НАЦРТ

На основу члана 11. став 4. Закона о информационој безбедности („Службени гласник РС“, број 91/25),

Савет Регулаторног тела за електронске комуникације и поштанске услуге, дана 28. априла 2026. године, електронским путем, доноси

ПРАВИЛНИК
о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја

Члан 1.

Овим правилником утврђује се општа методологија за процену ризика у приоритетним и важним информационо-комуникационим системима од посебног значаја (у даљем тексту: ИКТ системи од посебног значаја).

Члан 2.

Акт о процени ризика ИКТ система од посебног значаја израђује се у складу са општом методологијом за процену ризика, која је дата је у Прилогу 1. овог правилника и чини његов саставни део.

Актом о процени ризика из става 1. овог члана врши се процена ризика у ИКТ системима од посебног значаја с обзиром на степен изложености ризику, величину оператора ИКТ система од посебног значаја и извесност појаве инцидента и његове озбиљности, као и његов потенцијални друштвени и економски утицај.

Члан 3.

Процена ризика у ИКТ системима од посебног значаја обухвата идентификацију претњи, рањивости и могућих инцидената, која се заснива на Каталогу претњи информационе безбедности, који је дат у Прилогу 2. овог правилника и чини његов саставни део.

Члан 4.

Овај правилник ступа на снагу осмог дана од дана објављивања у „Службеном гласнику Републике Србије“.

ПРЕДСЕДНИК САВЕТА

Драган Ковачевић

Број:

У Београду, __. _____ 2026. године

ПРИЛОГ 1.

ОПШТА МЕТОДОЛОГИЈА ЗА ПРОЦЕНУ РИЗИКА У ИКТ СИСТЕМИМА ОД ПОСЕБНОГ ЗНАЧАЈА

1. Увод

Општа методологија за процену ризика у приоритетним и важним ИКТ системима од посебног значаја (у даљем тексту: методологија) представља оквир за спровођење обавезе процене ризика прописане Законом о информационој безбедности („Службени гласник РС", број 91/25, у даљем тексту: ЗИБ). У складу са Законом оператори ИКТ система од посебног значаја дужни су да донесу Акт о процени ризика за ИКТ системе (у даљем тексту: акт о процени ризика) израђен у складу са овом методологијом. Методологија обезбеђује јединствен и стандардизован приступ процени ризика и примењује се као основни методолошки оквир, а посебно је намењена операторима ИКТ система од посебног значаја који немају интерним актом уређену процену ризика. Заснива се на ITSRM методологији Европске комисије (одлука Комисије (EU, Euratom) 2017/46 од 10. јануара 2017. године о сигурности комуникационих и информационих система у Европској комисији), ENISA „*Interoperable EU Risk Management Toolbox*“ и међународним стандардима NIST SP 800-30 Rev.1 и ISO/IEC 27005:2022. Примена методологије има за циљ правовремено и ефикасно доношење одлука о примени мера заштите, као и смањење ризика и последица безбедносних инцидената.

Ова методологија представља смернице за спровођење процене ризика у ИКТ системима од посебног значаја. Операторима ИКТ система од посебног значаја, који већ имају успостављену процену ризика засновану на сценаријима, процесима или другом методолошком приступу, она служи као референтни оквир за проверу усклађености, а не као обавеза за поновно спровођење процене. Услови усклађености постојеће процене са захтевима ове методологије детаљније су дефинисани у тачки 5. методологије.

Акт о процени ризика обезбеђује систематску идентификацију, анализу и процену ризика по информациону безбедност ИКТ система, у складу са законом, узимајући у обзир степен изложености ризику, величину и значај оператора, вероватноћу и озбиљност безбедносних инцидената, као и њихов потенцијални друштвени и економски утицај. На основу овог акта доноси се акт о безбедности ИКТ система од посебног значаја, којим се утврђују техничке, организационе, административне и физичке мере заштите, сразмерне идентификованим ризицима.

Акт о процени ризика подлеже редовној ревизији најмање једном годишње, као и у случају значајних измена у претњама, рањивостима, технолошком или организационом окружењу, ради обезбеђивања сталне усклађености са законом и одговарајућег нивоа заштите ИКТ система од посебног значаја.

Доношење Акта о процени ризика, као и Акта о безбедности ИКТ система од посебног значаја је одговорност и задатак органа управљања оператора ИКТ система од посебног значаја.

У циљу заштите ИКТ система од посебног значаја препорука је да Акт о процени ризика буде поверљив документ који није јавно доступан. Акт о процени ризика може се давати искључиво на увид лицима која су законом овлашћена да га захтевају, без

могућности достављања или прослеђивања ван оператора ИКТ система од посебног значаја.

2. Коришћени појмови

У методологији користе се појмови из области информационе безбедности, ИКТ система и процеса управљања ризицима. У наставку су наведени појмови и њихова значења у контексту ове методологије:

Појмови	Значење
Анализа ризика	Процес разумевања природе ризика и утврђивања нивоа ризика. Представља основу за вредновање ризика и доношење одлука о третману ризика.
Вероватноћа догађања	Шанса да се одређени догађај или претња оствари.
Власник ресурса	Особа која је одговорна за ресурсе.
Власник ризика	Особа која је одговорна и овлашћена да управља ризиком.
Вредност ризика	Комбинација негативног утицаја и вероватноће појаве ризика, односно вероватноће догађања.
Догађај (*event*)	Појава или промена одређеног скупа околности која може имати значај за безбедност или пословање.
Идентификација ризика	Процес препознавања и описивања ризика.
Инцидент	Сваки догађај који угрожава расположивост, интегритет, аутентичност, непорецивост или поверљивост података који се чувају, преносе или обрађују или услуге које се пружају, односно које су доступне путем ИКТ система.
Инхерентни ризик	Вредност ризика пре примене мера заштите.
Интегритет	Својство које осигурава да подаци или информације нису промењени или уништени на неовлашћени начин од када су креирани, пренети или ускладиштени.
Информисана одлука (*informed decision*)	Одлука о поступању са ризиком коју доноси орган управљања оператора ИКТ система од посебног значаја на основу документованих резултата процене ризика, узимајући у обзир идентификоване претње, процењени утицај и вероватноћу, расположиве мере заштите и пословни контекст.
Мере заштите	Техничке, организационе, административне и физичке мере за управљање безбедносним ризицима ИКТ система.

Појмови	Значење
Поступање са ризиком	Третирање ризика ради смањења, елиминације или превенције негативних последица.
Поверљивост (*confidentiality*)	Својство којим се осигурава да су информације и функције ИКТ система доступне само овлашћеним лицима.
Преостали ризик (*residual risk*)	Ризик који преостаје након поступања са ризиком, односно након примене мера заштите.
Прихватање ризика	Свесна одлука о прихватању одређеног ризика.
Претња	Свака околност, догађај или радња која може да угрози, поремети или на други начин штетно утиче на ИКТ систем, кориснике система и друга лица са јасном вероватноћом настајања штете у случају да изостане реакција.
Процена ризика	Процена ризика, у смислу ове методологије, је систематски процес идентификације, анализе и вредновања ризика који могу утицати на ресурсе оператора ИКТ система од посебног значаја, са циљем да се обезбеде информисане одлуке о поступању са тим ризицима. Процена ризика обухвата и поступање са ризиком и праћење ризика као саставне фазе целокупног циклуса управљања ризицима информационе безбедности.
Расположивост (*availability*)	Један од три кључна атрибута информационе безбедности, својство којим се осигурава доступност и употребљивост ИКТ система на захтев овлашћеног субјекта или процеса онда када им је потребан.
Ресурси (*asset*)	Све што има вредност за оператора ИКТ система од посебног значаја, укључујући податке, хардвер, софтвер, локације и људске ресурсе.
Ризик	Функција негативног утицаја специфичне последице и вероватноће њеног настанка.
Управљање ризицима	Свеобухватан процес усмерен на контролу ризика унутар ИКТ система од посебног значаја.
Утицај (*impact*)	Степен негативних последица по остваривање пословних циљева у случају реализације ризика.
Фреквенција	Мера учесталости појаве одређеног догађаја.

3. Тим/Радна група за спровођење процене ризика

С обзиром на комплексност процеса процене ризика, пре започињања процене ризика неопходно је да орган управљања оператора ИКТ система од посебног значаја,

који је одговоран за спровођење овог процеса, именује тим/радну групу, који/а ће реализовати целокупан процес процене ризика.

Препорука је да орган управљања оператора ИКТ система од посебног значаја обезбеди квалитетну едукацију чланова тима за процену ризика и размотри успостављање сталног механизма за праћење безбедносних ризика, размену искустава и координацију активности у области информационе безбедности.

Орган управљања оператора ИКТ система од посебног значаја дефинише опсег за анализу ризика, укључујући и дефинисање периода на који се процена ризика односи.

Орган управљања оператора ИКТ система од посебног значаја је одговорно за одобравање плана за поступање са ризиком.

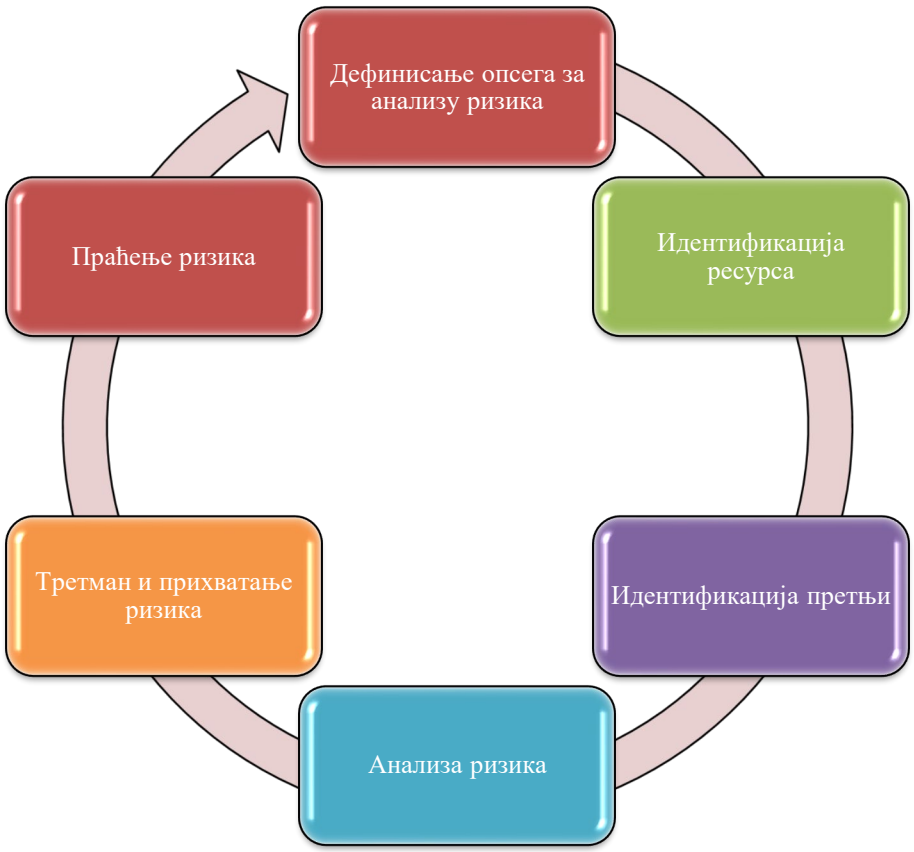
4. Процена ризика

Процена ризика је систематски процес идентификације, анализе и вредновања ризика који могу утицати на ресурсе оператора ИКТ система од посебног значаја, са циљем да се обезбеде информисане одлуке о управљању тим ризицима.

Процена ризика дефинисана овом методологијом је процена ризика заснована на ресурсима у оквиру које се ризици идентификују, анализирају и вреднују полазећи од вредности и значаја ресурса, као и од идентификованих претњи, рањивости и могућих последица по поверљивост, интегритет и расположивост информација и ИКТ система.

Процена ризика (*Графикон 1*) обухвата следеће процесе:

1. Дефинисање опсега (контекста) за анализу ризика;
2. Идентификација ресурса која је у опсегу анализе ризика;
3. Идентификација претњи које утичу на ИКТ систем од посебног значаја унутар контекста;
4. Анализа ризика – рангирање и вредновање;
5. Поступање са ризиком и прихватање ризика;
6. Праћење ризика.



Графикон 1: Процена ризика

4.1. Дефинисање опсега (контекста) за анализу ризика

Дефинисање опсега (контекста) за анализу ризика је процес у оквиру којег се утврђују основни критеријуми, оквир и обим спровођења процене ризика и представља почетну фазу процеса управљања ризицима.

Дефинисање оквира за анализу ризика обухвата:

- анализу надлежности оператора ИКТ система од посебног значаја;
- утврђивање заинтересованих страна и њихових очекивања и потреба од оператора ИКТ система од посебног значаја (корисници, запослени, регулатор, партнери, итд.);
- идентификацију екстерних и интерних изазова (компетенције запослених, застарели системи, велика зависност од треће стране, итд.);
- дефинисање критеријума за процену и прихватање ризика, као и
- успостављање одговарајуће организације/тима за управљање ризицима.

Кроз дефинисање оквира за анализу ризика, односно контекста, оператор ИКТ система од посебног значаја обезбеђује јасно и документовано разумевање сопствених пословних циљева, законских и регулаторних обавеза, релевантних заинтересованих страна и њихових очекивања, као и специфичних карактеристика информационог система који је предмет анализе. На тај начин оператор ИКТ система од посебног

значаја успоставља оквир за спровођење активности идентификације, анализе, процене ризика и поступања са ризицима информационе безбедности.

Дефинисање оквира за анализу ризика обезбеђује доследност, упоредивост и поузданост резултата процене ризика.

4.1.1. Опис система

Први корак у процени ризика је израда описа система унутар контекста оператора ИКТ система од посебног значаја који укључује дефинисање обима процене, укључених компоненти и ограничења у оквиру којих се процена спроводи.

Опис система унутар контекста укључује:

- основне податке о оператору ИКТ система од посебног значаја;
- опис главних пословних циљева и процеса;
- информације које се обрађују у сваком процесу;
- информационе системе који подржавају процесе;
- коришћени хардвер и софтвер - инфраструктура,
- лиценце и сертификате;
- добављаче, контакте и SLA параметре;
- редундантност система и евентуалне „*single point of failure*“ тачке;
- локације процеса и инфраструктуре;
- зависности међу процесима;
- потребне људске ресурсе и њихове компетенције за одржавање система.

Опис система може постојати као посебан документ, али мора бити редовно ажуриран у складу са променама система. Елементи наведени у овом одељку су оријентациони, оператор ИКТ система од посебног значаја их прилагођава свом контексту и обиму процене, водећи рачуна да опис система омогућава јасно разумевање граница система који је предмет анализе.

Приликом израде описа система препоручује се да оператор ИКТ система од посебног значаја узме у обзир и стратегију развоја информационог система, имајући у виду да планиране технолошке и организационе промене могу бити извор нових ризика, које је неопходно размотрити у оквиру процене ризика. Уколико оператор ИКТ система од посебног значаја не располаже формализованом стратегијом развоја информационог система, препоручује се да образложи разлоге због којих стратешко планирање развоја информационог система није формализовано.

4.1.2. Опис информационих система

Након описа система следи опис информационих система оператора ИКТ система од посебног значаја који обухвата:

- назив и намену система;
- функционалности и везу са пословним процесима;
- врсте и класификацију података;
- критичност по пословне процесе;
- политику и учесталост резервних копија;
- опис корисника;
- архитектуру система;

- комуникацију са интерним и екстерним системима;
- начин одржавања – интерни или екстерни;
- добављаче и SLA параметре;
- зависности и ограничења система.

Оператор ИКТ система од посебног значаја може идентификовати више независних система који могу имати различите карактеристике.

4.2. Идентификација ресурса која је у опсегу анализе ризика

Идентификација ресурса која је у опсегу анализе ризика представља процес препознавања свих ресурса који имају вредност за оператора ИКТ система од посебног значаја и који захтевају примену одговарајућих мера заштите.

Ресурс је све што представља вредност за оператора ИКТ система од посебног значаја и захтева примену одговарајућих мера заштите. Приликом идентификације ресурса неопходно је узети у обзир да се ИКТ систем не своди искључиво на хардверске и софтверске компоненте, већ обухвата шири спектар ресурса, укључујући локације, хардвер, софтвер, запослене, информације и треће стране.

Процес идентификације ресурса спроводи се у обиму који омогућава прикупљање потпуних и релевантних информација за адекватну процену ризика. Начин на који се спроводи идентификација ресурса, односно ниво детаљности, утиче на количину и врсту информација који се прикупљају током процене ризика, при чему се прецизност и дубина анализе могу постепено унапређивати кроз поновљене циклусе процене ризика.

Идентификација ресурса коју је потребно заштити и процена њене вредности (у смислу утицаја који ће оператор ИКТ система од посебног значаја претрпети у случају инцидента) су од кључног значаја приликом анализе ризика. У том смислу, предлаже се дефинисање специфичних категорија ресурса и прецизирање свих ресурса које категорије ресурса обухватају.

Сваки ИКТ систем може обухватити следеће категорије ресурса:

- Локације;
- Хардвер (обухвата и мрежне уређаје и електронску комуникациону инфраструктуру у смислу ЗИБ-а);
- Софтвер;
- Запослене (по улогама) и њихове компетенције;
- Информације – нематеријална имовина;
- Треће стране (добављачи и партнери).

Резултат процеса идентификације ресурса је израда регистра ресурса (*Табела 1*), који оператор ИКТ система од посебног значаја прилагођава својим потребама и организационом контексту и најмање садржи следеће податке:

- Назив ресурса – име које ће се користити за то средство у оквиру анализе ризика;

- Власник – име или радно место одговорне особе за правилно управљање или коришћење средства;
- Категорија – како је дефинисано у претходном делу ове методологије;
- Локација – где је физички постављено средство (уколико је примењиво).

Назив ресурса	Власник	Категорија	Локација	Остало
Апликација 1	Петар Петровић	Софтвер	Дирекција	
Сервер 1	Директор ИТ	Хардвер	Дата центар	

Табела 1: Регистар ресурса

Оператор ИКТ система од посебног значаја може користити било које производе, услуге, апликације или алате за документовање регистра ресурса.

4.3. Идентификација претњи

Идентификација претњи је процес систематског и свеобухватног препознавања претњи које могу негативно утицати на ИКТ системе, пословне процесе и ресурсе оператора ИКТ система од посебног значаја.

Идентификација претњи спроводи се након што су ИКТ системи, пословни процеси и ресурси у опсегу процене ризика јасно дефинисани. Циљ овог процеса је систематично и свеобухватно препознавање претњи које могу негативно утицати на идентификоване ресурсе оператора ИКТ система од посебног значаја.

Идентификација претњи спроводи се кроз неколико корака (*Графикон 2*).

Графикон 2: Идентификација претњи

4.3.1. Коришћење Каталога претњи информационе безбедности

Оператор ИКТ система од посебног значаја користи Каталог претњи информационе безбедности (у даљем тексту: Каталог претњи), који је саставни део ове методологије, као основни извор за идентификацију претњи. Оператор ИКТ система од посебног значаја може користити и сопствени каталог претњи уколико покрива исте основне категорије претњи као Каталог претњи из ове методологије.

Каталог претњи обухвата следеће категорије претњи:

- природне претње;

- индустријске претње;
- грешке и ненамерни пропусти;
- намерни напади;
- претње повезане са услугама које се пружају операторима ИКТ система од посебног значаја, укључујући услуге рачунарства у облаку и услуге трећих лица;
- инсајдерска претња.

4.3.2. Утврђивање примењивих категорија претњи

Оператор ИКТ система од посебног значаја утврђује које категорије претњи су релевантне за његов контекст, узимајући у обзир карактеристике ИКТ система.

4.3.3. Повезивање претњи са ресурсима

За сваки идентификовани ресурс оператор ИКТ система од посебног значаја идентификује појединачне претње из Каталога претњи које могу утицати на те ресурсе. При томе се води рачуна да поједине претње могу бити примењиве само на одређене категорије ресурса (нпр. хардвер, софтвер, информације, људски ресурси).

4.3.4. Анализа утицаја претњи

За сваку идентификовану претњу утврђују се потенцијалне последице по:

- поверљивост;
- интегритет;
- расположивост информација и ИКТ система, као и
- извор претње (намерни, случајни, природни).

Препорука је да оператор ИКТ система од посебног значаја, у оквиру анализе утицаја претњи, документује и рањивости ресурса које су релевантне за идентификоване претње, јер познавање рањивости доприноси прецизнијој процени вероватноће и утицаја.

4.3.5. Идентификација додатних претњи

Уколико оператор ИКТ система од посебног значаја препозна претње које нису обухваћене Каталогом претњи, такве претње се документују у засебном интерном документу на који се акт о процени ризика позива, уз образложење њихове релевантности.

4.3.6. Документовање резултата

Резултати идентификације претњи документују се кроз дефинисање уређених релација између ресурса и претњи (*Табела 2*). Ове релације представљају основу за даљу анализу и вредновање ризика.

Ресурс	Претња
Софтвер 1	Вирус Грешка у подацима Неовлашћени упад
Хардвер 1	Пожар Квар Неовлашћени приступ

Табеле 2: Ресурс – претња

4.4. Анализа ризика – рангирање и вредновање

Анализа ризика је процес у оквиру којег се врши процена значаја идентификованих ризика кроз анализу утицаја и вероватноће догађања претњи, и представља централну фазу процеса управљања ризицима информационе безбедности.

Анализа ризика представља основ за управљање ризицима и полазну тачку за дефинисање циљева информационе безбедности усмерених на заштиту ресурса оператора ИКТ система од посебног значаја, односно доношење одлука о приоритетима, избору мера заштите и поступању са идентификованим ризицима.

Процена ризика у области информационе безбедности заснива се на анализи комбинације два кључна фактора: утицаја и вероватноће догађања.

- **Утицај** представља озбиљност последица, које могу настати по ресурсе уколико се претња реализује.
- **Вероватноћа догађања** означава процену шансе да се одређена претња или нежељени догађај заиста оствари.

Комбиновањем процењених вредности утицаја и вероватноће догађања, оператор ИКТ система од посебног значаја добија вредност ризика, што омогућава њихово рангирање и приоритизацију.

С обзиром на то да је прецизна процена утицаја и вероватноће догађања често изазовна, у овој методологији се користе предефинисани критеријуми за вредности, односно квалитативна анализа ризика.

4.4.1. Вредности за утицај

Негативан утицај представља један од два основна фактора за одређивање вредности ризика у оквиру квалитативне анализе ризика. Под негативним утицајем подразумева се степен штете који може настати по ресурсе оператора ИКТ система од посебног значаја и повезане пословне процесе у случају реализације одређене претње.

Ради једноставније и доследне процене, негативан утицај се вреднује коришћењем скале од 1 до 5, у складу са документом *„Interoperable EU Risk Management Toolbox“* (*Табела 3*).

Сваки оператор ИКТ система од посебног значаја може дефинисати своје оквире, вредности и рангирање утицаја у односу на своје потребе.

Утицај	Вредност	Опис
Веома висок - катастрофалан	5	-Реализација претње изазива катастрофалне последице по пословање. -Цурење информација које могу угрозити опстанак оператора ИКТ система од посебног значаја. - Цурење података о личности великог обима или осетљивих категорија података које може изазвати значајну штету по права и слободе физичких лица. -Непоправљиви кварови или трајни прекиди у раду система. - Недоступност која захтева екстремне напоре за

Утицај	Вредност	Опис
		повратак функционалности или је трајна. -Озбиљан негативан утицај на репутацију или запослене уз значајну медијску пажњу. -Престанак свих услуга које пружа оператор ИКТ система од посебног значаја. -Законске санкције или велике новчане казне. - Последице су скоро неповратне или ненадокнадиве (нпр. смрт, немогућност рада).
Висок – критичан	4	- Реализација изазива значајне негативне последице по пословање. - Цурење информација које озбиљно угрожава интересе оператора ИКТ система од посебног значаја. - Цурење података о личности које угрожава права и слободе физичких лица и може резултовати новчаним казнама у складу са прописима о заштити података о личности. - Наставак недоступности услуга са значајним оперативним проблемима. - Пад угледа оператора ИКТ система од посебног значаја. - Финансијски губици или додатни трошкови због претње.
Средњи – просечан	3	- Реализација изазива умерен негативни ефекат по пословање. - Цурење информација које утичу на интересе оператора ИКТ система од посебног значаја. - Привремена штета угледу. - Изоловани инциденти са минималним утицајем. - Потенцијалне казне или мањи финансијски губици.
Низак - маргиналан	2	- Реализација претње има ограничен утицај на пословање. - Цурење информација које су штетне, али не угрожавају виталне интересе. - Недостатак доступности услуга само изазива неугодности. - Могућа медијска критика, али без значајних последица. - Мали губици који се лако надокнађују (нпр. изгубљено време).
Веома низак - занемарљив	1	- Реализација претње има незнатан или минималан утицај на пословање.

Табела 3: Вредности за утицај

4.4.2. Вредности за вероватноћу догађања

Вероватноћа догађања представља други кључни фактор за одређивање укупне вредности ризика у оквиру квалитативне анализе ризика. Она означава процену шансе да се одређена претња оствари у контексту постојећих ИКТ система и пословних процеса оператора ИКТ система од посебног значаја.

За лакшу и доследну процену, вероватноћа догађаја се вреднује коришћењем скале од 1 до 5, у складу са документом *„Interoperable EU Risk Management Toolbox“* (*Табела 4*).

Оператор ИКТ система од посебног значаја може, у складу са својим потребама и специфичностима, дефинисати сопствене оквире, вредности и начин рангирања вероватноће догађања, како би обезбедио поуздану и усаглашену процену ризика.

Вероватноћа догађања	**Вредност**	**Опис**
Веома висока	5	Претња ће се скоро сигурно остварити због постојања рањивости које се могу искористити, а одговарајуће мере заштите не постоје. (вероватноћа реализације у периоду од 0 до 90 дана)
Висока	4	Претња ће се вероватно остварити, јер постоје рањивости које се могу искористити, а постојеће мере заштите су неефикасне или застареле. (вероватноћа реализације у периоду од 90 до 180 дана)
Средња	3	Претња се потенцијално може остварити због постојећих рањивости, иако постоје одређене мере заштите, које би могле бити ефикасније. (вероватноћа реализације у периоду од 180 дана до 1 године)
Ниска	2	Претња се вероватно неће остварити јер су све повезане рањивости покривене одговарајућим мерама заштите. (вероватноћа реализације у периоду од 1 до 3 године)
Веома ниска	1	Мало је вероватно да ће се претња остварити, будући да су све повезане рањивости ефикасно неутралисане мерама заштите.

Табела 4: Вредности за вероватноћу догађања

4.4.3. Матрица ризика

Матрица ризика (*Табела 5*) се користи за израчунавање ризика и њихову категоризацију према нивоу озбиљности. Вредности приказане у матрици и регистру ризика (*Табела 7*) односе се на инхерентни ризик, односно ризик пре примене мера заштите.

Након што се за сваки део ресурса процени негативни утицај и вероватноћа догађања, израчунава се вредност идентификованог ризика према следећој формули:

Вредност ризика = (Вредност утицаја) × (Вредност вероватноће догађања)

Вероватноћа догађања	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
	Утицај					

Табела 5: Матрица ризика

У складу с матрицом ризика, израчунава се ниво ризика (*Табела 6*) који може имати једну од следећих нивоа озбиљности:

Веома висок ризик
Висок ризик
Средњи ризик
Низак ризик
Веома низак ризик

Табела 6: Нивои озбиљности ризика

По завршетку овог процеса, сви ризици су идентификовани и квантификовани и приступа се следећим корацима:

- креирање регистра ризика, и
- одређивање прихватљивог ризика.

Сваки оператор ИКТ система од посебног значаја може дефинисати своје оквире, вредности и рангирање ризика у односу на своје потребе.

4.4.4. Одређивање прихватљивог ризика

Прихватљив ризик дефинише се као ниво ризика који оператор ИКТ система од посебног значаја сматра прихватљивим у контексту својих циљева, ресурса и пословних процеса. Овај ниво ризика одражава равнотежу између постизања циљева и прихватања одређеног степена изложености ризицима или недостатка мера заштите.

Пошто оператори ИКТ система од посебног значаја имају различиту толеранцију према ризику, дефинисање прихватљивог нивоа ризика зависи од специфичних пословних циљева и контекста. На основу утврђеног прихватљивог нивоа ризика, оператор ИКТ система од посебног значаја доноси одлуку о томе које ризике мора третирати, односно које ризике треба прихватити.

Оператор ИКТ система од посебног значаја дефинише критеријуме за утврђивање прихватљивог ризика, који служе као основа за доношење одлука о управљању ризицима.

4.4.5. Израда регистра ризика

Регистар ризика представља документ који оператори ИКТ система од посебног значаја користе за праћење, документовање и управљање идентификованим ризицима. Вредности ризика евидентиране у регистру ризика представљају инхерентни ризик, ризик процењен пре примене мера заштите. Преостали ризик након примене мера заштите документује се у регистру поступања са ризиком (*Табела 8*).

Регистар пружа свеобухватан преглед ризика, укључујући њихове карактеристике, вероватноћу, потенцијални утицај, стратегије поступања са ризиком и статус мера предузетих ради смањења или контроле ризика.

Регистар ризика (*Табела 7*) треба да садржи најмање следеће елементе:

- Назив ресурса;
- Претња;
- Вредности вероватноће догађања;
- Вредност утицаја;
- Вредност ризика (како је дефинисано у матрици)
- Имплементиране мере заштите;
- Поступање са ризиком (из тачке 4.5. ове методологије);
- Власник ризика.

Регистар ризика се редовно ажурира, посебно након периодичне процене ризика, како би се осигурало да информације остану актуелне и релевантне.

Ресурс	Претња	Вероватноћа догађања	Утицај	Ризик	Имплементиране мере заштите	Поступање са ризиком	Власник ризика
Сервер АБЦ	Пожар	1	4	4	Систем за гашење пожара	Прихваћен преостали ризик	Директор ИКТ

Табела 7: Регистар ризика

4.5. Поступање са ризиком

Поступање са ризиком обухвата активности и одлуке које оператор ИКТ система од посебног значаја предузима ради управљања идентификованим ризицима, са циљем њиховог смањења, контроле или прихватања.

Поступање са ризиком подразумева спровођење активности или доношење одлука у вези са идентификованим ризицима, њиховим нивоом озбиљности и начином поступања. Процес укључује примену различитих стратегија и мера с циљем смањења вероватноће настанка ризика и ублажавања последица које ризици могу имати на безбедност информација.

Поступање са ризиком може се спровести једном од следећих стратегија:

- прихватање ризика;
- пребацивање/дељење ризика;
- избегавање ризика;
- третман – обрада ризика.

Одлуку о одабиру стратегије за поступање са ризиком доноси власник ризика.

Идентификовани ризици и одабране стратегије поступања представљају основу за имплементацију мера заштите којима се утврђују конкретне техничке, организационе, административне и физичке мере сразмерне идентификованим ризицима, у складу са чланом 10. ЗИБ-а. На тај начин процена ризика остварује свој пуни оперативни ефекат.

4.5.1. Прихватање ризика

Прихватање ризика представља свесну одлуку оператора ИКТ система од посебног значаја да не предузима додатне мере за смањење или контролу одређених идентификованих ризика, већ да их задржи на одређеном, прихватљивом нивоу. Овај приступ подразумева да оператор ИКТ система од посебног значаја препознаје одређени степен изостанка безбедности или потенцијалну изложеност ризику, али оцењује да се ризик може толерисати у односу на постизање пословних циљева. Такође, прихватање ризика се примењује када су друге опције, попут преноса ризика или његовог потпуног избегавања, непрактичне или неекономичне.

Овај приступ захтева транспарентност, јасну комуникацију с релевантним учесницима, као и стално праћење и ревизију, како би се осигурало да одлуке о прихватању ризика подржавају дугорочну одрживост ИКТ система од посебног значаја.

4.5.2. Пребацивање или дељење ризика

Пребацивање или дељење ризика подразумева да оператор ИКТ система од посебног значаја дели управљање ризиком са трећом страном која је у могућности да га ефикасно контролише. То не значи да оператор ИКТ система од посебног значаја преноси одговорност за ризик, већ остаје примарно одговоран, али одређене активности у управљању ризиком се деле. Важно је напоменути да се може делити одговорност за управљање ризиком, али не и за последице које ризик може изазвати.

Најчешћи начини пребацивања или дељења ризика су:

- осигурање: примењује се као мера за ублажавање последица ризика, којом се уговара накнада штете (најчешће у новчаном облику или кроз замену изгубљеног ресурса) у случају материјализације ризика;

- поверавање трећој страни *(outsourcing)*: примењује се као организациона мера у оквиру које се одређене активности управљања или смањења ризика поверавају трећој страни, при чему одговорност за управљање ризиком остаје на оператору ИКТ система од посебног значаја.

4.5.3. Избегавање ризика

Када идентификовани ризици имају превисоку вредност или када трошкови спровођења других мера превазилазе очекиване користи, може се донети одлука о потпуном избегавању ризика. То се постиже повлачењем из планираних или постојећих активности, изменом начина обављања активности или променом услова под којима се делатност спроводи.

На пример, за ризике узроковане природом, једна од ефикасних мера може бити физичко пресељење објеката за обраду информација на локацију где је ризик елиминисан или под контролом. Међутим, у пракси, опција потпуног избегавања ризика ретко је примењива за операторе ИКТ система од посебног значаја.

4.5.4. Третман – обрада ризика

Циљ поступка модификације ризика је смањење идентификованих ризика на прихватљив ниво, због чега се ова опција често назива и умањење ризика.

Управљање ризиком врши се увођењем, уклањањем или прилагођавањем мера заштите, тако да преостали (*residual*) ризик може бити процењен као прихватљив, у складу са критеријумом прихватљивости ризика. При одабиру мера заштите, важно је узети у обзир трошкове набавке, имплементације, администрације, рада, праћења и одржавања, у односу на вредност ресурса који се штити.

Иако се модификација ризика често наводи као последња опција, она би у пракси требало да буде најчешће примењивана, јер показује да оператор ИКТ система од посебног значаја свесно утиче на ниво ризика коришћењем мера заштите.

Приликом примене ове стратегије, обавезно је израчунати преостали ризик након спровођења мера и евидентирати га у регистар ризика.

Када се одабере стратегија за третман ризика, оператор ИКТ система од посебног значаја документује регистар поступања са ризицима (*Табела 8*) који садржи најмање следеће информације:

- Ресурс;
- Претња;
- Ризик;
- Препоручена мера заштите (акциони план за имплементацију) и буџет потребан за имплементацију;
- Власник ризика;
- Рок за имплементацију;
- Одговорно лице за имплементацију;

- Преостали ризик.

Ресурс	Претња	Ризик	Препоручена мера заштите и буџет	Власник ризика	Рок за имплементацију	Одговорно лице за имплементацију	Преостали ризик

Табела 8: Регистар поступања са ризиком

Табела 8 попуњава се за све ризике без обзира на одабрану стратегију поступања. За ризике за које је одабрана стратегија смањења, обавезно се попуњавају колоне о препорученој мери заштите и року за имплементацију. За ризике за које је одабрана стратегија прихватања, преноса или избегавања, у колони преосталог ризика документује се ризик који остаје након донете одлуке.

4.5.5. Комуницирање ризика

Комуницирање ризика није стратегија поступања са ризиком у смислу претходних одељака, већ представља хоризонталну активност која се спроводи током целог процеса управљања ризицима и предуслов је за доношење информисане одлуке о избору стратегије поступања. Комуникација о ризицима представља процес размене и дељења информација о ризицима између доносилаца одлука и других релевантних учесника, с циљем постизања заједничког разумевања и договора о управљању ризицима. Ефикасна комуникација је важна, јер утиче на квалитет одлука и осигурава да сви укључени, како они који спроводе мере за управљање ризицима, тако и заинтересоване стране, разумеју разлоге доношења одлука и основ за спровођење одређених активности.

У оквиру ове методологије, конкретан корак у комуникацији о ризицима је одржавање радног састанка тима за процену ризика са заинтересованим учесницима након што су ризици идентификовани и вредновани. Током састанка прикупљају се повратне информације од учесника који су повезани са одређеним ризицима, како би се размотриле могуће стратегије њихове обраде и донеле информисане одлуке.

Оператор ИКТ система од посебног значаја треба да утврди временски оквир за доношење одлуке о начину поступања са ризиком у односу на ниво озбиљности (*Табела 9*).

Веома висок ризик – хитно третирање ризика
Висок ризик – третирање ризика у року од 3 месеца
Средњи ризик – третирање ризика у року од 12 месеци
Низак ризик – прихватање ризика уз редовну

евалуацију за промене
Веома низак ризик - прихватање ризика

Табела 9: Препоручени рокови за доношење одлуке о начину поступања са ризиком

Временски оквири за третирање ризика наведени у табели представљају препоручене оквире за доношење одлуке о начину поступања са ризиком, а не обавезујуће рокове за реализацију мера. Уколико природа ризика не омогућава реализацију у наведеном року, оператор ИКТ система од посебног значаја документује разлоге и дефинише реалан рок за реализацију. Оператор ИКТ система од посебног значаја може дефинисати сопствене рокове у складу са својим пословним контекстом и расположивим ресурсима.

4.6. Праћење ризика

Праћење ризика представља континуиран процес којим се обезбеђује да процена ризика, примењене мере и дефинисани критеријуми остану релевантни у односу на промене у контексту оператора ИКТ система од посебног значаја.

Процена ризика није једнократан или статичан, већ континуиран и репетитиван процес. Редовном проценом ризика, неки ризици могу у потпуности нестати, неки се могу смањити (нпр. применом мера заштите), док се нови ризици могу појавити.

Стално праћење и преиспитивање неопходни су како би се обезбедило да контекст, исход процене ризика и поступања са ризиком, као и планови органа управљања остану релевантни и адекватни за дате околности. Оператор ИКТ система од посебног значаја треба редовно да верификује да су критеријуми који се користе за мерење ризика и његових елемената још увек валидни и конзистентни са пословним циљевима, стратегијама и политикама, и да се промене пословног контекста узимају у обзир на адекватан начин током процеса управљања ризиком.

Процену ризика потребно је спроводити најмање једном годишње или одмах након значајних промена у ИКТ системима и процесима које они подржавају. На тај начин оператор ИКТ система од посебног значаја обезбеђује континуирано сагледавање постојећих ризика и благовремено и систематично управљање мерама за ублажавање и отклањање утврђених ризика.

5. Минимални захтеви усклађености у складу са чланом 11. став 5. ЗИБ-а

Постојећа интерна процена ризика сматра се усклађеном са овом методологијом ако садржи следеће елементе:

5.1. Опсег процене

Документовано дефинисан опсег (контекст) процене, период на који се процена односи и границе система који је предмет анализе.

5.2. Регистар ресурса

Регистар ресурса са најмање следећим подацима: назив, категорија, власник и процена вредности по CIA триади. Категорије ресурса не морају бити идентичне категоријама из одељка 4.2, довољно је да покривају исте врсте ресурса.

5.3. Идентификација претњи

Документована идентификација претњи релевантних за ресурсе у опсегу процене, са назнаком извора претње и циљаног ресурса. Оператор ИКТ система од посебног значаја може користити сопствени каталог претњи уколико покрива исте основне категорије претњи као Каталог претњи из ове методологије.

5.4. Процена вероватноће и утицаја

Документована процена вероватноће и утицаја за сваку идентификовану претњу по ресурсу, на основу унапред дефинисаних скала. Скале не морају бити идентичне скалама из одељака 4.4.1 и 4.4.2, под условом да су документоване пре спровођења процене, доследно примењене и омогућавају разврставање ризика у најмање три нивоа. Критеријуми за процену утицаја морају укључивати последице по поверљивост, интегритет и расположивост.

5.5. Регистар ризика

Регистар ризика са најмање следећим елементима: идентификована претња, погођени ресурс, процена вероватноће догађања, процена утицаја, вредност ризика и власник ризика. Регистар мора јасно назначити да ли приказане вредности представљају инхерентни или преостали ризик. Вредност ризика може бити изражена квалитативно или квантитативно, уз услов да је примењени метод документован.

5.6. Поступање са ризиком

Документована одлука о поступању са сваким идентификованим ризиком, са назнаком одабране стратегије, роком и власником ризика. Одлука о прихватању ризика мора бити експлицитно документована и одобрена од стране органа управљања.

5.7. Прихватљиви ниво ризика

Документовано дефинисан прихватљиви ниво ризика са критеријумима за одређивање које ризике оператор прихвата без даљег поступања. Критеријуми морају бити утврђени пре спровођења процене и одобрени од стране органа управљања.

5.8. Периодична ревизија

Документовано дефинисана динамика периодичне ревизије, не ређа од једном годишње, са условима за ванредну ревизију у случају значајних промена у претњама, рањивостима, технолошком или организационом окружењу.

ПРИЛОГ 2.

КАТАЛОГ ПРЕТЊИ ИНФОРМАЦИОНЕ БЕЗБЕДНОСТИ

Увод

Каталог претњи информационе безбедности пружа преглед претњи којима може бити изложена имовина оператора ИКТ система од посебног значаја.

Каталог претњи информационе безбедност (у даљем тексту: Каталог претњи) омогућава идентификацију широког спектра претњи са којима се оператор ИКТ система од посебног значаја може сусрести, и помаже у разумевању могућих последица које те претње могу имати на безбедност информационих система.

Каталог претњи се користи у оквиру **процеса 4.3. Идентификација претњи** у складу са методологијом, у коме се врши препознавање претњи које могу негативно утицати на ИКТ системе, пословне процесе и имовину оператора ИКТ система од посебног значаја.

Каталог претњи је креиран на основу докумената *"Detailed Catalogues – IT Security Risk Management Methodology v1.2"* и *" IT-Grundschutz-Compendium"*. Каталог претњи не представља збир свих претњи из наведених извора, већ листу претњи које су непосредно примењиве на процену ризика коју спроводе оператори ИКТ система од посебног значаја.

Свака претња у Каталогу претњи је представљена на следећи начин:

<table>
<tr><td colspan="3">Назив претње</td></tr>
<tr><td>Врста имовине на коју претња утиче
(локација, запослени, хардвер, софтвер, информације, треће стране)</td><td>Параметар безбедности на који претња утиче
(поверљивост, интегритет, расположивост)</td><td>Извор претње
(намерно, случајно, природно)</td></tr>
<tr><td colspan="3">Опис претње</td></tr>
<tr><td colspan="3">Мапирање на постојеће каталоге</td></tr>
</table>

Каталог претњи

1. Природне претње

1.1. Ватра

Ватра, пожар		
Локација Хардвер	Расположивост	Природно
Ватра, било случајним или намерним деловањем, може уништити локацију на којој је смештен ИКТ систем или коришћени хардвер.		
ITSRM: [N.1] *Fire* *IT-Grundschutz-Compendium: G 0.1 Fire*		

1.2. Вода

Вода		
Локација Хардвер	Расположивост	Природно
Вода, било случајним или намерним деловањем, може оштетити или привремено онеспособити локацију на којој је смештен ИКТ систем или коришћени хардвер.		
ITSRM: [N.2] *Water* *IT-Grundschutz-Compendium: G 0.3 Water*		

1.3. Неповољни климатски услови

Неповољни климатски услови		
Локација Хардвер	Расположивост	Природно
Присутност прашине, корозивних или отровних гасова у ваздуху.		
ITSRM: [I.3] *Environmental pollution* *IT-Grundschutz-Compendium: G 0.2 Unfavourable Climatic Conditions*		

1.4. Природне катастрофе

Природне катастрофе

Локација Хардвер	Расположивост	Природно
Природне појаве које имају разоран утицај на људе и инфраструктуру. Узроци могу бити сеизмичког, климатског или вулканског порекла, укључујући земљотресе, поплаве, клизишта, цунамије, лавине и вулканске ерупције. Примери екстремних метеоролошких појава су олује са грмљавином, урагани и циклони. Изложеност овим ризицима зависи од географске локације ИКТ система од посебног значаја.		
ITSRM: [N.*] *Other natural disasters* *IT-Grundschutz-Compendium: G 0.5 Natural Disasters*		

2. Индустријске претње

2.1. Неповољни услови температуре и/или влажности

Неповољни услови температуре и/или влажности		
Хардвер Локација ИКТ услуге	Расположивост	Природно
Недостаци у климатизацији простора који превазилазе радне границе опреме, попут прекомерне топлоте, ниске температуре, превелике влаге и сл.		
ITSRM: [I.7] *Unsuitable temperature or humidity conditions*		

2.2. Прекид енергетског напајања

Прекид енергетског напајања		
Локација Хардвер ИКТ услуге	Расположивост	Природно
Прекид у снабдевању електричном енергијом од стране оператора дистрибутивне мреже или енергетских компанија. Већина ових поремећаја је веома кратка, често краћа од једне секунде, али чак и прекид од само 10 ms може довести до поремећаја у раду ИТ система.		
ITSRM: [I.6] *Power interruption* *IT-Grundschutz-Compendium: G 0.8 Failure or Disruption of the Power Supply*		

2.3. Електромагнетно загађење

Електромагнетно загађење

Локација Хардвер ИКТ услуге	Расположивост Интегритет	Намерно Случајно Природно
Радио-сметње, магнетна поља, ултраљубичасто зрачење и сличне појаве које могу утицати на рад ИКТ система. У ову категорију спадају и топлотни ефекти изазвани оштећењем опреме или неповољним временским условима, као и оштећења настала услед изузетно јаких електромагнетних поља. Такође, обухвата присуство уређаја који генеришу топлоту и могу довести до квара или уништења опреме, деловање особа које користе електромагнетно зрачење ради ометања комуникација или рада уређаја, као и електромагнетне импулсе из нуклеарних извора.		
ITSRM: [I.4] *Electromagnetic pollution* *IT-Grundschutz-Compendium: G 0.12 Electromagnetic Interference*		

2.4. Квар хардвера или софтвера

Квар хардвера или софтвера		
Хардвер Софтвер	Расположивост	Намерно Случајно Природно
Кварови на хардверу или софтверу могу бити последица грешака у производњи или се могу појавити током рада система. Код система специфичне намене понекад је тешко утврдити да ли је квар физичког или логичког порекла, али та разлика најчешће нема значајан утицај на последице. Такође, у ову категорију спадају намерни физички или логички напади који доводе до квара опреме.		
ITSRM: [I.5] *Hardware or software failure* *IT-Grundschutz-Compendium: G 0.25 Failure of Devices or Systems*		

2.5 Квар комуникационих услуга

Квар комуникационих услуга		
ИКТ услуга	Расположивост	Случајно Намерно
Сметње, прекиди или неадекватно димензионисање телекомуникационих услуга (телефонија, приступ интернету, мрежна инфраструктура). У ову категорију спада и саботажа или ометање телекомуникационих инсталација од стране особа које имају приступ опреми (разводни ормари, спољњи каблови и слично).		
ITSRM: [I.8] *Communications services failure* *IT-Grundschutz-Compendium: G 0.9 Failure or Disruption of Communication Networks*		

2.6. Прекид основних услуга које су предмет набавке или других услуга

Прекид основних услуга које су предмет набавке или других услуга		
ИКТ услуга Локација	Расположивост	Случајно Намерно
Прекид у набавци услуге или ресурси од којих зависи рад опреме, на пример: папир за штампач, тонер, клима уређаји и слично.		
ITSRM: [I.9] *Interruption of other services or essential supplies* *IT-Grundschutz-Compendium: G 0.10 Failure or Disruption of Supply Networks*		

2.7. Деградација медијума

Деградација медијума		
Хардвер Локације ИКТ услуге	Расположивост	Случајно Намерно
Логички или физички догађаји који изазивају неисправност опреме (нпр. медијума за чување података) или настају као последица протока времена.		
ITSRM: [I.10] *Media degradation*		

2.8. Ризик примене енкрипције у условима развоја квантног рачунарства

Ризик примене енкрипције у условима развоја квантног рачунарства		
Софтвер ИКТ услуге	Поверљивост Интегритет	Случајно Намерно
Будућа немогућност постојећих криптографских алгоритама (нпр. RSA, ECC) да обезбеде поверљивост и интегритет података услед очекиване рачунарске моћи квантних рачунара, који могу решити математичке проблеме (попут факторизације простих бројева) на којима почива савремена асиметрична криптографија. Ово ствара ризик од накнадног дешифровања данас прикупљених података *("Harvest Now, Decrypt Later")* и захтева правовремену миграцију на пост-квантну криптографију.		

2.9. Пренос злонамерног софтвера применом преносних носача података

Пренос злонамерног софтвера применом преносних носача података

Хардвер Софтвер Запослени ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно Намерно
Уношење малициозног кода у информациони систем путем физичких медијума за складиштење (USB меморије, екстерни дискови, CD/DVD, мобилни уређаји), чиме се заобилазе мрежне мере заштите. Ово укључује аутоматско покретање малвера приликом повезивања уређаја, искоришћавање рањивости драјвера или намерно остављање инфицираних медијума на јавним местима ради компромитовања система *(Baiting* напад).		
IT-*Grundschutz-Compendium: OPS.1.1.4 Protection Against Malware*		

2.10. Отицање компромитујућег електромагнетног зрачења

Отицање компромитујућег електромагнетног зрачења		
Хардвер ИКТ услуге	Поверљивост Интегритет	Случајно Намерно
Нежељена емисија електромагнетних сигнала из информационо-комуникационе опреме (нпр. рачунари, каблови, штампачи) која може бити прикупљена и анализирана од стране нападача у близини ради обнављања обрађених података (TEMPEST напад).		
IT-*Grundschutz-Compendium: G 0.13 Interception of Compromising Interference Signals*		

3. Грешке и ненамерни пропусти

3.1. Корисничке грешке

Корисничке грешке		
Хардвер Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Грешке корисника приликом коришћења услуга, укључујући радне грешке, грешке при уносу података или при употреби хардвера и софтвера.		
ITSRM: [E.1] *User errors*		

3.2. Грешке администратора система/безбедности

Грешке администратора система/безбедности		
Хардвер Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Грешке запосленог који је одговоран за инсталацију и рад система или безбедности. Администратор система или безбедности може направити радну грешку, грешку при уносу података или приликом коришћења хардвера или софтвера.		
ITSRM: [E.2] *System/Security administrators errors*		

3.3. Грешке праћења (записи)

Грешке праћења (записи)		
Хардвер Софтвер ИКТ услуге	Интегритет	Случајно
Неправилни записи о активностима, укључујући недостатак записа, непотпуне записе или нетачно датиране записе (управљање логовима).		
ITSRM: [E.3] *Monitoring errors (logs)* IT- *Grundschutz-Compendium: OPS.1.1.5 Logging*		

3.4. Грешке у конфигурацији

Грешке у конфигурацији		
Хардвер Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Унос погрешних конфигурационих података. У већини случајева сва имовина зависи од исправне конфигурације, која је у надлежности администратора и укључује приступне привилегије, активности корисника, евиденцију активности, рутирање и слично.		
ITSRM: [E.4] *Configuration errors*		

3.5. Организациони недостаци

Организациони недостаци

Запослени	Расположивост	Случајно
Ситуације у којима није јасно ко, шта и када треба да предузме, укључујући мере које се односе на имовину или извештавање управљачкој хијерархији. У ову категорију спадају неусклађене радње, грешке настале пропустом и слични инциденти.		
ITSRM: [E.7] *Organizational deficiencies* IT- *Grundschutz-Compendium: ORP.1 Organisation*		

3.6. Ширење злонамерног софтвера (малвера)

Ширење злонамерног софтвера (малвера)		
Софтвер	Поверљивост Интегритет Расположивост	Случајно
Ненамерно ширење вируса, шпијунског софтвера, црва, тројанаца, логичких бомби и других облика злонамерног кода.		
ITSRM: [E.8] *Malware diffusion* IT- *Grundschutz-Compendium: G 0.39 Malware*		

3.7. Случајна измена података

Случајна измена података		
Хардвер Софтвер Запослени Локације ИКТ услуге	Интегритет	Случајно
Ненамерна измена података. Ова претња се примарно односи на саме податке, док за информације похрањене на дигиталним медијумима постоје специфичне претње.		
ITSRM: [E.15] *Accidental alteration of the information*		

3.8. Уништење података

Уништење података		
Хардвер Софтвер Запослени Локације ИКТ услуге	Расположивост	Случајно

Ненамерни губитак података. Ова претња се примарно односи на саме податке, док за информације похрањене на дигиталним медијумима постоје специфичне претње.
ITSRM: [E.18] *Destruction of information* IT- *Grundschutz-Compendium: G 0.45 Data Loss*

3.9. Цурење података

Цурење података		
Хардвер Софтвер Запослени Локације ИКТ услуге	Поверљивост	Случајно
Неовлашћено разоткривање информација због непажње или индискреције. У ову категорију спадају вербална индискреција, непажљиво руковање електронским медијумима, штампаним копијама и сличним облицима података.		
ITSRM: [E.19] *Information leaks* IT- *Grundschutz-Compendium: G 0.46 Loss of Integrity of Sensitive Information*		

3.10. Рањивост софтвера

Рањивост софтвера		
Софтвер	Поверљивост Интегритет Расположивост	Случајно
Грешке у коду које изазивају неправилно функционисање софтвера без намере корисника, али које могу имати последице по поверљивост података, интегритет, расположивост или оперативну способност система.		
ITSRM: [E.20] *Software vulnerabilities* IT- *Grundschutz-Compendium: G 0.28 Software Vulnerabilities or Errors*		

3.11. Грешке у одржавању/ажурирању софтвера

Грешке у одржавању/ажурирању софтвера		
Софтвер	Интегритет Расположивост	Случајно
Грешке у процедурама или контролама током ажурирања система, укључујући познате грешке које је произвођач исправио, али које и даље могу утицати на употребу система. Обухватају и грешке у дизајну, инсталационе грешке или радне		

грешке настале током модификација, које могу изазвати неправилно функционисање система.
ITSRM: [E.21] *Defects in software maintenance/updating* IT- *Grundschutz-Compendium: OPS.1.1.3 Patch and Change Management*

3.12. Квар система због исцрпљености ресурса

Квар система због исцрпљености ресурса		
Хардвер ИКТ услуге	Расположивост	Случајно
Недостатак довољног броја ресурса може изазвати квар система када је радно оптерећење прекомерно. У ову категорију спада преоптерећење простора за чување података (нпр. резервни простор, складиштење поштанских сандучића, радни простор), као што је случај са засићеним поштанским сандучићем када је његов власник дуже одсутан. Такође, укључује и засићење изазвано преоптерећењем система када се истовремено обрађује превише захтева.		
ITSRM: [E.24] *System failure due to exhaustion of resources* IT- *Grundschutz-Compendium: G 0.27 Lack of Resources*		

3.13. Губитак опреме

Губитак опреме		
Хардвер	Поверљивост Расположивост	Случајно
Губитак опреме директно доводи до недостатка ресурса за пружање услуга, односно до нерасположивости тих услуга. Све врсте опреме могу бити погођене. У случају рачунара или сервера који садрже податке, може доћи и до цурења информација. У ову категорију спада и неовлашћено прибављање електронских медијума (хард-дискови, дискови за резервне копије, УСБ кључеви, ЗИП дискови, уклоњиви дискови и слично) или папирних копија (пописи, непотпуни исписи, поруке и слично) које су намењене рециклирању, а које садрже осетљиве информације.		
ITSRM: [E.25] *Equipment loss* IT- *Grundschutz-Compendium: G 0.17 Loss of Devices, Storage Media and Documents*		

3.14. Недостатак запослених

Недостатак запослених		
Запослени	Расположивост	Случајно
Изненадна нерасположивост квалификованог или одговорног запосленог због		

болести или других околности ван њихове контроле, што може утицати на континуитет рада и извршавање критичних функција.
ITSRM: [E.28] *Staff shortage* IT- *Grundschutz-Compendium: G 0.33 Shortage of Personnel*

3.15. Недостатак свести и специфичних знања о информационој безбедности

Недостатак свести и специфичних знања о информационој безбедности		
Запослени	Расположивост	Случајно
Оператор ИКТ система од посебног значаја не поседује довољну стручну компетенцију у области информационе безбедности, а не постоје ни програми за подизање свести запослених о значају и принципима безбедног руковања информацијама.		
IT- *Grundschutz-Compendium: ORP.3 Awareness and Training in Information Security*		

3.16. Неадекватно управљање привилегијама

Неадекватно управљање привилегијама		
Софтвер Запослени	Поверљивост Интегритет	Случајно
Ненамерно додељивање прешироких права приступа корисницима која превазилазе њихове пословне потребе.		
IT- *Grundschutz-Compendium: G 0.31 Incorrect Use or Administration of Devices and Systems*		

3.17. Недостатак организованог система управљања информационом безбедношћу

Недостатак организованог система управљања информационом безбедношћу		
Запослени	Расположивост	Случајно
Оператор ИКТ система од посебног значаја нема успостављен систем управљања информационом безбедношћу, нити су јасно дефинисане улоге и одговорности за планирање, спровођење и надзор активности у овој области.		
IT- *Grundschutz-Compendium: ISMS.1 Security Management*		

3.18. Недостатак система за детекцију инцидената

Недостатак система за детекцију инцидената		
Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Током свакодневних ИКТ операција може доћи до различитих инцидената и техничких грешака. Постоји ризик да запослени не препознају безбедносне инциденте међу њима, што може довести до тога да напад или покушај напада прође непримећен и остане без правовремене реакције.		
IT- *Grundschutz-Compendium: DER.1 Detecting Security-Relevant Events*		

3.19. Неадекватно планирање континуитета пословања

Неадекватно планирање континуитета пословања		
Софтвер Запослени ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Код оператора ИКТ система од посебног значаја не постоји довољно развијен нити организован процес планирања који би обезбедио континуитет пословања у случају непожељних догађаја који доводе до нерасположивости ИКТ система. Због изостанка дефинисаних процедура и припремљених резервних сценарија, оператор ИКТ система од посебног значаја остаје рањив на прекиде рада и продужену нерасположивост услуга.		
IT- *Grundschutz-Compendium: DER.4 Business Continuity Management*		

3.20. Неадекватно коришћење или изостанак коришћења криптографских контрола

Неадекватно коришћење или изостанак коришћења криптографских контрола		
Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Код оператора ИКТ система од посебног значаја не постоји одговарајућа примена криптографских механизама који би требало да обезбеде да се осетљиви подаци, било у мировању или у транзиту, не преносе и не чувају у читљивом и незаштићеном облику. Овакав недостатак излаже информације ризику од неовлашћеног приступа и компромитовања.		

IT- *Grundschutz-Compendium: CON.1 Crypto Concept*

3.21. Грешке у процедурама резервних копија (*Backup*)

Грешке у процедурама резервних копија (*Backup*)		
Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно
Неуспех у прављењу копија или недостатак провере њихове исправности.		
IT- *Grundschutz-Compendium: CON.3 Backup Concept*		

4. Намерни напади

Намерни напади су намерни пропусти које узрокују запослени или нападачи.

4.1. Манипулација евиденцијом активности (логови)

Манипулација евиденцијом активности (логови)		
Хардвер Софтвер ИКТ услуге	Интегритет	Намерно
Намерно мењање, брисање или прикривање логова и других записа активности ради уклањања трагова, доказа или индикатора компромитације, чиме се отежава откривање и анализа безбедносних инцидената.		
ITSRM: [A.3] *Manipulation of activity records* IT- *Grundschutz-Compendium: OPS.1.1.5 Logging*		

4.2. Манипулација конфигурацијским датотекама

Манипулација конфигурацијским датотекама		
Хардвер Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Намерно
Неправилно подешавање конфигурационих параметара на системима, мрежној опреми или апликацијама. Већина ИКТ имовине зависи од исправне конфигурације, која је у потпуности у рукама администратора. Овде спадају грешке у додели приступних привилегија, конфигурацији сервиса и активности, вођењу евиденције догађаја, мрежном усмеравању и другим кључним поставкама, што може довести до		

нарушавања безбедности или нерасположивости система.
ITSRM: [A.4] *Manipulation of the configuration files*

4.3. Маскирање идентитета

Маскирање идентитета		
Софтвер Хардвер ИКТ услуге	Поверљивост Интегритет	Намерно
Нападач се представља као овлашћени корисник система како би искористио његове привилегије за неовлашћене активности, укључујући приступ информацијама, манипулацију подацима, обману или превару. Претњу могу представљати запослени, као и особе изван ИКТ система од посебног значаја.		
ITSRM: [A.5] *Masquerading of identity* IT- *Grundschutz-Compendium: G 0.36 Identity theft*		

4.4. Злоупотреба права приступа

Злоупотреба права приступа		
Софтвер ИКТ услуге Локације	Поверљивост Интегритет Расположивост	Намерно
Корисници имају одређени ниво привилегија који је додељен ради обављања њихових задатака. Злоупотреба настаје када те привилегије користе за активности изван својих одговорности, укључујући неовлашћен приступ систему ради измене, брисања или додавања функционалности, као и извођење других неовлашћених радњи.		
ITSRM: [A.6] *Abuse of access privileges* IT- *Grundschutz-Compendium: G 0.32 Misuse of Authorisation*		

4.5. Злоупотреба ресурса

Злоупотреба ресурса		
Софтвер ИКТ услуге Локације	Поверљивост Интегритет Расположивост	Намерно

Коришћење ресурса ИКТ система у сврхе које нису планиране или одобрене, обично у личном интересу, укључујући играње игара, личне претраге на интернету, личне базе података, инсталирање личних програма, чување личних података и сличне активности.
ITSRM: [A.7] *Misuse*

4.6. Ширење малвера

Ширење малвера		
Софтвер	Поверљивост Интегритет Расположивост	Намерно
Свесно и циљано уношење или дистрибуирање вируса, шпијунског софтвера, црва, тројанаца, логичких бомби и других облика малвера ради нарушавања поверљивости, интегритета или расположивости система и података.		
ITSRM: [A.8] *Malware diffusion* IT- *Grundschutz-Compendium: G 0.39 Malware*		

4.7. Неовлашћен приступ

Неовлашћен приступ		
Софтвер Хардвер ИКТ услуге Локација	Поверљивост Интегритет	Намерно
Нападач успева да приступи ресурсима система без потребне ауторизације, најчешће искоришћавањем рањивости у механизмима идентификације и аутентификације. Особа изнутра или споља приступа информационом систему и користи његове услуге како би извршила операције, приступила подацима или их украла.		
ITSRM: [A.11] *Unauthorized access* IT- *Grundschutz-Compendium: G 0.23 Unauthorised Access to IT Systems*		

4.8. Анализа саобраћаја

Анализа саобраћаја		
ИКТ услуге	Поверљивост	Намерно
Без потребе да прегледа садржај комуникације, нападач може доћи до значајних закључака анализом њеног порекла, одредишта, обима и учесталости размене података. Ова техника, позната као „праћење саобраћаја“, може открити обрасце		

комуникације, потенцијалне циљеве и осетљиве односе унутар система.
ITSRM: [A.12] *Traffic analysis* IT- *Grundschutz-Compendium: NET.1.2 Network Management*

4.9. Прислушкивање

Прислушкивање		
Хардвер Софтвер Запослени ИКТ услуге	Поверљивост	Намерно
Нападач стиче приступ информацијама које му не припадају, при чему се сам садржај информација не мења. Особа која има приступ комуникационој опреми или медијумима, или се налази унутар домета комуникационог преноса, може користити специјализовану (често врло скупу) опрему за пресретање, слушање, складиштење и анализирање пренетих података или гласовне комуникације.		
ITSRM: [A.14] *Eavesdropping* IT- *Grundschutz-Compendium: G 0.15 Eavesdropping*		

4.10. Намерна измена информација

Намерна измена информација		
Хардвер Софтвер Локације Запослени ИКТ услуге	Интегритет	Намерно
Свесна и циљана измена података ради остваривања користи, обмане или наношења штете информационом систему, оператору ИКТ система од посебног значаја или корисницима.		
ITSRM: [A.15] *Deliberate alteration of the information* IT- *Grundschutz-Compendium: G 0.22 Manipulation of Information*		

4.11. Уништавање информација

Уништавање информација		
Хардвер Софтвер Локације	Расположивост	Намерно

Запослени ИКТ услуге		
Свесно и циљано уништавање података ради остваривања користи, прикривања трагова или наношења штете оператору ИКТ система од посебног значаја, корисницима или информационом систему.		
ITSRM: [A.18] *Destruction of information*		

4.12. Откривање информација

Откривање информација		
Хардвер Софтвер Локације Запослени ИКТ услуге	Поверљивост	Намерно
Свесно и циљано нарушавања поверљивости података ради остваривања користи, прикривања трагова или наношења штете оператору ИКТ система од посебног значаја, корисницима или информационом систему.		
ITSRM: [A.19] *Disclosure of information* IT- *Grundschutz-Compendium: G 0.19 Disclosure of Sensitive Information*		

4.13. Манипулација софтвером

Манипулација софтвером		
Софтвер	Поверљивост Интегритет Расположивост	Намерно
Свесна и циљана измена функционалности програма ради остваривања посредне користи када га овлашћена особа користи. Нападач убацује програм, код или наредбе како би изменио уобичајено понашање апликације или додао неовлашћену функционалност оперативном систему. Ова претња може угрозити информациони систем у било којој фази његовог животног циклуса, током дизајна, тестирања, производње, рада, транспорта или одржавања.		
ITSRM: [A.22] *Software manipulation* IT- *Grundschutz-Compendium: G 0.21 Manipulation with Hardware or Software*		

4.14. Манипулација хардвером

Манипулација хардвером		
Хардвер	Поверљивост Расположивост	Намерно
Свесна и циљана измена функционалности хардверске опреме ради остваривања посредне користи у тренутку када је користи овлашћена особа. Таква манипулација може укључивати додавање, уклањање или модификовање компоненти или функција са циљем нарушавања интегритета, поузданости или безбедности система.		
ITSRM: [A.23] *Hardware manipulation* IT- *Grundschutz-Compendium: G 0.21 Manipulation with Hardware or Software*		

4.15. Ускраћивање услуга

Ускраћивање услуга		
Хардвер ИКТ услуге	Расположивост	Намерно
Недостатак расположивих ресурса доводи до квара система када је радно оптерећење превелико. Нападач може намерно изазвати ово стање симулирањем интензивне потражње за ресурсима кроз континуирано слање великог броја захтева, што резултира успоравањем или потпуном недоступношћу услуга.		
ITSRM: [A.24] *Denial of services* G 0.40 *Denial of Service*		

4.16. Крађа опреме

Крађа опреме		
Хардвер ИКТ услуге	Поверљивост Расположивост	Намерно
Крађа опреме доводи до губитка ресурса потребних за пружање услуга, што може резултирати делимичном или потпуном недоступношћу система. Било која врста опреме може бити мета крађе, при чему су најчешће погођени уређаји и информациони медијуми који садрже податке. Крађу могу извршити запослени унутар ИКТ система од посебног значаја, особе ван оператора ИКТ система од посебног значаја или привремено ангажовано особље, што утиче на ниво расположивости украденој опреми и потенцијалне последице, укључујући ризик од цурења информација.		
ITSRM: [A.25] *Theft* IT- *Grundschutz-Compendium: G 0.16 Theft of Devices, Storage Media and Documents*		

4.17. Деструктивни напад

Деструктивни напад		
Хардвер Запослени Локације и просторије ИКТ услуге	Расположивост	Намерно
Вандализам, тероризам, војна акција, итд. Намерно деловање које доводи до оштећења, уништења или ометања рада ИКТ система и инфраструктуре. Ову претњу могу извршити запослени, особе ван оператора ИКТ система од посебног значаја или привремено ангажовани.		
ITSRM: [A.26] *Destructive attack*		

4.18 Изнуђивање (*Ransomware*)

Изнуђивање (*Ransomware*)		
Хардвер Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Намерно
Намерно закључавање података уз захтев за откупнину и претњу да ће подаци бити јавно објављени.		

4.19. Социјални инжењеринг

Социјални инжењеринг		
Запослени	Поверљивост Интегритет Расположивост	Намерно
Манипулисање особама које из добре намере или поверења извршавају радње које су у интересу трећих страна или нападача, чиме се омогућава неовлашћен приступ, стицање информација или наношење штете систему.		
ITSRM: [A.30] *Social engineering* IT- *Grundschutz-Compendium: G 0.42 Social Engineering*		

4.20. Компромитација и злоупотреба МФП уређаја (штампачи, скенери, копири)

Компромитација и злоупотреба МФП уређаја (штампачи, скенери, копири)

Хардвер Софтвер	Поверљивост Интегритет Расположивост	Намерно
Злонамерни актери циљају мрежне уређаје за штампу, скенирање и копирање (МФП) као потенцијалне улазне тачке у ИКТ систем оператора. Ови уређаји су често занемарени у процесу управљања безбедношћу, а могу садржати осетљиве информације у интерној меморији, омогућити неовлашћени приступ мрежи или бити компромитовани путем застарелог *firmware*-а.		

5. Претње повезане са коришћењем спољних услуга (треће стране, услуге рачунарства у клауду)

5.1. Закључавање

Закључавање		
ИКТ услуге	Расположивост	Случајно
Претерано ослањање на услуге једног пружаоца може отежати или онемогућити промену пружаоца у будућности. Миграција на другог добављача може постати технички и организационо врло захтевна, чиме се повећава ризик од застоја или губитка контроле над кључним услугама.		
ITSRM: [SR.1] *Lock-in*		

5.2. Губитак управљања

Губитак управљања		
ИКТ услуге	Расположивост	Случајно Намерно
Губитак контроле и управљања може озбиљно угрозити стратегију оператора ИКТ система од посебног значаја и способност остваривања њених мисија и циљева. Таква ситуација може довести до неиспуњавања безбедносних захтева, нарушавања поверљивости, интегритета и расположивости података, као и до смањења перформанси и квалитета пружених услуга.		
ITSRM: [SR.2] *Loss of governance*		

5.3. Грешке код изолације

Грешке код изолације

ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно Намерно Природно
Ова категорија претње обухвата кварове у механизмима који обезбеђују одвајање чувања података, меморије, мрежног усмеравања и чак репутације између различитих корисника заједничке инфраструктуре. Последице могу укључивати губитак вредних или осетљивих података, нарушавање угледа и прекид пружања услуга.		
ITSRM: [SR.7] *Isolation failure*		

5.4. Несигурно или неефикасно брисање података

Несигурно или неефикасно брисање података		
ИКТ услуге	Поверљивост	Случајно Намерно
Брисање података са складишта не значи нужно да су подаци трајно уклоњени са уређаја или резервног медијума. Ако складиштење података на диску није шифровано, подацима касније може приступити други корисник, трећа страна (*outsourcing)* или пружалац услуга, што представља ризик од неовлашћеног приступа.		
ITSRM: [SR.11] *Insecure or ineffective deletion of data*		

5.5. Судски позив и е-откривање

Судски позив и е-откривање		
ИКТ услуге	Поверљивост Расположивост	Случајно Намерно
Органи за спровођење закона могу од оператера ИКТ система од посебног значаја захтевати достављање података у вези са кривичним поступцима, или информације могу бити потребне током грађанских парница. У неким случајевима, медијуми за чување података или други хардвер могу бити заплењени као доказ.		
ITSRM: [SR.19] *Subpoena and e-discovery*		

5.6. Ризик од промене јурисдикције

Ризик од промене јурисдикције		
ИКТ услуге	Поверљивост	Случајно

	Расположивост	Намерно
Када се подаци чувају или обрађују у дата центру који се налази у земљи која није земља корисника, промена надлежности и применљивих закона може значајно утицати на безбедност информација. Подаци клијената могу бити распоређени у више јурисдикција, од којих неке могу представљати висок ризик. Ако се дата центри налазе у земљама са високим ризиком, на пример у државама без владавине права, са непредвидивим правним оквиром и спровођењем, аутократским режимима или државама које не поштују међународне споразуме, локалне власти могу приступити подацима или извршити акције које угрожавају њихову сигурност.		
ITSRM: [SR.20] *Risk from changing of jurisdiction*		

5.7. Ризици заштите података о личности

Ризици заштите података о личности		
ИКТ услуге	Поверљивост	Случајно
Закон о заштити података о личности заснива се на претпоставци да је увек јасно где се налазе лични подаци, ко их обрађује и ко је одговоран за њихову обраду. Дистрибуирана окружења пружалаца услуга могу бити у супротности са овом претпоставком. Обрада података у другој земљи може изазвати проблеме у вези са применом законодавства о заштити података, а надлежни органи за заштиту података могу такву обраду сматрати незаконитом.		
ITSRM: [SR.21] *Data protection risks*		

5.8. Анализа инцидената и форензичка подршка

Анализа инцидената и форензичка подршка		
ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно Намерно
У случају инцидента, апликације и услуге хостоване код пружаоца услуга се тешко истражују јер се записивање може дистрибуирати на више сервера и дата центара, који се налазе у различитим земљама и подлежу различитим прописима.		
ITSRM: [SR.38] *Incidence analysis and forensics support* IT-*Grundschutz-Compendium: DER.2.2 Provisions for IT Forensics*		

5.9. Напади уз коришћење вештачке интелигенције

Напади уз коришћење вештачке интелигенције		
Софтвер Запослени ИКТ услуге	Интегритет Расположивост	Намерно
Злонамерни актери користе алате и технике вештачке интелигенције за аутоматизацију, убрзавање или унапређење сајбер напада на ИКТ системе. Ови напади укључују аутоматизовано генерисање малициозног кода, креирање уверљивог фишинг садржаја прилагођеног конкретним метама, заобилажење мера заштите и убрзано откривање рањивости. Употреба вештачке интелигенције значајно повећава обим, брзину и прецизност напада, чинећи их тежим за откривање и одбрану.		

5.10. Напади усмерени на системе вештачке интелигенције

Напади усмерени на системе вештачке интелигенције		
Софтвер ИКТ услуге	Поверљивост Интегритет Расположивост	Намерно
Злонамерни актери циљају саме системе ВИ које оператор користи у оквиру свог ИКТ система, са циљем њиховог компромитовања, манипулације или онеспособљавања. Ови напади укључују тровање података за обуку модела (*data poisoning*), нападе на улазне податке система ВИ (*adversarial attacks*) којима се систем ВИ наводи на погрешне одлуке или предвиђања, крађу модела и неовлашћени приступ подацима коришћеним за обуку.		

5.11. Безбедност ланца снабдевања

Безбедност ланца снабдевања		
Софтвер ИКТ услуге	Поверљивост Интегритет	Случајно Намерно
Заштита интегритета и поузданости производа, компоненти и услуга кроз све фазе, од пројектовања, производње и транспорта до испоруке. Циљ је спречавање уношења малициозних измена, фалсификованих делова или скривених рањивости пре него што стигну у информациони систем.		

6. Инсајдерска претња

Инсајдерска претња		
Хардвер Софтвер Запослени Локације ИКТ услуге	Поверљивост Интегритет Расположивост	Случајно Намерно
Ризик по информациону безбедност који потиче од особа изнутра, запослених, бивших запослених, партнера, који имају легитиман приступ системима, мрежама или подацима. Ова претња може бити намерна (злонамерни инсајдер који краде податке, наноси штету или олакшава нападе споља), ненамерна (непажња, људска грешка, занемаривање процедура) или резултат компромитованих креденцијала (инсајдер чији су налози преузети од стране нападача).		

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
Природна	Ватра			X			X	X			X	
Природна	Вода			X			X	X			X	
Природна	Неповољни климатски услови			X			X	X			X	
Природна	Природне катастрофе			X			X	X			X	
Индустријска	Неповољни услови температуре и/или влажности			X			X	X			X	X
Природна	Прекид енергетског напајања			X			X	X			X	X
Индустријска	Електромагнетно загађење		X	X	X	X	X	X			X	
Индустријска	Квар хардвера или софтвера			X	X	X	X	X	X			
Индустријска	Квар комуникационих услуга			X	X	X						X
Индустријска	Прекид основних услуга које су			X	X	X					X	X

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
	предмет набавке или других услуга											
Индустријска	Деградација медијума			X	X	X		X			X	X
Индустријска	Ризик примене енкрипције у условима развоја квантног рачунарства	X	X		X	X			X			X
Индустријска	Пренос злонамерног софтвера применом преносних носача података	X	X	X	X	X		X	X	X		X
Индустријска	Отицање компромитујућег електромагнетног зрачења	X	X		X	X		X				X
Грешка или ненамерни пропусти	Корисничке грешке	X	X	X		X		X	X			X
Грешка или ненамерни пропусти	Грешке администратора система/безбедности	X	X	X		X		X	X			X
Грешка или ненамерни	Грешке праћења (logs)		X			X		X	X			X

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апли кације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
пропусти												
Грешка или ненамерни пропусти	Грешке у конфигурацији	X	X	X		X		X	X			X
Грешка или ненамерни пропусти	Организацион и недостаци			X		X				X		
Грешка или ненамерни пропусти	Ширење злонамерног софтвера (малвера)	X	X	X		X			X			
Грешка или ненамерни пропусти	Случајна измена података		X			X		X	X	X	X	X
Грешка или ненамерни пропусти	Уништење података			X		X		X	X	X	X	X
Грешка или ненамерни пропусти	Цурење података	X				X		X	X	X	X	X
Грешка или ненамерни пропусти	Рањивост софтвера	X	X	X		X			X			
Грешка или ненамерни пропусти	Грешке у одржавању / ажурирању софтвера		X	X		X			X			
Грешка или ненамерни пропусти	Квар система због исцрпљености ресурса			X		X		X				X
Грешка или	Губитак	X		X		X		X				

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
ненамерни пропусти	опреме											
Грешка или ненамерни пропусти	Недостатак запослених			X		X				X		
Грешка или ненамерни пропусти	Недостатак свести и специфичних знања о информационој безбедности			X		X				X		
Грешка или ненамерни пропусти	Неадекватно управљање привилегијама	X	X			X			X	X		
Грешка или ненамерни пропусти	Недостатак организованог система управљања информационом безбедношћу			X		X				X		
Грешка или ненамерни пропусти	Недостатак система за детекцију инцидената	X	X	X		X			X			X
Грешка или ненамерни пропусти	Неадекватно планирање континуитета пословања	X	X	X		X			X	X		X
Грешка или ненамерни пропусти	Неадекватно коришћење или изостанак коришћења криптографск	X	X	X		X			X			X

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апли кације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
	их контрола											
Грешка или ненамерни пропусти	**Грешке у процедурама резервних копија (*Backup*)**	**X**	**X**	**X**		**X**			**X**			**X**
Намерни напади	**Манипулација евиденцијом активности (*logs)***		**X**		**X**			**X**	**X**			**X**
Намерни напади	**Манипулација конфигурацијс ким датотекама**	**X**	**X**	**X**	**X**			**X**	**X**			**X**
Намерни напади	**Маскирање идентитета**	**X**	**X**		**X**			**X**	**X**			**X**
Намерни напади	**Злоупотреба права приступа**	**X**	**X**	**X**	**X**				**X**		**X**	**X**
Намерни напади	**Злоупотреба ресурса**	**X**	**X**	**X**	**X**				**X**		**X**	**X**
Намерни напади	**Ширење малвера**	**X**	**X**	**X**	**X**				**X**			
Намерни напади	**Неовлашћен приступ**	**X**	**X**		**X**			**X**	**X**		**X**	**X**
Намерни напади	**Анализа саобраћаја**	**X**			**X**							**X**
Намерни напади	**Прислушкива ње**	**X**			**X**			**X**	**X**	**X**		**X**
Намерни напади	**Намерна измена информација**		**X**		**X**			**X**	**X**	**X**	**X**	**X**

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
Намерни напади	Уништавање информација			X	X			X	X	X	X	X
Намерни напади	Откривање информација	X			X			X	X	X	X	X
Намерни напади	Манипулација софтвером	X	X	X	X	X			X			
Намерни напади	Манипулација хардвером	X		X	X			X				
Намерни напади	Ускраћивање услуга			X	X			X				X
Намерни напади	Крађа опреме	X		X	X			X				
Намерни напади	Деструктивни напад	X			X			X		X	X	X
Намерни напади	Изнуђивање (*ransomware*)	X	X	X	X			X	X			X
Намерни напади	Социјални инжењеринг	X	X	X	X					X		
Намерни напади	Компромитација и злоупотреба МФП уређаја	X	X	X	X			X	X			
Претње повезане са услугама	Закључавање			X		X						X
Претње повезане са коришћењем спољних услуга	Губитак управљања			X	X	X						X
Претње повезане са коришћењем	Грешке код изолације	X	X	X	X	X						X

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
спољних услуга												
Претње повезане са коришћењем спољних услуга	Несигурно или неефикасно брисање података	X			X	X						X
Претње повезане са коришћењем спољних услуга	Судски позив и е-откривање	X		X	X	X						X
Претње повезане са коришћењем спољних услуга	Ризик од промене јурисдикције	X		X	X	X						X
Претње повезане са коришћењем спољних услуга	Ризици заштите података	X				X						X
Претње повезане са коришћењем спољних услуга	Анализа инцидената и форензичка подршка	X	X	X	X	X						X
Претње повезане са коришћењем спољних услуга	Напади уз коришћење вештачке интелигенције		X	X	X				X	X		X

Категорије претњи	Претња	Безбедност (поверљивост, интегритет, расположивост)			Извор (намерне, случајне, природне)			Категорије имовине				
		П	И	Р	Н	С	П	Хардвер, уређаји, опрема	Софтвер/апликације	Запослени	Локације и просторије	Организациона инфраструктура (укључујући ИКТ услуге)
Претње повезане са коришћењем спољних услуга	Напади усмерени на системе вештачке интелигенције		X	X	X				X			X
Претње повезане са коришћењем спољних услуга	Безбедност ланца снабдевања	X	X		X	X			X			X
Инсајдерска претња	Инсајдерска претња	X	X	X	X	X		X	X	X	X	X

О б р а з л о ж е њ е

I. Правни основ

Правни основ за доношење Правилника о општој методологији за процену ризика у информационо-комуникационим системима од посебног значаја (у даљем тексту: Правилник), садржан је у чл. 11. став 4. и 55. став 4. Закона о информационој безбедности („Службени гласник РС“, број 91/25, у даљем тексту: Закон).

Одредбом члана 11. став 4. Закона је прописано да се акт о процени ризика израђује у складу са општом методологијом за процену ризика у приоритетним и важним ИКТ системима од посебног значаја коју доноси орган, односно организација у којој се обављају послови Националног ЦЕРТ-а.

II. Разлози за доношење

Одредбом члана 55. став 4. Закона је прописана обавеза да орган, односно организација у којој се обављају послови Националног ЦЕРТ-а, у року од девет месеци од дана ступања на снагу овог закона, донесе општу методологију за процену ризика у ИКТ системима од посебног значаја из члана 11. став 4. овог закона.

Имајућу у виду наведено Регулатор је, у складу са чланом 11. став 4. Закона, утврдио општу методологију за процену ризика у ИКТ системима од посебног значаја.

III. Објашњење појединих решења

Одредбом члана 1. Правилника прописан је предмет правилника.

У члану 2. Правилника прописано је да се акт о процени ризика ИКТ система од посебног значаја израђује у складу са општом методологијом за процену ризика у ИКТ системима од посебног значаја, која је дата у Прилогу 1. овог правилника и чини његов саставни део.

Одредбом члана 3. Правилника прописано је да процена ризика у ИКТ системима од посебног значаја обухвата идентификацију претњи, рањивости и могућих инцидената, која се заснива на Каталогу претњи информационе безбедности, који је дат у Прилогу 2. овог правилника и чини његов саставни део.

У члану 4. Правилника уређено је ступање на снагу овог правилника.

IV. Предлог даљих активности

Предлаже се да Савет Регулатора размотри и усвоји Нацрт овог правилника, као и да се исти, након тога, у складу са одредбама чл. 36. и 37. Закона, о електронским комуникацијама

(„Службени гласник РС“, број 35/23, у даљем тексту: ЗЕК), упути на јавне консултације у трајању од 30 дана.

Након спроведених јавних консултација, извршиће се обрада и анализа приспелих мишљења и Савету Регулатора ће се доставити одговарајући Предлог правилника.

По усвајању наведеног Предлога правилника, овај општи акт ће, сагласно одредби члана 27. став 2. ЗЕК-а, у делу који се односи на обавезу објављивања донетих аката Регулатора у складу са законом којим се уређује државна управа и одредби члана 57. став 1. Закона о државној управи („Службени гласник РС“, бр. 79/05, 101/07, 95/10, 99/14, 30/18 - др. закон и 47/18), бити упућен надлежном министарству, ради прибављања мишљења о његовој уставности и законитости. По добијеном мишљењу надлежног министарства, предметни правилник ће бити објављен у „Службеном гласнику Републике Србије“.

V. Средства за спровођење Правилника

За спровођење овог правилника није потребно обезбедити посебна средства у финансијском плану Регулатора.