

## **Základní terminologie**

Kyberprostor = Virtuální prostředí spojující uživatele s požadovanými systémy. Jedná se elektronické médium, spojující globální počítačovou síť.

Kybernetický útok = Jakékoliv úmyslné jednání útočníka v kyberprostoru, které směřuje proti zájmu bezpečnosti dat jiné osoby.

### **Typy útoků:**

- Aktivní útok
  - Používání nástrojů či vlastního skriptu pro přímý útok. Jedná se o formu útoku, kde se aktivně snažíme proniknout skrz zabezpečení systému a získat nad ním kontrolu. Trestný čin, je-li to proti vůli majitele systému.
- Pasivní útok
  - Diagnostika, průzkum systému a jeho slabín. Jde čistě jen o analýzu slabín pro následné zneužití, do systému se nijak nenabouráváme. Pořád se jedná o trestnou činnost.
- Vnější útok
  - Vzdálené nabourání a přístup do systému a jeho kompromitace. Často bývá nahodilé a nepodnikané, ale může se také jednat o koordinovaný zločin.
- Vnitřní útok
  - Autorizovaná osoba přistoupí k zařízení, ale nesprávně používá systém. Může jít o akt z nenávisti vůči nadřízené osobě nebo o jiný druh social engineeringu.

### **Typy hackerů:**

- Novic, Scripteed
  - Malé znalosti v IT, není znalec v oboru, nepíše si vlastní programy. Používá skripty z internetu.
- Blackhat
  - Člověk s většími znalostmi IT. Opisuje kód a zaměřuje se na nenáročné metody (phishing).

- Insider
  - Profesionál v oboru, čerpá znalosti ze svého povolání. Potencionálně nebezpečný, může znalosti buď využít nebo zneužít (Use/Abuse přístup).
- Old hacker
  - Starší legie programátorů, nemá kriminální úmysly, své znalosti používá ke komunitnímu nebo vlastnímu užitku. (Ripování her, videí...)
- Tvůrce virů
  - Neznalci v oboru, nemají kriminální pozadí. Vytvářejí náhodné viry bez přímého účelu.
- Zloděj
  - Jeho jediná motivace je krádež. Je schopen outsourcovat práci aby se dostal k cíli.
- Hacker
  - Profesionální zločinec, často pracuje v organizované skupině.
- White hat, Etický hacker
  - Pomocí znalosti hackingu diagnostikuje informační systémy za účelem zdokonalení jejich zabezpečení a zalepení bezpečnostních děr.

## Malware

- Jakýkoliv škodlivý software

## Červ

- Škodlivý kód, který se šíří ze systému na systém s jediným účelem reprodukce a otevírání cest pro další viry.

## Ransomware

- Škodlivý kód, který zamezuje v přístupu na zařízení pomocí metod jako je například šifrování. Často jde o finanční vydírání.

## Phishing

- Podvodná metoda pro získávání citlivých dat.

## Pharming

- Podvodná metoda předcházející phishingu. Jde o přesun na samotnou podvodnou stránku. (Falšování adres, názvů, rozesílání emailů, atd.)

## Social Engineering

- Soubor metod a technik pro fyzické získání přístupu do daného systému. Jde o interakci s daným prostředím za účelem kompromitace zabezpečení. Nemusí jít jen o interakci se systémem, ale i o interakci s jejich uživateli či administrátory.

## Spyware

- Škodlivý kód, který nemá za úkol kompromitovat systém, ale jen ho odposlouchávat a získávat od uživatele cenné a citlivé údaje pro další zneužití.

## Druhy virů:

- Boot virus
  - Napadá systémové oblasti disku. Při restartu se zapíše do zaváděcího oddílu na disku a zůstává tak nedotknutelný i po reinstalaci operačního systému.
- Souborový virus
  - Napadá pouze COM a EXE soubory se spustitelným kódem. V napadeném programu přepíše část kódu a tím změní jeho velikost a chování.
- Multipartitní virus
  - Kombinace výhod a nevýhod boot virů a souborových virů. Napadá soubory i systémové oblasti.
- Makroviry
  - Napadá makra v dokumentech, kde přepisuje kód viru tak, aby mohl být spustitelný před makro při spuštění v dokumentu. Nejčastější druh viru v kancelářích.

- **Stealth virus**
  - Chrání se před detekcí antivirovým programem za použití tzv. “stealth technik”. Pokouší se přebrat kontrolu nad funkcemi operačního systému a při pokusu o čtení infikovaných objektů vrací hodnoty odpovídající původnímu stavu.
- **Rezidentní viry**
  - Po svém spuštění zůstává v paměti, odebírá systému paměť pro operace.
- **Trojský kůň**
  - Malware, který se tváří jako nějaký jiný software. Může jít o funkční aplikaci (např. Photoshop), která na pozadí skrývá škodlivý software. Jediný způsob jak jej identifikovat je pomocí antivirové ochrany, která rozpozná nesrovnalosti v certifikátu nebo v kódu samotném, pomocí virových databází.
- **Polymorfní viry**
  - Neustále mění svůj kód, aby znesnadnil svou detekci antivirovým programům, které se řídí podle virových databází.

## **Softwarová ochrana:**

- **Antivirový program**
  - Program specializovaný na detekci a odstranění virů a jejich škodlivých kódů. Řídí se nejčastěji podle tzv. virové databáze, která určuje známé druhy virů, pomocí kterých antivirus identifikuje škodlivé soubory. Nejdůležitější aspekt u antivirů je aktualizovat pravidelně virovou databázi.
- **Firewall**
  - Monitoruje a filtruje síťový provoz, aby zabraňoval neoprávněnému přístupu a chránil systém před škodlivými útoky z internetu.
- **Behaviorální analýza**
  - Sleduje chování softwaru a identifikuje podezřelé aktivity, čímž umožňuje rychlou reakci na neznámé hrozby.

- Šifrování dat
  - Zabraňuje neoprávněnému přístupu k citlivým údajům tím, že přenáší data ve formě, která je srozumitelná pouze pro oprávněné osoby nebo zařízení.
- Webová ochrana
  - Filtruje a blokuje přístup k nebezpečným webovým stránkám obsahující malware , phishingové pokusy nebo jinak nebezpečný obsah.

## **Hardwarová ochrana:**

- Trusted Platform Module (TPM)
  - Hardwarový čip integrovaný přímo do počítače nebo jiného zařízení. Poskytuje bezpečné prostředí pro ukládání klíčů, hesel a dalších citlivých informací.
- Secure boot
  - Bezpečnostní funkce, která zajistí, že při spuštění zařízení jsou použity pouze ověřené a podepsané komponenty. Zabrání spuštění neautorizovaného nebo modifikovaného kódu.
- Hardware firewall
  - Hardwarový filtr proti neoprávněným síťovým přístupem nebo útokům. Funguje i když zrovna nefunguje SW (např. při restartu či výpadku).
- Biometrické identifikátory
  - Odblokování zařízení na základě biometrických údajů, jako jsou např. otisky prstů, rozpoznání obličeje, atd.
- Hardware encryption
  - Podpora pro hardwarové šifrování a dešifrování dat. Umožňuje větší škálu bezpečnosti při přenosu dat. Nelze kompromitovat softwarovým útokem.
- Firmwareové zabezpečení
  - Může zabránit modifikaci nebo útoku na nižší úroveň počítače (BIOS/UEFI).

- Hardwarové dvoufázové ověření
  - Kombinace něco co uživatel zná + něco co má. (Např. Heslo a bezpečnostní klíč).
- Hardware Security Modules (HSM)
  - Fyzická zařízení nebo moduly navržené pro bezpečnou správu klíčů. Jsou používány především v bankovníctví a průmyslu.