ДРЖАВНА
РЕВИЗОРСКА ИНСТИТУЦИЈА

РЕЗИМЕ
ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
„Управљање информационим системима у јавним предузећима за обједињену наплату“

26. јануар 2021. године

У претходно спроведеним ревизијама финансијских извештаја и правилности пословања утврђена су неслагања у евиденцијама учесника у систему обједињене наплате. Поред тога информациони системи у јавним предузећима који врше обједињену наплату, и у предузећима која врше комуналне услуге (даваоци услуга) нису ажурирани и усклађени. Неажурност база података за последицу може имати мање приходе, више трошкове наплате, али и могуће судске процесе (трошкове) због притужби грађана на ажурност евиденција. Такође, безбедност ових система треба да буде на нивоу који обезбеђује поузданост података, а то подразумева интегритет, комплетност, тачност, конзистентност и очување података, безбедност информационог система и континуитет пословања, уважавајући сврху за коју се ти подаци и системи користе.

Кључни циљ ревизије је оцена да ли опште ИТ контроле и апликативне контроле спречавају, откривају и отклањају неефикасности у управљању информационим системима јавних предузећа за обједињену наплату комуналних услуга у три највећа града у Републици Србији.

Да бисмо остварили циљ ревизије формулисали смо главно ревизорско питање.

Да ли се на адекватан начин управља информационим системом јавног предузећа за обједињену наплату комуналних услуга?

Ревизијом смо обухватили активности ЈКП за обједињену наплату у Београду, Новом Саду и Нишу у периоду 2018–2019. године. Такође, за поједине анализе користили смо и податке из 2020. године.

Кључна порука овог Извештаја је:

Неопходно унапређење управљања информационим системима у ЈКП за обједињену наплату ради спречавања последица нежељених догађаја.

У наставку су дати закључци до којих смо дошли у поступку ревизије:

Закључак 1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису успоставили ефективан план континуитета пословања и план опоравка од хаварије.

Шта смо пронашли:

Налаз 1.1: Субјекти ревизије нису препознали и дефинисали значајне ИТ ризике, а што може негативно утицати на управљање информационим системима.

Налаз 1.2: Субјекти ревизије нису вршили процену утицаја на пословање ни за препознате ризике, а што може негативно утицати на управљање информационим системима.

Налаз 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.

Налаз 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.

Налаз 1.5: ЈКПОН-Ниш није интерним актом уредила успостављени процес израде резервних копија података што може довести до неадекватног поступања у случају кадровске промене.

Закључак 2: Управљање безбедношћу информационих система није потпуно адекватно, јер није успостављено управљање инцидентима.

Шта смо пронашли:

Налаз 2.1: Субјекти ревизије поседују Акт којим уређују питања у вези информационе безбедности.

Налаз 2.2: Субјекти ревизије нису успоставили управљање инцидентима.

Налаз 2.3: Субјекти ревизије нису донели и спровели план комуникације у вези сајбер претњи.

Налаз 2.4: У ЈКПОН-Ниш нису документоване изјаве запослених у вези преузимања одговорности.

Налаз 2.5: Иако субјекти ревизије поседују минималну потребну опрему за онемогућавање неовлашћеног мрежног приступа они не врше редовно преглед покушаја упада у мрежу.

Закључак 3: Поред постојећих општих и апликативних контрола улаза, обрачуна и излаза података, неопходно је обезбедити аутоматизовано усаглашавање, као и додатне заштитне механизме.

Шта смо пронашли:

Налаз 3.1: ЈКП „Инфостан технологије“ Београд и ЈКПОН-Ниш нису обезбедили усаглашавање података на аутоматизован начин.

Налаз 3.2: Субјекти ревизије нису применили заштитни механизам који обезбеђује обраду података унетих само употребом апликације.

Налаз 3.3: ЈКП „Инфостан технологије“ Београд није обезбедио избор датума последње измене као критеријум за извештавање.

Налаз 3.4: Структура базе података није у довољној мери усклађена са прописаним обавезама мера заштите (псеудонимизације) личних података корисника у информационом систему.

Државна ревизорска институција, након спроведене ревизије сврсисходности пословања „Управљање информационим системима у јавним предузећима за обједињену наплату“, је дала следеће препоруке субјектима ревизије, да:

- донесу План пословног континуитета;
- ИТ ризике уврсте у Регистар;
- врше процену утицаја ризика на пословање;
- израде План за ванредне ситуације;
- израде Планове опоравка од хаварије;
- успоставе процес управљања инцидентима;
- успоставе процес обавештавања и обучавања запослених о сајбер претњама;
- превентивно врше редовни преглед журнала на опреми ИС;
- обезбеде системе за електронско усклађивање евиденција са пружаоцима комуналних услуга;
- обезбеде заштитне хеш механизме за податке који се преносе кроз комуникационе канале;
- обезбеде заштитне механизме који ће осигурати да апликација обрађује само податке унетих употребом апликације;
- да приликом израде извештаја омогуће избор датума последње измене из претходног извештајног периода;
- израде Процену утицаја обраде на личне податке и план имплементације псеудонимизације личних података корисника.