**Lez1 12/11/2024**

**Introduzione al corso**

sicurezza generale = prevenire il ..

**Rischio:** probabilità di subire perdita danni da un attacco

**Rischio = Probabilità verifica \* Danno**

**Sicurezza: conoscenza/consapevolezza/evoluzione** rispetto ai rischiper prevenire vulnerabilità

**sicurezza informatica:**

insieme di prodotti, regole e comportamenti di protezione

principi di **Confidenzialità Integrità Disponibilità (CID** o **CIA)**

**Vulnerabilità:** pto/pti deboli in vari lvls

**Exploit:** attacco che sfrutta vulnerabilità

fare danni, o modificare comportamenti

eseguire rootkit (diventare adm)

i rootkit permettono di creare **backdoor:** accesso al sistema evitando procedure di sicurezza

generalmente usate per scopi di sviluppo o malevoli

***0-day vulnerability:*** vulnerabilità che causano danno immediato, invisibili e frequenti

ci sono delle normative e linee guida che consentano allo sviluppatore di fixare le cose

tipicamente dichiarate da aziende altrimenti da tizi 0 sbatti

è a livello penale

**Attacco:** accesso non autorizzato

**Attivi**(implicano impatto su integrità e disponibilità dati)

**Mascheramento:** impersonare qualcun altro per compiere azioni

**Ripetizione:** imita azioni fatte da qualcun altro intercettandole

**Modifica:** cambiamento di dati e generare casini(grande scala pericolo)

**DoS: Denial of Service:** buttare giù il sito, inondando il sito di richieste e bloccandolo **DDoS: Distributed Denial of Service:** stesso concetto ma + macchine attaccano una vittima

**Passivi**(implicano impatto su autenticazione e riservatezza, non sempre immediati)

**Intercettazione**

**Sniffing:** attacchi alla crittografia dei messaggi

**Attaccanti:** macchine / individuo / gruppo

**malware:** strumento per attaccare

*alcuni tipi:*

**Virus**(si attacca al codice eseguibile)

**Worm**(gira, fa danni)

**Trojan**(fa tutt’altro che quello che è, es finto pdf)

**Botnet**(macchina diversa ma controllata da attaccante connessa con quella originale)(derivano gli attacchi DDoS)

**Ransomware** (programma ruba dati e mette ostaggio, crittografa file nella macchina)

**Spyware** (spia azioni vittima, ottenere info)

**social engineering:** attaccanti umani che sfruttano psiche e sensibilità personale (interne o ext)

**minacce interne:** particolare per aziende, danni causati da lavoratori, “soluzione” contratti, ma meh

**cyber attackers**

**script kiddies:** bimbi hacker

**White hat**

hacker etico, lavoro aziende, legale, test di penetrazione, spacca a fin di bene

**Gray hat**

caotico buono, simili al bianchi ma no contratti, a volte illegali, ma risolvono nì

**Black hat**

il contrario dei white hat

**Crittografia**

situa Alice Bob, Eve intercetta

concetto è A codifica messaggio M con funzione da mandare a B che poi decodificare……..

il messaggio è sempre decodificabile