

Počítačové pirátstvo, počítačová kriminalita


Autori: Daniel Magdolen

Adam Cápalka

" It takes 20 years to build a reputation and a few minutes of cyber-incident to ruin it."

"If you think you know-it-all all about cybersecurity, this discipline was probably ill-explained to you."

Stephane Nappo



Čo je počítačová kriminalita a pirátstvo

Počítačová kriminalita - protiprávne jednanie s využitím informačných technológií, najmä počítačov, na páchanie trestnej činnosti. Ide o útoky na zber, prenos, uchovávanie, spracovávanie, a distribúciu informácií (dát, údajov) prostredníctvom výpočtovej techniky.

Počítačové pirátstvo - je nezákonná činnosť, ktorá zahŕňa nelegálne kopírovanie, distribúciu, používanie alebo predaj softvéru, digitálneho obsahu či iných počítačových zdrojov bez súhlasu vlastníka autorských práv

Rozdelenie kriminality

1. Trestné činy vo vzťahu k počítaču, jeho príslušenstvu a iným nositeľom informácií ako vecí hmotných – **majetková kriminalita**
2. Trestné činy vo vzťahu k software, k údajom, resp. uložených informácií (počítač je cieľ útoku, predmet trestného činu) – **informačná kriminalita**
3. Trestné činy, pri ktorých je počítač prostriedkom k páchaniu (čo nevylučuje súbeh s jednaniami podľa bodu 2.) – **hospodárska kriminalita** (obvykle podvody apod.).

Priama a nepriama kriminalita

Trestné činy spojené so zasahovaním do hardwaru sú zamerané útoky proti počítaču – proti hmotnému majetku.

Trestné činy spojené so zasahovaním do softwaru sú páchané pomocou počítača, t.j. útok na údaje, databázy a počítačové programy – útok proti nehmotnému majetku.

Príklady počítačovej kriminality

- ❑ Kybernetické útoky
- ❑ Šírenie malvéru – vírusy, trójske kone, ransomware
- ❑ Počítačové podvody a krádeže identity – phishing, spear phishing, smishing
- ❑ Finančné podvody – falošné eshopy, internet banking
- ❑ Neoprávnené získavanie a zneužívanie údajov – SQL Injection, data breaches, útoky na heslá
- ❑ Denial-of-Service (DoS) útoky – zahltenie serverov, narušenie dostupnosti služieb
- ❑ Kyberšikana

Motivácia počítačovej kriminality (MOMM)

Motivations - (Kto a prečo) **Opportunities** - (Čo, kedy a kde) **Means** - (Spôsoby) **Methods** - (Druhy metód)



Rozdelenie pirátstva

- 1. Softvérové pirátstvo** – nelegálna distribúcia alebo používanie komerčného softvéru, často cez torrentové stránky, zdieľanie súborov, alebo kópie bez licencie.
- 2. Pirátstvo digitálneho obsahu** – nezákonné zdieľanie alebo sťahovanie digitálnych médií, ako sú filmy, hudba, elektronické knihy, videohry či iný autorsky chránený obsah, bez súhlasu autora alebo vlastníka práv.
- 3. Cracking** – neoprávnené modifikovanie softvéru s cieľom odstrániť ochranné mechanizmy, ako sú licenčné kódy alebo ochrana proti kopírovaniu, aby sa softvér mohol používať bez zakúpenia originálnej licencie.
- 4. Nelegálne získavanie hesiel a prístupov** – neoprávnený prístup k počítačovým systémom, databázam alebo sieťam za účelom získania osobných informácií, softvéru či digitálneho obsahu.

Dôsledky počítačového pirátstva

01

Ekonomické dôsledky:

- Straty pre firmy
- Pokles daňových príjmov
- Strata pracovných miest

02

Právne dôsledky:

- Trestné stíhanie a pokuty
- Súdne spory

03

Technologické dôsledky:

- Malvér a škodlivý softvér
- Znížená kvalita a podpora

04

Spoločenské dôsledky:

- Negatívny vplyv na inovácie
- Porušovanie autorských práv
- Krádež osobných údajov

Bezpečnosť v
súčasnej dobe

Podceňovaná

Málo financovaná

Nedostatočná osveta

Technologické výzvy

Globálne riziko

Dôležitosť počítačovej kriminality

Detekcia a monitorovanie

Zlepšenie schopnosti identifikovať a analyzovať potenciálne hrozby, spolu s neustálym dohľadom a analýzou sieťových aktivít na odhalenie abnormálneho správania.

Responzivita a prevencia

Rýchla a efektívna reakcia na bezpečnostné udalosti a incidenty, spolu s preventívnymi opatreniami, ktoré sú základom pre minimalizáciu rizík a nebezpečenstiev.

Aktualizácia a vývoj bezpečnostných riešení

Aktualizácie, vylepšovanie a prispôsobovanie bezpečnostných riešení sú nevyhnutné na udržanie kroku s meniacimi hrozbami a potrebnou ochranou pred vznikajúcimi zraniteľnosťami.

Vzdelávanie, tréning a spolupráca

Posilnenie postavenia jednotlivcov a organizácií prostredníctvom vedomostí, zručností a partnerstiev s cieľom zvýšiť odolnosť voči kybernetickej bezpečnosti.

Ochrana informácií

Ochrana citlivých údajov a zabezpečenie dôvernosti, integrity a dostupnosti.

Technologické inovácie a výskum

Posúvanie možností, čo umožňuje vytváranie nových aplikácií, softvéru a ďalších digitálnych produktov, dávajúc možnosť vyjadriť kreativitu a zlepšujúc naše každodenné životy.

Vedeli ste, že...

Každých 39 sekund
je uskutočnený
kybernetický útok ?

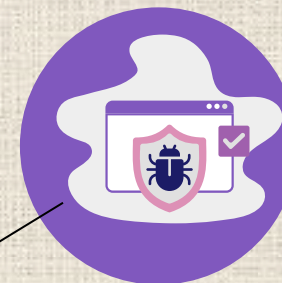
KRIMINÁLNIK

- vandalizmus
- nelegálne aktivity
- phishing



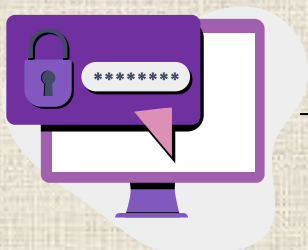
REKREAČNÝ

- sláva
- obmedzené technické zdroje
- malvér



HAKTIVISTA

- emocionálne konanie
- veľké siete
- ransomvér



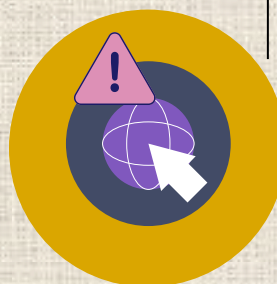
ORGANIZOVANÝ ZLOČIN

- ekonomický zisk
- vysoké technické zručnosti
- DDoS



ŠTÁTOM SPONZOROVANÝ

- vysoko sofistikované útoky
- kybernetická vojna



Obmedzenia bezpečnostných postupov a ich zlepšenie

Zraniteľnosť voči novým hrozbám

Ľudský faktor

Zastarané softvérové a hardvérové riešenia

Nedostatky v implementácii

Nedostatočná odborná príprava

Dostupnosť zdrojov

Pravidelné aktualizácie a vývoj

Viacúrovňové bezpečnostné riešenia

Investície do výskumu a vývoja

Bezpečnostné audity a hodnotenie rizík

Penetračné testovanie

Pravidelné školenia a workshopy

Certifikácie a odborné kurzy

Ďakujeme za pozornost'