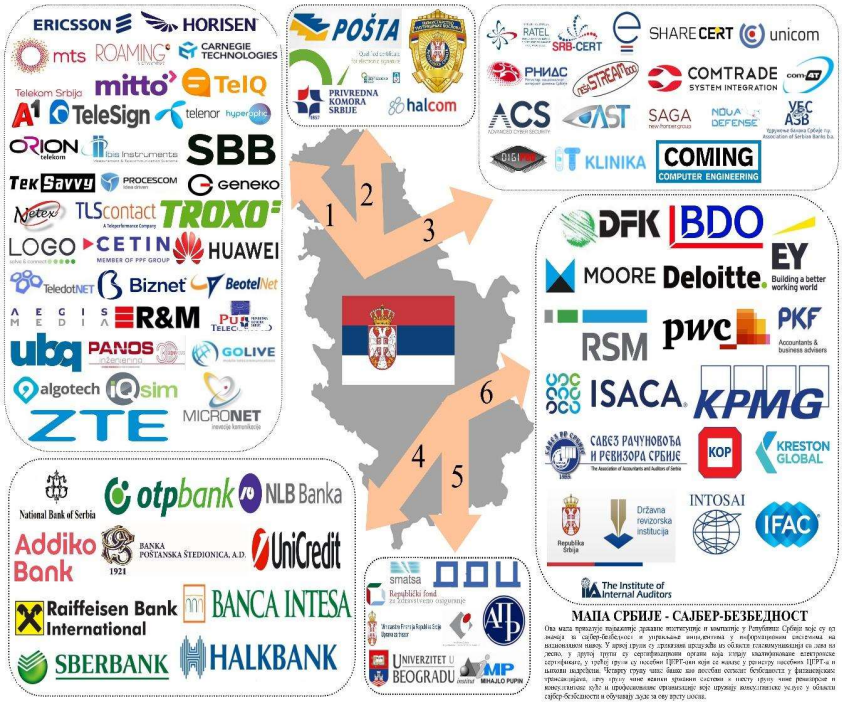
РЕЗИМЕ
ИЗВЕШТАЈА О РЕВИЗИЈИ СВРСИСХОДНОСТИ ПОСЛОВАЊА
„Управљање инцидентима у ИКТ системима од посебног значаја“

НЕДОСТАТАК АДЕКВАТНЕ РАЗМЕНЕ ИНФОРМАЦИЈА О ИНЦИДЕНТИМА СЛАБИ ИНФОРМАЦИОНУ БЕЗБЕДНОСТ, МОЖЕ ДОВЕСТИ ДО ЕСКАЛАЦИЈЕ И ТРАЈНОГ ГУБИТКА ИНФОРМАЦИОНЕ ИМОВИНЕ

Државна ревизорска институција је уочила недостатке у управљању информационом безбедношћу код руковалаца ИКТ система од посебног значаја, посебно код органа јавне управе. Влада Републике Србије је донела Стратегије и прописе којима је успостављен 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.



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 друшта 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 синхоризованим деловањем на примени мера заштите оснажиће се њена укупна отпорност и штитиће се информациона имовина од потенцијалне штете и губитака.

Препоруке

Државна ревизорска институција дала је препоруке Министарству трговине, туризма и телекомуникација да:

- успоставе листу приоритета ИКТ СоПЗ према степену критичности у циљу обезбеђења ефикасног тока опоравка критичне информационе инфраструктуре.
- да у сарадњи са другим надлежним организацијама утврде стварне потребе за обукама, стручним усавршавањем, редовним обавештавањем, као и друге активности намењених крајњим корисницима, запосленима на ИТ пословима у државним органима и организацијама које управљају критичном информационом у циљу јачања свести о значају информационе безбедности и превентивним мерама заштите.
- 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.
- изврше категоризацију оператора ИКТ система по величини и критичности, дефинишу минималне/обавезне мере према категорији оператора.
- да у сарадњи са надлежним органима прикупе податке о технолошким решењима оператора ИКТ СоПЗ, обезбеде систем за аутоматизовано обавештавање између CERT-ова и партнера, обезбеде имплементацију и примену.
- обезбеде 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.
- да коришћењем одговарајућих извора прибаве све неопходне податке како би могли да оцене ИТ ризике, пропишу нивое заштите по приоритетима у циљу обезбеђивања ефикасне заштите.
- да се применом дефинисаних критеријума изврши адекватна процена ризика за избор надзираних субјеката.
- успоставе систем колегијалног прегледа од стране овлашћених лица која су компетентна за утврђивање могућих рањивости код оператора ИКТ СоПЗ.