РЕПУБЛИКА СРБИЈА
ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

ПОСЛЕРЕВИЗИОНИ ИЗВЕШТАЈ О МЕРАМА ИСПРАВЉАЊА

ЈКП „ИНФОРМАТИКА“, НОВИ САД

по ревизији сврсисходности пословања „Управљање информационим системима у јавним предузећима за обједињену наплату“

Број: 400-735/2020-03/38
Београд, 26. мај 2021. године

Садржај

1. УВОД

У Извештају о ревизији сврсисходности пословања „Управљање информационим системима у јавним предузећима за обједињену наплату“ број: 400-735/2020-03/26 од 23. децембра 2020. године.

С обзиром да све откривене несврсисходности нису биле отклоњене у току ревизије, Институција је од субјекта ревизије, Јавно комунално предузеће "Информатика" Нови Сад Булевар цара Лазара 3, 21102 Нови Сад, (у даљем тексту: ЈКП Информатика – Нови Сад), захтевала достављање одазивног извештаја.

Субјект ревизије у остављеном року од 90 дана није доставио одазивни извештај. Узимајући у обзир ванредне околности због пандемије вируса COVID-19 и примене мера[1] заштите јавног здравља, ограниченог кретања, броја људи у просторијама, као и друга ограничења, достављен је потписан и оверен извештај од стране одговорног лица 26.маја 2021. године.

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.

[1] Уредба о мерама за спречавање и сузбијање заразне болести COVID-19 „Службени гласник РС“, бр. 151/2020-3, 152/2020-4, 153/2020-46, 156/2020-6, 158/2020-3, 1/2021-3, 17/2021-3, 19/2021-18, 22/2021-3, 29/2021-3, 34/2021-3, 48/2021-4.

2. НЕСВРСИСХОДНОСТИ И МЕРЕ ИСПРАВЉАЊА

2.1.1 Субјекти ревизије нису препознали и дефинисали значајне ИТ ризике, а што може негативно утицати на управљање информационим системима

2.1.1.1 Опис несврсисходности

Иако је успостављен Регистар ризика нису обухваћени значајни ИТ ризици који могу изазвати поремећаје у пословању, делимичним, краткотрајним као и дужим прекидима у пружању услуга. То може довести до умањења поверења корисника у способност ЈКП да обављају додељене послове због којих су основани.

2.1.1.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да дефинишу све значајне ИТ ризике као и потребне елементе на основу којих у складу са оцењеним утицајем на пословање може се одредити адекватна мера у циљу избегавања или умањења негативног утицаја на пословање .

У документу Процедура управљања ризицима дефинисана је методологија која се користи у процени и третману ризика у пословању ЈКП „Информатика“ Нови Сад с обзиром на поверљивост, интегритет и доступност информација које се налазе у дефинисаном подручју Система за управљање безбедношћу информација (ISMS), а према захтевима стандарда ISO/IEC 27001 и у складу са ISO/IEC 27005 - менаџмент ризицима по безбедност информација.
Регистар ризика садржи све значајне ИТ ризике, процену ризика у складу са прописаном методологијом, постојеће мере и начин спровођења третмана ризика према захтевима стандарда ISO/IEC 27001.

Докази: *ЈКП „Информатика“ Нови Сад доставила је документе: Процедура управљања ризицима; Регистар ризика ЈКП „Информатика" Нови Сад; Листа мера безбедности; Каталог претњи; Каталог рањивости*

2.1.1.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу.**

2.1.2 Субјекти ревизије нису вршили процену утицаја на пословање ни за препознате ризике, а што може негативно утицати на управљање информационим системима.

2.1.2.1 Опис несврсисходности

ЈКП „Информатика“ Нови Сад нема документовану процену утицаја на пословање, а приоритете у опоравку одређује на основу стручне процене и искуства тренутно запослених на ИТ пословима.

2.1.2.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да израде Процену утицаја на пословање обухватајући све значајне пословне процесе, информационе

системе и услуге, одреди очекивана времена и тачке опоравка за сваки ресурс као и смернице које мере применити

До дана достављања одазивног извештаја након ревидирања Регистра ризика реализована је Методологија управљања ризицима коју чине:

- Идентификација ресурса и њихових власника;
- Идентификације вредности ресурса у односу на поверљивост, доступност и интегритет;
- Идентификације претњи;
- Идентификације рањивости;
- Вероватноћа појаве претњи који могу угрозити ове ресурсе;
- Оцењивање рањивости;
- Израчунавање укупног ризика;
- Идентификације власника ризика;
- Процена и третман ризика кроз одабир и примену мера безбедности.

ЈКП „Информатика“ Нови Сад је у току разматрања мера које ће бити предузете у наредном периоду.

2.1.2.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.1.3 Субјекти ревизије немају планове за ванредне ситуације, јер оснивач није својим планом дефинисао задатке и обавезе за ове ЈКП, што може довести до штете и губитака

2.1.3.1 Опис несврсисходности

Оснивач Град Нови Сад није обавестио ЈКП које мере и активности за спречавање и умањење последица катастрофа треба да планира и шта се од ЈКП очекује у ванредним ситуацијама. ЈКП Информатика Нови Сад нема документован План континуитета пословања у ванредним ситуацијама, и досадашње поступање је одређено на основу стручне процене и искуства тренутно одговорних запослених лица.

2.1.3.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да покрене иницијативу код оснивача да им одреди потребне елементе у оквиру Плана заштите и спасавања, ради израде Плана за рад у ванредним ситуацијама.

ЈКП „Информатика“ Нови Сад је ЈКП „Информатика“ Нови Сад израдила је План заштите и спасавања, који је предала Министарству унутрашњих послова, Одељењу за ванредне ситуације, како би добила сагласност на исти у сладу са Законом.

Докази: *ЈКП „Информатика“ Нови Сад доставила документе: Захтев за сагласност на План заштите и спасавања за ЈКП „Информатика“ Нови Сад; План заштите и спасавања за ЈКП „Информатика“ Нови Сад.*

2.1.3.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**.

2.1.4 Субјекти ревизије немају свеобухватне планове опоравка од хаварије информационог система којим би дефинисали тај процес, иако поседују знање и искуство у превазилажењу хаваријских догађаја

2.1.4.1 Опис несврсисходности

ЈКП „Информатика“ Нови Сад је за потребе опоравка ИС у случају хаварије имплементирала решење „VMware Site Recovery Manager“ или скраћено „СРМ“. „Site Recovery Manager“ (СРМ) инфраструктура се састоји из два подсистема.

ЈКП „Информатика“ Нови Сад није доставила доказе да су усвојили и примењују План опоравка од хаварије.

2.1.4.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да успоставе свеобухватни План опоравка од хаварије и врше његово редовно ажурирање.

Ревидирање процедуре План опоравка од хаварије је у току.

Након усвајања Плана опоравка од хаварије радиће се на његовом успостављању.

2.1.4.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.1.5 Субјекти ревизије нису успоставили управљање инцидентима.

2.1.5.1 Опис несврсисходности

Законом о информационој безбедности је предвиђено успостављање јединственог система за пријем обавештења о инцидентима као информациони систем у који се уносе подаци о инцидентима у ИКТ системима од посебног значаја који могу да имају значајан утицај на нарушавање информационе безбедности, а које је успоставило регулаторно тело РАТЕЛ.

Обавеза сваког ЈКП да о инцидентима у ИКТ систему обавештава је уређена Уредбом којом су одређени сви неопходни елементи инцидената, који се достављају електронским путем.

Иако је успостављен процес управљања рекламацијама, до сада нису успоставили електронску евиденцију са свим елементима инцидената на начин који би омогућио електронско достављање обавештења надлежном органу.

2.1.5.2 Исказане мере исправљања

Одговорним лицима ЈКПОН – Ниш препоручено је да успоставе процес управљања инцидентима који ће омогућити благовремен и ефикасан одговор у случају нарушавања безбедности или функционалности информационог система и организује обавештавање надлежног органа електронским путем.

ЈКП „Информатика“ Нови Сад је предузела активности на успостављању ефикасног система управљања инцидентима. Након усвајања Процедуре управљања инцидентима радиће се на њеној реализацији и примени.

2.1.5.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.1.6 Субјекти ревизије нису донели и спровели план комуникације у вези сајбер претњи

2.1.6.1 Опис несврсисходности

Корисници информационог система нису редовно обавештавани нити обучавани како да препознају претње из сајбер простора.

2.1.6.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да успоставе процес обавештавања и обучавања запослених чија радна места су изложена сајбер нападима, планира и организује обучавање о новим обавезама која утичу на безбедност информационог система.

ЈКП „Информатика“ Нови Сад донела је посебан План екстерних и интерних обука запослених у вези са информационом безбедношћу, а Планом стручног усавршавања запослених (Q2.HR.02-2 ISO 27001:2013) обезбедила је и неопходна средства за њихову реализацију у 2021. години. Такође, ЈКП „Информатика“ Нови Сад организовала је и спровела за све запослене у марту и мају 2021. године две велике обуке у вези са Системом за управљање безбедношћу информација ISO 27001:2013 и подизањем свести о значају информационе безбедности за пословање предузећа. Обавештавање запослених регулисано је Процесом комуницирања екстерног и интерног ISO 27001:2013 и Упутством за запослене Q3.BI.01, а сви запослени на своје мејл адресе редовно добијају извештаје о претњама из сајбер простора (SOPHOS Quarantine Report). У овим извештајима наводе се све мејл адресе у карантину које су блокиране због нежељене поште, вируса, лоших екстензија датотека, забрањених израза или грешака у испоруци, а запослени су упућени да за сва питања обрате администратору поште.

Докази: Достављени су документи: План организовања екстерних и интерних обука у вези са безбедношћу информационог система за 2021. годину; План стручног усавршавања запослених Q2.HR.02-2 ISO 27001:2013; Презентација интерне обуке која је спроведена у марту месецу 2021; Презентација обуке запослених која је спроведена у мају месецу 2021; Евалуација интерне обуке запослених у вези са Системом за управљање безбедношћу информација ISO 27001:2013 (извештај) 03-05-1; Процес комуницирања екстерног и интерног ISO 27001:2013; Упутство за запослене Q3.BI.01; SOPHOS Quarantine Report; Kaspersky Managed protection JKP Informatika.

2.1.6.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**.

2.1.7 Иако субјекти ревизије поседују минималну потребну опрему за онемогућавање неовлашћеног мрежног приступа они не врше редовно преглед покушаја упада у мрежу.

2.1.7.1 Опис несврсисходности

Законом о информационој безбедности дефинише да је информационо-комуникациони систем (ИКТ систем) технолошко-организациона целина која обухвата: електронске комуникационе мреже у смислу закона који уређује електронске комуникације; уређаје или групе међусобно повезаних уређаја, таквих да се у оквиру уређаја, односно у оквиру барем једног из групе уређаја, врши аутоматска обрада података коришћењем рачунарског програма; податке који се воде, чувају, обрађују, претражују или преносе помоћу средстава у сврху њиховог рада, употребе, заштите или одржавања; организациону структуру путем које се управља ИКТ системом; и све типове системског и апликативног софтвера и софтверске развојне алате.
ИКТ систем је повезан на интернет мрежу и неопходно је обезбедити мрежне уређаје који ће спречавати неовлашћени приступ информационим ресурсима, иако је мера успостављена не врши се периодична провера журнала активности и покушаја пробоја заштите.

2.1.7.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да успоставе редовно прегледавање ЛОГ датотека (журнала) мрежних уређаја за спречавање упада и свих постојећих система и сачињава о томе записник.

ЈКП „Информатика“ Нови Сад је започела анализу тржишта и понуда везаних за Log Management Software у циљу реализације ове препоруке.

2.1.7.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.1.8 Субјекти ревизије нису применили заштитни механизам који обезбеђује обраду података унетих само употребом апликације.

2.1.8.1 Опис несврсисходности

Недостаје механизам хеш заштите који обезбеђује комплетност преузетих података од комуналних предузећа пружалаца услуге као и комплетност измене података која спречава да апликација не обрађује податке исправљене од стране администратора базе, мада се подаци о овим изменама могу очитати индиректно у журналу базе података.
Могуће грешке у рачунима могу настати као последица погрешно очитаних и/или унетих података у систем чије се исправке обављају успостављеним процедурама рекламације.

2.1.8.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да обезбеде механизам хеш заштите којим би се спречила могућност да апликација обрађује податке који нису комплетни, или обрађени употребом апликације.

ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.

2.1.8.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

2.1.9 Структура базе података није у довољној мери усклађена са прописаним обавезама мера заштите (псеудонимизације) личних података корисника у информационом систему.

2.1.9.1 Опис несврсисходности

ЈКП „Информатика“ Нови Сад је задужила лице за заштиту података и сада је у поступку процене утицаја обраде на безбедност података. На својој званичној презентацији www.nsinfo.co.rs дато је обавештење о обради података о личности у којем се наводи врста података, сврха обраде, начин чувања и одговорности у случају незаконите обраде. Наплата комуналних услуга грађанима-корисницима није могућа без личних података, имена и презимена, адресе становања и јединственог матичног броја грађанина ради идентификовања власника непокретности-обвезника плаћања комуналних услуга. Спровођење општих и посебних обавеза почела је од 21. августа 2019. године и реч је о сложеним организационим, кадровским и техничким мерама заштите (члан 42, ЗЗЛП) које требају обезбедити личне податке грађана у информационом систему предузећа за обједињену наплату. Поред захтева пројектовања „безбедног дизајна“ и „подразумеване безбедности“ предвиђена је примена псеудонимизације личних података која намеће измену модела базе података и уноси нови ризик функционисања апликације. Овај процес без значајних ресурса, људи, програмирања, тестирања апликације није могуће завршити у овако кратком року. Број табела у бази података обједињене наплате (Видети Табелу 9.) је 469, а број табела у којима се појављују лични подаци је 40, указује на потребу доброг детаљног планирања измене и унапређења модела базе података у стратешком периоду од 3 – 5 година.

2.1.9.2 Исказане мере исправљања

Одговорним лицима ЈКП „Информатика“ Нови Сад препоручено је да након израде Процене утицаја обраде на заштиту личних података израде план имплементације псеудонимизације личних података корисника.

ЈКП „Информатика“ Нови Сад је започела активности на спровођењу ове препоруке.

2.1.9.3 Оцена мера исправљања

Описану меру исправљања оцењујемо као **задовољавајућу**. Оцена је извршена имајући у виду приоритет дате препоруке, односно период у коме је објективно могуће предузети мере исправљања.

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 мишљење да ли су мере исправљања задовољавајуће.

Оцењујемо, да су мере исправљања, описане у одазивном извештају који је поднео субјект ревизије **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 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
26. мај 2021. године