Provjera ranjivosti u službi unapređenja sigurnosti mreže i mrežom dostupnih servisa i usluga

Marko Stanec
Nacionalni CERT

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Sadržaj

- O Nacionalnom CERT-u
- Što je ranjivost?
- Provjera ranjivosti računalnog sustava
- Umjesto zaključka

O Nacionalnom CERT-u

- Osnovan je 2008. godine u skladu sa Zakonom o informacijskoj sigurnosti
- Zadaća mu je očuvanje sigurnosti javnih informatičkih sustava u RH
- Korisnici Nacionalnog CERT-a:
  - Građani RH
  - Poslovni subjekti – tvrtke, banke i sl.
  - ISP-ovi, abuse službe, pružatelji hosting usluga
  - Institucije
  - …
  - Generalno gledajući - svi korisnici interneta u RH

CARNet HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA CROATIAN ACADEMIC AND RESEARCH NETWORK

Nacionalni CERT

Usluge Nacionalnog CERT-a

- Proaktivne mjere:
  - novosti, sigurnosne preporuke, tehnički dokumenti, sigurnosni alati
  - javni nastupi, brošure
  - provjera ranjivosti

- Reaktivne mjere:
  - prikupljanje informacija o kompromitiranim računalima i incidentima (HR@SRU)
  - obrada incidenata
  - analiza softvera i forenzika malvera i poslužitelja po potrebi

Što je ranjivost?

- Slabost računalnog sustava koju je moguće slučajno aktivirati ili namjerno iskoristiti
- Stanje ili skup stanja koja mogu omogućiti nekoj prijetnji da utječe na resurse računalnog sustava
- Prisutna u bilo kojem djelu računalnog sustava
- Najčešće u korisničkim programima i operativnom sustavu (greške u programskom kodu)
- Ranjivost sama po sebi ne izaziva štetu, potrebna je prijetnja

Iskorištavanje ranjivosti

- Uvjeti za iskorištavanje ranjivosti:
  - prisutnost nedostatka u sustavu
  - pristup nedostatku od strane napadača
  - sposobnost napadača da iskoristi nedostatak

- Iskorištavanje ranjivosti dovodi do ugrožavanja osnovnih značajki sigurnosti informacijskog sustava:
  - tajnost
  - cjelovitost
  - dostupnost

Primjeri propusta SSL/TLS protokola

- Kriptografski protokoli za sigurnu komunikaciju putem interneta
- **Heartbleed**
  - omogućeno dohvaćanje korisničkih podataka, ključeva, certifikata
- **POODLE**
  - kompromitacija sigurne komunikacije
- **FREAK**
  - kompromitacija sigurne komunikacije

Posljedice iskorištavanja ranjivosti

- Gubitak efektivnosti
- Nepovoljni uvjeti poslovanja
- Gubitak poslovanja
- Gubitak ugleda
- Financijska šteta

Što je provjera ranjivosti?

- Postupak identifikacije poznatih ranjivosti računalnih sustava i mreža
- Korištenje specijaliziranih alata
- Analiza dobivenih rezultata
- Generiranje izvještaja

Postupak provjere ranjivosti

- Prikupljanje podataka o uređajima spojenima u pojedini segment mreže:
  - Vrsta i tip uređaja
  - Inačica operativnog sustava
  - Popis otvorenih portova
  - Popis pokrenutih servisa
- Pridruživanje informacija o pronađenim ranjivostima
- Generiranje odgovarajućeg izvještaja
- Temeljita analiza dobivenih rezultata

Kada raditi provjeru ranjivosti sustava?

- Izmjene u konfiguraciji uređaja
- Izmjene u topologiji mreže
- Dodavanje novog uređaja u mrežu
- Dodavanje novih servisa i usluga
- Kod objave novih kritičnih ranjivosti
- Periodički – barem jednom godišnje

Umjesto zaključka...

„Jedini informacijski sustav koji je zaista siguran je onaj koji je ugašen, isključen iz napajanja, zaključan u sefu od titana, zakopan u betonskom bunkeru, te okružen nervnim plinom i dobro naoružanim čuvarima. Čak ni tad, ne bih se baš kladio na njega."

Eugene H. Spafford

Computer Operations, Audit and Security Technology (COAST)

Purdue University