ДРЖАВНА РЕВИЗОРСКА ИНСТИТУЦИЈА

РЕЗИМЕ
ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА

„Управљање инцидентима у ИКТ системима од посебног значаја“

31. јануар 2023. године

Државна ревизорска институција је спровела ревизију сврсисходности пословања „Управљање инцидентима у ИКТ системима од посебног значаја“.

У претходном периоду је уочила недостатке у управљању информационом безбедношћу код руковалаца ИКТ система од посебног значаја, посебно код органа јавне управе. Зато је Влада Републике Србије донела Стратегије и прописе којима је успоставила Национални CERT са посебним CERT-овима, самостални CERT-ови, CERT у органима власти и CERT академске мреже Републике Србије. Они прикупљају и размењују информације о могућим ризицима и инцидентима, затим обавештавају, упозоравају и саветују лица која управљају ИКТ системима, као и јавност Републике Србије да предузму активности како би предупредили настанак штете и спречили ширење негативних последица по информациону имовину.

Неразумевање ових питања, низак ниво свести о припадности једном систему и друштву, избегавање пријављивања, мали број пријављених инцидената CERT-у, као и други недостаци у примени Закона о информационој безбедности намећу потребу унапређења ове области, посебно у заштити критичне информационе инфраструктуре (даље КИИ) која је од виталног значаја за опстанак друштва у критичним и кризним ситуацијама.

Ова ревизија је имала за циљ да оцени ефикасност управљања инцидентима у ИКТ системима од посебног значаја у складу са Законом о информационој безбедности.

Ревизијом је обухваћено надлежно министарство, док су ЦЕРТ-ови били извори информација о функционисању целокупног система.

ДРИ је утврдила да:

Услед недостатка адекватне размене информација о инцидентима слаби укупна информациона безбедност критичне инфраструктуре, посебно ИКТ система од посебног значаја, онемогућавајући јачање укупне сајбер безбедности што излаже информациону имовину ризику од оштећења и могућег трајног губитка.

Управљање инцидентима је потреба и обавеза свих оператора ИКТ система без обзира на сложеност, али обим имплементираних мера заштите треба прилагодити њиховом

значају/критичности за функционисање друштва и државе у целини. Пријава инцидента и боље реаговање на њихово решавање када имамо ограничене ресурсе није могућа без доброг планирања и утврђивања листе приоритета. Јачање свести о значају информационе безбедности у свим њеним аспектима о већој видљивости у јавном и интернет простору јачаће њену отпорност и укупну информациону безбедност критичне информационе инфраструктуре.

Јединствени систем за управљање инцидентима мора да омогући непосредно објављивање информација о инцидентима одмах по пријави, као и хитно обавештавање оператора који имају исте рањивости, као и целокупне јавности, како би свако могао предузети превентивне мере и активности на спречавању ескалације проблема. Хронични недостатак ИТ стручњака на инспекцијским пословима, на пословима информационе заштите у јавној управи, може решавати овлашћивањем и ангажовањем правних и физичких лица тј. ИТ стручњака из области информационе безбедности. Разменом информација о инцидентима свих делова државног система и синхронизованим деловањем на примени мера заштите оснажиће се њена укупна отпорност и штитиће се информациона имовина од потенцијалне штете и губитака.