Bezbjednost i zaštita informacionih sistema

2. Sigurnost

Definicija i ciljevi sigurnosti. Model, metode i aspekti zaštite.

Prof. dr Nikola Žarić

e-mail: zaric@ucg.ac.me

Definicija sigurnosti

Uvijek treba imati na umu: apsolutna sigurnost ne postoji

Sigurnost je proces održavanja prihvatljivog nivoa rizika, a ne završno stanje, tj. nije konačni proizvod. Sigurnost kao proces zasnovan je na:

(1) Procjeni (assesment)

- Smatra se posebnom akcijom, zato što je u vezi sa polisama, procedurama, upravljačkim funkcijama, tehničkom procjenom stanja sigurnosti i drugom regulativom.
- Ako bilo koji od ovih elemenata unese grešku u procjenu, sve sledeće operacije imaće posljedice toga

Definicija sigurnosti

(2) Odgovoru (response)

- Odgovor je **proces oporavka, tj. liječenja od posljedica upada**.

- **Aktivnosti u okviru** odgovora mogu se izvesti po principu:
  - “zakrpi i nastavi”, koji predviđa posjedovanje **kopija podataka**, ili
  -“goni i presudi”, koji predviđa primjenu **digitalne forenzike**

- Ranija praksa je predviđala prvenstveno oporavak funkcionalnosti sistema koje su oštećene napadom.

- Novija praksa se zasniva na pravnim sredstvima i prikupljanju dokaza protiv napadača.

Definicija sigurnosti

(3) Riziku (risk)

Rizik, u kontekstu sigurnosti je mjera opasnosti, tj. mogućnost da se desi oštećenje ili gubitak neke informacije, hardvera, intelektualne svojine, prestiža ili ugleda.

Rizik treba definisati eksplicitno, kao što je na primjer “rizik kompromitacije integriteta baze klijenata“ ili “rizik odbijanja servisa od strane *on-line* portala banke“.

Rizik se obično izražava u obliku jednačine rizika :

Rizik = Prijetnja X Ranjivost X Vrijednost imovine

Definicija sigurnosti

(4) Prijetnji (threat)

Prijetnja je **“strana” sa sposobnostima i namjerama da eksploatiše ranjivost napadnute “ strane “**

- Ova definicija prijetnje je stara nekoliko decenija i konzistentna je sa načinom koji se koristi da se opišu teroristi.
- Prijetnja je ili **struktuirana** ili **nestruktuirana**.
- Struktuirane prijetnje su sa formalnom metodologijom, finasijskim sponzorom i definisanim ciljem. Ove prijetnje uključuju ekonomske špijune, organizovane kriminalce, strane obavještajne službe i takozvane „informatičke ratnike“.

Definicija sigurnosti

(5) Ranjivosti (vulnerability)

Ranjivost je **slabost u nekoj vrijednosti, resursu ili imovini koja može biti iskorišćena**, tj. eksploatisana.

Ranjivost se **uvodi kroz loš dizajn, implementaciju ili "zagađenje" sistema**:

- Loš dizajn je greška kreatora sistema. Proizvođač koji piše loš kod (kod koji sadrži bagove) kreira osjetljiv proizvod koji se može lakše "razbiti". Napadač će iskoristiti slabosti u arhitekturi softvera.
- Implementacija je odgovornost klijenta koji instalira proizvod, da se pridržava dokumentacije proizvođača.

Definicija sigurnosti

- Zagađenje” se odnosi na mogućnost da se dostigne stepen “iznad” namjeravane upotrebe proizvoda.

Dobro dizajnirani softverski proizvod treba da izvrši namjeravanu funkciju i ništa više od toga.

Na primjer, Web server koji publikuje stranice u inet/wwwroot direktorijumu, ne smije dozvoliti da korisnik iz njega “preskoči” i u komandno okruženje.

Odluke koje ponekad donesu proizvođači opreme i softvera i korisnici mogu da dovedu do “zagađenja“.

Definicija sigurnosti

Sofverska ranjivnost

Postoji više tipova softverskih ranjivosti. Neke su rezultat nenamjernih grešaka u kodu:

- Jedan primjer iz loše programerske prakse: zbog propusta da se provjeri dužina niza prije smiještanja u fiksni broj karaktera otvara se mogućnost izvršenja zlonamjernog programa unutar legitimnog programa.

- Zapravo, kada se niz smiješta u odredište koje je kraće od njegove dužine dešava se *buffer overflow* i legitimni program može biti prepisan zlonamjernim kodom.

Definicija sigurnosti

Drugi primjer ja korišćenje programskih *backdoor* rutina radi održavanja programa. Programeri postavljaju *backdoor* rutine da bi kasnije, ako zatreba, zaobilazili mehanizme kontrole.

Ostale ranjivosti softvera su povezane sa dizajnom aplikacije.

Provjera programa od strane drugih smanjuje ranjivosti proizvedenu nenamjernim greškama ili *backdoor* kodom i predstavlja dobru programersku praksu.

Ostale vrste ranjivosti je teže eliminisati ali ih je moguće kontrolisati kombinacijom tehnologije i ustanovljenih procedura rada.

Definicija sigurnosti

Ranjivost usljed konfigurisanja

Ako se u organizaciji koristi više bezbjednosnih proizvoda, tada svi bezbednosni sistemi moraju biti konfigurisani tako da se poslovne aplikacije izvršavaju efikasno.

Ispunjenje ovog zahtjeva otvara mogućnost da se unesu greške, na primjer:

- Otvaranje portova na mrežnoj barijeriji koji inače ne bi bili otvoreni ,
- Korišćenje starije verzije VPN klijetna koji je manje siguran i kompatibilan sa drugim aplikacijama ,
- Postavljanje parametra za filtriranje sadržaja manje sigurnih nego sto je preporučljivo.

Definicija sigurnosti

Web ranjivost

Web aplikacije se najčešće sastoje od programskog koda koji se nalazi i izvršava na serverskoj strani i u interakciji je sa bazama podataka i ostalim izvorima dinamičkog sadržaja. Zbog njihove raširenosti, Web aplikacije su postale kritične sigurnosne tačke u komunikaciji između klijenta i servera.

Njihova otvorenost čini ih izloženim prijetnjama sa Interneta, zbog čega su Web aplikacije meta neovlašćenih korisnika. Dodatni problem predstavlja i sve veća kompleksnost Web aplikacija, kao i sve veći broj razvijenih tehnologija i programskih jezika.

Definicija sigurnosti

Indentifikovanjem ranjivosti Web aplikacije omogućava potencijlanom napadaču korišćenje različitih napadačkih tehnika. Ove tehnike se takođe nazivaju i **klasom napada**.

Neke od klasa napada su:

- **SQL ubacivanje** (*SQL Injection*) ,
- **Unakrsno skriptovanje** (*Cross-site Scripting*),
- **RFI** (*Remote File Inclusion*),
- **LFI** (*Local File Inclusion*),
- **Preopterećenje memorije** (*Buffer Overflow*) i drugi.

Definicija sigurnosti

Vrijednost imovine

Vrijednost imovine je mjera vremena i resursa potrebnih da se neka imovina zamijeni ili povrati u svoje prethodno stanje.

Zato se kao ekvivalentan termin može koristiti i “cijena zamjene”.

Server baze podataka koji drži informacije o kreditnim karticama klijenata je više vrijednosti ili cijene zjemene nego radna stanica u nekoj laboratoriji za testiranje softverskih proizvoda.

Ciljevi sigurnosti

Fundamentalni princip sigurnosti informacija, podataka i računarskih mreža zasniva se na sledeća tri elementa:

1. **Povjerljivost (confidentiality)**

Podrazumeva sprečavanje namjernih i nenamjernih pokušaja otkrivanja sadržaja poruka.

Gubitak povjerljivosti može se ostvariti namjernim otkrivanjem podataka ili pogrešnim definisanjem i sprovođenjem prava pristupa na mrežu

Ciljevi sigurnosti

2. Integritet (integrity)

To je mehanizam za obezbjeđenje integriteta i sastoji se u:

- Zabrani modifikacije podataka od strane neautorizovanih lica ili procesa
- Zabrani neautorizovanih izmjena podataka od strane autorizovanih lica ili procesa
- Konzistentnosti podataka interno i eksterno

3. Raspoloživost (availability)

U okviru koncepta sigurnosti raspoloživost obezbjeđuje pouzdan pristup podacima i mrežnim resursima

CIA = Confidentiality , Integrity, Availability