Pregled najznačajnijih sigurnosnih problema u CARNet mreži

Nataša Glavor

Hrvatska akademska i istraživačka mreža - CARNet

natasa.glavor@carnet.hr

Sažetak

CARNet CERT je na osnovu prikupljenih podataka u protekloj godini sastavio popis najznačajnijih sigurnosnih problema u CARNet mreži. Podaci su prikupljeni iz većeg broja izvora: incidenata prijavljenih CARNet CERT-u i Abuse službi, upita i informacija dobivenih od korisnika, podataka iz usluge provjere ranjivosti, podataka dobivenih od drugih CARNetovih odjela, te izvještaja dobivenih od drugih organizacija u svijetu.

1. Uvod

Kada govorimo o problemima u kontekstu informacijske sigurnosti, govorimo o rizicima za sigurnost informacijskog sustava koji zahtijevaju našu pozornost. Pritom se rizik se najčešće definira kao umnožak vjerojatnosti (engl. likelihood) i utjecaja (engl. impact) nekog negativnog događaja:

RIZIK = VJEROJATNOST * UTJECAJ

To znači da negativni događaj s većom vjerojatnosti i manjim utjecajem može imati jednaki rizik kao događaj s velikim utjecajem i manjom vjerojatnošću. Negativni događaji s velikom vjerojatnošću i utjecajem predstavljaju najveći rizik za informacijski sustav.

U ovom radu iznesen je pregled najvećih sigurnosnih problema u CARNet mreži prema riziku. CARNet mreža je velik i složen sustav u kojem nije jednostavno precizno kvantificirati rizike te stoga ovi problemi nisu poredani po značaju.

2. Sigurnosni problemi

E-mail spam je vjerojatno najznačajniji sigurnosni problem na Internetu. Iako jedna spam poruka ima zanemariv utjecaj u odnosu na ostale vrste napada, zbog svoje velike učestalosti e-mail spam ima značajne posljedice. Prema konzervativnoj procjeni, gotovo 80 do 85% ukupnog e-mail prometa otpada na spam poruke. Osim opterećenja mrežnih i računalnih resursa, šteti koju uzrokuje spam treba pribrojiti i troškove sustava za filtriranje spama u koje se ulažu značajna financijska sredstva i ljudski resursi. E-mail spam koristi se i za druge vrste napada, primjerice phishing.

Phishing je oblik napada koji nema veliku učestalost, u smislu broja korisnika koji "nasjednu" na prijevaru, ali zbog velikog utjecaja u slučaju uspješnog napada, ukupan rizik je vrlo visok. To se posebice odnosi na napade na korisnike internet bankarstva, pri čemu uspješno izvršen napad ima za posljedicu izravno otuđenje sredstava s bankovnog računa žrtve. U CARNet mreži zabilježeni su phishing napadi na webmail sustave i socijalne mreže. Takvi napadi najčešće imaju za svrhu slanje spama korištenjem računa korisnika, a iako ne

uzrokuju izravnu financijsku štetu, mogu uzrokovati značajne neugodnosti vlasnicima provaljenih korisničkih računa.

Botneti (mreže zaraženih računala s centraliziranim upravljanjem) zbog svoje raširenosti predstavljaju značajan sigurnosni problem na čitavnom Internetu. Botneti se upotrebljavaju za izvođenje različitih tipova napada, primjerice slanja spana, distribuirane DoS napade, krađu lozinki i distribuciju ilegalnih sadržaja. Jedan od najpoznatijih i tehnički najsofticiranijih botneta koji se proširio Internetom zadnje dvije godine nosi naziv Conficker ili Downadup.

Napadi na web aplikacije čine više od 60% svih pokušaja napada na Internetu. Umetanje SQL koda, Cross-site Scripting i umetanje PHP koda najčešći su tipovi ovih napada. Provaljene web aplikacije služe za širenje malicioznog sadržaja i postavljanje lažnih stranica koje služe za phishing napade.

Napadi na klijentske aplikacije Ranjivosti u klijentskim aplikacijama su postale značajnije od ranjivosti u operacijskim sustavima. Najčešće napadane aplikacije su Adobe PDF Reader, QuickTime, Adobe Flash i Microsoft Office, a korisnici često ne trebaju niti otvoriti malicioznu datoteku da bi napad funkcionirao.