Република Србија
МИНИСТАРСТВО ИНФОРМИСАЊА
И ТЕЛЕКОМУНИКАЦИЈА
Број: 401-00-43/2023-04
16.03.2023. године
Немањина 22-26
Београд

ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

БЕОГРАД
Макензијева 41

На основу члана 40. став 1. Закона о Државној ревизорској институцији („Службени гласник РС“ бр. 101/05, 54/07, 36/10 и 44/18), Министарство информисања и телекомуникација, Немањина 22-26, Београд, правни следбеник субјекта ревизије (Министарства трговине, туризма и телекомуникација) подноси

ИЗВЕШТАЈ О СПРОВОЂЕЊУ ПРЕПОРУКА РАДИ ОТКЛАЊАЊА НЕСВРСИСХОДНОСТИ ОТКРИВЕНИХ У РЕВИЗИЈИ

„Управљање инцидентима у ИКТ системима од посебног значаја“

Број и датум извештаја о ревизији: 400-392/2022-03/10 од дана 16. децембара 2022. године, достављен Министарству 21. децембра 2022. године

Несврсисходности које су обухваћене налазима и закључцима, за које је у поступку ревизије утврђено да би њиховим отклањањем средства од стране субјекта ревизије била употребљена економичније, ефикасније и ефективније, као и у складу са планираним циљевима:

I

Несврсисходности које су обухваћене налазима приоритета 1, које је могуће отклонити у року од 90 дана:

1) Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији број: 400-392/2022-03/10 нису утврђене несврсисходности приоритета 1.

II

Несврсисходности које су обухваћене налазима приоритета 2, које је могуће отклонити у року до годину дана.

2) Извештајем о спровођењу препорука ради отклањања несврсисходности откривених у ревизији број: 400-392/2022-03/10 нису утврђене несврсисходности приоритета 2.

III

Несврсисходности које су обухваћене налазима приоритета 3, које је могуће отклонити у року од једне до три године.

РБ	Препорука	Мера исправљања		Функција или звање лица одговорног за предузимање мере исправљања	Период у којем се планира предузимање мере исправљања
1	успоставити листу приоритета ИКТ система од посебног значаја према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре	У складу са чланом 6. Закона о информационој безбедности („Службени гласник“ бр. 6/2016, 94/2017 и 77/2019) утврђени су ИКТ системи од посебног значаја, а чланом 6а утврђене су обавезе оператора ИКТ система од посебног значаја. Закон не предвиђа дефинисање листе приоритета према степену критичности, већ прописује једнако уређење обавеза и поступање према операторима ИКТ система од посебног значаја. Ради спровођења препоруке потребно је размотрити измене Закона о информационој безбедности које би створиле правни основ за њену реализацију у смислу утврђивања обавезе. У том смислу, МИТ је започело активности на припреми измена и допуна Закона о информационој безбедности, утврдило циљеве који се желе постићи изменом закона и упутило допис дана 1. марта 2023. године надлежним институцијама и другим	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.	министар	*три године*

		организацијама које се баве питањима информационе безбедности ради именовања својих представника у радној групи за израду нацрта текста закона. Формирање радне групе предвиђено је до краја марта 2023. године када сви позвани одреде своје представнике.			
2	у сарадњи са другим надлежним организацијама утврдити 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	Канцеларија за информационе технологије и електронску управу, уз подршку пројекта Унапређења услуга електронске управе - EDGE Светске банке, спроводи пројекат посвећен обукама државних службеника и намештеника за подизање свести и правилно поступање у вези са информационом безбедношћу. Министарство информисања и телекомуникација препознато је као један од учесника у имплементацији пројекта. У првом кварталу 2023. спроводи се иницијална фаза пројекта, тачније анализа потреба за обукама, као и детаљни план имплементације пројекта. Пројектом је предвиђена обука за око 5000 државних службеника.	Након окончања фазе анализе потреба и израде плана детаљне имплементације, током 2023. и 2024. године приступиће се 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.	министар	*три године*
3	изменити страницу на сајту МТТТ и преусмерити кориснике на Национални CERT и апликацију за пријављивање на домену cert.rs, и	Законом о информационој безбедности прописано је да надлежни орган (Министарство информисања и телекомуникација)	Министарство информисања и телекомуникација ће израдити предлог одредби којима се Закон о информационој безбедности мора		

	прописати ту обавезност за све CERT-ове за које су надлежни	или Национални ЦЕРТ обавештења о инцидентима примају преко јединственог система за пријем инцидената, а законом је предвиђено да се обавештења могу поднети или на веб страници надлежног органа или на веб страници Националног ЦЕРТ-а. Оцењено је да тренутно не постоји законски основ за преусмеравање, с обзиром да је прописано да оператор може пријавити инцидент надлежном органу или Националном ЦЕРТ-у по сопственом избору. Ради спровођења препоруке биле би неопходне законске измене које би другачије дефинисале ову надлежност. Такође, законска измена је потребна и да би се обавеза упућивања на веб страницу Националног ЦЕРТ-а прописала осталим ЦЕРТ-овима. У том смислу, како је наведено у тексту поводом препоруке под р.б. 1, Министарство је у процесу формирања радне групе за израду нацрта текста Закона о изменама и допунама Закона о информационој безбедности.	изменити да би се омогућила примена препоруке и предложити га радној групи на разматрање.	министар	*три године*
4	извршити категоризацију оператора ИКТ система по величини и	С обзиром на то да је недавно усвојена НИС 2 Директива Европске уније (Directive (EU)	Министарство информисања и телекомуникација припремиће сет одредби за измену		

	критичности, дефинисати минималне/обавезне мере према категорији оператора	2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union), као и да је један од основних циљева измене и допуне Закона о информационој безбедности усклађивање са овом Директивом, која прописује ревидирани приступ дефинисању оператора ИКТ система од посебног значаја према сету критеријума који их сврстава у 2 главне категорије, Министарство информисања и телекомуникација је приступило спровођењу процедуре за измену овог закона како је назначено у образложењу за препоруку под р.б.1.	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.	министар	*три године*
5	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	Национални ЦЕРТ почев од трећег квартала 2022. године успоставља платформу за размену информација и претњама у сајбер простору (МИСП платформа) у сарадњи са Министарством информисања и телекомуникација. Редовно се одржавају састанци са корисницима платформе како би они били упознати с њеним перформансама, правилима коришћења, правилима приватности и	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	министар	*три године*

		протоколима. Планирано је да корисници платформе буду самостални ЦЕРТ-ови, посебни ЦЕРТ-ови и оператори ИКТ система од посебног значаја.	безбедности да се укључе у овај процес.		
6	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	Платформа и механизми описани у претходној препоруци под р.б. 5 односе се и на реализацију ове препоруке имајући у виду да МИСП платформа има функционалности које омогућавају достављање обавештења, односно упозорења о инцидентима, који класификују сајбер претњу у складу са ТЛП протоколом и корисницима пружа остале релевантне информације које су потребне за благовремено реаговање.	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.	министар	*три године*
7	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	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.	министар	*три године*

		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.			
8	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.	министар	*три године*
9	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.	министар	*три године*

Докази који се прилажу уз овај извештај да ће мере исправљања бити предузете:

- Допис за формирање радне групе за измену и допуну Закона о информационој безбедности;
- Извод из извештаја Националног ЦЕРТ-а за четврти квартал 2022. године (информација о МИСП платформи);

- Презентација пројекта Унапређења услуга електронске управе - EDGE Светске банке, спроводи пројекат посвећен обукама државних службеника и намештеника за подизање свести и правилно поступање у вези са информационом безбедношћу.

Доказе о отклањању несврсисходности доставићемо након истека рока за предузимање мера.

МИНИСТАР

др Михаило Јовановић