ДРЖАВНА
РЕВИЗОРСКА
ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ О МЕРАМА ИСПРАВЉАЊА МИНИСТАРСТВА ИНФОРМИСАЊА И ТЕЛЕКОМУНИКАЦИЈА, ПАРИСКА 7, 11000 БЕОГРАД

по ревизији сврсисходности пословања „Управљање инцидентима у ИКТ системима од посебног значаја“

Број: 400-392/2022-03/14
Београд, 28. април 2023. године

Садржај:

1. УВОД....3
2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА....4
2.1 Утврђивање листе приоритета....4
2.1.1 Листа приоритета ИКТ СоПЗ према степену критичности и планирање ангажовања ЦЕРТ тимова....4
2.1.1.1 Опис несврсисходности....4
2.1.1.2 Исказане мере исправљања....4
2.1.1.3 Оцена мера исправљања....4
2.2 Свест о значају информационе безбедности....4
2.2.1 Јачање свести о значају информационе безбедности стварним потребама за обукама за све заинтересоване стране....4
2.2.1.1 Опис несврсисходности....4
2.2.1.2 Исказане мере исправљања....5
2.2.1.3 Оцена мера исправљања....5
2.3 Видљивост CERT-ова у јавности....5
2.3.1 Недовољна видљивост важности CERT-ова у јавности и различити садржаји на интернет локацијама CERT-ова за пријављивање инцидената....5
2.3.1.1 Опис несврсисходности....5
2.3.1.2 Исказане мере исправљања....5
2.3.1.3 Оцена мера исправљања....5
2.4 Категоризација оператора....6
2.4.1 Категоризација оператора ИКТ СоПЗ по величини и критичности....6
2.4.1.1 Опис несврсисходности....6
2.4.1.2 Исказане мере исправљања....6
2.4.1.3 Оцена мера исправљања....6
2.5 Превентивно обавештавање оператора ИКТ СоПЗ....6
2.5.1 Обавештавање оператора са истим рањивостима....6
2.5.1.1 Опис несврсисходности....6
2.5.1.2 Исказане мере исправљања....7
2.5.1.3 Оцена мера исправљања....7
2.6 Објављивање аларма....7
2.6.1 Непостојање механизма непосредног објављивања аларма по пријави инцидента....7
2.6.1.1 Опис несврсисходности....7
2.6.1.2 Исказане мере исправљања....7
2.6.1.3 Оцена мера исправљања....7
2.7 Евиденција оператора ИКТ СоПЗ....8
2.7.1 МИТ је израдило страницу на званичној интернет презентацији намењену упису....8
2.7.1.1 Опис несврсисходности....8
2.7.1.2 Исказане мере исправљања....8

2.7.1.3 Оцена мера исправљања 8
2.8 Технолошка решења оператора ИКТ СоПЗ 9
2.8.1 Евиденција оператора ИКТ СоПЗ није обухватила податке о технолошким решењима који су неопходни за процену ИТ ризика 9
2.8.1.1 Опис несврсисходности 9
2.8.1.2 Исказане мере исправљања 9
2.8.1.3 Оцена мера исправљања 9
2.9 Инспекцијски надзор 9
2.9.1 МИТ обавља инспекцијски надзор са једним инспектором над операторима 9
2.9.1.1 Опис несврсисходности 9
2.9.1.2 Исказане мере исправљања 9
2.9.1.3 Оцена мера исправљања 10
3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА 10

1. УВОД

У Извештају о ревизији „Управљање инцидентима у ИКТ системима од посебног значаја“ број: 400-392/2022-03/10 од 20. децембра 2022. године Државна ревизорска институција (у даљем тексту Институција) је.

С обзиром да све откривене несврсисходности нису биле отклоњене у току ревизије, Институција је од субјекта ревизије захтевала достављање одазивног извештаја.

Субјект ревизије је у остављеном року од 90 дана доставио одазивни извештај, који је потписало и печатом оверило одговорно лице.

У одазивном извештају су приказане мере исправљања утврђених несврсисходности. У послеревизионом поступку смо прегледали одазивни извештај и оценили његову веродостојност и оценили да ли су мере исправљања задовољавајуће.

У овом извештају:

- приказујемо несврсисходности које су обелодањене у извештају о ревизији за које је захтевано предузимање мера исправљања,
- резимирамо предузете мере исправљања и
- дајемо мишљење о томе да ли су мере за исправљање стања, исказане у одазивном извештају, задовољавајуће.

2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

2.1 Утврђивање листе приоритета

2.1.1 Листа приоритета ИКТ СоПЗ према степену критичности и планирање ангажовања ЦЕРТ тимова

2.1.1.1 Опис несврсисходности

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.

2.1.1.2 Исказане мере исправљања

Препорука: МИТ да успостави листу приоритета ИКТ система од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре.

У циљу реализације препоруке, Министарство информисања и телекомуникација ће радној групи за измену Закона о информационој безбедности предложити решење којим би се створио законски основ за успостављање листе приоритета ИКТ система од посебног значаја према степену критичности и дефинисале одговорности за њено спровођење. Приликом израде решења водиће се рачуна да се предложе релевантни критеријуми за процену степена критичности (као што су утицај на друштво-број корисника, економски ефекат, утицај на окружење и др.). Уколико то буде било потребно, Министарство ће предузети и друге мере у смислу доношења подзаконских аката за реализацију препоруке.

2.1.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности, али како је дата препорука да се успостави листа приоритета ИКТ система од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре. Очекује се као крајњи резултат успостављање листе приоритета ИКТ система од посебног значаја по степену критичности.

2.2 Свест о значају информационе безбедности

2.2.1 Јачање свести о значају информационе безбедности стварним потребама за обукама за све заинтересоване стране

2.2.1.1 Опис несврсисходности

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.

2.2.1.2 Исказане мере исправљања

Препорука: МИТ 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.

МИТ ће након окончања фазе анализе потреба и израде плана детаљне имплементације, током 2023. и 2024. године приступити реализацији обука у складу са налазима иницијалне фазе пројекта. Министарство информисања и телекомуникација узеће учешће у свакој фази реализације пројекта с циљем да допринесе јачању свести о значају информационе безбедности.

2.2.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности и активности у оквиру постојећег пројекта унапређења услуга електронске управе (EDGE – Enabling Digital Governance) проширење тема обука.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је за сада само планирало да у оквиру постојећег пројекта унапређења услуга електронске управе (EDGE – Enabling Digital Governance) прошири теме обука на све заинтересоване стране наведене у препоруци. Очекујемо извештаје о спроведеним обукама намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом инфраструктуром.

2.3 Видљивост CERT-ова у јавности

2.3.1 Недовољна видљивост важности CERT-ова у јавности и различити садржаји на интернет локацијама CERT-ова за пријављивање инцидената

2.3.1.1 Опис несврсисходности

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.

2.3.1.2 Исказане мере исправљања

Препорука: МИТ 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.

Министарство информисања и телекомуникација ће израдити предлог одредби којима се Закон о информационој безбедности мора изменити да би се омогућила примена препоруке и предложити га радној групи на разматрање.

2.3.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности и активности у оквиру

постојећег пројекта унапређења услуга електронске управе (EDGE – Enabling Digital Governance) проширење тема обука.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је само изменило своју страницу на званичној интернет презентацији, али је неопходно да се та обавеза пропише за CERT-ове.

2.4 Категоризација оператора

2.4.1 Категоризација оператора ИКТ СоПЗ по величини и критичности

2.4.1.1 Опис несврсисходности

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..

2.4.1.2 Исказане мере исправљања

Препорука: МИТ да извршити категоризацију оператора ИКТ система по величини и критичности, дефинисати минималне/обавезне мере према категорији оператора.

Министарство информисања и телекомуникација припремиће сет одредби за измену Закона о информационој безбедности које ће предложити радној групи на разматрање, а којима је предвиђено усклађивање са НИС2 директивом у смислу категоризације ИКТ система од посебног значаја према различитим критеријумима. Изменом закона створиће се правни оквир и за реализацију препоруке.

2.4.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности, али како је дата препорука да се изврши категоризација оператора ИКТ система од посебног значаја по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора. Очекује се као крајњи резултат дефинишу категорије оператора и адекватан низ мера заштите за сваку категорију.

2.5 Превентивно обавештавање оператора ИКТ СоПЗ

2.5.1 Обавештавање оператора са истим рањивостима

2.5.1.1 Опис несврсисходности

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.

2.5.1.2 Исказане мере исправљања

Препорука: МИТ да у сарадњи са надлежним органима прикупити податке о технолошким решењима оператора ИКТ СоПЗ, обезбедити систем за аутоматизовано обавештавање између CERT-ова и партнера, обезбедити имплементацију и примену.

Министарство информисања и телекомуникација ће наставити да буде укључено у развијање системског приступа за консолидацију података о раним упозорењима о сајбер претњама у машинском облику што ће наставити да буде континуирана активност. Циљ је да се побољша ефикасност механизама раног и аутоматизованог упозоравања, као и да се заинтересује што већи број субјеката информационе безбедности да се укључе у овај процес.

2.5.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности, али како је дата препорука да се прикупе подаци о технолошким решењима које користе оператори ИКТ система од посебног значаја, биће неопходно проширити листу са елементима неопходним за превентивно обавештавање оператора који употребљавају иста технолошка решења у циљу превенције нежељених догађаја.

2.6 Објављивање аларма

2.6.1 Непостојање механизма непосредног објављивања аларма по пријави инцидента

2.6.1.1 Опис несврсисходности

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. МИТ 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.

2.6.1.2 Исказане мере исправљања

Препорука: МИТ да обезбедити 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.

Министарство информисања и телекомуникација континуирано ће наставити да доприноси развоју система и механизама за машинску обраду података о сајбер инцидентима и наставиће да сарађује са Националним ЦЕРТ-ом и осталим надлежним органима и операторима ИКТ система ради омогућавања благовремене размене података и правовременог реаговања уз очување података о личности и приватности.

2.6.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности и активности у оквиру

постојећег пројекта унапређења услуга електронске управе (EDGE – Enabling Digital Governance) проширење тема обука.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је за сада само планирало да у оквиру постојећег пројекта унапређења услуга електронске управе (EDGE – Enabling Digital Governance) појача своје ангажовање које подразумева координацију активности свих надлежних ЦЕРТ-ова како би се успоставио алармни систем за обавештавање.

2.7 Евиденција оператора ИКТ СоПЗ

2.7.1 МИТ је израдило страницу на званичној интернет презентацији намењену упису

2.7.1.1 Опис несврсисходности

МИТ 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.

2.7.1.2 Исказане мере исправљања

Препорука: МИТ да коришћењем одговарајућих извора прибавити све неопходне податке како би се могли оценити ИТ ризици, прописати нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите.

Министарство информисања и телекомуникација прикупља податке из инспекцијског надзора над операторима ИКТ система од посебног значаја, као и од надлежних органа у чијој надлежности се налазе ИКТ системи од посебног значаја, у циљу оцене безбедносних ризика и прописивања нивоа заштите. Такође, Министарство има приступ подацима годишњим статистичким извештајима о инцидентима чији подаци могу допринети реализацији препоруке, а очекује се да ће и израда МИСП платформе Националног ЦЕРТ-а допринети већој информисаности о претњама, ризицима и инцидентима. Поред тога, као што је наведено и код препорука под р.б. 1,3, и 4, кроз измене и допуне Закона о информационој безбедности размотриће се додатни механизми за оцену ИТ ризика.

На основу прикупљених информација из поменутих извора, као и кроз категоризацију оператора ИКТ система од посебног значаја на основу свеобухватне анализе података, Министарство информисања и телекомуникација прописаће нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите.

2.7.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности, та активност је започета, али тек по спровођењу измена и прикупљању неопходних података, могуће је извршити процену ИТ ризика као и да се на крају пропишу нивои заштите.

2.8 Технолошка решења оператора ИКТ СоПЗ

2.8.1 Евиденција оператора ИКТ СоПЗ није обухватила податке о технолошким решењима који су неопходни за процену ИТ ризика

2.8.1.1 Опис несврсисходности

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.

2.8.1.2 Исказане мере исправљања

Препорука: МИТ да применом дефинисаних критеријума извршити адекватну процену ризика за избор надзираних субјеката.

Министарство информисања и телекомуникација прикупља податке из инспекцијског надзора, као и од надлежних органа у чијој надлежности се налазе ИКТ системи од посебног значаја, у циљу оцене безбедносних ризика надзираних субјеката.

На основу прикупљених информација, Министарство информисања и телекомуникација оцениће ризик и према томе правити план надзора субјеката.

2.8.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је започело активности на реализацији препоруке, а пошто се планови инспекцијског надзора доносе за наредну годину, потпуно спровођење ове мере ће се видети тек у години након усвојених измена Закона.

2.9 Инспекцијски надзор

2.9.1 МИТ обавља инспекцијски надзор са једним инспектором над операторима

2.9.1.1 Опис несврсисходности

МИТ 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.

2.9.1.2 Исказане мере исправљања

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

Реализација ове препоруке подразумева измену Закона о информационој безбедности Министарство је у поступку формирања радне групе за израду нацрта текста Закона о изменама и допунама Закона о информационој безбедности.

Министарство информисања и телекомуникација припремиће предлог одредби које ће бити упућене радној групи на разматрање, а које ће представљати правни основ за реализацију препоруке.

2.9.1.3 Оцена мера исправљања

Доказ: Допис Министарству одбране, где се обавештавају да се приступило изради Нацрта закона о изменама и допунама Закона о информационој безбедности.

Описану меру исправљања оцењујемо као **делимично задовољавајућу**.

Објашњење: Министарство информисања и телекомуникација је започело активности на реализацији препоруке, а пошто се очекује успостављање законске могућности ангажовања овлашћених правних и физичких лица за спровођење колегијалног прегледа мера ће у потпуности бити спроведена након примене усвојених измена Закона.

3. МИШЉЕЊЕ О ИСКАЗАНИМ МЕРАМА ИСПРАВЉАЊА

Прегледали смо одазивни извештај, који је поднео субјект ревизије. Оценили смо да је одазивни извештај, који је потписало и печатом оверило одговорно лице субјекта ревизије, веродостојан.

Вредновање мера исправљања смо оценили на основу њиховог описа и достављене документације. Сматрамо да смо добили довољне и одговарајуће доказе да можемо изрећи оцену о мерама исправљања.

Оцењујемо, да су мере исправљања, описане у одазивном извештају који је поднео Субјект ревизије **делимично задовољавајуће.**

Напомена:

У складу са одредбама члана 37. Закона о Државној ревизорској институцији, а након истека рокова исказаним у одазивном извештају, потребно је да обавештавате Државну ревизорску институцију о предузетим мерама и активностима о отклањању откривених несврсисходности према роковима из одазивног извештаја и доставите одговарајуће доказе.

По истеку три године Државна ревизорска институција ће утврђивати ефекте остварене након спровођења препорука и отклањања откривених неправилности /несврсисходности.

У ове ефекте укључиће се и ефекти које будете ви исказали предузетим мерама и активностима из одазивног извештаја.

Генерални државни ревизор

_____

Др Душко Пејовић
Државна ревизорска институција
Макензијева 41
11000 Београд, Србија
27. март 2023. године