Cybersecurity

Sigurnost u kontekstu IT tehnologija možemo definirati kao kontinuirani proces zaštite digitalnih informacija i IT resursa (računala, serveri, usmjernici, preklopnici itd…) od unutarnjih i vanjskih zlonamjernih ili slučajnih prijetnji.

Ovaj proces obuhvaća detekciju, prevenciju i odgovor na prijetnje kroz korištenje sigurnosnih politika, programskih alata i IT servisa...

Vrste hakera:

- Amaterski (Skript kiddies) – vrlo malo znanja posjeduju te koristi postojeće alate i gotove upute
- White Hat – Otkrivaju slabosti u sustavu kako bi ga osnažili tako što ranjivosti komuniciraju prema vlasniku
- Grey Hat – Na pola puta između White i Black
- Black Hat – Zlonamjerni hakeri koji upadaju u sustave kako bi ih onesposobili u bilo kojem smislu
- Organizirani hakeri (Cyber teroristi, cybercriminals, cyberwarriors) – Skupine hakera koje financiraju velike organizicije ili države u svrhu špijunaže, sabotaže, itd…

CIA TROKUT

1. **Povjerljivost (engl. Confidentiality)-privatnost podataka**

   Povjerljivost podataka bi trebala biti zajamčena propisanim korporativnim politikama koje ograničavaju pristup podacima neovlaštenim osobama.

   Povjerljivost osiguravamo kriptiranjem, Username/password, višestrukom autentikacijom i minimiziranjem dostupnosti osjetljivih podataka

2. **Integritet (engl. Integrity)**

   Ovo bi bila konzistentnost podataka i vjerodostojnost podatak tijekom životnog ciklusa podataka.

   Podaci se ne smiju mijenjati prilikom prijenosa.

   Checksum (hash) se koristi za provjeru integriteta podatka, a za zaštitu se koriste File permissions i user access control mehanizmi uz svakako osiguran backup podataka

3. **Dostupnost (engl. Availability)**

   Održavanje opreme, operativnih sustava i softwarea up-to-date kao i izrada backupa osigurava dostupnost podataka u slučaju njihovog gubitka uzrokovanog ljudskim faktorom ili višom silom.

   Za povrat podataka moraju postojati pripremljene procedure.

   Uređaji poput Firewalla, ali i razni drugi mehanizmi mogu štititi od napada poput DoS napada koji imaju za cilj učiniti podatke/uslugu nedostupnom

POSLJEDICE NAPADA:

- Reputation loss
- Data loss
- Loss of sales and revenue
- Loss of intelectual properties
- Identity theft
- …

VRSTE NAPADA

1. **Reconnaissance attack-** ovo je zapravo priprema za napad..npr skeniranje portova ili traženje ranjivih osoba (za social engineering)…
2. **DOS napad-** napada kojim se želi neka usluga učiniti nedostupnom, obično se radi velikim količinama prometa prema ciljanom servisu, ali može se koristiti i posebno dizajniran promet za specifičan servis (koji ga onda sruši)
3. **DDoS-isto kao DoS**, ali s više lokacija odjednom
4. **Man in the middle-** napad koji za cilj ima presretanje komunikacije bez znanja sudionika u komunikaciji s ciljem dobivanja osjetljivih informacija (lozinke, username,…)
5. **Wi-fi password cracking-** hakiranje wireless AP-a u svrhu pristupa mreži (može se koristiti social engineering, brute force napad, network sniffing)
6. **Social engineering-** vrsta napada u kojoj napadač pokušava manipulirati žrtvom kako bi napravila radnje kojima će otkriti povjerljive informacije
    - **Phishing-** napadač šalje email u kojem se predstavlja kao netko drugi kako bi zadobio povjerenje žrtve
    - **Pretexting** –laganje u svrhu dobivanja osjetljivih informacija (npr. lažno se predstavljamo da zovemo iz banke)
    - **Tailgating-** Napadač prati osobu koja ima pravo pristupa sigurnoj lokaciji
    - **Something for something-** napadač traži osobne podatke u zamjenu za poklon

DOS/DDOS NAPADI U REALNOM VREMENU

DoS napadi ciljaju na dostupnost (Availability) sustava

Primjer DoS napada je TCP SYN Flood

- Zloupotrebljava 3-way handshake mehanizam tako što napadač šalje brojne segmente s postavljenom SYN zastavicom (bitom)
- Žrtva na svaki upit odgovara sa SYN/ACK
    - Napadač ne odgovori žrtvi s ACK
    - Započinje nove konekciju
    - Žrtva ostane bez resursa
    - Legitimni korisnici više ne mogu pristupiti serveru.
- Napadač obično koristi lažnu IP adresu tako da kada žrtva odgovara na SYN od napadača, zapravo šalje SYN/ACK na IP adresu koja uopće nije inicirala komunikaciju
- Zbog usmjeravanja prometa na internetu bez obzira što napadač lažira IP adresu odgovor će otići prema mreži u kojoj se ta IP adresa zaista nalazi

KAKO POSTIĆI SIGURNO OSOBNO IT OKRUŽENJE

- Kontrola pristupa svojim računima (višestruka autentikacija)
- Antimalware zaštita na svim uređajima koje koristimo
- Firewall-na računalu ga ne isključivati
- Držati operativne sustave i software up-to-date prema preporukama proizvođača (automatic update)
- Osigurati primjereno wireless mrežu (enkripcija i skriveni SSID)
- Koristiti primjerene lozinke (Passphrases)
- Kriptirati svoje podatke i raditi backup (offsite-cloud)
- Ne izlagati se u velikoj mjeri na internetu
- U mailovima ne klikati na linkove bez provjere („mouse over" to confirm legitemate sources)
- Ne koristiti istu lozinku za sve korisničke račune (Use password manager software)
- Zaključavati računalo ako niste kraj računala
- Slijediti preporuke i smjernice organizacije u kojoj radite

LOZINKE

- Ne koristite riječi ili imena iz rječnika ni na jednom jeziku
- Nemojte koristiti uobičajene pravopisne pogreške riječi iz rječnika
- Nemojte koristiti imena računala ili imena računa
- Korisite posebne znakove kao ! @ # $ % ^ & * ( )
- Lozinka bi trebala imati 10 ili više znakova

PASSPHRASES

- Korisite posebne znakove kao ! @ # $ % ^ & * ( )
- Što dulje to bolje
- Izbjegavajte uobičajene ili poznate izjave, na primjer, stihove iz popularne pjesme