Otklanjanje incidenata u području informacijske i kibernetičke sigurnosti

Sadržaj:

1. Uvod

HAC (u daljnjem tekstu Naručitelj), proglašen je operatorom ključnih usluga u prometnom sektoru te je dužan provesti mjere za podizanje kibernetičke sigurnosti na prihvatljiv nivo sukladno Zakonu i Uredbi o kibernetičkoj sigurnosti operatora ključnih usluga i davatelja digitalnih usluga NN 68/18 (u daljnjem tekstu „Zakon“ i „Uredba“).

Obrambena perspektiva daje uvid u spremnost organizacije za obranu i odaziv na kibernetičke incidente. S tim u vezi Naručitelj nabavlja usluge upravljanja i odaziva na incidente s ciljem smanjivanja potencijalnih šteta od kibernetičkih napada, a koji bi mogli narušiti raspoloživost, integritet ili povjerljivost informacijske imovine ili poslovnih procesa Naručitelja.

2. Opseg projekta

Obveza odabranog Ponuditelja je u suradnji s Naručiteljem definirati proces upravljanja i odaziva na kibernetičke incidente. Upoznavanje s ispravnim procedurama i komunikacijom u slučaju kibernetičkog incidenta primjenjujući primjere dobre prakse ključni je dio upravljanja i odaziva na kibernetičke incidente, dok ovisno od opsega i prirode samog incidenta, od Ponuditelja se traži reakcija kroz sljedeće aktivnosti:

- Identifikacija kibernetičkog incidenta
- Suzbijanje kibernetičkog incidenta
- Oporavak od kibernetičkog incidenta

Ukoliko se utvrdi postojanje incidenta, od Ponuditelja se traži identifikacija istoga koristeći neke od navedenih aktivnosti:

- Pregled snimljenog mrežnog prometa
- Trijaža
- Nadzor mrežnog prometa u stvarnom vremenu
- Forenzička analiza računala, poslužitelja, mobilnih i mrežnih uređaja
- Analiza malvera
- Root-cause analiza

Ponuditelj mora osigurati dežurne inženjere odgovarajuće stručnosti koji će biti po potrebi na raspolaganju Naručitelju u režimu 24/7 i u slučaju sigurnosnog incidenta odazvati se najkasnije unutar 4 sata od poziva na dežurni telefon ili poruku elektroničke pošte. Vrijeme odaziva moguće je izvršiti dolaskom na lokaciju Naručitelja, i/ili daljinskim pristupom, a sve zavisno od težine i utjecaja kibernetičkog incidenta koje prijavi Naručitelj. Za slučaj bodovanja, u obzir će se uzeti vrijeme potrebno dolaska Ponuditelja na lokacije Naručitelja.

Ponuditelj mora Naručitelju pružati kontinuiranu podršku u otkrivanju izvora incidenta, otklanjanja i minimiziranja štete, te prikupljanja dokaza i informacija o tijeku incidenta sve do zatvaranja incidenta.

Naručitelj će osigurati udaljeni ili fizički pristup računalno- komunikacijskoj mreži Naručitelja i svim potrebnim sustavima (npr. sustavu za pretragu i korelaciju događaja (engl. SIEM), imeničkom direktoriju (engl. Active Directory), sustavu za distribuciju softvera, itd.) i kontakte sa relevantnim osobljem (administratorima sustava, vlasnike zahvaćenih sustava i slično).
Obrada dobivenih informacija nakon završetka incidenta predat će se Naručitelju u obliku izvještaja. Izvještaj mora sadržavati Izvršni sažetak, detaljan tehnički opis samog incidenta, te preporuke u otklanjanju i unapređenju informacijske infrastrukture Naručitelja, uz preporuke za primjenu svih potrebnih kontrola (tehničkih, administrativnih, organizacijskih).