше прописану обавезу и што је онемогућило потпуно успостављање Евиденције оператора ИКТ СоПЗ;
- Налаз 3.2: Евиденција оператора ИКТ СоПЗ није обухватила податке о технолошким решењима који су неопходни за процену ИТ ризика, што онемогућава да се одреде значајни или критични оператори као надзирани субјекти у процесу инспекцијског надзора;
- Налаз 3.3: МТТТ обавља инспекцијски надзор са једним инспектором над операторима ИКТ СоПЗ, што је недовољно у односу на потенцијални број надзираних субјеката, због чега могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

У циљу побољшања управљања инцидентима у ИКТ системима од посебног значаја Државна ревизорска институција даје следеће препоруке Министарству трговине, туризма и телекомуникација:

1. да успоставе листу приоритета ИКТ система од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре. (Налаз 1.1.) – Приоритет 3[1].
2. да у сарадњи са другим надлежним организацијама утврде стварне потребе за обукама, стручним усавршавањем, редовним обавештавањем, као и за другим активностима намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом инфраструктуром у циљу

[1] Приоритет 3 - Несврсисходности које је могуће отклонити у року до три године.

јачања свести о значају информационе безбедности и превентивним мерама заштите. (Налаз 1.2.) – Приоритет 3.

3. да измене страницу на сајту МТТТ и преусмере кориснике на Национални CERT и апликацију за пријављивање на домену cert.rs, и пропишу ту обавезност за све CERT-ове за које су надлежни. (Налаз 1.3.) – Приоритет 3.
4. да изврше категоризацију оператора ИКТ система по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора. (Налаз 2.1.) – Приоритет 3.
5. да у сарадњи са надлежним органима прикупе податке о технолошким решењима оператора ИКТ СоПЗ, обезбеде систем за аутоматизовано обавештавање између CERT-ова и партнера, обезбеде имплементацију и примену. (Налаз 2.2.) – Приоритет 3.
6. да обезбеде механизам објављивања аларма по пријави инцидента, означавањем врсте инцидента, нивоа опасности, анонимизоване податке о технолошким решењима погођених ИКТ СоПЗ као и могућим плановима реаговања на исте. (Налаз 2.3.) – Приоритет 3.
7. да коришћењем одговарајућих извора прибаве све неопходне податке како би могли да оцене ИТ ризике, пропишу нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите. (Налаз 3.1.) – Приоритет 3.
8. да се применом дефинисаних критеријума изврши адекватна процена ризика за избор надзираних субјеката.(Налаз 3.2.) –Приоритет 3.
9. да успоставе систем колегијалног прегледа од стране овлашћених лица која су компетентна за утврђивање могућих рањивости код оператора ИКТ система од посебног значаја. (Налаз 3.3.) – Приоритет 3.

Генерални државни ревизор

др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
16. децембар 2022. године

II Увод

Државна ревизорска институција спровела је ревизију сврсисходности пословања „Управљање инцидентима у ИКТ системима од посебног значаја" у периоду од марта до септембра 2022. године[2]. Ревизија сврсисходности пословања је спроведена у складу са Законом о Државној ревизорској институцији[3], Пословником Државне ревизорске институције[4] и Програмом ревизије Државне ревизорске институције за 2022. годину.
Ревизија је обављена на начин и према поступцима утврђеним оквиром ревизорских стандарда Међународне организације врховних ревизорских институција (INTOSAI), Кодексом професионалне етике државних ревизора, принципима Међународних стандарда врховних ревизорских институција (ISSAI), Методолошким правилима и смерницама за ревизију сврсисходности пословања и Методолошким правилима и смерницама за ИТ ревизију Државне ревизорске институције.

1. Проблем

У претходним годинама Државна ревизорска институција је уочила недостатке у управљању информационом безбедношћу код руковалаца ИКТ система од посебног значаја, посебно код органа јавне управе. Влада Републике Србије је донела „Стратегију развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године" као наставак Стратегије развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године. У делу који се односи на информациону безбедност Стратегија је усклађена са Директивом о мрежној и информационој безбедности ЕУ (енгл.: *Network and Information Security Directive* - NIS *Directive*), и како је предвиђено Законом успостављен је Национални CERT са посебним CERT-овима, самостални CERT-ови и CERT у органима власти.

Примарно задужење Националног CERT-а је прикупљање и размењивање информација о могућим ризицима и инцидентима, а потом обавештавање, упозоравање и саветовање лица која управљају ИКТ системима, као и јавности Републике Србије да предузму активности у домену превенције како би се предупредио настанак штета и спречио сваки облик ескалације негативних последица по информациону имовину. Циљ Националног CERT-а је и подизање свести о значају информационе безбедности путем давања смерница за спровођење превентивних мера заштите, како код грађана, тако и код привредних субјеката и органа јавне власти. Разумевање и ниво свести о овим питањима, број инцидената у претходном периоду од којих је мали број пријављен CERT-у као и други недостаци у примени Закона о информационој безбедности указује на то да постоји значајан простор за унапређење ове области. Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја[5] дефинисане су групе инцидената које су оператори ИКТ система од посебног значаја дужни да пријављују надлежном CERT-у.

[2] Број ревизије 400-1118/2019-03.
[3] „Службени гласник РС", бр. 101/05, 54/07, 36/10 и 44/18-др.закон.
[4] „Службени гласник РС", број 9/09.
[5] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС", број 11 од 7. фебруара 2020)

2. Циљ ревизије

Циљ ревизије је обезбеђивање основе за пружање независног уверавања и оцене ефикасности управљања инцидентима у ИКТ системима од посебног значаја у складу са Законом о информационој безбедности.

Изабрана тема је повезана са Циљем 2 из Стратешког плана ДРИ за период 2019–2023, где је одређено да ће ДРИ утврдити проблеме и предложити решења за међусекторске проблеме на свим нивоима, ради унапређивања одговорности и транспарентности. Односно у оквиру овог стратешког циља реализоваће се потциљ 2.5: Унапредити јавно управљање и коришћење информационих технологија (ИТ)[6].

Инциденти у области информационе безбедности су обично повезани са нарушеном безбедношћу информационо-комуникационих система, што може бити провала у систем, приступ подацима који није требало да буде омогућен, изазивање проблема у раду система и слично. Крајње последице таквих инцидената најчешће излазе из оквира самог ИКТ система и односе се на послове, организације и људе који се непосредно или посредно ослањају на ИКТ систем. На пример, прекид рада информационог система у банци може онемогућити банку да опслужује своје клијенте, а клијента банке може довести у ситуацију да не може да плати рачун својом кредитном картицом. Такви инциденти ширих размера могу угрозити функционисање државе, привреде и друштва, због чега се одређују ИКТ системи од посебног значаја за које постоји законска обавеза старања о информационој безбедности у складу са Законом.

Како је Закон о информационој безбедности предвидео МТТТ руководи Телом за координацију послова информационе безбедности, а задатак му је 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 значајан утицај на нарушавање информационе безбедности у Републици Србији.

3. Ревизијска питања

Како бисмо остварили циљ ревизије, усмерили смо се на прибављање одговора на следећа ревизијска питања:

1. Да ли се адекватно планирају активности на обезбеђивању управљања инцидентима у ИКТ системима од посебног значаја?
2. У којој мери управљање инцидентима у ИКТ системима од посебног значаја умањује ИТ ризике на критичну инфраструктуру?
3. Да ли су успостављени адекватан надзор и контрола управљања инцидентима у ИКТ системима од посебног значаја?

Питања која смо формулисали се односе на три најризичније области, на основу процене ризика коју смо спровели на бази доступних, тј. прикупљених података у фази планирања и истраживања предложене теме ревизије.

[6] Стратешки план Државне ревизорске институције за период 2019–2023. године **http://www.dri.rs/upload/documents/Opsti_dokumenti/DRI%20Strateski%20plan2018-2023.pdf**

4. Обим и ограничења ревизије

Ревизијом смо обухватили управљање инцидентима као значајан део укупног система информационе безбедности са посебним тежиштем управљања безбедношћу критичне информационе инфраструктуре.

Као надзорни орган који је предлагач закона, који контролише и прати његову измену Министарство за трговину, туризам и телекомуникације субјект је ревизије којем ће се помоћи да читав систем обезбеђења подигне на виши ниво функционалности. Зато су нам извори информација били: Национални CERT, CERT републичких органа посебни CERT-ови и Посебни CERT Nova Defense чији Центар за подршку корисницима смо и посетили.

Предмет ревизије су активности које је субјекат ревизије предузимао у погледу планирања, спровођења и вршења надзора у области информационе безбедности са тежиштем на систему обавештавања и извештавања о насталим инцидентима.

Ревизијом смо обухватили период 2019–2021. године, али смо за одговоре на нека ревизијска питања обухватили и дужи временски период.

Поступци ревизије су изведени у периоду од маја до октобра 2022. године у циљу доношења налаза, закључака и препорука заснованих на доказима који су прикупљени током ревизије.

У поступку ревизије нисмо испитивали:

- Да ли финансијски извештаји субјекта ревизије истинито и објективно приказују њихово финансијско стање, резултате пословања и новчане токове, у складу са прихваћеним рачуноводственим начелима и стандардима;
- Финансијске трансакције и одлуке у вези са примањима и приходима и расходима и издацима, ради утврђивања одговора на питање – да ли су односне трансакције извршене у складу са законом, другим прописима и за планиране сврхе;
- Међусобне обавезе и потраживања органа јавне управе која су обухваћена ревизијом.

У циљу потврђивања информација из документације и прикупљања података који нису доступни у документима, обавили смо интервјуе, послали упитнике субјекту ревизије и изворима информација.

5. Методологија у поступку рада

Да бисмо формулисали ревизорска питања и касније одговорили на њих, анализирали смо стратегије, законске и подзаконске прописе који се односе на област информационе безбедности, као и податке и информације које смо добили од извора информација.

У циљу планирања ревизије сврсисходности пословања, а ради прибављања информација у вези са планирањем, спровођењем и надзором над активностима у области информационе безбедности обавили смо интервју са представницима Националног CERT-а, спровели самопроцену Националног CERT-а и посебних CERT-ова. (детаљније погледати у Прилогу 2.) и интервјуе са представницима: Министарства трговине, туризма и телекомуникација.

На основу прикупљених информација у фази планирања дефинисали смо потенцијални проблем, циљ ревизије, ревизорска питања, критеријуме, предмет ревизије, субјекте ревизије као и период који ће ревизија обухватити.

Током фазе спровођења ревизије, како бисмо одговорили на ревизорска питања односно испунили циљ ревизије, анализирали смо прикупљену документацију од субјекта ревизије као и од извора информација, спроводили интервјуе, слали упитнике и друго. Детаљнији опис коришћене методологије дат је у Прилогу 2.

III Опис предмета ревизије

1. Законодавни и институционални оквир

Закон о информационој безбедности у Републици Србији први пут је донет 2016. године у складу са тадашњим предлогом Директиве о мрежној и информационој безбедности ЕУ (енг: Network and Information Security Directive - NIS Directive, у даљем тексту: НИС директива). Појам информационе безбедности Закон дефинише као 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 и када је предвиђено и под контролом овлашћених лица.

Пријављивање инцидената који могу да имају значајан утицај на нарушавање информационе безбедности дефинисано је **Законом о информационој безбедности** и у складу са њим операторима ИКТ система од посебног је значаја[7] прописана обавеза пријављивања инцидената. Имајући у виду да је информациона безбедност саставни део свеукупне безбедности, и да је њено очување у функцији остваривања и поштовања права, слобода и интереса грађана, привреде и државе, сви друштвени чиниоци треба да буду свесни ризика повезаних са употребом технологије. Та свест се, између осталог, огледа и у ефикасној реакцији на инциденте, односно њиховом пријављивању надлежном органу. Дакле, ИКТ системи од посебног значаја су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга, може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно, може угрозити функционисање Републике Србије.

Министарство трговине, туризма и телекомуникација[8] (даље МТТТ) обавља послове државне управе у области информационог друштва који се односе на: предлагање политике и стратегије развоја информационог друштва; припрему закона, других прописа, стандарда и мера у области електронског пословања; мере за подстицање истраживања и развоја у области информационог друштва; припрему закона, других прописа, стандарда и мера у области информационог друштва и ИКТ; примену ИКТ; пружање информационих услуга; развој и функционисање информационо-комуникационе инфраструктуре; развој и унапређење академске, односно образовне и научноистраживачке рачунарске мреже; заштиту података и информациону безбедност; међународне послове у области информационог друштва; стварање услова за приступ и реализацију пројеката из делокруга тог Министарства који се финансирају из средстава предприступних фондова Европске уније, донација и других облика развојне помоћи, као и друге послове одређене законом. У претходном периоду дигитализација јавне управе у Републици Србији добила је значајно убрзање, док се информациона безбедност није развијала том брзином.

МТТТ пружа стручну и административно-техничку подршку Телу за координацију послова информационе безбедности, коме је задатак 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

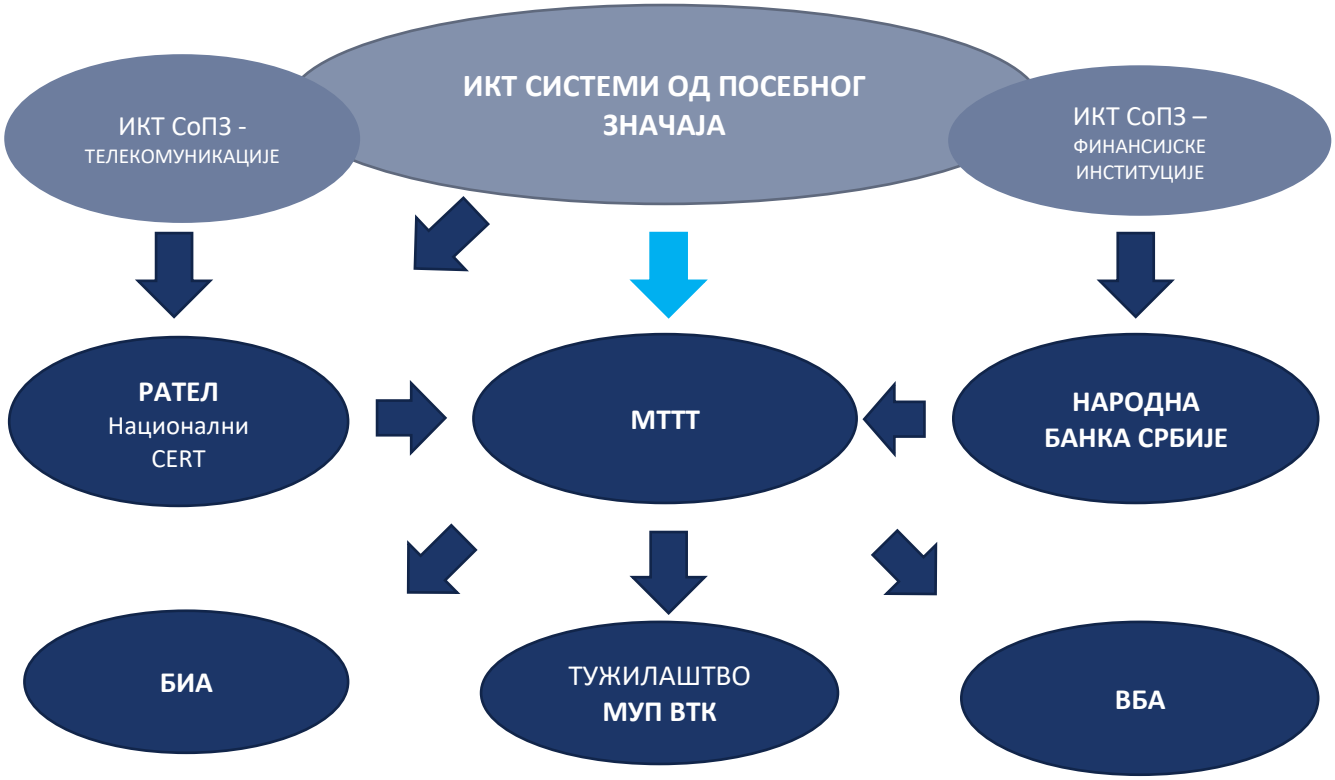
[7] Закон о информационој безбедности (Службени гласник РС, бр. 6/2016, 94/2017 и 77/2019) у члану 6. дефинише ИКТ системе од посебног значаја све системе који се користе за обављање послова од значаја за Републику Србију и њено функционисање.

[8] Министарство за трговину, туризам и телекомуникације, на основу члана 9 Закона о министарствима, „Службени гласник РС“, бр. 128/2020.

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 значајан утицај на нарушавање информационе безбедности у Републици Србији.

Изменама и допунама Закона из 2019. године, уведена је обавеза МТТТ-а да успоставља и води евиденцију ИКТ система од посебног значаја и ставља је на располагање Националном CERT-у. Ова евиденција би требало да садржи основне идентификационе податке ИКТ система од посебног значаја. Постојећи оператор ИКТ система од посебног значаја има обавезу да се упише у евиденцију у року од 90 дана од дана усвајања Правилника о упису у регистар који доноси МТТТ, односно у року од 90 дана од успостављања новог ИКТ система од посебног значаја. Закон је, између осталог, регулисао оснивање Националног центра за превенцију безбедносних ризика (Национални CERT) као тела задуженог за координацију превенције и заштите од безбедносних ризика у ИКТ системима на националном нивоу, а у великој мери се позабавио регулисањем тзв. ИКТ система од посебног значаја и њиховим мерама заштите.

Информациона безбедност је аспект безбедности који се односи на безбедносне ризике повезане са употребом ИКТ, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.[9] Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[10] дефинисано је 28 мера заштите.



Слика број 1. Законски оквир за размену информација о инцидентима

9 Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, „Службени гласник РС“, бр. 53/2017.

10 Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, „Службени гласник РС“, број 94 од 24. новембра 2016.

Законом о информационој безбедности[11] је инцидент дефинисан као сваки догађај који има стваран негативан утицај на безбедност мрежних и информационих система.

2. Управљање инцидентима у ИКТ системима

Утицајем пандемије вируса 2020–2021. године на дигитализацију услуга које се у све већем броју пружају електронским путем, јавља се и све већа потреба за подизањем нивоа информационе безбедности. Појам информационе безбедности у нашој легислативи примарно је био усмерен на информациону безбедност ИКТ СоПЗ у складу са Законом о информационој безбедности, затим је постао важан сегмент како за грађане тако и за привреду, а свест о њеној важности се све више повећава. Међутим, ризици информационе безбедности постоје како на страни државе односно ИКТ система од посебног значаја, тако и на страни грађана и привреде који су први на удару високотехнолошког криминала.

Пријављивање инцидената који могу да имају значајан утицај на нарушавање информационе безбедности дефинисано је Законом о информационој безбедности и у складу са њим је операторима ИКТ система од посебног значаја прописана обавеза пријављивања инцидената. Имајући у виду то да је информациона безбедност саставни део свеукупне безбедности, и да је њено очување у функцији остваривања и поштовања права, слобода и интереса грађана, привреде и државе, сви друштвени чиниоци треба да буду свесни ризика повезаних са употребом технологије. Та свест се, између осталог, огледа и у ефикасној реакцији на инциденте, односно њиховом пријављивању надлежном органу. Дакле, ИКТ системи од посебног значаја су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно, може угрозити функционисање Републике Србије. У ту сврху намењена је званична презентација на домену **https://www.cert.rs**.

Доношењем Закона наметнута је јасна обавеза приватним и јавним субјектима да примене одговарајуће мере заштите информационих система, што се нарочито односи на ИКТ системе од посебног значаја као системе који се користе за послове државних органа, обраду посебних врста података о личности и обављање делатности од општег интереса, попут електронских комуникација.

Обавеза сваког оператора да о инцидентима у ИКТ систему обавештава надлежни орган и то је уређено Уредбом[12] којом су дефинисани сви неопходни елементи инцидената, који се достављају електронским путем. Сложеност материје и важност одређивања ових елемената као и само пријављивање инцидента поверено је особи коју одговорно лице именује.

Министарство у чијој је надлежности Закон о информационој безбедности предузело је низ активности на унапређењу прописа континуираним унапређењима побољшало систем информационе безбедности успостављањем евиденције оператора, начином обавештавања о инцидентима, као и навођењем обавеза оператора ИКТ СоПЗ које су дужни спроводити.

Сврха управљања инцидентима је да се услуге које се пружају корисницима, врате у нормалан рад што је брже могуће, након нежењеног догађаја – инцидента, и тако умање негативни утицај догађаја на пружање услуга, што је и главни циљ постојања услужне организације.

---

[11] Члан 2 Закона о информационој безбедности.

[12] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Сл. гласник РС“, бр. 11/2020) и претходна Уредба о поступку достављања података, листи, врстама и значају инцидената и поступку обавештавања о инцидентима у ИКТ системима од посебног значаја („Сл. Гласник РС“ бр. 94/2016).

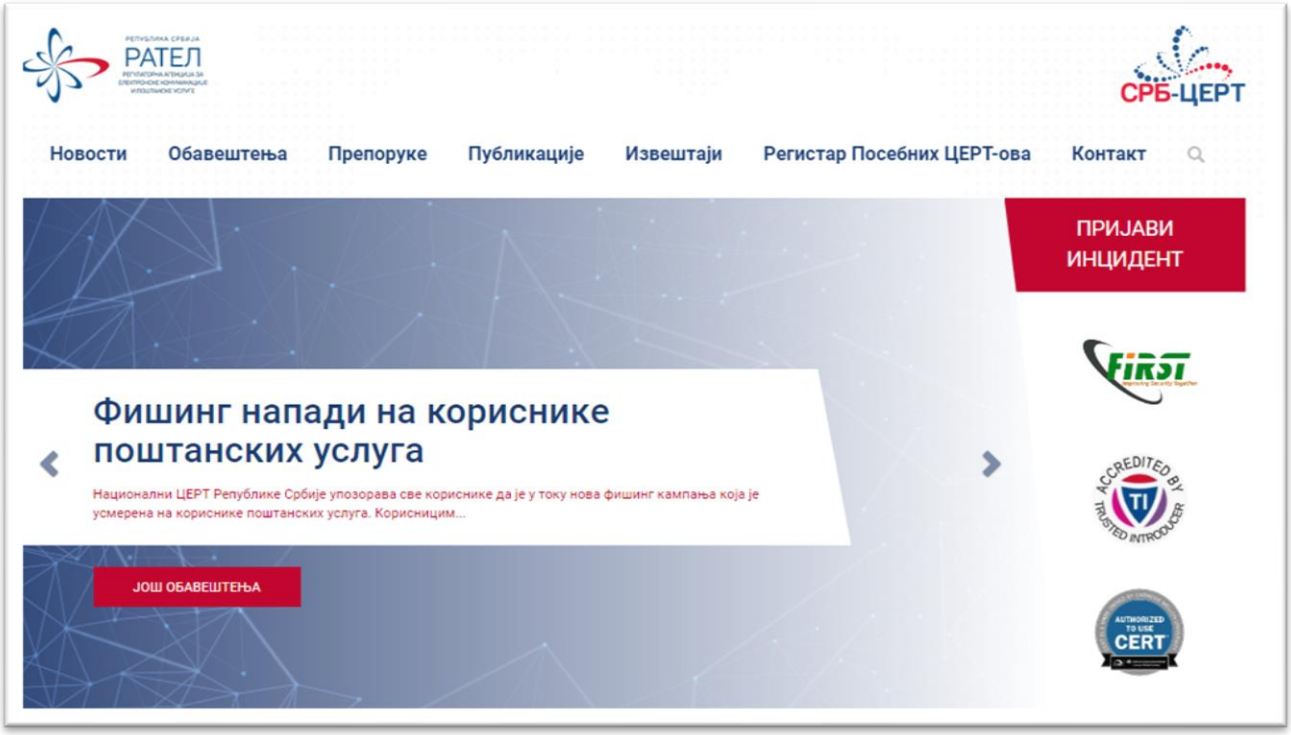
Велики или критични инцидент може се дефинисати као поремећај услуге или смањење квалитета услуге такве величине да омета способност организације да испуни своје обавезе у погледу услуга за значајан број корисника – грађана. Велики или критични инцидент захтева хитан одговор да би се функционалност вратила у предвиђено стање. На инциденте није имуна ниједна организација, а догађаји могу довести до губитка или прекида рада, услуга или функција и резултирати неуспехом услужне организације да испуни своје обавезе у погледу услуга.

Догађаји могу настати као резултат стварног или покушаја неовлашћеног приступа да се наруши или потенцијално наруши доступност, интегритет или поверљивост информација или система, неовлашћено откривање, крађа, корупција или уништавање информација или оштећење система.

Догађаји могу укључивати све, од кршења безбедности до напада ускраћивањем услуге.

Управљање инцидентима укључује оне активности које идентификују, документују, анализирају и адресирају догађаје и спречавају да се будући догађаји понове.

У циљу остваривања стратешког циља Владе Републике Србије развоја и унапређења информационе безбедности у Републици Србији, Национални CERT врши превенцију и заштиту од ризика путем размене информација, праћења актуелних ризика и подизања свести грађана, привредних субјеката и органа власти о значају информационе безбедности.



Слика број 2. Званична интернет презентација – Национални CERT

IV Закључци

На основу спроведене ревизије закључили смо:

Услед недостатка адекватне размене информација о инцидентима слаби укупна информациона безбедност критичне инфраструктуре, посебно ИКТ система од посебног значаја, онемогућавајући јачање укупне сајбер безбедности што излаже информациону имовину ризику од оштећења и могућег трајног губитка.

Закључак је донет на основу налаза и донетих закључака о појединачним питањима, и то:

1. Јачање сајбер отпорности и укупне информационе безбедности КИИ није могуће без утврђивања листе приоритета ИКТ СоПЗ, јачања свести о значају информационе безбедности у свим њеним аспектима и веће видљивости у јавном и интернет простору;
2. Процес управљања инцидентима ИКТ СоПЗ не препознаје организациону сложеност, величину и критичност оператора за ефикасну имплементацију мера заштите, технолошка решења која користе оператори и потребу непосредног објављивања информација о инцидентима који су у току, што умањује постојеће позитивне ефекте на оснаживању сајбер отпорности;
3. Постојећи контролни и инспекцијски механизам не обезбеђује адекватну надзорну функцију Министарства, стварајући ризик да инциденти ескалирају и угрозе информациону имовину критичне инфраструктуре.

ЗАКЉУЧАК 1: Јачање сајбер отпорности и укупне информационе безбедности КИИ није могуће без утврђивања листе приоритета ИКТ СоПЗ, јачања свести о значају информационе безбедности у свим њеним аспектима и веће видљивости у јавном и интернет простору.

Наш циљ у овом делу извештаја, био је да одговоримо на прво ревизијско питање, односно да ли се адекватно планирају активности на обезбеђивању управљања инцидентима у ИКТ системима од посебног значаја.

Закључак представља сублимиране одговоре на следећа питања:

1. Да ли су успостављене листе приоритета приликом ангажовања постојећих CERT тимова у случају појаве више инцидената истовремено?
2. Да ли постоји програм стручног усавршавања запослених у операторима ИКТ СоПЗ, као и друге активности јачања свести о информационој безбедности?
3. Да ли је обезбеђен јединствени систем за пријављивање инцидената, доступан свим CERT-овима ОДУ, Операторима ИКТ СоПЗ и корисницима електронских услуга државне управе?

На основу утврђених налаза чији критеријуми су прописани Законом о информационој безбедности, подзаконским и другим актима, као и доброј пракси у области информационе безбедности. Период обухваћен ревизијом планиран је „Стратегијом развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године“, која је уредно допуњавана. На њу се надовезала и „Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године“, чији је саставни део Акциони план за постизање циљева, чија се реализација оцењује једном годишње.

Налаз 1.1: Без утврђивања листе приоритета ИКТ СоПЗ према степену критичности, није било могуће планирати ангажовање постојећих CERT тимова за умањење последица инцидената као и успоставити ефикасан ток опоравака критичне информационе инфраструктуре.

Законом о информационој безбедности[13] и Законом о критичној инфраструктури[14] дефинисани су сектори и одређени су системи, мреже, објекти или њихови делови, чији прекид функционисања или прекид испоруке роба, односно услуга може имати озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно, може угрозити функционисање Републике Србије.

Уредбом о критеријумима за идентификацију критичне инфраструктуре и начину извештавања о критичној инфраструктури Републике Србије[15] дефинисани су критеријуми ИКТ сектора. Како је МТТТ задужено за идентификацију и одређивање критичне инфраструктуре у ИКТ сектору уједно има и задатак да донесе листу приоритета ИКТ система од посебног значаја и тако олакша операторима доношење Безбедносног плана[16] за управљање ризиком.

Закон о информационој безбедности је одредио операторе ИКТ система од посебног значаја, али није извршена приоритизација према степену критичности. Закон о информационој безбедности и подзаконски акти који се доносе на основу тог закона треба да приоритизују ИКТ системе од посебног значаја по степенима критичности у циљу обезбеђења ефикасног тока опоравка ИКТ система.

У току спровођења ревизије донета Уредба је дефинисала критеријуме за идентификацију критичне инфраструктуре као и начин извештавања. Под критичном инфраструктуром у

[13] „Сл. Гласник РС“, 6/2016-50, 94/2017-9, 77/2019-16.
[14] „Сл. Гласник РС“, 87/2018-41.
[15] „Сл. Гласник РС“, 69/2022 од 24. јуна 2022.
[16] „Сл. Гласник РС“, 87/2018-41.

сектору телекомуникационе и информационе технологије подразумевају се системи, мреже, објекти или њихови делови чији прекид рада проузрокује:

1) прекид пружања услуга оператора електронских комуникација са учешћем од најмање 10% корисника на одговарајућем тржишту на територији Републике Србије;
2) прекид пружања услуга оператора који управља емисионом инфраструктуром на територији Републике Србије;
3) прекид пружања сервиса електронске управе за грађане, привреду и институције Републике Србије у смислу критичне инфраструктуре која подразумева информационе системе у целини – од физичког нивоа Дата центара где су смештени системи, преко комуникационе и серверске инфраструктуре, до апликативног нивоа;
4) прекид обављања послова изградње, развоја, унапређења и управљања образовном и научноистраживачком рачунарском мрежом Републике Србије;
5) прекид пружања услуге размене интернет саобраћаја (енгл. „internet exchange point“);
6) прекид обављања послова управљања регистром националног интернет домена и системом за именовање на мрежи (ДНС системи).

Процена критичности елемената инфраструктуре је важан задатак у обезбеђивању заштите КИИ државе и битно се разликује од процене ризика. Приликом процене критичности треба узети у обзир могућност да елемент КИИ буде неисправан, оштећен, уништен или на други начин избачен из функције и питање – какав негативан утицај може имати на живот и здравље грађана, економију, националну безбедност итд. Главни критеријуми могу бити:

- утицај на друштво – број корисника;
- економски ефекат – вредност, губици буџета на различитим нивоима, економски губици КИИ;
- утицај на окружење – број повезаних система;
- политички утицај – поверење јавности у државне институције, утицај на међународне односе државе;
- утицај на националну безбедност и одбрану;
- утицај на функцију других елемената КИИ.

Процена такође узима у обзир и размере негативног утицаја, интезитет, време трајања негативног утицаја, као и време за враћање и опоравак КИИ.

Као добра пракса[17] у циљу обезбеђивања ефикасног управљања КИИ, треба извршити категоризацију КИИ по степену критичности:

- **Критични системи** – ИКТ системи на нивоу државне управе;
- **Витални системи** – ИКТ системи на нивоу покрајинских управа;
- **Важни системи** – ИКТ системи на нивоу локалних самоуправа;
- **Потребни системи** – ИКТ системи за чију заштиту брину оператори који мора да реагују у кризним ситуацијама.

У циљу заштите критичне инфраструктуре, оператори критичне инфраструктуре дужни су да израде Безбедносни план оператора за управљање ризиком и на исти прибаве сагласност Министарства одмах, а најкасније шест месеци по одређивању система, мрежа, објеката или њихових делова за критичну инфраструктуру. Са друге стране, CERT тимови су ограниченог броја и у случају истовременог напада на више оператора критичне информационе инфраструктуре, ради ефикасне заштите и опоравка, неопходно је одредити приоритете и редослед поступања.

[17] NIST (2018). NISTIR 8179 Criticality Analysis Process Model Prioritizing Systems and Components, **https://csrc.nist.gov/publications/detail/nistir/8179/final**.

Безбедносни план оператора за управљање ризиком јесте документ којим се утврђују мере смањења ризика, дефинишу одговорности и одређују дужности, те се успоставља оквир за поступање у циљу отклањања, односно смањења последица безбедносних претњи дефинисаних у анализи ризика, која је саставни део плана. Методологију, начин израде и садржај Безбедносног плана оператора за управљање ризиком прописује Министар надлежан за унутрашње послове[18].
Безбедносни планови треба да обухвате све активности оператора и CERT тимова у складу са Методологијом, омогућавајући располагање са ограниченим ресурсима којима није могуће пружити заштиту и опоравак свих ИКТ система од посебног значаја са којима располажу сви оператори истовремено.

Неадекватно планирање и употреба постојећих ресурса, неблаговремено реаговање у случају инцидената који су високог и веома високог нивоа опасности, могу довести до угрожавања критичне информационе инфраструктуре и наведених последица по националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно могу угрозити функционисање Републике Србије.

Препорука: Препоручујемо одговорним лицима да успоставе листу приоритета ИКТ система од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре.

Налаз 1.2: Јачање свести о значају информационе безбедности без планирања које се заснива на стварним потребама за обукама, стручним усавршавањем, редовним информисањем, као и другим активностима, намењеним крајњим корисницима, запосленима на ИТ пословима и операторима које управљају КИИ, слаби отпорност целокупног друштва на будуће инциденте.

Општи циљ Стратегије[19] је развој и унапређење информационе безбедности у Републици Србији и њено одржавање на адекватном нивоу, а с обзиром на то да су доношењем прописа у овој области дефинисани ИКТ системи од посебног значаја, мере заштите, надлежни органи, изазов за остварење циља налази се у стварању предуслова за континуирано унапређење кадрова, како кроз увођење посебних програма на универзитетима из области информационе безбедности, тако и кроз континуирано обучавање и усавршавање запослених у релевантним институцијама који се баве информационом безбедношћу.

У Стратегији[20] за период од 2021. до 2026. године чији је циљ развијено информационо друштво и електронска управа у служби грађана и привреде и унапређена информациона безбедност грађана, јавне управе и привреде, дефинисан је посебни циљ 3 – Унапређење информационе безбедности грађана, јавне управе и привреде.

Акционим планом за реализацију Стратегије дефинисане су мере за праћење резултата на спровођењу стратешког плана, и у првој мери за постизање посебног циља 3, Подизање свести

[18] Министарство унутрашњих послова је донело „Упутство о Методологији израде и садржају процене ризика од катастрофа и плана заштите и спасавања“, „Службени гласник РС“, број 80 од 8. новембра 2019. године које тематски кореспондира са предметном методологијом о начину израде и садржају Безбедносног плана оператора за управљање ризиком критичне инфраструктуре.

[19] Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, „Службени гласник РС“, бр. 53/2017.

[20] Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године , „Службени гласник РС“, број 86 од 3. септембра 2021.

и знања у области информационе безбедности грађана, јавних службеника и привреде, дате су и циљане вредности на крају стратешког периода.

Министарство прати реализацију Акционог плана и већ крајем 2021. године превазишло је планиране вредности за број обучених запослених у области информационе безбедности.

Да би се планирао адекватан број и обим активности, неопходно је проценити стварне потребе за стручним усавршавањем. Зато је Директор Националне академије за јавну управу донео Упутство[21] којим се уређује методологија за утврђивање потреба за стручним усавршавањем, односно извори и врсте информација, начин прикупљања и обраде података, појединачне врсте метода и техника чијом применом се обезбеђује прикупљање и анализа прикупљених информација о потребама за стручним усавршавањем запослених у органима јавне управе, извештај о анализи потреба за стручним усавршавањем, као и друга питања од значаја за утврђивање потреба за стручним усавршавањем.

За прикупљање и анализу информација о потребама за стручним усавршавањем, изворно, користе се евиденције о запосленима. Министарство не води евиденцију запослених на пословима ИБ у органима државне управе и/или код оператора ИКТ система од посебног значаја. У евиденцији постоје подаци за контакт са администраторима ИКТ система од посебног значаја (телефони, мејлови), чији је део посла и информациона безбедност, али свакако то нису сви запослени на пословима информационе безбедности међу операторима ИКТ система од посебног значаја.

Ограниченим ресурсима није могуће постићи адекватан ниво стручног усавршавања крајњих корисника, запослених на ИТ пословима у државним органима и организацијама које управљају критичном информационом инфраструктуром.

Неадекватно планирање и употреба постојећих ресурса, доводе до неблаговременог реаговања у случају инцидената који су високог и веома високог нивоа опасности и могу довести до угрожавања критичне информационе инфраструктуре.

Препорука: Препоручујемо одговорним лицима да у сарадњи са другим надлежним организацијама утврде стварне потребе за обукама, стручним усавршавањем, редовним обавештавањем, као и за другим активностима намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом инфраструктуром у циљу јачања свести о значају информационе безбедности и превентивним мерама заштите.

Налаз 1.3: Недовољна видљивост важности CERT-ова у јавности и различити садржаји на интернет локацијама CERT-ова за пријављивање инцидената стварају конфузију код лица који пријављују инцидент и доводе до неадекватног и неблаговременог реаговања учесника у систему заштите критичне информационе имовине.

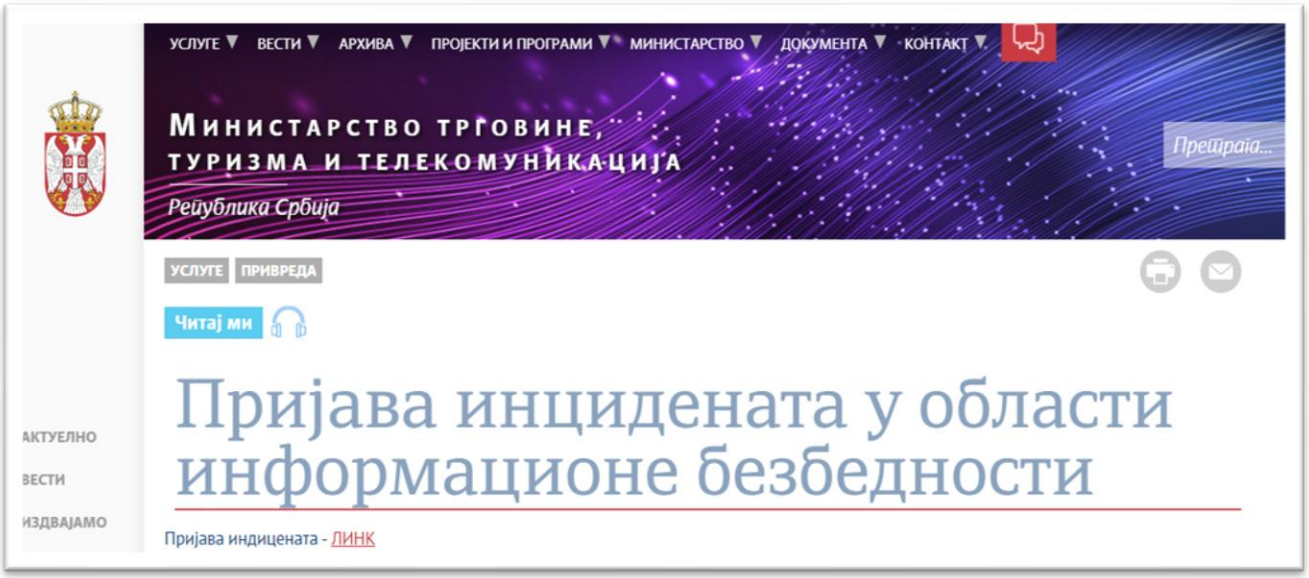
У Стратегији[22] за период од 2021. до 2026. године чији је циљ развијено информационо друштво и електронска управа у служби грађана и привреде и унапређена информациона безбедност грађана, јавне управе и привреде, дефинисан је посебни циљ 1 „Унапређење дигиталних знања и вештина грађана, подизање капацитета запослених у јавном и приватном сектору за коришћење нових технологија и унапређење дигиталне инфраструктуре у образовним установама“.

[21] Упутство о методологији за утврђивање потреба за стручним усавршавањем у органима јавне Управе, „Службени гласник РС“, број 32 од 3. маја 2019.

[22] Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године , „Службени гласник РС“, број 86 од 3. септембра 2021.

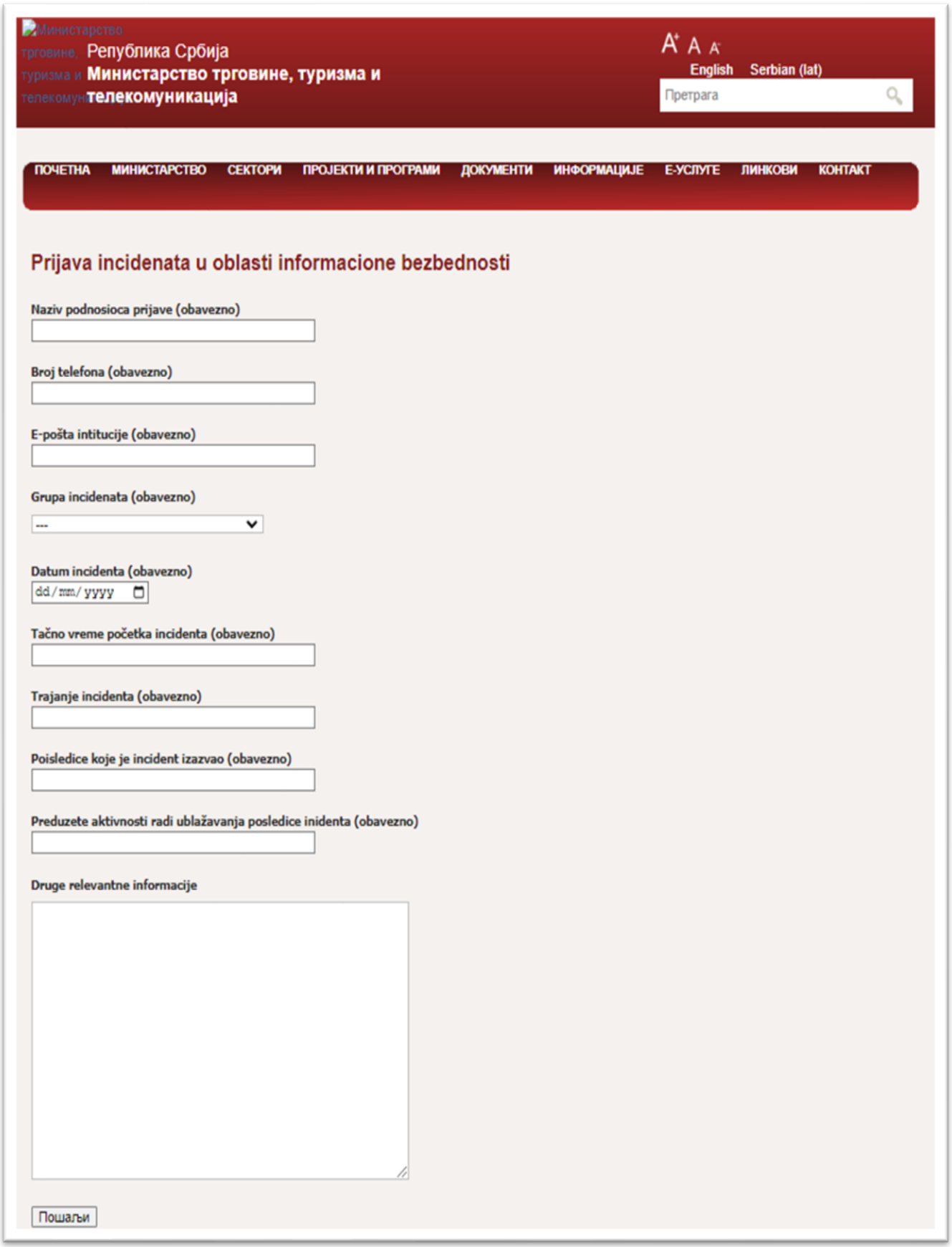
На подизању свести о ризицима коришћења интернета као изузетно добар начин показала се медијска кампања коју Министарство континуирано спроводи са јавним медијским сервисом која на занимљив и поучан начин тему безбедности представља деци, као и њиховим родитељима. Када је у питању промовисање теме информационе безбедности, налази из извештаја Светске банке говоре да „у Србији постоји ограничена медијска покривеност теме информационе безбедности и то само на ad hoc начин и да је питање информационе безбедности веома мало присутно у друштвеним медијима. Када су у питању јавни службеници свест о важности информационе безбедности варира у зависности од окружења с тим да је чињеница да се повећава ниво свести, делом захваљујући расту обуке за подизање свести које се организују за јавне службенике. Међутим, начин размишљања о информационој безбедности и даље остаје неуједначен у јавној управи."

У случају инцидента који значајно угрожава информациону безбедност, по пријави инцидента Национални CERT ступа у контакт са оператором ИКТ система од посебног значаја и даје му потребне смернице и препоруке. Уколико је инцидент у мрежи републичких органа, контактира се CERT републичких органа. Тужилаштву и МУП-у се пријављује инцидент ако је у питању кривично дело (најчешће га прво пријави сам оператор ИКТ система). Уколико је инцидент веома озбиљан у смислу да се може нанети тешка штета држави, грађанима и привреди и не може да се отклони редовним радом надлежних органа, сазива се Тело за координацију, а у прописима постоји могућност да се у најкритичнијим случајевима укључи Републички штаб за ванредне ситуације. Током инцидента све време одржава се контакт са оператором ИКТ система и прати ситуација. По завршетку инцидента МТТТ процењује да ли је потребно предузети друге кораке. Систем за пријем обавештења о инцидентима који одржава Министарство и коме приступ има и Национални CERT обухвата податке који се уносе преко две различите веб форме.

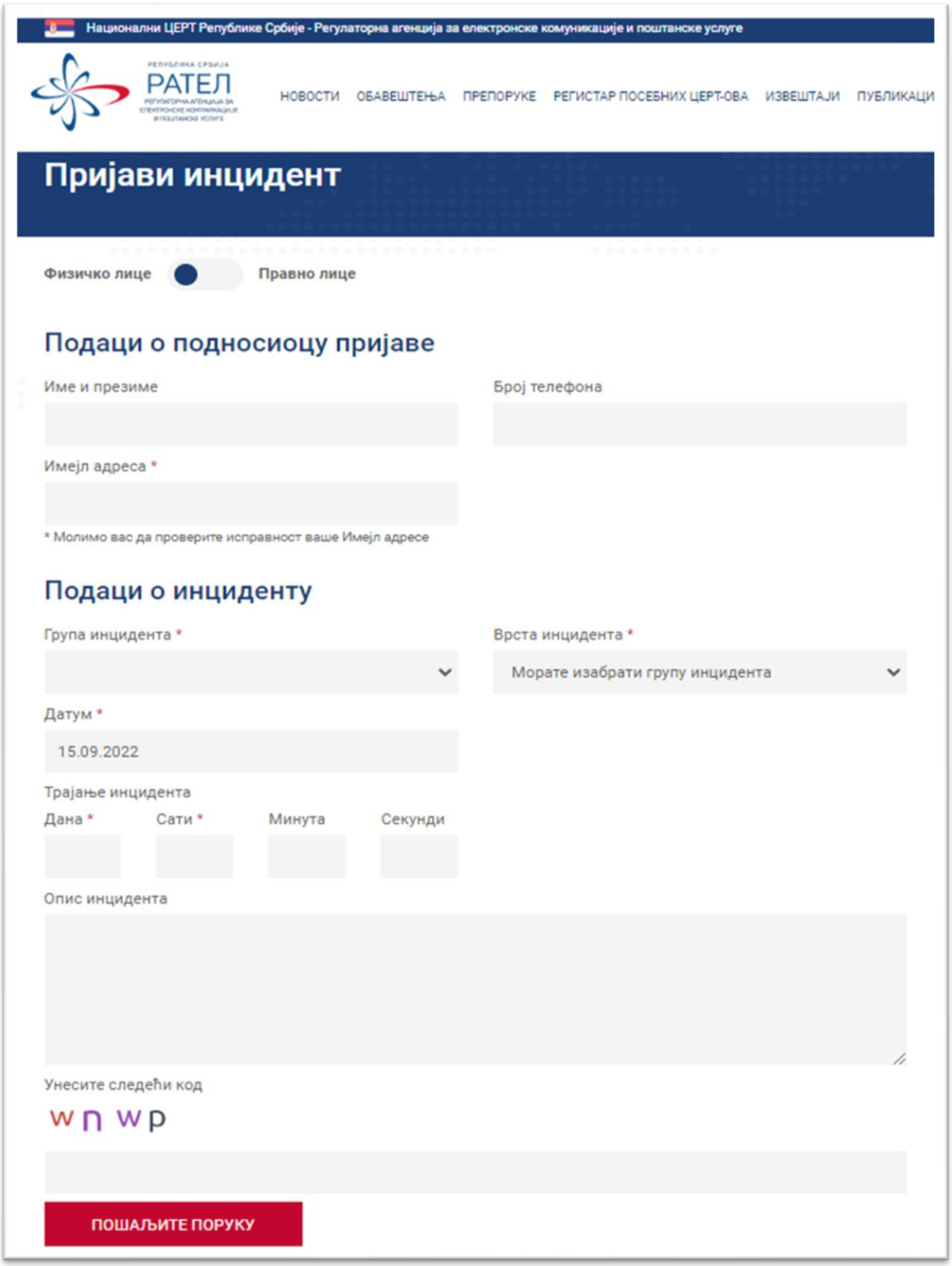


Слика број 3. Страница за пријављивање инцидента – Министарства

Веб форма за пријаве се налази на адреси **https://arhiva.mtt.gov.rs/prijava-incidenata-u-oib-2/** и иако је на локацији старог сајта, још увек је у употреби, линк на новом сајту https://mtt.gov.rs/tekst/31608/prijava-incidenata-u-oblasti-informacione-bezbednosti.php води ка линку старог сајта.



Слика број 4. Стара страница за пријављивање инцидента – Министарства



Слика број 5. Страница за пријављивање инцидента – Национални CERT

Инцидент се може пријавити и телефонским путем у случају хитности или ако није могуће другачије (нпр. оператор ИКТ система од посебног значаја привремено нема приступ интернету). У том случају службено лице уноси у систем податке дате у телефонском разговору. У систему се налазе подаци који се траже у веб форми (име и презиме подносиоца, контакт подаци, тип инцидента, датум инцидента, трајање инцидента, опис инцидента).

Јединствени систем је доступан само у интерној мрежи (интранет МТТТ) и осим у случају Националног CERT-а није му могуће приступити споља. Интеграција са засебним системом Националног CERT-а у који пристижу подаци пријављени директно Националном CERT-у и који се прослеђују у систем.

Пријаву инцидената је практично могуће извршити на две различите интернет локације, једна коју одржава МТТТ https://arhiva.mtt.gov.rs/prijava-incidenata-u-oib-2/ и другу на званичној страници Националног CERT-а https://www.cert.rs/. Пријављивање инцидента на више места може довести Оператора у конфузију и онемогућити ефикасно и благовремено реаговање надлежних органа, стварајући ризик од ескалације на друге ИКТ СоПЗ. Повећање броја ИКТ система који су жртва инцидента, умањује се могућност ефикасног дејства постојећих CERT тимова.

Препорука: Препоручујемо одговорним лицима да измене страницу на сајту МТТТ и преусмере кориснике на Национални CERT и апликацију за пријављивање на домену cert.rs, и пропишу ту обавезност за све CERT-ове за које су надлежни.

ЗАКЉУЧАК 2: Процес управљања инцидентима ИКТ СоПЗ не препознаје организациону сложеност, величину и критичност оператора за ефикасну имплементацију мера заштите, технолошка решења која користе оператори и потребу непосредног објављивања информација о инцидентима који су у току, што умањује постојеће позитивне ефекте на оснаживању сајбер отпорности.

Наш циљ у овом делу извештаја, био је да одговоримо на друго ревизијско питање, односно у којој мери управљање инцидентима у ИКТ системима од посебног значаја умањује ИТ ризике на критичну инфраструктуру.

Закључак представља сублимиране одговоре на следећа питања:

1. Да ли прописане мере за умањење ИТ ризика омогућавају ефикасну примену у свим операторима ИКТ СоПЗ без обзира на сложеност организације?
2. Да ли ЈСПОИ[23] врши обавештавање оператора ИКТ СоПЗ према врсти инцидента и врсти ИКТ система са којима располажу?
3. Да ли ЈСПОИ врши обавештавање јавности по евидентирању насталог инцидента, док је још информација важна за превентивно деловање јачања информационе отпорности ИКТ СоПЗ?

На основу утврђених налаза чији критеријуми су прописани Законом о информационој безбедности, подзаконским и другим актима, као и доброј пракси у области информационе безбедности. Период обухваћен ревизијом је планиран „Стратегијом развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године“, која је уредно допуњавана. На њу се надовезала и „Стратегија развоја информационог друштва и информационе безбедности у Републици Србији за период од 2021. до 2026. године“, чији је саставни део Акциони план за постизање циљева, чија се реализација оцењује једном годишње. У систему обавештавања и јављања о насталим инцидентима постоји претходни корак, а то је идентификација или детекција инцидента. Безбедносни инцидент у својој суштини показују да су системи и подаци у мрежи компромитовани или злоупотребљени. Један безбедносни инцидент може бити део већег циљаног напада као што је ускраћивање услуге (DDoS), рансомвер или нека друга врста како је наведено у табели **Error! Reference source not found.**. Безбедносни напади могу утицати не само на финансије ваше организације, већ и на њену репутацију. Због тога је кључно открити безбедносни инцидент чим се догоди, одмах ублажити претњу и обуздати или смањити утицај напада. Просечно време за откривање напада се креће од 95 до 800 дана што указује да нападачи имају довољно времена да остваре своје злонамерне циљеве.

Откривање безбедносних инцидената или кршења података представља изазов за организације из различитих разлога. Често укључује откривање правих догађаја од огромног броја лажних аларма. Иако вам општи превентивни системи као што су заштитни зидови и антивирусни софтвер дају упозорења о девијантном понашању, они не пружају ширу слику. За свако активирано упозорење, потребно је да истражите зашто је покренуто, што повећава време решавања ситуације. Општи превентивни системи дају ограничене податке. На пример, ако су акредитиви запосленог украдени и користе се за приступ критичним ресурсима, тешко је ово означити као девијантно понашање и означити као инцидент осим ако није доступно више контекстуалних информација. Решења за безбедносне информације и управљање догађајима (СИЕМ) повезују пословне контекстуалне информације са мрежном активношћу како би се открили инциденти у реалном времену.

[23] ЈСПОИ - Јединствени систем за пријем обавештења о инцидентима.

Налаз 2.1: Без извршене категоризације оператора ИКТ СоПЗ по величини и критичности, нису се могле дефинисати минималне/обавезне мере заштите према категоријама чиме се смањује ефикасност прописаних мера за умањење ИТ ризика.

Информациона безбедност је аспект опште безбедности који се односи на безбедносне ризике повезане са употребом ИКТ, укључујући безбедност података, уређаја, информационих система, мрежа, организација и појединаца.[24] Уредбом о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја[25] дефинисано је 28 мера заштите и то:

1. Успостављање организационе структуре (члан 2);
2. Безбедан рад на даљину и безбедна употреба мобилних уређаја (члан 3);
3. Едукација о начину функционисања и одговорности запослених који користе ИКТ систем (члан 4);
4. Заштита од ризика који настају при променама послова или кадровским променама (члан 5);
5. Идентификација и класификација информационих добара у оквиру ИКТ система (члан 6);
6. Класификовање података (члан 7);
7. Заштита носача података (члан 8);
8. Ограничење приступа подацима и средствима за обраду података (члан 9);
9. Одобравање овлашћеног приступа и спречавање неовлашћеног приступа ИКТ систему и услугама које ИКТ систем пружа (члан 10);
10. Утврђивање одговорности корисника за заштиту сопствених средстава за аутентикацију (члан 11);
11. Енкрипција (члан 12);
12. Физичка заштита објеката, простора, просторија односно зона у којима се налазе средства и документи ИКТ система и обрађују подаци у ИКТ систему (члан 13);
13. Заштита од губитка, оштећења, крађе или другог облика угрожавања безбедности средстава која чине ИКТ систем (члан 14);
14. Исправно и безбедно функционисање ИКТ система од посебног значаја (члан 15);
15. Заштита од злонамерног софтвера (члан 16);
16. Заштита од губитка података (члан 17);
17. Чување логова ИКТ система од посебног значаја (члан 18);
18. Обезбеђивање интегритета софтвера и оперативних система (члан 19);
19. Заштита од злоупотребе безбедносних слабости ИКТ система (члан 20);
20. Обезбеђивање да активности на ревизији ИКТ система имају што мањи утицај на функционисање система (члан 21);
21. Заштита података у комуникационим мрежама укључујући уређаје и водове (члан 22);
22. Безбедност података који се преносе унутар оператора ИКТ система, као и између оператора ИКТ система и лица ван оператора ИКТ система (члан 23);
23. Животни циклус ИКТ система од посебног значаја (члан 24);
24. Заштита података који се користе за потребе тестирања ИКТ система односно делова система (члан 25);
25. Заштита средстава оператора ИКТ система која су доступна пружаоцима услуга (члан 26);
26. Одржавање уговореног нивоа информационе безбедности и пружених услуга у складу са условима који су уговорени са пружаоцем услуга (члан 27);
27. Превенција и реаговање на безбедносне инцидентне претње (члан 28);
28. Континуитет обављања посла у ванредним околностима (члан 29).

---

[24] Стратегија развоја информационе безбедности у Републици Србији за период од 2017. до 2020. године, „Службени гласник РС“, бр. 53/2017.

[25] Уредба о ближем уређењу мера заштите информационо-комуникационих система од посебног значаја, „Службени гласник РС“, број 94 од 24. новембра 2016.

Мерама заштите ИКТ система се обезбеђује превенција од настанка инцидената, односно превенција и смањење штете од инцидената који угрожавају вршење надлежности и обављање делатности, а посебно у оквиру пружања услуга другим лицима. Остварење тог циља у јавној управи се започиње правним уређењем обавезних мера и основни су елемент Акта о информационој безбедности. Органи локалне самоуправе у већини нису донели Акт[26] и уредили мере заштите иако постоје модели као помоћне смернице. Свега трећина локалних самоуправа ангажује два и више запослених на ИТ пословима, петина нема запослених и те послове обављају привремено и повремено физичка лица и у мали број случајева те послове раде правна лица која се баве одржавањем мрежа или система.

Значајни ризици у тим организацијама се разликују, тако да у реакцији са главним проблемима и узроцима, као што су: недостатак свести код одговорних лица о значају информационе безбедности у заштити дигиталне имовине и њиховој одговорности; недостатак ИТ кадра; недостатак техничких и финансијских ресурса; застарела опрема, системи и мреже, неповољно утичу на ефикасност мера за умањење ризика.

Многе узроке не можемо решити у дужем временском периоду и добра искуства примене заштитних мера указују на сегментацију обавеза према сложености организација, тј. Њихову категоризацију и одређивање минималних стандардима за примену мера заштите према сложености органа јавне управе. Пример такве категоризације имамо у Закону о рачуноводству где је законодавац препознао 4. нивоа сложености привредних субјеката и прилагодио сложеност финансијског извештавања према сложености и величини привредних субјеката.

Или адекватнији пример добре праксе Националног центра за сајбер безбедност Велике Британије који је дефинисао 10. најважнијих корака (контрола) за постизање сајбер безбедности који су дати у наставку на слици испод. Ти кораци могу да буду пример добре праксе и сасвим добар оквир за одређивање минималних критичних контрола информационе безбедности за све, па и за оне по обиму најмање органе у Републици Србији.

Слика број 6. Кораци за постизање задовољавајућег нивоа сајбер безбедности

1. Управљање ризиком у вези ИКТ система;
2. Контрола приступа ИКТ систему;
3. Едукација запослених који користе ИКТ системе;
4. Безбедност података;
5. Управљање информационим добрима;
6. Чување логова активности корисника и мониторинг ИКТ система;
7. Пројектовање, изградња, одржавање и управљање ИКТ системом;
8. Управљање безбедносним инцидентима ИКТ система;
9. Управљање рањивостима и претњама током експлоатације ИКТ система;
10. Управљање услугама добављача ИКТ услуга и система;

Извор: Национални центар за сајбер безбедност Велике Британије

[26] Државна ревизорска институција, Извештај о ревизији сврсисходности пословања „Управљање информационим системом локалне пореске администрације“, 26. децембар 2021. године, **https://www.dri.rs/php/document/download/4354/1**

Препорука: Препоручујемо одговорним лицима да изврше категоризацију оператора ИКТ система по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора.

Налаз 2.2: Недовољно познавање технолошких решења која користе оператори онемогућило је благовремено обавештавање оператора са истим рањивостима и тиме је повећало могуће последице и утицај инцидената на ИТ ризике критичне информационе инфраструктуре.

У складу са чланом 6б Закона о информационој безбедности[27] и Правилником о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја („Службени гласник РС“ број 9/20), оператор ИКТ система од посебног значаја дужан је да се упише у Евиденцију.

Захтев за упис података у Евиденцију подноси се Министарству, електронским путем, на адресу **https://mtt.gov.rs/tekst/31598/upis-u-evidenciju-operatora-ikt-sistema-od-posebnog-znacaja.php** где се подаци достављају у форми електронског документа у оригиналу или у форми овереног дигитализованог акта, у складу са прописима којима се уређује електронски документ, на електронску адресу Министарства **evidencijaiktsistema@mtt.gov.rs**.

ИКТ СоПЗ су дефинисани чланом 6. Закона о информационој безбедности и то су системи који се користе: у обављању послова у органима власти; за обраду посебних врста података о личности, у смислу закона који уређује заштиту података о личности; у обављању делатности од општег интереса и другим делатностима, које су ближе дефинисане Уредбом о утврђивању Листе делатности у областима у којима се обављају делатности од општег интереса и у којима се користе информационо-комуникациони системи од посебног значаја („Службени гласник РС“, број 94/19); у правним лицима и установама које оснива Република Србија, аутономна покрајина или јединица локалне самоуправе за обављање делатности од општег интереса.

У Републици Србији не постоје обједињени подаци о технолошким решењима које користе оператори ИКТ СоПЗ и на тај начин недостају елементи о повезаним ризицима са другим операторима који потенцијално могу пријавити настали инцидент.

Јединствени систем за размену информација и обавештења о безбедносним инцидентима, претњама, рањивостима и мерама за ублажавање ризика у заштити информационе имовине као дела критичне инфраструктуре служи за координацију својих активности и реаговање на инциденте са одговарајућим партнерима. Најважнији аспект координације одговора на инциденте је дељење информација, где различите организације међусобно деле информације о претњама, нападима и рањивостима тако да знање сваке организације користи другој. Дељење информација о инцидентима је често обострано корисно јер исте претње и напади често утичу на више организација истовремено.[28]

Услед непостојања података о технолошким решењима изостаје и адекватна размена информација о инцидентима која је предвиђена између самосталних CERT-ова, Републичког CERT-а и других, где није успостављена обавезност обавештавања и свако процењује без јасних критеријума да ли треба да обавештава друге операторе ИКТ СоПЗ као и да ли да координира активности са партнерима или не.

[27] Закон о информационој безбедности („Сл. гласник РС“, бр. 6/2016, 94/2017 і 77/2019)

[28] NIST SP800-61 Rev.2 - Водич за управљање рачунарским безбедносним инцидентима – Глава 4, Дељење информација и координација **https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final**

Услед недостатка правовремених информација и изостанка појачане пажње оператори ИКТ СоПЗ може доћи до ескалације инцидента и оператори могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

Препорука: Препоручује се одговорним лицима да да у сарадњи са надлежним органима прикупе податке о технолошким решењима оператора ИКТ СоПЗ, обезбеде систем за аутоматизовано обавештавање између CERT-ова и партнера, обезбеде имплементацију и примену.

Налаз 2.3: Непостојање механизма непосредног објављивања аларма по пријави инцидента, док информација има значај за предузимање превентивних мера заштите у спречавању ескалирања претње по информациону имовину, повећало је рањивост система заштите критичне информационе инфраструктуре.

У складу са чланом 11 Закона о информационој безбедности[29] и Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја[30] оператори ИКТ СоПЗ су дужни да доставе Националном CERT-у статистичке податке о свим инцидентима у ИКТ систему у претходној години најкасније до 28. фебруара текуће године.

Национални CERT обједињене статистичке податке о свим инцидентима доставља Надлежном органу и објављује их на веб страници Националног CERT-а. Објављени извештаји о статистичким подацима о свим инцидентима у ИКТ СоПЗ за 2020. и 2021. годину налазе се на локацији **https://www.cert.rs/izvestaji.html**, а врсту, форму и начин достављања статистичких података утврђује Национални CERT.

ЈСПОИ је информациони систем у који се уносе подаци о инцидентима у ИКТ СоПЗ који могу да имају значајан утицај на нарушавање информационе безбедности који би требао да омогући обавештавање јавности док још информација важна за превентивно деловање и спречавање ескалације инцидента.

Оператори ИКТ СоПЗ треба да аутоматизују размену информација о инцидентима и успоставе ефикасну координацију јер је ефикаснија и економична, која се можда неће у потпуности аутоматизовати због безбедности информација и поверења. Али скраћивање времена реакције и превенције, умањује ризик од ескалације инцидената.

Оператори ИКТ СоПЗ достављају обавештења о инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности без одлагања, а најкасније наредног радног дана од дана сазнања о настанку инцидента, преко веб странице Министарства или Националног CERT-а у ЈСПОИ.

Обавештавање јавности на интернет презентацијама се заснива на процени сваког учесника у систему јављања и обавештавања о инцидентима (сви CERT-ови) да ли је инцидентима који могу да имају значајан утицај на нарушавање информационе безбедности.

Услед недостатка правовремених информација и изостанка појачане пажње оператори ИКТ СоПЗ могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

Препорука: Препоручујемо одговорним лицима да обезбеде механизам објављивања аларма по пријави инцидента, означавањем врсте инцидента, нивоа опасности, анонимизоване податке о технолошким решењима погођених ИКТ СоПЗ као и могућим плановима реаговања на исте.

[29] „ Службени гласник РС“, бр. 6/2016, 94/2017 і 77/2019.
[30] „Службени гласник РС“, бр 11/2020 од 7. фебруара 2020.

ЗАКЉУЧАК 3: Постојећи контролни и инспекцијски механизам не обезбеђује адекватну надзорну функцију Министарства, стварајући ризик да инциденти ескалирају и угрозе информациону имовину критичне инфраструктуре.

Циљ у овом делу извештаја, био је да одговоримо на треће ревизијско питање, односно ли је успостављен адекватан надзор и контрола управљања инцидентима у ИКТ системима од посебног значаја.

Закључак представља сублимиране одговоре на следећа питања:

1. Да ли је успостављена и да ли се води Евиденција оператора ИКТ СоПЗ?
2. Да ли садржај Евиденције може да обезбеди довољно података да се изврши адекватна процена ризика за избор надзираних субјеката и повећа ефикасност надзора?
3. Да ли обухват планираних инспекцијских надзора може да обезбеди адекватну заштиту ИКТ СоПЗ у Републици Србији?

Инспекцијски надзор над применом Закона о информационој безбедности ("Службени гласник РС ", бр. 6/16, 94/17 и 77/19), Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17) и других прописа којима се уређује делатност везана за информациону безбедност и електронско пословање, обавља инспектор за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности, сагласно овлашћењима утврђеним чл. 28. и 29. Закона о информационој безбедности и чл. 64. и 65. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању.

У Одсеку за информациону безбедност и електронско пословање запослен је један инспектор за инспекцијски надзор над применом прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационе безбедности.

Годишњи план инспекцијског надзора доноси инспекција, на основу прикупљених података и праћења и анализирања стања у области надзора из свог делокруга и процењеног ризика, и исти је спроведен кроз оперативне (шестомесечне, тромесечне и месечне) планове инспекцијског надзора.

Налаз 3.1: МТТТ је израдило страницу на званичној интернет презентацији намењену упису, а то је било недовољно да оператори изврше прописану обавезу и што је онемогућило потпуно успостављање Евиденције оператора ИКТ СоПЗ.

Као што је већ наведено у налазу 2.2 прописано је да се Оператори морају уписати у Евиденцију оператора ИКТ СоПЗ. Изменама ЗИБ 2019. године прецизније су одређени оператори ИКТ СоПЗ који су обавезни да се упишу у Евиденцију, али и даље не постоји процена колики број Оператора има обавезу да се евидентира. Број евидентираних оператора је 1234, иако је надлежно Министарство упућивало званичне дописе са обавештењем о обавези уписа. Дописи су од фебруара и јуна 2020. године чији ефекти су умањени ванредним стањем због епидемије корона вируса. Исто обавештење је послато и објављено на сајту у чијем је називу реч архива, додата након преласка на нови сајт, а што је могуће имало негативан ефекат на упис **https://arhiva.mtt.gov.rs/vesti/obavestenje-o-obavezi-upisa-u-evidenciju-operatora-informaciono-komunikacionih-sistema-od-posebnog-znacaja/**. Истовремено је обавештење изашло на сајту РАТЕЛ-а **https://www.ratel.rs/cyr/blog/pocheo-upis-u-evidentsiju-operatora-ikt-sistema-od-posebnog-znachaja** у садржају обавештења је линк ка празној страници без преусмеравања. При том се Захтев доставља у форми електронског документа у оригиналу или

у форми овереног дигитализованог акта, у складу са прописима којима се уређује електронски документ, на електронску адресу Министарства evidencijaiktsistema@mtt.gov.rs.

Уредбом о Листи делатности детаљније је прописано делатност из члана 6. тачка 3), док за тачке 1) и 2) није предвиђено прецизније прописивање.

Органи власти који потпадају под ЗИБ дефинисани чланом 2. тачка 15) су:

- Државни органи, орган аутономне покрајине, орган јединице локалне самоуправе, организација и друго правно или физичко лице коме је поверено вршење јавних овлашћења.
- Из јавног сектора под Операторе потпадају правна лица (јавна предузећа, акционарска друштва/доо у власништву државе, установе, агенције) али ако обављају неке од делатности из тачке 3) – енергетика, здравство, саобраћај и др.

Оператори који обрађују податке о личности, тачка 2), сматрају они који обрађују посебне врсте података о личности из члана 17. Закона о заштити података о личности:

- Расно или етничко порекло;
- Политичко мишљење;
- Верско, филозофско уверење, чланство у синдикату;
- Генетски подаци;
- Биометријски подаци;
- Подаци о здравственом стању, сексуалном животу или сексуалној оријентацији.

Током примене закона утврђена је потреба за изменом и допуном одређених норми, у циљу ефикаснијег спровођења закона у пракси. Сходно томе, Нацртом закона предвиђено је успостављање Евиденције оператора како би се унапредила повезаност свих релевантних актера у области информационе безбедности. Предлагач Закона је очекивао да ће Надлежни орган и Национални CERT имати могућност интензивније сарадње са свим операторима ИКТ СоПз, нарочито у случају када се дешава инцидент, у смислу пружања подршке, препорука и савета за заштиту.

Сврха успостављања Евиденције није у потпуности постигнута, што указује да није довољно прописати обавезу, казнене одредбе, мора се успоставити јасна и стварна сврха. Подаци за процену ризика, за обавештавање оператора са повезаним ризицима, за процену и класификацију критичности КИИ, и друго, а свим неевидентираним операторима ускратити услуге надлежног Министарства или свих Министарстава итд. Евидентирање је обавеза Оператора ИКТ СоПЗ и на такав начин Министарство не може никада знати када је евиденција комплетна.

Препорука: Препоручујемо одговорним лицима да коришћењем одговарајућих извора прибаве све неопходне податке како би могли да оцене ИТ ризике, пропишу нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите.

Налаз 3.2: Евиденција оператора ИКТ СоПЗ није обухватила податке о технолошким решењима који су неопходни за процену ИТ ризика, што онемогућава да се одреде значајни или критични оператори као надзирани субјекти у процесу инспекцијског надзора.

Као што је већ наведено у налазу 2.2 прописано је да се Оператори морају уписати у Евиденцију оператора ИКТ СоПЗ. У складу са чланом 6б Закона о информационој безбедности и Правилником о подацима које садржи евиденција оператора информационо-комуникационих система од посебног значаја („Службени гласник РС“ број 9/20), оператор ИКТ система од посебног значаја дужан је да се упише у Евиденцију.

Евиденција садржи следеће податке:

1) назив, матични број и седиште оператора ИКТ система од посебног значаја;
2) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон администратора ИКТ система од посебног значаја;
3) име и презиме, службена адреса за пријем електронске поште и службени контакт телефон одговорног лица ИКТ система од посебног значаја;
4) податак о врсти ИКТ система од посебног значаја, у складу са чланом 6. Закона о информационој безбедности;
5) веб страница оператора ИКТ система од посебног значаја;
6) број локација на којима се ИКТ систем од посебног значаја налази.

У Евиденцију се уписују све промене података које могу настати.

Образац 1

Министарство трговине, туризма и телекомуникација
Немањина 22-26
11 000 Београд

ЗАХТЕВ
ЗА УПИС ПОДАТАКА У ЕВИДЕНЦИЈУ ИКТ СИСТЕМА ОД ПОСЕБНОГ ЗНАЧАЈА

Подаци		**Оператор ИКТ система од посебног значаја**	
Назив			
Матични број			
Седиште	Улица и број		
	Место		
	Поштански број		
Веб страница			
Број локација			
Подаци		**Администратор ИКТ система од посебног значаја**	**Одговорно лице ИКТ система од посебног значаја**
Име и презиме			
Службена адреса за пријем електронске поште			
Службени контакт телефон			

Слика број 7. Образац Захтева за упис у Евиденцију

Евиденција оператора ИКТ СоПЗ није обухватила податке о технолошким решењима који су неопходни за процену степена критичности што је вези са ИТ ризицима целокупне КИИ како је наведено у налазу 1.1. што уједно представља основ за адекватну процену ИТ ризика за избор надзираних субјеката и повећање ефикасности надзора.

Да би одабрали адекватно проценили ризике, неопходно је идентификовати сва информациона добра[31] и одредити одговорност за њихову заштиту; што значи обухватити опрему, оперативне системе, софтвер и запослене у операторима ИКТ СоПЗ.

Поред података о називу, седишту, контакт подацима администратора и одговорног лица, област делатности оператора, Евиденција може да садржи и друге допунске податке о ИКТ систему од посебног значаја које прописује Надлежни орган.

Услед недостатка адекватних критеријума за процену ИТ ризика оператора ИКТ СоПЗ, сви надзирани оператори у инспекцијским плановима имају средњи ниво ризика. Критеријуми се могу заснивати на: броју грађана који користе информационе услуге тог ИКТ система, број других ИКТ система са којима се размењују подаци, број запослених, вредност опреме, вредност софтвера, вредност лиценци, трошкови одржавања, итд.

Кроз дефинисање критеријума за процену ризика и прибављање података допуном евиденције или на други погодан начин потребно је извршити класификацију надзираних субјеката према степену ризика и у складу са тим планирати надзор.

Избор оператора ИКТ СоПЗ чији прекид функционисања или прекид испоруке роба односно услуга може да има озбиљне последице на националну безбедност, здравље и животе људи, имовину, животну средину, безбедност грађана, економску стабилност, односно може угрозити функционисање Републике Србије.

Препорука: Препоручујемо одговорним лицима да се применом дефинисаних критеријума изврши адекватна процена ризика за избор надзираних субјеката.

Налаз 3.3: МТТТ обавља инспекцијски надзор са једним инспектором над операторима ИКТ СоПЗ, што је недовољно у односу на потенцијални број надзираних субјеката, због чега могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

Инспекцијски надзор над применом Закона о информационој безбедности ("Службени гласник РС", бр. 6/16, 94/17 и 77/19), Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању („Службени гласник РС”, број 94/17) и других прописа којима се уређује делатност везана за информациону безбедност и електронско пословање, обавља инспектор за примену прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности, сагласно овлашћењима утврђеним чл. 28. и 29. Закона о информационој безбедности и чл. 64. и 65. Закона о електронском документу, електронској идентификацији и услугама од поверења у електронском пословању.

У Одсеку за информациону безбедност и електронско пословање запослен је један инспектор за инспекцијски надзор над применом прописа у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационе безбедности.

Годишњи план инспекцијског надзора доноси инспекција, на основу прикупљених података и праћења и анализирања стања у области надзора из свог делокруга и процењеног ризика, и исти је спроведен кроз оперативне (шестомесечне, тромесечне и месечне) планове инспекцијског надзора.

[31] Информациона добра обухватају податке у датотекама и базама података, програмски кôд, конфигурацију хардверских компонената, техничку и корисничку документацију, записе о коришћењу хардверских компоненти, података из датотека и база података и спровођењу процедура ако се исти воде, унутрашње опште акте, процедуре и слично, по Закону о информационој безбедности.

У складу са датим овлашћењима, инспектор за примену закона у области електронског документа, електронске идентификације и услуга од поверења у електронском пословању и информационој безбедности ће приликом редовних, односно ванредних надзора, утврђивати:

1) да ли је донет Акт о безбедности;
2) да ли је Акт о безбедности донет у складу са постојећим прописима (члан 8. ЗИБ и Уредба о ближем садржају Акта о безбедности ИКТ система од посебног значаја, начину провере и садржају извештаја о провери безбедности ИКТ система од посебног значаја);
3) да ли су примењене мере заштите;
4) да ли је извршена годишња провера усклађености примењених мера заштите;
5) да ли је у складу са прописима сачињен извештај о годишњој провери ИКТ система од посебног значаја;
6) да ли је извршен упис у Евиденцију оператора ИКТ система од посебног значаја.

МТТТ обавља инспекцијски надзор са једним инспектором над операторима ИКТ система од посебног значаја, што је недовољно у односу на потенцијални број надзираних субјеката, а за последицу могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

МТТТ је у ревидираном периоду 2019-2021. обавило инспекцијски надзор над 40 оператора што је у односу на пријављени број од 1.234 и очекивани број недовољно.

Висока изложеност ИТ ризицима, чести испади ИКТ система, отежано пружање услуга грађанима, повећање неповерења у државне органе и могу претрпети финансијске, материјалне и друге последице по дигиталну имовину.

Хронични недостатак ИТ стручњака на инспекцијским пословима, на пословима информационе заштите у јавној управи, може се решавати овлашћивањем и ангажовањем правних и физичких лица тј. ИТ стручњака из области информационе безбедности.

Препорука: Препоручујемо одговорним лицима да успоставе систем колегијалног прегледа од стране овлашћених лица која су компетентна за утврђивање могућих рањивости код оператора ИКТ система од посебног значаја.

V Накнадни догађаји

У уводном делу извештаја, у оквиру Обухвата ревизије, навели смо да је субјект ревизије било Министарство трговине, туризма и телекомуникација, као и да је ревизијом био обухваћен период од 2019. до 2021. године, уз коришћење података из ранијег периода. Такође, у уводном делу извештаја, навели смо да су поступци ревизије изведени у периоду од јануара до октобра 2022. године, у циљу доношења налаза и закључака. У овом делу извештаја наводимо догађаје који су наступили у току спровођења ревизије, који немају утицаја на налазе и закључке до којих смо дошли спроводећи ревизију, али су од значаја за боље разумевање извештаја.

Даном ступања на снагу Закона о изменама и допунама Закона о министарствима[1], односно од 22. октобра 2022. године, Министарство трговине, туризма и телекомуникација наставља рад, у складу са делокругом утврђеним овим законом, као Министарство информисања и телекомуникација. Утврђени делокруг обухвата, између осталог, обављање послова државне управе који се односе на информационо друштво. Такође, ступањем на снагу Закона о изменама и допунама Закона о министарствима, Министарство информисања и телекомуникација преузима од Министарства трговине, туризма и телекомуникација права, обавезе, предмете, опрему, средства за рад и архиву за вршење својих надлежности у области информационог друштва, утврђених овим законом.

VI Захтев за доставу одазивног извештаја

Субјекти ревизије су, на основу члана 40. став 1. Закона о Државној ревизорској институцији, дужни да поднесу Државној ревизорској институцији писани извештај о отклањању откривених несврсисходности (одазивни извештај) у року од 90 дана почев од наредног дана од дана уручења овог извештаја.

Одазивни извештај мора да садржи:

1) навођење ревизије, на коју се он односи;

2) кратак опис несврсисходности у пословању, које су откривене ревизијом;

3) приказивање мера исправљања.

Мере исправљања су мере које субјект ревизије предузима да би отклонио несврсисходности у свом пословању или мере умањење ризика од појављивања одређене несврсисходности у свом будућем пословању за чије предузимање субјект ревизије мора поднети уз одазивни извештај одговарајуће доказе.

Субјекти ревизије су обавезни да у одазивном извештају искажу мере исправљања по основу откривених несврсисходности односно свих закључака и налаза датих у Извештају о ревизији сврсисходности пословања, као и да поступи по датим препорукама. За мере исправљања је дужан да уз одазивни извештај достави доказе према следећем:

1. За налазе, односно несврсисходности првог приоритета, односно које је могуће отклонити у року од 90 дана субјекти ревизије су у обавези да доставе доказе о отклањању несврсисходности односно предузимању мера исправљања;
2. За налазе, односно несврсисходности другог приоритета, односно које је могуће отклонити у року до годину дана субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице;
3. За налазе, односно несврсисходности трећег приоритета, односно које је могуће отклонити у року од једне до три године субјекти ревизије су у обавези да доставе акциони план у којем ће описати мере и активности које ће бити предузете ради отклањања несврсисходности или смањења ризика од појављивања несврсисходности у будућем пословању као и планирани период предузимања мера и одговорно лице.

На основу члана 40. став 2. Закона о Државној ревизорској институцији одазивни извештај је јавна исправа која је потписана и оверена печатом од стране одговорног лица субјекта ревизије.

Државна ревизорска институција ће оценити веродостојност одазивног извештаја, тј. провериће истинитости навода о мерама исправљања, предузетим од стране субјекта ревизије, подносиоца одазивног извештаја. У случају потребе извршиће се и оцена да ли су мере исправљања исказане у одазивном извештају задовољавајуће.

Сагласно члану 57. став 1. тачка 3) Закона о Државној ревизорској институцији, ако субјекат ревизије у чијем су пословању откривене несврсисходности, не подносе у прописаном року Институцији одазивни извештај, против одговорног лица субјекта ревизије поднеће се захтев за покретање прекршајног поступка.

Ако се оцени да одазивни извештај не указује да су откривене несврсисходности отклоњене на задовољавајући начин, сматра се да субјект ревизије крши обавезу доброг пословања. Ако се ради о незадовољавајућем отклањању значајне несврсисходности, сматра се да постоји тежи облик кршења обавезе доброг пословања. У овим случајевима Државна ревизорска институције је овлашћена да предузима мере сагласно члану 40. ст 7. до 13. Закона о Државној ревизорској институцији.

ПРИЛОЗИ

1. Прилог 1 – Студија случаја „Сајбер инцидент“

Шта се десило?

Нападач је компромитовао налог добављача услуге/извођача. Вероватно је да је нападач купио лозинку на Дарк вебу, након што је мобилни телефон извођача био заражен малвером, који је омогућио разоткривање креденцијала. Нападач је затим више пута покушао да се пријави у компромитовани систем. Сваки пут, корисник службеног мобилног телефона је добијао двофакторски захтев за одобрење пријаве, који је у почетку блокирао приступ. На крају, корисник службеног мобилног телефона случајно или је намерно (да спречи досађивање) прихватио једну ауторизацију, што је било довољно, да се нападач успешно пријави.

Одатле је нападач приступио неколико других налога запослених, што је на крају дало нападачу повећане дозволе за бројне софтверске алате. Нападач је затим послао поруку на Slack канал у целој компанији, што су многи видели, и реконфигурисао DNS да прикаже шему запосленима на неким интерним сајтовима.

Како је реаговао ИТ запослени за безбедност?

Наш ИТ запослени за безбедност који надгледа безбедност мреже, омогућио је нашим тимовима да брзо идентификују проблем и да одговоре. Наши главни приоритети су били:

- да осигурамо да нападач више нема приступ нашим системима;
- да осигурамо да кориснички подаци безбедни;
- да ИКТ услуге буду што пре доступне и
- да се истражи обим и утицај инцидента.

Кључне радње које смо предузели и предузимамо:

1. Идентификовали смо све налоге запослених који су били компромитовани или потенцијално компромитовани и блокирали њихов приступ ИКТ системима, и захтевали ресетовање лозинке;
2. Онемогућили смо многе интерне софтверске алате који су компромитовани или потенцијално могу бити;
3. Ротирали смо кључеве (ефикасно ресетујући приступ) за многе наше интерне ИКТ услуге;
4. Закључали смо нашу базу кодова, спречавајући било какве нове промене кода;
5. Када смо враћали приступ интерним софтверским алатима, захтевали смо од запослених да се поново аутентификују;
6. Пооштрили смо интерна правила за мултифакторску аутентификацију (МФА).

Додали смо додатно праћење нашег унутрашњег окружења како бисмо још боље пратили сваку даљу сумњиву активност.

Какав је био утицај?

Нападач је приступио неколико интерних ИКТ система, а наша истрага се фокусирала на утврђивање да ли је било штете. Истрага још није завршена.

Прво и најважније, нисмо видели да је нападач приступио производним (тј. јавним) ИКТ системима који покрећу наше апликације.

Прегледали смо све корисничке налоге, базе података које користимо за чување осетљивих корисничких информација, као што су бројеви кредитних картица, подаци о банковном рачуну корисника или историја путовања.

Прегледали смо нашу базу кодова и нисмо открили да је нападач направио било какве промене. Такође нисмо открили да је нападач приступио подацима о клијентима или корисницима које чувају наши добављачи у облаку. Чини се да је нападач преузео неке интерне поруке, као и да је приступио информацијама или их преузео са интерног алата који наш финансијски тим користи за управљање неким фактурама. Тренутно анализирамо та преузимања.

Нападач је могао да приступи нашој контролној апликацији за надзор где истраживачи безбедности пријављују грешке и рањивости. Међутим, сви извештаји о грешкама којима је нападач могао да приступи су отклоњени.

Током читавог периода, били смо у могућности да све наше јавне услуге одржавамо оперативним и неометаним радом. Пошто смо уклонили неке интерне алате, операције корисничке подршке су биле минимално погођене и сада су се вратиле у нормалу.

Ко је одговоран?

Верујемо да су овај нападач (или нападачи) повезани са хакерском групом која је све активнија током последњих годину дана. Ова група обично користи сличне технике за циљање технолошких компанија, а само у 2022. је пробила Мицрософт, Циско, Самсунг, Нвидиа и Окта, између осталих. Такође су током викенда објављени извештаји да је овај исти хаковао још једну фирму. У блиској смо координацији са Специјалним тужилаштвом за високо-технолошки криминал и Министарством правде по овом питању и наставићемо да подржавамо њихове напоре.

Шта даље?

У оквиру истраге радимо са неколико водећих компанија за дигиталну форензику. Такође ћемо искористити ову прилику да наставимо да јачамо наше политике, праксе и технологију како бисмо додатно заштитили ИКТ систем од будућих напада.

Слика број 8. Највећих 15 претњи у сајбер (интернет) простору

Извор: Европска агенција за сајбер безбедност, https://www.enisa.europa.eu/

2. Прилог 2 – Методологија у поступку рада

У ревизији су коришћене технике прикупљање података и докумената у електронском облику (папирна документа ће се дигитализовати), анализа прикупљених података, анализе тренда и учешћа, интервјуи са одговорним лицима и друге технике. У процесу планирања ревизије сврсисходности пословања, а ради прибављања информација, за планирање, спровођење и надзор над активностима у области информационе безбедности обавили смо интервју са представницима Националног CERT-а, спровели самопроцену Националног CERT-а и посебних CERT-ова. Уредбом о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја[32] дефинисане су групе инцидената које су оператори ИКТ система од посебног значаја дужни да пријављују надлежном CERT-у, као што се може видети у следећој табели.

Табела 1. Листа група и врста безбедносних инцидената

Група инцидената	Врста инцидента
Инсталирање злонамерног софтвера у оквиру ИКТ система (малвер, енгл. „malware")	Вирус
	Црв(енгл. „worm")
	Рансомвер(енгл. „ransomware")
	Тројанац
	Шпијунски софтвер(енгл. „spyware")
	Руткит(енгл. „rootkit")
Неовлашћено прикупљање података	Скенирање портова
	Пресретање података између рачунара и сервера(енгл. „sniffing")
	Социјални инжењеринг(лажно представљање и други облици)
	Компромитовање или цурење података(енгл. „data breaches")
Превара	Фишинг(енгл. „phishing")
	Неовлашћено коришћење ресурса(енгл. „cryptojacking" и други облици)
Покушаји упада у ИКТ систем	Покушај искоришћавања рањивости система
	Покушај откривања креденцијала(енгл. „brute force attack", „dictionary attack" и сл.)
Упад у ИКТ систем	Откривање или неовлашћено коришћење привилегованих налога(енгл. „privileged account compromise")
	Откривање или неовлашћено коришћење непривилегованих налога(енгл. „unprivileged account compromise")
	Неовлашћени приступ апликацији
	Мрежа заражених уређаја(енгл. „botnet")
Недоступност или ограничена доступност ИКТ система	Напад са циљем онемогућавања или ометања функционисања ИКТ система(енгл. „denial-of-service attack" – DoS)
	Дистрибуирани напад са циљем онемогућавања или ометања функционисања ИКТ система(енгл. „distributed denial-of-service attack" – DDoS)
	Саботажа
	Прекид у функционисању система или дела система(енгл. „outage")
Угрожавање безбедности података	Неовлашћен приступ подацима
	Неовлашћена измена или брисање података
	Криптографски напад
Оперативни инциденти	Отказивање хардверских компоненти
	Проблеми у раду са софтверским компонентама
Инциденти физичко-техничке безбедности	Крађа хардверских компоненти
	Пожар
	Поплава
Остали инциденти	Инциденти који не спадају у горе наведене категорије

Извор: Уредба о поступку обавештавања о инцидентима у ИКТ системима од посебног значаја

[32] Уредба о поступку обавештавања о инцидентима у информационо-комуникационим системима од посебног значаја („Службени гласник РС", број 11 од 7. фебруара 2020);

Сложеност материје и важност одређивања ових елемената као и само пријављивање инцидента поверено је особи коју одговорно лице именује. Национални CERT врши превенцију и заштиту од ризика путем размене информација, праћења актуелних ризика и подизања свести грађана, привредних субјеката и органа власти о значају информационе безбедности. Истом Уредбом су одређени и нивои опасности и које су то околности за сваки ниво како би оператори могли пријавити значај самог инцидента и они си приказани у следећој табели.

Табела 2. Ниво опасности безбедносних инцидената

Ниво опасности	Последице инцидента
Веома висок	У случају наступања околности угрожавања, ометања рада или онемогућавања рада ИКТ система од посебног значаја, а када су ризици, претње или настале последице инцидента по становништво, материјална добра или животну средину таквог обима и интензитета да њихов настанак или последице није могуће спречити или отклонити редовним деловањем надлежних органа и служби, због чега је за њихово ублажавање и отклањање неопходно употребити посебне мере, додатне снаге и средства уз појачан режим рада.
Висок	Када су ризици и претње или настале последице инцидента по становништво, материјална добра или животну средину таквог обима и интензитета да је њихов настанак или последице могуће спречити или отклонити редовним деловањем надлежних органа и служби.
Средњи	Када су ризици, претње или настале последице инцидента таквог обима и интензитета да могу бити отклоњена заједничким деловањем ИКТ система од посебног значаја у коме се инцидент десио и Националног CERT-а.
Низак	Када су ризици, претње или настале последице инцидента таквог обима и интензитета да могу бити отклоњене деловањем ИКТ система од посебног значаја.

Извор: Уредба о поступку обавештавања о инцидентима у ИКТ системима од посебног значаја

Надлежни орган који врши надзор над применом закона је Министарство надлежно за послове информационе безбедности, односно Министарство трговине, туризма и телекомуникација. МТТТ врши послове инспекције за информациону безбедност преко Инспекције за информациону безбедност, утврђује да ли су ИКТ системи испунили услове прописане Законом и налаже мере ИКТ системима. Додатно, МТТТ води веб страницу јединствени систем за пријем обавештења о инцидентима оператора ИКТ система од посебног значаја, надзире рад Националног CERT-а, остварује међународну сарадњу у области безбедности ИКТ система и предузима превентивне мере за безбедност и заштиту деце на интернету (едукација, информисање, давање савета и слично). За послове Националног CERT-а надлежна је Регулаторна агенција за електронске комуникације и поштанске услуге (РАТЕЛ). Овакво тело постоји у 102 земље света, односно у готово свим европским земљама. Надлежности националних CERT-ова се, у зависности од специфичности инфраструктуре, разликују од државе до државе, али то је увек експертска организација чија је главна надлежност координација и комуникација на националном и међународном нивоу, ради превенције и управљања ризицима у овој области. Национални CERT је надлежан да прати инциденте на националном нивоу, да пружа рана упозорења, узбуне и најаве и информише релевантна лица о ризицима и инциденти- ма, да реагује по пријављеним или на други начин откривеним инцидентима, тако што пружа савете на основу расположивих ин-формација лицима која су погођена инцидентом и предузима друге потребне мере из своје надлежности на основу добијених сазнања.

Ово тело такође прати пријављене инциденте на националном нивоу и на основу прикупљених података континуирано израђује анализе ризика и инцидената, подиже свест код грађана, привредних субјеката и органа јавне власти о значају информационе безбедности, води евиденцију Посебних CERT-ова, те извештава МТТТ као Надлежни орган на кварталном нивоу о предузетим активностима. Важно је разумети да Национални CERT најчешће неће бити у позицији да реагује и помогне ИКТ системима у кризним и хитним ситуацијама, с обзиром на то да су његове надлежности у овом моменту превасходно превентивног карактера. Измене и

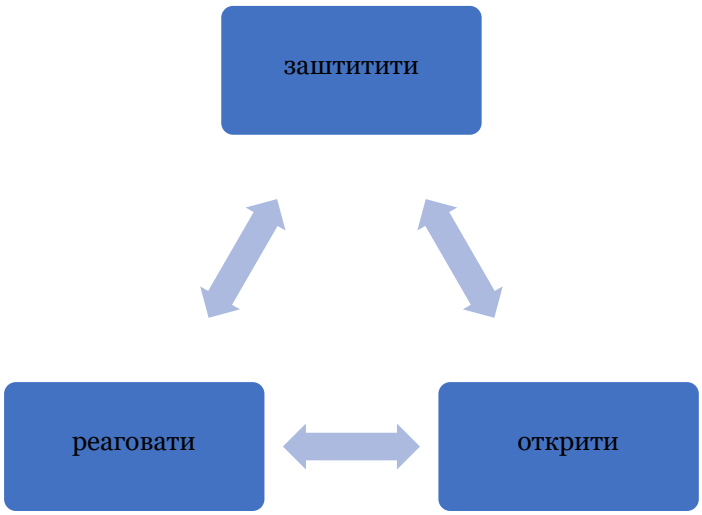
допуне Закона из 2019. годи- не уређују и обраду података о личности лица које се обрати Националном CERT-у, те набраја које конкретно личне податке Национални CERT може том приликом обрађивати, а сврха такве обраде је евидентирање поднетих пријава, информисање подносиоца о статусу предмета и евентуално упућивање пријаве надлежним органима ради даљег поступања. CERT органа власти (Центар за безбедност ИКТ система у органима власти) обавља пословне који се односе на заштиту од инцидената у ИКТ системима органа власти, осим ИКТ система самосталних оператора. Послове CERT-а органа власти обавља орган надлежан за пројектовање, развој, изградњу, одржавање и унапређење рачунарске мреже републичких органа, односно Канцеларија за информационе технологије и електронску управу. CERT органа власти је задужен за заштиту Јединствене информационо-комуникационе мреже електронске управе и координацију и сарадњу са операторима ИКТ система које повезује ова мрежа у циљу превенције инцидената, откривања и прикупљања информација о инцидентима и отклањању њихових последица, као и давање стручних препорука за заштиту ИКТ система органа власти, осим када су у питању ИКТ системи за рад са тајним подацима.

Слика број 9. Мапа сајбер безбедности у Републици Србији

Тако је обухват ревизије „Управљање инцидентима у ИКТ системима од посебног значаја“ представља границе ревизије и директно је везана за циљ ревизије. Обухват ревизије дефинисан је предметом који ће ревизор процењивати и о коме ће извештавати, документа или евиденције које ће се испитивати, период који се прегледа, и локације које ће се обухватити. Тим за

реаговање на рачунарске хитне случајеве (CERT) је група стручњака за безбедност информација одговорних за заштиту, откривање и реаговање на инциденте сајбер безбедности организације. CERT се може фокусирати на решавање инцидената као што су повреде података и напади ускраћивања услуге, као и на обезбеђивање упозорења и смерница за руковање инцидентима. CERT-ови такође спроводе текуће кампање подизања свести јавности и ангажују се у истраживању чији је циљ побољшање безбедносних система. Без обзира да ли се зову CERT, CSIRT, IRT или било који други сличан назив, улога свих компјутерских тимова за хитне случајеве је прилично упоредива. Све ове организације покушавају да остваре исте циљеве везане за реаговање на инциденте, односно реаговање на инциденте у вези са рачунарском безбедношћу како би повратили контролу и минимизирали штету, обезбеђујући или помажу у ефикасном реаговању на инциденте и опоравку и спречавајући да се инциденти у рачунарској безбедности поново понове. Генерално, тим за реаговање на инциденте одговоран је за заштиту организације од рачунарских, мрежних или проблема са сајбер-безбедношћу који угрожавају организацију и њене информације. Универзални модел за реаговање на инциденте који се већ дуго користи је модел „заштитити, открити и реаговати“ који је приказан у наставку.

Слика број 10. Модел заштитити, открити и реаговати



Концепт заштите се односи на то да се увери да је организација предузела неопходне мере и мере предострожности како би се осигурала пре него што се појаве проблеми са сајбер-безбедношћу. Ова област се фокусира на проактивне стратегије пре него на реактивне стратегије. Неке од тих стратегија заштите су:

1. Направите организациони план реаговања на инциденте.
2. Извршите процену или анализу ризика.
3. Креирајте ажурно управљање залихама имовине
4. Имплементирајте алате за скенирање рањивости и системе за откривање упада (ИДС).
5. Обезбедите обуку о свести о безбедности за све запослене.
6. Конфигурација градње, управљање рањивостима и закрпама
7. Развити безбедносне планове, политике, процедуре и материјале за обуку о реаговању на инциденте.
8. Детаљне смернице за кориснике о томе које безбедносне проблеме треба пријавити и скицирати процес за израду извештаја.
9. Направите приручнике о одговорима на инциденте за уобичајене типове инцидената.
10. Увести унутрашње и екстерне одбрамбене мере које се редовно ажурирају на основу тренутних претњи.

11. Поново процените ефикасност процедура сваки пут када дође до инцидента.

На инциденте се не може реаговати ако се не открију. У ствари, многе организације могу да потрају недељама или месецима за откривање безбедносних инцидената. Уобичајена стратегија детекције је имплементација одбрамбене мрежне архитектуре користећи технологију као што су рутери, заштитни зидови, системи за откривање и превенцију упада, мрежни монитори и безбедносни оперативни центри (енг. SOC – Security Operations Center). Ефикасно откривање захтева време и труд. Такође захтева висок ниво разумевања како мрежа организације заиста функционише. Уобичајена питања на која треба одговорити пре израде стратегије откривања укључују:

1. Које су апликације увек у употреби?
2. Како изгледа нормалан мрежни саобраћај?
3. Који се мрежни протоколи користе?
4. Који мрежни протоколи никада не би требало да се појављују на мрежи?
5. Који су нормални обрасци коришћења пропусног опсега, укључујући јачину и правац?
6. Који уређаји треба да буду повезани на мрежу?
7. Ко су власници система и података за ове прикључене хостове и уређаје?

Да би се утврдило да ли мрежа не ради исправно, да ли хостује нежељене апликације или има ненормалне обрасце саобраћаја, неопходно је бити у стању да у потпуности окарактеришете како би мрежа и системи повезани са њом требало да раде. Ако се не разуме правилан рад система, онда није могуће знати када тај систем не функционише како је предвиђено. Управљање системом захтева да сваки део мреже мора бити документован и базиран. Ово се може постићи са:

1. Програм за управљање софтверском имовином (CAM) који утврђује шта би требало да буде тамо и ко је власник, као и које апликације и пословне функције подржава свако средство. Поред тога, треба спроводити редовне провере у односу на основну вредност имовине.
2. Програм за управљање и безбедност апликација који укључује власнике апликација, овлашћене кориснике, карактеризацију преноса података и другог саобраћаја за који су апликације одговорне.
3. Промените, конфигуришите и програме за управљање закрпама да бисте знали да је мрежа постављена онако како би требало да буде.
4. Основна линија коришћења пропусног опсега и рутинска провера пропусног опсега у односу на основну линију.
5. Основне линије тока мреже и континуирано праћење ради хватања одступања од основне линије.

Са праксама заштите и откривања, важно је разумети да сви елементи ових модела процеса морају бити изграђени унапред пре него што се може десити било каква активност реаговања. Многе организације не успевају да планирају реаговање на инциденте или не примењују било коју стратегију заштите и откривања и стога не могу да знају да ли су њихове мреже и системи безбедни или не. Када се открије рачунарски безбедносни инцидент, може да почне формални одговор на инцидент. Реаговање на рачунарски безбедносни инцидент има неколико корака. Први корак је када тим добије извештај о инциденту од неког саставног дела, као што је корисник, пословни партнер или члан особља оперативног центра за безбедност. Чланови тима затим анализирају извештај о инциденту да би разумели шта се дешава и креирали тренутну стратегију за враћање контроле и спречавање даље штете. Коначно, стратегија се претвара у план који се затим спроводи за опоравак од инцидента и повратак нормалном раду што је пре могуће. Национални институт за стандарде и технологију (NIST) развио је сопствени модел реаговања на инциденте који је постао популаран међу онима који реагују на инциденте,

посебно у оквиру Федералне извршне власти САД. NIST модел користи изразе „садржати, искоренити и опоравити“ да опише свој модел одговора на инциденте и процес. Специјална публикација NIST-а за руковање инцидентима рачунарске безбедности, СП-800-61, детаљно описује овај модел одговора на инцидент. Анализирајући прибављене податке, стратегију и законодавни оквир у фази планирања смо обавили анкетирање посебних CERT-ова о стању њихових организација и зрелости пословних процеса, упоређујући их са Националним CERT-ом.

Реакција на инциденте је процес откривања безбедносних догађаја који утичу на мрежне ресурсе и информациона средства, а затим предузимање одговарајућих корака за процену и чишћење онога што се догодило. Одговор на инциденте у вези са сајбер-безбедношћу је критичан за данашње пословање јер, једноставно речено, постоји много тога за изгубити. Од најједноставнијих зараза злонамерним софтвером до нешифрованих лаптоп рачунара који су изгубљени или украдени до компромитованих акредитива за пријаву и изложености базама података, и краткорочне и дугорочне последице ових инцидената могу имати трајан утицај на пословање. Кршења безбедности могу захтевати обавештење, што резултира неповерењем купаца, губитком репутације, регулаторним казнама, правним таксама и трошковима чишћења. И све то може доћи одједном - на начин на који чак и финансијски најсигурнији од предузећа могу имати проблема да апсорбују.

Приступ у ревизији Управљања инцидентима у ИКТ системима од посебног значаја је са фокусом на узроке проблема. Како бисмо одговорили на ревизијска питања користили смо податке из периода 2019-2021. године. За поједине ревизорске доказе, како бисмо реалније приказали управљање инцидентима коришћена су Методолошка правила и смернице за ИТ ревизију[33], Приручник за ИТ ревизију IDI/INTOSAI[34] и Смерница за ИТ ревизију ISSAI 5300[35] и Методологија процене зрелости CERT-Европска агенција за ИТ безбедност ЕНИСА. У ревизији су коришћене технике прикупљање података и докумената у електронском облику (папирна документа ће се дигитализовати), анализа прикупљених података, анализе тренда и учешћа, интервјуи са одговорним лицима и друге технике.

Нарочити фокус и додатна пажња је стављена на осигурање функције инспекцијског надзора ове области. Да би биле прикупљене довољне и релевантне информације потребне за процену ефикасности управљања инцидентима у ИКТ системима од посебног значаја, коришћене су следеће методе ревизорског рада:

- интервјуи са надлежним представницима субјекта ревизије (информатика и корисници);
- прегледи доступне документације у вези са предметом ревизије;
- увид у свакодневне активности које се спроводе у оквиру редовног рада информационог система;
- посете локацијама на којима се спроводе активности у вези са радом информационог система.

Мреже, софтвер и крајњи корисници могу да достигну само одређени ниво отпорности и може да дође до превида и грешака. Важно је шта сте унапред урадили да бисте смањили утицај безбедносног инцидента на вашу организацију. Не можете спречити постојање хакера, али

---

[33] Одлуку о доношењу Методолошких правила и смерница донео председник Државне ревизорске институције 26. децембра 2019. године.

[34] Приручник усвојен на XXI Конгресу INTOSAI одржаном у Пекингу, Кина, октобар 2013. године.

[35] Верзија усвојена 2016. године, Међународне стандарде врховних ревизорских институција, ISSAI 5300, издаје INTOSAI, Међународна организација врховних ревизорских институција. www.issai.org

можете бити проактивни у превенцији и реаговању. Зато су поседовање функционалног тима, одговарајућих технологија и добро написаног плана реаговања на инциденте од суштинског значаја да бисте могли да одговорите на такве догађаје на брз и професионалан начин. Важан аспект разумевања реаговања на инциденте је употпуњавање неопходних елемената у вашем безбедносном програму да бисте направили разлику између претњи и рањивости које су приказане у наставку.

Претња: Индикација или подстицај, као што је криминални хакер или непоштени запослени, који настоји да искористи рањивост за незаконито стечену добит.

Рањивост: Слабост у рачунарском систему, пословном процесу или људима који се могу искористити.

Размена обавештења и информација о насталим безбедносним инцидентима у информационој инфраструктури има превасходно за циљ спречавање ескалације негативних последица и у суштини спречавање хакера да постигну циљ. Од суштинског значаја да свака организација има и одговарајућу заштиту информационог система. Циљ безбедности информационог система је заштита података организације тако што се смањује ризик од губитка поверљивости, интегритета и доступности те информације на прихватљив ниво. Због сложености и улоге информационих система, безбедност информација је важан део у пословању и између осталог заштита личних података поступцима псеудомизације или енкрипцијом.

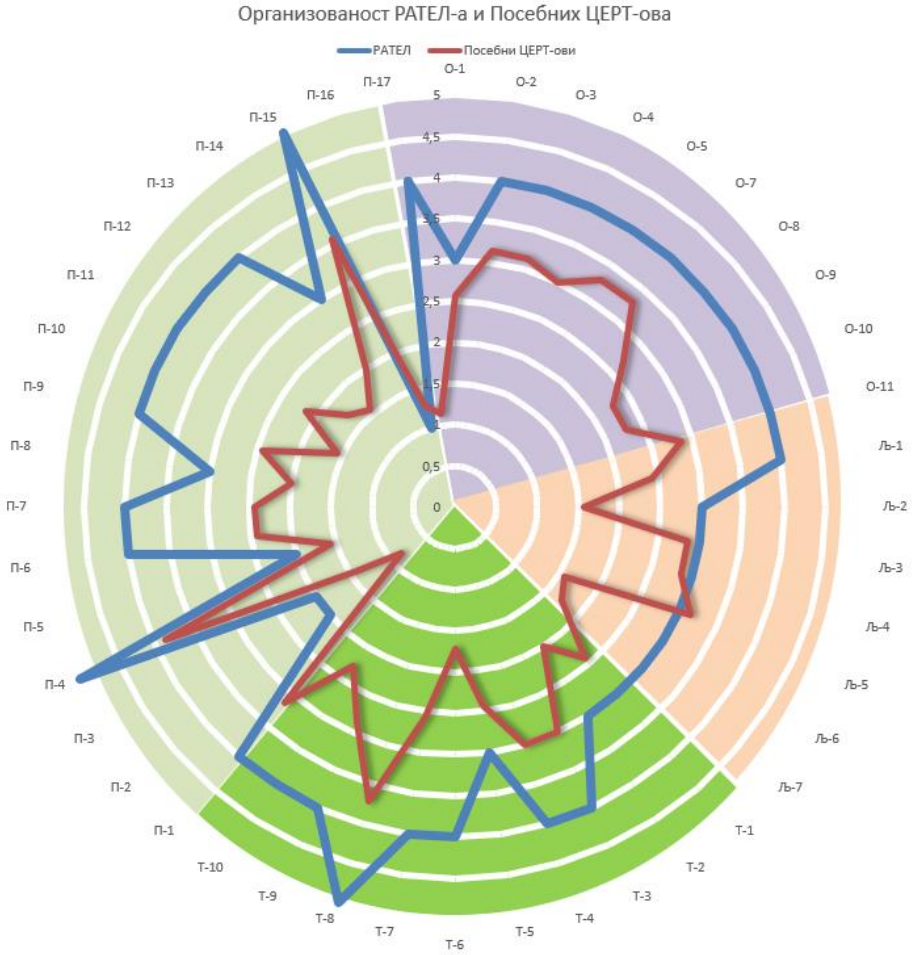
У току спровођења конкретног ревизорског ангажмана били би спроведени интервјуи са руководиоцима посебних CERT-ова и прибавили смо податке и информације о њиховој организационој развијености (зрелости организације) да одговори на обавезе. Тестирање овог питања су обавили већином по методологији процене зрелости Европске агенције за ИТ безбедност ENISA. Истовремено су спроведени и интервјуи са одговорним лицима у МТТТ у вези активности које спроводе на пословима обезбеђења ресурса за подршку Националном и посебним CERT-овима да успоставе ефикасне тимове за брзе интервенције код органа власти и других субјеката критичне информационе инфраструктуре.

Анкетирањем посебни CERT-ови су извршили самопроцену зрелости свог тима по основу 44 параметра СИМ3 в1 модела. СИМ3 в1 је такође у основи шеме сертификације у оквиру TF-CSIRT и такође га користи FIRST за свој процес чланства. За неколико параметара, ENISA CSIRT оквир зрелости захтева виши ниво процене него што је то потребно у оквиру шеме сертификације. Ово је због захтева Директиве NIS1 који су идентификовани за CSIRT -ове које је одредила држава чланица ЕУ.

Скоринг метода подразумева додељивање целобројних вредности које ће представљати вредности обележја. Када скала која је првобитно додељена обележјима није прецизно дефинисана, да би се избегао проблем неједнакости између категорија, истраживачи су често слободни да доделе вредности које по њима најприродније описују дате вредности обележја, што значи да могу да користе негативне бројеве, половине или било које друге вредности. Додељивање вредности на Ликертову скалу је најпопуларнији начин примене овог скоринг модела и имаће своју примену у раду.

Примењујући скоринг методу и одбацивањем екстремних вредности, извршили смо усредњавање и упоређивање са Националим CERT-ом како би оценили просечну зрелост посебних CERT-ова.

Слика број 11. Резултати иницијалног упитника за РАТЕЛ и посебне CERT-ове



Слика број 12. Легенда за самопроцену зрелости CERT-а

РБ	Наслов
О-1	Мандат
О-2	Учесници
О-3	Управа
О-4	Одговорност
О-5	Опис услуге
О-7	Опис нивоа услуге
О-8	Класификација инцидената
О-9	Учешће у постојећим CERT оквирима
О-10	Организациони оквир
О-11	Безбедносна политика
Љ-1	Кодекс понашања/пракса/етика
Љ-2	Лична отпорност запослених
Љ-3	Опис скупа вештина
Љ-4	Интерна обука
Љ-5	(Екстерна) техничка обука
Љ-6	(Екстерна) комуникацијска обука
Љ-7	Екстерно умрежавање
Т-1	Листа ИТ ресурса
Т-2	Листа извора информација
Т-3	Консолидовани систем е-поште
Т-4	Систем за праћење инцидената

РБ	Наслов
Т-5	Отпоран телефон
Т-6	Отпорна е-пошта
Т-7	Отпоран приступ Интернету
Т-8	Сет алата за превенцију инцидената
Т-9	Сет алата за откривање инцидената
Т-10	Скуп алата за решавање инцидената
П-1	Ескалација на ниво управљања
П-2	Ескалација на функцију притиска
П-3	Ескалација у правну функцију
П-4	Процес превенције инцидената
П-5	Процес откривања инцидената
П-6	Процес решавања инцидената
П-7	Процеси специфичних инцидената
П-8	Процес ревизије/повратне информације
П-9	Процес доступности у хитним случајевима
П-10	Најбоља пракса Интернет присутност
П-11	Питање процеса безбедног руковања информацијама
П-12	Процес извора информација
П-13	Процес видљивости у јавности
П-14	Процес извештавања
П-15	Статистички процес
П-16	Процес састанка
П-17	Процес колегијалне размене

Упитник за посебне CERT-ове

У циљу планирања ревизије и упознавањем са темом, идентификацијом потенцијалних проблема и ради прикупљање релевантних података, ревизорски тим је послао анкету на е-мејл адресе свих посебних CERT-ова који су извор информација у овој ревизији.

Упитником смо желели да у поступку самопроцене свих посебних CERT-ова се упознамо са нивоом организације и слабостима са којима се суочавају професионалне организације које обављају послове посебних CERT-ова, тј. пружалаца интернет услуга као критичне инфраструктуре од интереса за грађане Републике Србије.

Прибављени су одговори на 44 питања организованих у групама: организационе способности, људски ресурси, технолошка опремљеност и организованост пословних процеса. У прилогу 3 дата су сва питања и могући одговори о самопроцени стања.

3. Прилог 3 – Упитник за самопроцену зрелости CSIRT

За посебне CERT-ове

Овим упитником желимо да прикупимо информације о стању организационе зрелости CERT-а у Републици Србији, људским ресурсима, техничкој опремљености и успостављеним пословним процесима за постизање циљева постојања.

Државна ревизорска институција спроводи истраживање у вези организационе зрелости CERT-ова у Републици Србији. Анкета која је пред Вама послата је свим регистрованим CERT-овима, и она ће нам послужити да прикупимо и оценимо постојеће стање и расположиве ресурсе.

Анкета о самопроцени садржи 4 групе питања. У вези организације 10 питања, људских ресурса са којима располажете 7 питања, техничке опремљености 10 питања и успостављених пословних процеса 17 питања. На свако питање могуће је дати само један одговор и сва су обавезна. Анкета за самопроцену је урађена на основу препоруке Европске агенције за информациону безбедност.

Процењено време за одговарање је 40 мин. Термини CERT и CSIRT су у овом случају синоними.

Процена организационих способности и услова

Да ли ваш CSIRT има мандат?

[Помоћ: Мандат дефинише задатак вашег тима. У идеалном случају, мандат је одређен на највишем руководећем или политичком нивоу (у последњем случају може чак бити укорењен у законодавству).] (Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо разговарали о томе и формално не знамо свој мандат или задатак. Ми само радимо свој посао.
2. Имамо прилично добру идеју да радимо је оно што смо добили да урадимо, али то никада није записано.
3. Ми немамо формално писмено овлашћење, па смо написали нешто за своје потребе. Руководство нашег тима ово није званично одобрило.
4. Имамо писмени мандат вишег руководства који наш тимски менаџмент сматра меродавним. У периодичном прегледу нашег тима проверава се да ли и како испуњавамо свој мандат.

Да ли ваш CSIRT има јасну конститутивност, односно циљну групу за коју радите CSIRT, вашу „базу клијената“?

[Помоћ: Изборна јединица може бити интерна за вашу организацију, или може бити екстерна (или обоје).] (Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Знамо своју изборну јединицу, али то никада није записано.
3. Немамо формалну писану дефиницију изборне јединице, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писану дефиницију изборне јединице коју је одобрило руководство нашег тима.
5. Имамо писану дефиницију изборне јединице коју је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли и у којој мери служимо овој изборној јединици и да ли је дефиницију потребно прилагодити.

Шта вашем CSIRT-у може да уради према вашим корисницима како би остварио своју улогу и испунио свој мандат?

[Помоћ: Овлашћења вашег тима могу се кретати од само саветодавног, до могућности примене и/или ескалације.] (Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Знамо свој ауторитет, али он никада није записан.
3. Немамо формалну писану дефиницију ауторитета, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писану дефиницију овлашћења коју је одобрио менаџмент нашег тима.
5. Имамо писану дефиницију овлашћења коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли смо и како усклађени са овим ауторитетом и да ли је то довољно да испунимо свој мандат.

Шта се од вашег CSIRT-а очекује да уради према вашим корисницима како би остварио своју улогу и испунио свој мандат?

(Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Знамо своју одговорност, али она никада није записана.
3. Немамо формалну писану дефиницију одговорности, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писану дефиницију одговорности коју је одобрио менаџмент нашег тима.
5. Имамо писану дефиницију одговорности коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли и како испуњавамо ову одговорност.

Које су услуге које ваш CSIRT нуди својим корисницима?

[Помоћ: Ово би могло да укључи различите услуге као што су реаговање на инциденте, руковање рањивостима, анализа малвера и друге – плус повезане практичне аспекте као што су контакт информације и сервисни прозори. Важан аспект који треба размотрити је да ли је верзија описа услуге доступна (барем) вашим корисницима – да се објави рфц-2350 је препоручени начин да се то уради.] (Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме. Ми само радимо свој посао.
2. Знамо које услуге нудимо, али то никада није записано.
3. Немамо формални писани опис услуге, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писмени опис услуге који је одобрио менаџмент нашег тима и он је стављен на располагање нашим клијентима.
5. Имамо писмени опис услуге који је одобрио менаџмент нашег тима и он је стављен на располагање нашим клијенти. У периодичном прегледу нашег тима проверава се да ли и како пружамо ове услуге.

Да ли су нивои услуга дефинисани за услуге које нуди ваш CSIRT?

[Помоћ: Ово може да варира од нечег тако једноставног као што је захтев за слањем прве (људске) реакције на извештаје о инцидентима у одређеном временском периоду, до опсежнијих захтева типа „СЛА“.] (Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Имамо основно разумевање нивоа услуге који се од нас очекује, али то никада није записано.

3. Немамо формални писани опис нивоа услуге, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писани опис нивоа услуге који је одобрио менаџмент нашег тима.
5. Имамо писани опис нивоа услуге који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли и како испуњавамо ниво(е) услуге.

Да ли ваш CSIRT користи шему класификације инцидената када снима инциденте?

[Помоћ: Класификације инцидената обично садрже „врсте“ инцидената или категорије инцидената. Међутим, топло је препоручљиво да они такође укључују аспекте „озбиљност/утицај“ и „приоритет“ – јер ће то омогућити логичан начин за решавање већег броја инцидената у исто време, а такође и назначити када може доћи до ескалације.](Кратко објашњење: Изаберите један од следећих одговора)

1. Ми не класификујемо инциденте, само се бавимо њима.
2. Разумемо да постоје различите врсте инцидената, али то не износимо експлицитно. Ако неком инциденту треба посветити посебну пажњу, само се бавимо њиме у складу са тим.
3. Немамо формалну писану класификацију инцидената, па смо је написали за сопствене потребе. Наше руководство то није формално одобрило.
4. Имамо писмену класификацију инцидента коју је одобрило руководство нашег тима.
5. Имамо писмену класификацију инцидента коју је одобрило руководство нашег тима. У периодичном прегледу нашег тима пажња је посвећена различитим врстама инцидената и начину на који смо их поступили.

Да ли ваш CSIRT учествује у добро успостављеној сарадњи CSIRT-а, било директно или преко "узводног" CSIRT-а чији је ваш тим клијент/клијент?

[Помоћ: Ова врста учешћа је неопходна да бисте били ефективни члан националне/секторске/регионалне/светске сарадње CSIRT-а.](Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Знамо у којој сарадњи (сарадњи) CSIRT учествујемо, али то никада није записано.
3. Немамо званичну писану изјаву о сарадњи CSIRT-а у којој учествујемо, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо званичну писану изјаву о сарадњи CSIRT-а у којој учествујемо, коју је одобрило руководство нашег тима и подржано од стране буџета.
5. Имамо званичну писану изјаву о сарадњи CSIRT-а у којој учествујемо, коју је одобрило руководство нашег тима и подржано од стране буџета. У периодичном прегледу нашег тима проверава се да ли и колико активно учествујемо у овој сарадњи и које су користи од тога.

Да ли ваш CSIRT има кохерентан оквирни документ који служи као контролни документ за тим, познат и као „поглавље тима“ или „организациони оквир“?

[Помоћ: Ова повеља би требало да обједини описе за О-1 до О-9 и евентуално још неке СИМ3 параметре. У многим случајевима, тимови траже одобрење вишег менаџмента своје организације за свој статут – препоручено, али не и обавезно. РФЦ-2350 се понекад предлаже као повеља тима, али иако РФЦ-2350 покрива неке од "О" параметара, он не покрива све њих, и што је још важније, није замишљен да буде контролни документ, већ јавни опис услуге за CSIRT.] (Кратко објашњење: Изаберите један од следећих одговора)

1. Када нисмо стварно разговарали о овоме.

2. Имамо кохерентан поглед на нашу организациону структуру, али то никада није записано.
3. Немамо формално писани организациони оквир, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писани организациони оквир који је одобрио менаџмент нашег тима.
5. Имамо писани организациони оквир који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима, тестира се да ли је оквир ажуран и ефикасан.

Да ли ваш CSIRT или оснивачи имају безбедносну политику или оквир у оквиру којег ваш тим функционише?

[Помоћ: Политика за ваш тим може бити експлицитан или имплицитан део политике за ширу организацију – или ваш CSIRT може имати засебну безбедносну политику. Пошто CSIRT обично има специфичне ИТ/безбедносне захтеве (нпр. жели да прима нефилтрирану е-пошту, да има неки начин за покретање тестова без да буде блокиран од стране заштитног зида, специфичне захтеве за шифровањем, итд.), вреди размотрити посебну политику.](Кратко објашњење: Изаберите један од следећих одговора)

1. Никада нисмо стварно разговарали о овоме.
2. Знамо каква безбедносна ограничења важе, али она никада нису записана.
3. Немамо формалну писану безбедносну политику која се односи на нас, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писану безбедносну политику која се односи на нас, коју је одобрио менаџмент нашег тима.
5. Имамо писану безбедносну политику која се односи на нас, коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли испуњавамо ову политику и да ли она функционише за нас.

Процена капацитета људских ресурса

Да ли ваш CERT/CSIRT има скуп правила или упутства за чланове CSIRT-а о томе како да се понашају професионално, потенцијално и ван посла – поверљивост и поузданост су међу кључним квалитетима?

[Помоћ: Кодекс праксе CSIRT поузданог уводника служи као пример и може се користити у ову сврху. Кодекс понашања за организацију домаћина тима може постојати, али је ретко довољан јер се не дотиче специфичних аспеката CSIRT-а. Напомена: понашање ван посла је релевантно, јер се од чланова CSIRT-а може очекивати да се понашају одговорно и приватно и када су у питању рачунари и безбедност.]

1. Никада нисмо стварно разговарали о овоме.
2. Знамо каква се радна етика од нас очекује, али она никада није записана.
3. Немамо формално писани кодекс понашања, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писани кодекс понашања који је одобрио менаџмент нашег тима.
5. Имамо писани кодекс понашања који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је и како овај код коришћен и да ли служи својој сврси.

Да ли је особље вашег CSIRT-а довољно осигурано, такође када се један или више чланова разболи, на одмору, дају отказ, итд?

[Помоћ: Три члана тима (са скраћеним радним временом) сматрају се апсолутним минимумом како би се осигурало да у било ком тренутку бар неко може да се јави на телефон, или да прочита е-пошту и уради нешто. У зависности од понуђених услуга и уговора о нивоу услуга,

може бити потребан знатно већи број (стални и/или ad hoc) да би се обезбедила доступност чак у временима краткорочних изазова или криза.]

1. Ово је ван нашег делокруга.
2. Имамо довољно људи на послу да бисмо били отпорни, али то никада није написано у писаној форми.
3. Немамо званичну изјаву о броју расположивог особља CSIRT-а, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо званичну изјаву о броју расположивог особља CSIRT-а које је одобрило руководство нашег тима.
5. Имамо званичну изјаву о броју расположивог особља CSIRT-а које је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се какво је било кадровско стање и да ли је постојао довољан отпор.

Да ли ваш CSIRT има опис вештина потребних на позицијама CSIRT-а које имате у свом тиму?

[Помоћ: То могу бити позиције као што су „(виши) руководилац инцидентима“, „истраживач сајбер безбедности“, „генерални менаџер“ и друге. Вештине не би требало да буду само техничке природе/знања, јер су и меке вештине неопходне за рад CSIRT-а, као што су вештине комуникације и презентације, тимска игра, флексибилност.]

1. Никада нисмо стварно разговарали о овоме. Наше особље је искусно.
2. Знамо какве вештине треба да имамо, али оне никада нису записане.
3. Немамо формални писани опис вештина, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо писани опис вештина који је одобрио менаџмент нашег тима.
5. Имамо писани опис вештина који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је ова вештина довољна да се ухвати у коштац са тренутним претњама и инцидентима.

Да ли ваш CSIRT (или организација домаћин) нуди било какав облик интерне обуке како би обучио нове чланове тима и побољшао вештине постојећих, о темама релевантним за рад CSIRT-а?

[Помоћ: Ово може бити обука на послу, као и у учионици или друге врсте традиционалне обуке.]

1. Не нудимо ову врсту обуке.
2. Имамо идеје о интерној обуци и/или неформално обучавамо чланове тима, али никада нисмо записивали ништа о захтевима за обуку, темама или материјалима.
3. Немамо формални интерни програм обуке, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо интерни програм обуке који је одобрио менаџмент нашег тима.
5. Имамо интерни програм обуке који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је овај интерни програм обуке спроведен у довољној мери да задовољи потребе за обуком тима.

Да ли ваш CSIRT омогућава особљу да добије релевантну техничку обуку?

[Помоћ: Ово се обично ради екстерно – попут ТРАНСИТС, ЕНИСА CSIRT обуке или комерцијалних програма обуке (CERT/ЦЦ, САНС, итд.) – али у неким већим организацијама такве обуке су такође (делимично) доступне интерно.]

1. Немамо могућности, времена и новца за овакву обуку.
2. Шаљемо људе на такве обуке када је то потребно, али немамо писану политику о томе.

3. Немамо формални програм техничке обуке, па смо написали нешто за своје потребе што помаже у слању нашег особља на такве обуке. Наш менаџмент није формално одобрио овај програм.
4. Имамо програм техничке обуке који је одобрио менаџмент нашег тима, што нам омогућава да своје особље шаљемо на такве обуке.
5. Имамо програм техничке обуке који је одобрио менаџмент нашег тима, што нам омогућава да своје особље шаљемо на такве обуке. У периодичном прегледу нашег тима проверава се да ли је овај технички програм обуке довољно искоришћен да задовољи потребе за обуком тима.

Да ли ваш CSIRT дозвољава особљу да прође релевантну комуникацијску обуку?

[Помоћ: То обично раде спољни тренери, али у неким већим организацијама такве обуке су доступне и интерно. Имајте на уму да се овај параметар не односи само на разговоре са новинарима: у сваком аспекту рада CSIRT-а, људска комуникација је од највеће важности, било да се ради о писању е-поште или савета, или разговору са људима преко телефона или на састанцима . То може укључивати кризну комуникацију, што је за неке CSIRT-ове (нпр. национални и владини тимови) важна тема.]

1. Немамо могућности, времена и новца за овакву обуку.
2. Шаљемо људе на такве обуке када је то потребно, али немамо писану политику о томе.
3. Немамо формални програм комуникацијске обуке, па смо написали нешто за своје потребе што помаже у слању нашег особља на такве обуке. Наш менаџмент није формално одобрио овај програм.
4. Имамо програм обуке за комуникацију који је одобрио менаџмент нашег тима, што нам омогућава да своје особље шаљемо на такве обуке.
5. Имамо програм обуке за комуникацију који је одобрио менаџмент нашег тима, што нам омогућава да своје особље шаљемо на такве обуке. У периодичном прегледу нашег тима проверава се да ли је овај програм комуникацијске обуке довољно искоришћен да задовољи потребе тима за обуком.

Да ли се ваши чланови CSIRT-а шаљу на састанке са другим CSIRT-овима и другим релевантним професионалцима за сајбер безбедност?

[Помоћ: Ово не само да побољшава ниво и ефикасност вашег сопственог тима, већ такође доприноси сарадњи CSIRT-а широм света, што је опет од суштинског значаја за успех свих, укључујући и ваш ЦСИР]

1. Немамо могућности, времена и новца за ову врсту активности.
2. На такве састанке идемо кад можемо, али о томе ништа није записано.
3. Немамо формалну писану изјаву о нашем спољном умрежавању, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо званичну писану изјаву о нашем спољном умрежавању, коју је одобрио менаџмент нашег тима.
5. Имамо званичну писану изјаву о нашем спољном умрежавању, коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли и колико активно пратимо наше екстерно умрежавање и које су предности.

Технологија-Процена опремљености са адекватном опремом и потребним алатима за остварење мисије

Да ли ваш CSIRT има приступ листи или бази података која описује хардвер, софтвер, итд. Коју користе корисници, или барем у виталним организационим деловима корисника, тако да CSIRT може да пружи циљане савете?

[Помоћ: Ово питање се односи на „управљање имовином“ (ИСО терминологија) или „базу података за управљање конфигурацијом“ (ЦМДБ: ИТИЛ терминологија). CSIRT обично неће одржавати ЦМДБ, али барем морају имати приступ њему ако постоји. У недостатку напредног решења, CSIRT може размотрити одржавање ограничене верзије такве листе сам, уз помоћ својих безбедносних контаката у изборној јединици.]

1. Заиста не знамо.
2. Имамо добру идеју о најважнијим ИТ ресурсима, али не постоји списак за ово.
3. Немамо формалну листу ИТ ресурса, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо приступ званичној листи ИТ ресурса и ово је одобрило руководство нашег тима.
5. Имамо приступ званичној листи ИТ ресурса и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли је ова листа корисна и довољно тачна за циљеве нашег тима.

Да ли ваш CSIRT одржава листу извора (инфо фидова, веб локација, новина, твитова, итд.) одакле добијају информације о рањивости/трендовима/скенирању?

[Помоћ: Када постоји таква листа, она би требало да има неку врсту оцене важности извора – нпр. подела на примарне, секундарне и терцијарне изворе.]

1. Ми немамо такву листу. Не проверавамо систематски изворе, већ реагујемо на извештаје о инцидентима.
2. Знамо наше најважније изворе и проверавамо их, али не постоји списак за ово.
3. Немамо формалну листу извора информација, па смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо званичну листу извора информација које је одобрио менаџмент нашег тима.
5. Имамо званичну листу извора информација које је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је ова листа корисна и довољна за циљеве нашег тима.

Да ли ваш CSIRT држи сву CSIRT е-пошту у једном спремишту отвореном за све чланове тима?

1. Е-пошта CSIRT-а иде на лаптопове/рачунаре чланова тима. Нема потребе да га држите на једном месту.
2. Чувамо CSIRT е-пошту у једном спремишту, али овај систем није под нашом контролом и не знамо много о њему.
3. Чувамо е-пошту CSIRT-а у једном спремишту. Наше руководство то није формално одобрило.
4. Чувамо е-пошту CSIRT-а у једном спремишту и ово је одобрило руководство нашег тима.
5. Чувамо е-пошту CSIRT-а у једном спремишту и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли ово спремиште испуњава наше захтеве.

Да ли ваш CSIRT користи систем за управљање проблемом/током рада, отворен за све чланове тима, да региструје инциденте и прати њихов ток посла?

[Помоћ: Типични примери таквих система су РТ(ИР), ОТРС или генерички системи за пријаву проблема – мањи тимови понекад користе једноставнија решења попут заједничке табеле.]

1. Решавамо инциденте, за њих немамо алатку за регистрацију.
2. Имамо начин да региструјемо и пратимо инциденте, али га нисмо документовали.

3. Имамо систем за праћење инцидената. Наше руководство то није формално одобрило.
4. Имамо систем за праћење инцидената и ово је одобрило руководство нашег тима.
5. Имамо систем за праћење инцидената и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли овај систем за праћење испуњава наше захтеве.

Да ли нивои сервиса телефонског система који је доступан вашем CSIRT-у задовољавају или премашују нивое услуга вашег тима?

[Помоћ: То јест: ако се телефонски систем поквари, можете ли очекивати да ће бити поправљен довољно брзо да и даље будете у мо испуните своје нивое услуге? Имајте на уму у том погледу да је телефонија све више заснована на ИП-у. Мобилни телефони су обично резервни механизам када стандардни телефонски систем тима није у функцији – и барем би требало бити могуће позвати под тим околностима. Сателитски телефони су још једна опција, а неки тимови могу имати приступ посебној, екстра безбедној, телекомуникационој инфраструктури.]

1. Ми заправо не знамо ништа о нивоима услуга нашег телефонског система и нисмо договорили никакву резервну шему (нпр. коришћење мобилних телефона).
2. Када се телефонски систем поквари, усвајамо резервну шему (нпр. коришћење мобилних телефона), али ово нисмо документовали.
3. Када се телефонски систем поквари, усвајамо резервну шему (нпр. коришћење мобилних телефона) и то смо документовали. Наше руководство то није формално одобрило.
4. Када се телефонски систем поквари, усвајамо резервну шему (нпр. коришћење мобилних телефона), то смо документовали и то је одобрило руководство нашег тима.
5. Када се телефонски систем поквари, усвајамо резервну шему (нпр. коришћење мобилних телефона), то смо документовали и то је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли ова резервна шема испуњава наше захтеве и да ли је довољно позната.

Да ли нивои услуга е-поште који је доступан вашем CSIRT-у задовољавају или премашују нивое услуга вашег тима, што је ситуација описана у одговорима испод као „довољно добра за наше сврхе“?

[Помоћ: То јест: ако се систем е-поште поквари, можете ли очекивати да ће бити поправљен довољно брзо да и даље будете у могућности да испуните своје нивое услуге?]

1. Ми заправо не знамо ништа о нивоима услуга нашег система е-поште.
2. Ниво услуге нашег е-мејл система је довољно добар за наше потребе, али за то немамо документацију.
3. Ниво услуге нашег е-мејл система је довољно добар за наше потребе и за то имамо неформалну документацију. Наше руководство то није формално одобрило.
4. Ниво услуге нашег е-мејл система је довољно добар за наше потребе, а за то имамо документацију коју је одобрио менаџмент нашег тима.
5. Ниво услуге нашег е-мејл система је довољно добар за наше потребе, а за то имамо документацију коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је ова отпорност е-поште довољна.

Да ли нивои услуга приступа Интернету који су доступни вашем CSIRT-у задовољавају или премашују нивое услуге вашег тима?

[Помоћ: То јест: ако приступ Интернету падне, да ли можете очекивати да ће бити поправљен довољно брзо да и даље будете у могућности да испуните своје нивое услуге?]

1. Ми заправо не знамо ништа о нивоима услуга нашег приступа Интернету.
2. Ниво услуге нашег приступа Интернету је довољно добар за наше потребе, али за то немамо документацију.
3. Ниво услуге нашег приступа Интернету је довољно добар за наше потребе и за то имамо неформалну документацију. Наше руководство то није формално одобрило.
4. Ниво услуге нашег приступа Интернету је довољно добар за наше потребе, а за то имамо документацију коју је одобрио менаџмент нашег тима.
5. Ниво услуге нашег приступа Интернету је довољно добар за наше потребе, а за то имамо документацију коју је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је ова отпорност приступа Интернету довољна.

Да ли ваш CSIRT има колекцију алата за спречавање инцидената у њиховој изборној јединици?

[Помоћ: Тим или ради или користи ове алате, или има приступ резултатима које они генеришу. Примери су IntelMK, TARANIS, IPS (системи за спречавање упада), скенери вируса, филтери за нежељену пошту, скенери портова.]

1. Ми смо искључиво тим за координацију/руковање инцидентима који није укључен у превенцију.
2. Никада нисмо стварно разговарали о овоме.
3. Имамо такве алате, али их нисмо навели или документовали.
4. Имамо такве алате и да бисмо ово снимили написали смо нешто за своје потребе. Наше руководство то није формално одобрило.
5. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима.
6. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли су ови алати довољни да испуне наше захтеве.

Да ли ваш CSIRT има колекцију алата који имају за циљ откривање инцидената када се догоде или ће се ускоро догодити?

[Помоћ: Тим или ради или користи ове алате, или има приступ резултатима које они генеришу. Примери су MISP, AbuseHelper, IntelMK, IDS-ови (системи за откривање упада), карантинске мреже, алати за анализу мрежног тока – али и ваши алати за примање извештаја о инцидентима (телефон, е-пошта).]

1. Никада нисмо стварно разговарали о овоме.
2. Имамо такве алате, али их нисмо навели или документовали.
3. Имамо такве алате и да бисмо ово снимили написали смо нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима.
5. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли су ови алати довољни да испуне наше захтеве.

Да ли ваш CSIRT има колекцију алата за решавање инцидената након што су се десили?

[Помоћ: Тим или ради или користи ове алате, или има приступ резултатима које они генеришу. Суштински елементи овог скупа алата су хардвер који ваш тим користи (рачунари, рутери/прекидачи, складиште итд.) и ваша повезаност (која може укључивати одвојене интернет везе за непредвиђене и/или тестирање). Други примери су комплети форензичких алата, ваш систем за праћење инцидената (РТИР, ОТРС итд.), али такође имајте на уму да сви чланови тима морају да имају лак приступ (ИРТ објекат, ТИ и ПРВА информација, итд.).]

1. Никада нисмо стварно разговарали о овоме.
2. Имамо такве алате, али их нисмо навели или документовали.
3. Имамо такве алате и да бисмо ово снимили написали смо нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима.
5. Имамо такве алате, документовали смо их и ово је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли су ови алати довољни да испуне наше захтеве.

Процеси - Процена зрелости неопходних процеса за остварење мисије

Да ли ваш CSIRT има процес да брзо и што директније информише/узбуни више руководство управљачког тела вашег тима, када се деси инцидент или претња која има и високу хитност и утицај (последња два су вероватно заснована на вашој класификацији инцидената, погледајте О -8)?

[Помоћ: Ако је изборна јединица ван ваше организације домаћина и постоји више независних организација, морате бити у могућности да ескалирате на све њих. Имајте на уму да ова врста ескалације по својој природи мора бити ефикасна у сваком тренутку, а не само током радног времена. А да би био ефикасан, ланац ескалације мора бити веома кратак.]

1. Никада нисмо стварно разговарали о овоме.
2. Имамо неформалан начин ескалације, али то никада није записано.
3. Немамо формални писани процес ескалације, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је овај процес коришћен на одговарајући начин и како је функционисао.

Да ли ваш CSIRT има процес да брзо и директно обавештава канцеларију за штампу ваше организације домаћина када дође до инцидента или претње која има велику хитност и утицај?

1. Никада нисмо стварно разговарали о овоме.
2. Имамо неформалан начин ескалације, али то никада није записано.
3. Немамо формални писани процес ескалације, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је овај процес коришћен на одговарајући начин и како је функционисао.

Да ли ваш CSIRT има процес да брзо и директно обавештава правну канцеларију ваше организације домаћина када дође до инцидента или претње која има велику хитност и утицај?

[Помоћ: Информисање правне службе]

1. Никада нисмо стварно разговарали о овоме.
2. Имамо неформалан начин ескалације, али то никада није записано.
3. Немамо формални писани процес ескалације, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима.

5. Имамо формални писани процес ескалације који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли је овај процес коришћен на одговарајући начин и како је функционисао.

Да ли ваш CSIRT има процес који описује активности које имају за циљ спречавање инцидената, укључујући употребу одговарајућег скупа алата?

[Помоћ: Ово укључује усвајање проактивних услуга као што су подизање свести о безбедности и издавање обавештења о претњи/рањивости/закрпама.]

1. Ми смо искључиво тим за координацију/руковање инцидентима који није укључен у превенцију.
2. Никада нисмо стварно разговарали о овоме.
3. Знамо како то радимо, али то нисмо документовали.
4. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима.
6. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује активности које имају за циљ откривање инцидената, укључујући употребу одговарајућег скупа алата (видети Т-9)?

[Помоћ: Имајте на уму да је пријем извештаја о инцидентима путем телефона или е-поште део откривања инцидената. Имајте на уму да се П-5 и П-6 често комбинују у једном процесу, који се често назива руковање инцидентом или процес управљања инцидентом.]

1. Знамо како то радимо, али то нисмо документовали.
2. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
3. Имамо формални писани процес који је одобрио менаџмент нашег тима.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује активности усмерене на решавање инцидената, укључујући коришћење одговарајућег скупа алата?

[Помоћ: Имајте на уму да се П-5 и П-6 често комбинују у једном процесу, који се често назива руковање инцидентом или процес управљања инцидентом.]

1. Никада нисмо стварно разговарали о овоме.
2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT обрађује одређене категорије инцидената, као што су, DDoS или проблеми са ауторским правима?

[Помоћ: Ова врста додатних информација је посебно корисна за типове инцидената који могу бити критични (нпр. DDoS) или за типове инцидената где је развијен стандардни начин поступања са њима (нпр. питања ауторских права). Имајте на уму да је П-7 можда већ део П-6.]

1. Све инциденте третирамо на исти начин, додатне информације нису доступне за различите врсте инцидената.
2. Имамо неке стандардне начине поступања са различитим типовима инцидената, али то нисмо документовали.
3. Немамо формално написане специфичне процесе инцидента, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо 1 или више формалних писаних специфичних процеса инцидента које је одобрило руководство нашег тима.
5. Имамо 1 или више формалних писаних специфичних процеса инцидента које је одобрило руководство нашег тима. У периодичном прегледу нашег тима проверава се да ли ови процеси функционишу како је предвиђено.

Да ли ваш CSIRT има процес који описује како се успостављање, људски аспекти, операције и процеси CSIRT-а прегледавају самопроценом, ревизијом и накнадним механизмом повратних информација?

[Помоћ: Оне елементе за које се сматра да нису у складу са стандардима треба узети у обзир за будућа побољшања.]

1. Никада нисмо стварно разговарали о овоме.
2. Имамо преглед, али ово нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима и више руководство, а виши менаџмент води у томе.

Да ли ваш CSIRT има процес који описује како доћи до CSIRT-а у хитним случајевима? Ко су кључни актери у овом процесу (ваша група?

[Помоћ: и/или само они CSIRT-ови који деле круг поверења са вашим тимом, као што су ТИ акредитовани тимови, ФИРСТ чланови или тимови мреже CSIRT-а?) и да ли имају приступ овом процесу? Имајте на уму да је нпр. за тимове акредитоване ТИ, доступност у хитним случајевима дефинисана као један од параметара.]

1. Никада нисмо стварно разговарали о овоме.
2. Кључне заинтересоване стране знају како да дођу до нас у хитним случајевима, али ми то нисмо документовали.
3. Немамо формални писани процес, стога смо нешто написали за своје потребе и учинили доступним нашим кључним заинтересованим странама. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је доступан нашим кључним заинтересованим странама и одобрен од стране нашег менаџмента тима. (Имајте на уму да се објављене информације, било унутар изборне јединице или у некој екстерној бази података (нпр. ТИ) такође рачунају као ниво 3.)
5. Имамо формални писани процес који је доступан нашим кључним заинтересованим странама и одобрен од стране нашег менаџмента тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује (1) начин на који CSIRT или стране које знају када да пријаве CSIRT-у генеричке, сигурносне псеудониме поштанских сандучића @org.tld – (2) присуство на вебу и (3) присуство на друштвеним мрежама?

[Помоћ: Минимални захтев: (1) Руковање следећим псеудонима поштанских сандучића (из РФЦ-2142 и најбоље праксе) је обезбеђено на такав начин да руковаоци или су део CSIRT-а или

знају CSIRT, чему служи и како да дођи до њега када је потребно: Безбедност: безбедност@ ; cert@ ; abuse@ E-mail: postmaster@ ИП бројеви и имена домена: hostmaster@ BBB: vebmaster@ ; www@ (2) Неки облик веб присуства за CSIRT, барем интерно. То присуство мора барем да објасни чему служи CSIRT, коме је и како се може доћи до њега и када. Додатне препоруке су (а) да се повеже рфц-2350 са тог присуства и (б) да се омогући безбедносна страница са косом цртом, то је страница као што је vvv.org.tld/securiti, која може да служи широј безбедносној сврси него само CSIRT. (3) Присуство на друштвеним мрежама је опционо, али се мора узети у обзир. Твитер, Фејсбук итд.]

1. Никада нисмо обраћали велику пажњу на ово.
2. Имамо неколико њих, али ово нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT обрађује поверљиве извештаје о инцидентима и/или информације?

[Помоћ: Ово такође има утицаја на локалне законске захтеве. Напомена: овај процес би такође требало да подржава употребу ТЛП-а, протокола за размену информација о семафору.]

1. Никада нисмо стварно разговарали о овоме.
2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT рукује различитим изворима информација доступним CSIRT-у (као што је дефинисано у повезаном алату, ако је доступно – види Т-2)?

1. Никада нисмо стварно разговарали о овоме.
2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT допире до својих корисника, не у вези са инцидентима, већ у погледу видљивости CSIRT-а, подизања свести и „ПР-а“?

[Помоћ: Овај процес би требало да обухвати све облике таквог приступа, од веб страница, преко билтена, савета до семинара, радионица, обука итд. Имајте на уму да би се, на пример, за националне CSIRT-ове овај процес такође односио на допирање до различитих сектора у друштву/економији којима тим служи.]

1. Никада нисмо стварно разговарали о овоме.

2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT извештава више руководство и/или Ц(И)СО њихове организације домаћина, тј. интерно?

1. Никада нисмо стварно разговарали о овоме.
2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима и више руководство. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује коју статистику инцидената, на основу њихове класификације инцидената (види О-8), CSIRT открива корисницима својих услуга и/или шире?

[Помоћ: Имајте на уму да се не ради о статистици у извештавању менаџмента: то је покривено П-14.]

1. Направили смо изричит избор да статистику извештавамо само интерно, а не корисницима наших услуга и шире.
2. Никада нисмо стварно разговарали о овоме.
3. Знамо како то радимо, али то нисмо документовали.
4. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима.
6. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има интерни процес састанка, који описује барем колико често се тим састаје?

1. Никада нисмо стварно разговарали о овоме.
2. Састајемо се редовно, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.

Да ли ваш CSIRT има процес који описује како CSIRT ради заједно са равноправним CSIRT-овима и/или са њиховим надлежним CSIRT-ом?

[Помоћ: Имајте на уму да надлежни CSIRT не постоји за многе водеће тимове, као што су национални тимови или корпоративни тимови; обично ће имати „вршњаке“ у свом сектору – за национални тим би природни вршњаци били други национални тимови.]

1. Никада нисмо стварно разговарали о овоме.
2. Знамо како то радимо, али то нисмо документовали.
3. Немамо формални писани процес, стога смо написали нешто за своје потребе. Наше руководство то није формално одобрило.
4. Имамо формални писани процес који је одобрио менаџмент нашег тима.
5. Имамо формални писани процес који је одобрио менаџмент нашег тима. У периодичном прегледу нашег тима проверава се да ли овај процес функционише како треба.