Sadržaj

Terminologija

Područje informacijske sigurnosti razvija se velikom brzinom. Glavni pokretači brzog razvoja su brojni sigurnosni incidenti i napadi koji se događaju na dnevnoj bazi. Kako bi se omogućila učinkovita obrada ovih događaja potrebno ih je na brz i jednostavan način klasificirati. Zbog razlika u opisu i terminologiji koje se koriste u klasifikacijama napada i incidenata nekad nije moguće obradu obaviti učinkovito i jednoznačno. Kako bi se izbjegle dvosmislenosti i nejasnoće prilikom klasifikacije prijetnji potrebno je definirati jedinstvenu terminologiju. Proces utvrđivanja terminologije sastoji se redom od identifikacije pojmova (koncepata), njihovog definiranja te pridavanje naziva. Definicije povezuju pojam koji se definira sa njemu najsrodnijim širim pojmom te na taj način određuje njegovo mjesto u strukturi znanja. Dodatno, one opisuju na koji se način taj pojam razlikuje od drugih pojmova u istom području znanja. Terminološka definicija mora biti dovoljno detaljna da razlikuje pojam i njegov naziv od drugih pojmova i njihovih naziva kako bi se izbjegle nejasnoće. Također, termini trebaju biti definirani tako da se izbjegnu preklapanja značenja. Cilj definiranja terminologije jest korištenje jedinstvenih termina za različite pojedince i organizacije pri sakupljanju, razmjeni i usporedbi informacija vezanih za određeno područje. Terminologija sigurnosnih incidenata jest sustav termina vezanih za sigurnost računalnih sustava. Organizacija CERT definira terminologiju vezanu za određivanje sigurnosnih incidenata u računarstvu, u nastavku je sažetak i objašnjenje najčešće korištenih termina, a detaljan popis se nalazi u dodatnoj literaturi pod [1].

Napad i napadač

Napad na sigurnosni sustav podrazumijeva bilo koji slijed akcija koji proizlazi iz inteligentne prijetnje, odnosno, inteligentni akt kojemu je cilj izbjeći sigurnosne usluge i prekršiti sigurnosne politike sustava. Napad može biti aktivan ili pasivan a izvršavati ga mogu unutarnji ili vanjski napadači. Napadač je osoba koja pokušava izvesti jedan ili više napada kako bi postigla određen cilj. Različiti napadači izvršavaju računalne napade iz različitih namjera. S obzirom na to tko su napadači, koji su njihovi motivi i namjere moguće ih je svrstati u sljedeće kategorije: hakeri, profesionalni kriminalci, zlonamjerni korisnici, vandali, špijuni, teroristi. Pojedine kategorije napadača i njihova motivacija nisu dio ovog rada, više informacija je dostupno u dodatnoj literaturi pod [17].

Meta i žrtva

Metom se smatra bilo koji računalni ili mrežni logički entitet (korisnički račun, proces ili podatak) ili

fizički entitet (komponenta, računalo, mreža). Žrtva je pojedinac ili organizacija koja je pretrpjela incident koji je opisan u izvještaju o incidentu.

Ranjivost

Ranjivost je bilo koji nedostatak ili slabost u dizajnu, implementaciji, radu ili upravljanju sustava koji se može iskoristiti za kršenje sustava sigurnosne politike. Većina sustava ima ranjivost neke vrste, ali to ne znači da su ti sustavi neupotrebljivi. Nije svaka prijetnja rezultat napada a tako ni svaki napad ne mora biti uspješan. Uspjeh ovisi o stupnju ranjivosti, snazi napada i učinkovitosti svih protumjera u uporabi. Ako su napadi potrebni za iskorištavanje ranjivosti vrlo složeni i teški za provesti, onda ranjivost može biti podnošljiva. Ako je korist koju napadač dobiva uspješnim iskorištavanjem ranjivosti dovoljno mala onda ranjivost može biti podnošljiva. Međutim, ako su napadi dobro definiran i jednostavni te ako je ranjivi sustav u upotrebi u širokom krugu korisnika postoji velika vjerojatnost da će biti dovoljno koristi za izvođenje napada.

Šteta i utjecaj

Šteta je namjerna ili nenamjerna posljedica napada koji utječe na normalan rad ciljanog sustava ili usluge. Utjecaj opisuje rezultat incidenta izražene u smislu zajednice korisnika (npr. financijski troškovi ili neki drugi poremećaj).

Događaj, incident i sigurnosni incident

Događaj je akcija usmjerena na metu koja namjerava utjecati na promjenu stanja mete. Točnije, vidljiva pojava u sustavu ili mreži. Incident je događaj koji može dovesti do nezgode ili nesreće koja nije ozbiljna. Sigurnosni incident je događaj koji uključuje kršenje sigurnosne politike, zakona i drugo. Predstavljaju veći problem od incidenata budući da utječu na sigurnost sustava. Sigurnosni incident može biti logičke, fizičke ili organizacijske prirode (npr. gubitak tajnosti, krađa informacija, požar, alarm koji ne radi ispravno). Sigurnosni incidenti mogu se izazvati namjerno ili slučajno (npr. ne zaključavanje vrata). U nastavku se razmatraju isključivo sigurnosni incidenti te će se koristiti pojam incident radi sažetosti.

Reference

1. [1] Arvidsson J., Taxonomy of the Computer Security Incident related terminology http://www.terena.org/activities/tf-csirt/iodef/docs/i-taxonomy_terms.html
2. [2] Howard J., An Analysis of Security Incidents on the Internet, CERT, 1999. http://www.cert.org/archive/pdf/JHThesis.pdf