Kybernetické hrozby a prevence

Kybernetická bezpečnost je soubor opatření, procesů a technologií, jejichž cílem je chránit sítě, počítače, programy a data před útoky, poškozením nebo neoprávněným přístupem. Boj mezi útočníky a obránci je neustálý proces, který se vyvíjí spolu s technologií.

1. Nejčastější typy kybernetických hrozeb

Hrozby můžeme dělit podle jejich cíle a způsobu provedení:

A. Sociální inženýrství (Social Engineering)

Útoky cílící na nejslabší článek bezpečnosti – člověka. Útočník využívá psychologii k získání citlivých údajů.

- **Phishing:** Podvodné e-maily nebo zprávy, které vypadají jako z banky či od kolegů, s cílem vylákat hesla.
- **Smishing / Vishing:** Podobné techniky využívající SMS zprávy nebo telefonní hovory.

B. Malware (Škodlivý software)

Software navržený k infiltraci nebo poškození systému.

- **Ransomware:** Zašifruje data uživatele a požaduje výkupné (ransom) za jejich odblokování.
- **Spyware:** Skrytě sleduje aktivitu uživatele a krade hesla či bankovní údaje.
- **Trojský kůň:** Program, který se tváří užitečně, ale obsahuje skrytý škodlivý kód.

C. Síťové útoky

Útoky zaměřené na infrastrukturu a dostupnost služeb.

- **DDoS (Distributed Denial of Service):** Zahlcení serveru obrovským množstvím požadavků z tisíců infikovaných zařízení (botnetů), což způsobí pád webu.
- **Man-in-the-Middle (MitM):** Útočník tajně odposlouchává komunikaci mezi dvěma stranami (časté na veřejných Wi-Fi).

—

2. Klíčové principy prevence

Obrana musí být vícevrstvá (tzv. **Defense in Depth**). Pokud jedna vrstva selže, další by měla útok zastavit.

A. Technická opatření

- **Multifaktorové ověřování (MFA/2FA):** Nejdůležitější ochrana. I když útočník získá heslo, bez druhého faktoru (kód v mobilu, fyzický klíč) se do účtu nedostane.
- **Pravidelné aktualizace:** Patchování zranitelností v operačním systému a softwaru.
- **Antivirus a Firewall:** Monitorování příchozího provozu a detekce známých hrozeb.
- **Šifrování:** Používání HTTPS, šifrování disků a zpráv (End-to-End Encryption).

B. Zálohování (Pravidlo 3-2-1)

Nejúčinnější obrana proti ransomware.

- Mít alespoň **3** kopie dat.
- Na **2** různých typech médií.
- **1** kopie musí být uložena mimo hlavní lokalitu (off-site / cloud).

—

3. Bezpečnostní procesy ve firmách

Organizace by se měly řídit uznávanými standardy (např. **ISO/IEC 27001** nebo **NIST Framework**).

- **Zero Trust architektura:** Princip „nikdy nevěř, vždy prověřuj“. Žádné zařízení ani uživatel v síti nemá automaticky důvěru.
- **Penetrační testování:** Pravidelné simulované útoky, které odhalují slabiny dříve než skuteční útočníci.
- **Vzdělávání zaměstnanců:** Školení v rozpoznávání phishingových kampaní.

—

4. Co dělat při napadení? (Incident Response)

Pokud dojde k úspěšnému útoku, je nutné mít připravený krizový plán:

```
1. **Izolace:** Odpojení napadeného zařízení od sítě, aby se zabránilo
šíření (zejména u ransomware).
2. **Analýza:** Zjištění rozsahu škod a způsobu průniku.
3. **Obnova:** Obnova systémů ze záloh a změna všech přístupových údajů.
4. **Poučení:** Analýza chyb a posílení obrany pro příště.
```

Související články:

- Kryptografie a šifrování dat
- Síťová bezpečnost: Firewally a VPN

- Penetrační testování v rámci QA

Tagy: security cyber_threats phishing ransomware malware mfa firewalls backup