Upravljanje sigurnosnim incidentima

Sigurnosni incidenti postali su svakodnevnica, kako u poslovnom tako i u privatnom životu. Sigurnosne prijetnje su sve veće i razornije, a posljedice koje iste ostavljaju često zahtjevaju velik financijski izdatak organizacije. Glavni problem, ukoliko se priča o sigurnosnim incidentima, je kako odreagirati na njih. Rizici koji dovode do incidenata prisutni su svuda oko nas te je potrebno pravilno preventivno djelovati kako bi spriječili nastanak sigurnosnog incidenta ili ukoliko do istog dođe, ublažili posljedice za organizaciju.

Sigurnosni incidenti uključuju sve događaje ili slabosti koje štetno djeluju na poslovanje i pružanje usluga određene organizacije, kao i na samu sigurnost.

Kako prepoznati sigurnosne događaje ili slabosti?
Svaki događaj koji na bilo koji način ugrožava povjerljivost, integritet i raspoloživost informacijske imovine organizacije smatra se sigurnosnim događajem ili slabosti koje treba prijaviti nadležnoj osobi / Timu za upravljanje sigurnosnim incidentima.

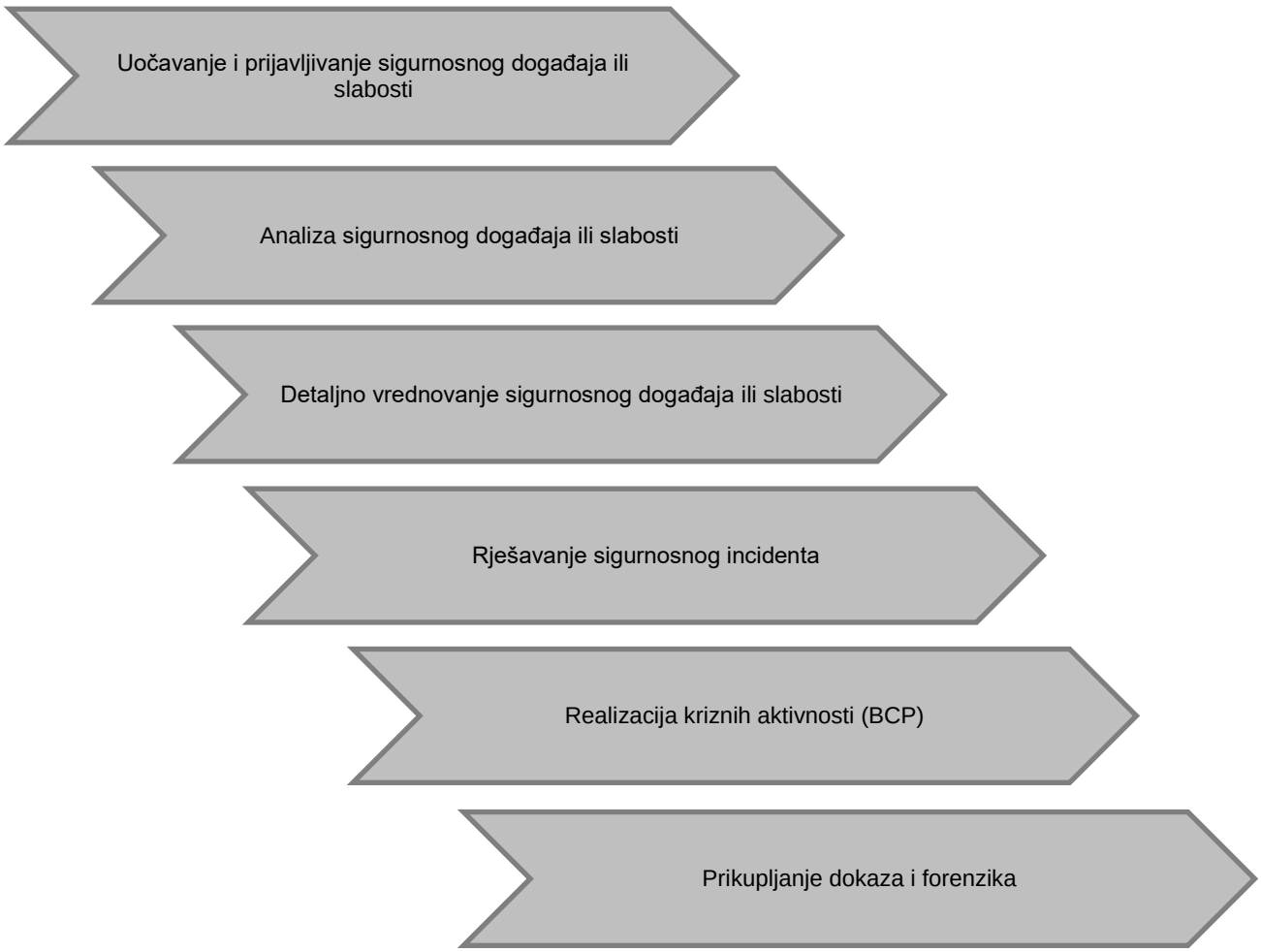
Što su zapravo sigurnosni incidenti?
Sigurnosni incident odnose se na neželjene ili neočekivane sigurnosne događaje koji imaju značajnu vjerojatnost ugrožavanja poslovnih aktivnosti. Neki od primjera sigurnosnih incidenata jesu:

- gubitak usluge, opreme ili uređaja,
- nepravilnost u radu sustava ili preopterećenje sustava,
- ljudske pogreške,
- nekontrolirane promjene sustava,
- nepravilnosti u radu softvera ili hardvera,
- odavanje povjerljivih informacija
- i dr.

Prvi korak u implementaciji procesa upravljanja sigurnosnim incidentima u organizaciji je prepoznati kritičnu imovinu organizacije, provesti procjenu rizika na istoj te definirati aktivnosti kojima će se upravljati tom imovinom na način da se smanji mogućnost nastanka sigurnosnog incidenta.

Kako bi proces upravljanja sigurnosnim incidentima bio učinkovit, organizacija mora imenovati Tim za upravljanje sigurnosnim incidentima čiji članovi su ključni zaposlenici, odgovorni za upravljanje rizicima iz područja IT-a, ljudskih resursa, sukladnosti sa zakonskom regulativom i dr.

Što uključuje proces upravljanja sigurnosnim incidentima?



Ključne aktivnosti procesa upravljanja sigurnosnim incidentima jesu:

- *uočavanje i prijavljivanje sigurnosnog događaja ili slabosti*

Kako bi se otkrili sigurnosni događaji ili slabosti potrebno je pratiti zapise o radu sustava – logove kao i upozorenja koja dolaze od nadzornih alata, npr. detektori, alarmi, antivirusni program i dr.

Bitno je podići svijest unutar organizacije da je dužnost svakog zaposlenika prijaviti uočeni sigurnosni događaj ili slabost.

- *analiza sigurnosnog događaja ili slabosti*

Po prijavi sigurnosnog događaja ili slabosti Tim za upravljanje sigurnosnim incidentima provodi analizu istih s ciljem utvrđivanja da li su uopće relevantni. Ukoliko nisu, o istome obavještava prijavitelja.

- *detaljno vrednovanje prijavljenog sigurnosnog događaja ili slabosti*

Ukoliko se analizom utvrdi da je prijavljeni sigurnosni događaj ili slabost relevantan, provodi se detaljno vrednovanje i donosi odluka o kategorizaciji istih za što je također zadužen Tim. Prilikom vrednovanja Tim može donijeti odluku da se prijavljeni sigurnosni događaj ili slabost prijavi CERT-u (Computer Emergency Response Team) kako bi se kvalitetno provelo vrednovanje sigurnosnog događaja ili slabosti. CERT je nacionalno tijelo koje reagira na računalno-sigurnosne incidente te preventivno djeluje na poboljšanju računalne sigurnosti informacijskih sustava.

Rezultat vrednovanja sigurnosnog događaja ili incidenta je definiranje vrste sigurnosnog incidenta, uzroka koji je doveo do istog te definiranje direktnih i indirektnih posljedica sigurnosnog incidenta na organizaciju (financijski gubitak, prekid poslovnih aktivnosti, nezadovoljenje zakonske regulative, gubitak ugleda i sl.). Temeljem provedenog vrednovanja ispunjava se Izvješće o sigurnosnom incidentu.

- *rješavanje sigurnosnog incidenta*

Rješavanje sigurnosnog incidenta sastoji se od neposrednog rješavanja, izvješćivanja uključenih strana i prikupljanja dokaza i forenzike.

Vrlo je bitno, nakon što se utvrdi da se radi o sigurnosnom incidentu, obavijestiti sve one koji su ugroženi i uključeni u postupak oporavka, bez obzira radi li se o zaposlenicima, vanjskim suradnicima ili trećoj strani.

S obzirom da je za organizaciju jako bitno da se u što kraćem vremenskom periodu ograniči širenje nastalog sigurnosnog incidenta, Tim za upravljanje sigurnosnim incidentima definira aktivnosti rješavanja istog i angažira odgovorne osobe za rješavanje. U slučaju da Tim odluči da organizacija nema resurse potrebne za rješavanje, isti se prosljeđuje vanjskim ugovornim stranama, odnosno provodi se eskalacija.

Nakon što se sigurnosni incident riješi o istome je potrebno izvijestiti sve one koji su bili uključeni u rješavanje istog.

- *realizacija kriznih aktivnosti (BCP)*

Ukoliko Tim za upravljanje sigurnosnim incidentima utvrdi da se sigurnosni incident ne može staviti pod kontrolu uz sve poduzete aktivnosti te isti ugrožava funkcioniranje sustava, potrebno je proglasiti krizno stanje i pokrenuti Plan kontinuiteta poslovanja.

Nakon što je sigurnosni incident riješen provodi se daljnja analiza uočenih sigurnosnih događaja, slabosti i incidenata, kao i nerelevantnih prijava te se traže mogući načini poboljšanja cjelokupne sigurnosti i načina upravljanja sigurnosnim incidentima. Navedena analiza provodi se s ciljem sprečavanja pojave novih sigurnosnih incidenata.

- *prikupljanje dokaza i forenzika*

Prilikom rješavanja sigurnosnog incidenta potrebno je voditi zapise, odnosno evidentirati dokaze o provedenim aktivnostima. Dokaze je potrebno prikupljati za potrebe interne analize problema te kao forenzičke dokaze u slučaju istrage ili pravnog postupka. Način pohrane, vrijeme čuvanja i pristup dokazima definira Tim za upravljanje sigurnosnim incidentima.

Sigurnosni incidenti su neizbježni te ih samim time organizacije trebaju prihvatiti i primjenom prethodno definiranih aktivnosti umanjiti nastalu štetu i poboljšati sigurnost napadnutog sustava.

Svaki identificirani sigurnosni incident potrebno je evidentirati, analizirati i utvrditi uzrok koji je doveo do istog kao i procijeniti posljedice koje ima na organizaciju. Ne postoji mjera koja će nam pružiti potpunu zaštitu te će i nakon primjene istih ostati rizik da se incident ponovi, ali će isti biti pod kontrolom.

Kako bi poboljšale kvalitetu svojih usluga organizacije trebaju primijeniti praksu rješavanja velikog broja incidenata u definiranom roku te uz što manje eskalacija. Neučinkovit proces upravljanja sigurnosnim incidentima potencijalno će povećati mogućnost nastanka incidenata kao i pojavu negativnih učinaka na organizaciju koji mogu dovesti i do prekida poslovanja.