

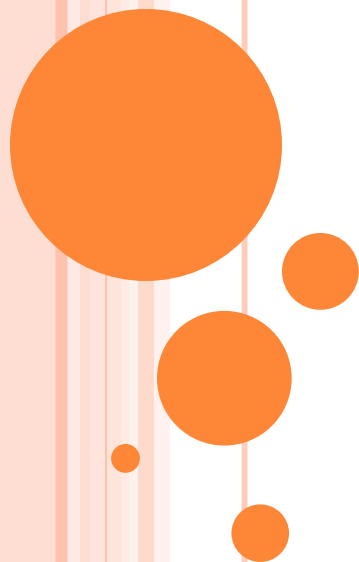
POČÍTAČOVÁ KRIMINALITA

Univerzita Komenského v Bratislave

Právnická fakulta

**Ústav práva informačných technológií a práva
duševného vlastníctva**

2018



POČÍTAČOVÁ KRIMINALITA

- Využívanie informačných technológií, najmä počítačov, na páchanie trestnej činnosti.
- Jej rozmach je priamoúmerný postupujúcej informatizácii spoločnosti.
- Európske krajiny považujú túto formu trestnej činnosti za jednu z globálnych hrozieb a jedným z nástrojov na jej potieranie je **Dohovor o počítačovej kriminalite z 23. novembra 2001.**
 - Slovenská republika ho ratifikovala v roku 2007.



POČÍTAČOVÁ KRIMINALITA

- Štáty EÚ sa dlhodobo zaoberali vymedzením pojmu počítačová kriminalita.
- Príslušné výbory EÚ sa dohodli na definícii počítačovej kriminality, podľa ktorej :

Počítačová kriminalita je nelegálne, nemorálne a neoprávnené konanie, ktoré zahŕňa zneužitie údajov získaných prostredníctvom výpočtovej techniky alebo ich zmenu.

- Počítačovú kriminalitu možno členiť na dve základné skupiny:
 - *priama počítačová kriminalita*
 - *nepriama počítačová kriminalita*



Priama počítačová kriminalita


- Trestné činy zamerané **proti počítaču** ako hmotnému majetku.
 - Jednoduché vyčíslenie škody, pretože poškodený vie presne koľko finančných prostriedkov vynaložil na kúpu počítača.

Nepriama počítačová kriminalita

- Trestné činy páchané **pomocou počítača**, t.j. útok na údaje, databázy a počítačové programy – útok proti nehmotnému majetku.



POČÍTAČOVÁ KRIMINALITA

- Počítače neumožňujú páchať nový typ trestnej činnosti.
 - Poskytujú novú technológiu a nové spôsoby na páchanie už známych trestných činov ako je napríklad sabotáž, krádež, neoprávnené užívanie cudzej veci, vydierane alebo špionáž.
 - Časté motívy páchania počítačovej kriminality:
 - *nedostatočný služobný postup* (zamestnanci sa cítia byť podhodnotení),
 - *hnev na nadriadených,*
 - *žarty a experimenty,*
 - *príležitostné činy* (zamestnanci využívajú bezpečnostné slabiny počítačových systémov svojich zamestnávateľov),
 - *ideologické dôvody.*
- 

NAJVÝRAZNEJŠIE OHROZENIA

1. **Útok na počítač, program, údaje** (vymazanie alebo pozmeňovanie dát, fyzické útoky, nelegálna tvorba a šírenie kópií programov)
2. **Neoprávnené užívanie počítača alebo komunikačného zariadenia** (napr. zamestnancami firiem pre svoj prospech)
3. **Neoprávnený prístup k údajom** (prenikanie do systémov obrany štátnych inštitúcií)
4. **Krádež počítača, programu, údajov, komunikačného zariadenia**
5. **Zmena v programoch a údajoch**
6. **Zneužívanie počítačových prostriedkov k páchaniu inej trestnej činnosti** (daňové podvody, falšovanie)
7. **Podvody páchané v súvislosti s výpočtovou technikou** (hry s finančným vkladom rozosielené následníkom)
8. **Šírenie poplašných správ** (Hoax)



FORMY POČÍTAČOVEJ KRIMINALITY

A) Warez

B) Hacking

C) Počítačové bankové krádeže

D) Ďalšie prejavy počítačovej kriminality



A) WAREZ

- Ide o **odstránenie resp. blokovanie ochranných prvkov** autorských diel chránených autorským právom a následné šírenie týchto diel zbavených ochrany za účelom zisku.



B) HACKING

- Ide o **neoprávnené vniknutie** do cudzieho počítača alebo do cudzieho počítačového systému inou než štandardnou cestou, pri obídení alebo prelomení jeho bezpečnostnej ochrany, teda bez patričných prístupových práv.
- Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva Hacker.
- Najčastejšie metódy na prienik do systému sú:
 - *Útok hrubou silou*
 - *Slovníkový útok*
 - *Odpočúvanie sieťovej komunikácie*
 - *Využitie neukončeného spojenia*
 - *Zadné vrátka*
 - *Odchytenie hesla*



ÚTOK HRUBOU SILOU

- Metóda, ktorá spočíva vo vyskúšaní všetkých možných kombinácií znakov.
- Útočník zostrojí program, ktorý sa pokúša postupným vyskúšaním všetkých možností uhádnuť vaše heslo.
- Rozlúšteniu takéhoto hesla zabránite použitím dostatočne dlhého hesla (pri súčasnom výkone počítačov sa odporúča minimálne 8 znakov).
- Dôležité je použiť čo najširší možný okruh znakov – malé i veľké písmená, čísla a ďalšie symboly. Toto heslo je potrebné tiež často meniť.
- Je nevhodné ukladať hesla na verejne dostupných počítačoch.



SLOVNÍKOVÝ ÚTOK

- Tento útok spočíva v skúšaní všetkých slov daného jazyka.
- Takémuto útoku sa dá predísť tak, že použijete heslo, ktoré nie je slovom žiadneho jazyka.
- Bezpečné heslo si môžete odvodiť napríklad takto: Vezmime si prvé písmená vety, ktorú si ľahko zapamätáme: A predsa sa točí. Galileo Galilei. Dostaneme Aprsto-GaGa.



ODPOČÚVANIE SIEŤOVEJ KOMUNIKÁCIE

- Vaše heslo sa dá veľmi jednoducho získať odpočúvaním nezabezpečených komunikačných liniek ako sú http:// a ftp://.
- Preto nikdy nezadávať svoje údaje do stránky, ktorá nie je zabezpečená šifrovanou komunikáciou https:// alebo ftps:// (poprípade inou).



VYUŽITIE NEUKONČENÉHO SPOJENIA

- Útočník môže využiť, že sa zabudnete odhlásiť zo systému.
- Využije otvorené spojenie, ktoré zneužije vo svoj prospech.
- Niektoré stránky sa proti takýmto útokom chránia automatickým ukončením spojenia pri nečinnosti (preto sa nedá odoslať mail, ktorý píšete dlhšie ako 15 minút).



ZADNÉ VRÁTKA

- Útočník zostrojí program nazývaný Backdoor, ktorý mu umožní pripojiť sa do systému bez nutnosti poznať správne používateľské meno a heslo.



ODCHYTENIE HESLA

- Útočník zostrojí program nazývaný Keylogger, ktorý zaznamenáva stlačené klávesy a takto získané údaje mu odosiela prostredníctvom Internetu.



C) POČÍTAČOVÉ BANKOVÉ KRÁDEŽE

○ Phishing

- Správy (najčastejšie e-mailové), ktoré pod určitou zámkou nabádajú ku zmene osobných údajov.

○ Pharming

- Táto metóda spočíva v presmerovaní názvu www stránky na inú adresu.

○ Spoofing

- Všetky metódy, ktoré používajú hackeri na zmenu totožnosti odosielaných správ.



D) ĎALŠIE PREJAVY POČÍTAČOVEJ KRIMINALITY

○ Sniffing

- Ide o neopravené odpočúvanie, resp. zachytávanie komunikácie na sieti, ktorého účelom je **monitoring diania na sieti, zachytávanie hesiel, čítanie cudzích emailov, správ a pod.**

○ Cybersquatting

- Znamená **neoprávnené registrovanie alebo užívanie domény**, ktoré znie totožne s názvom známeho subjektu s cieľom následného **špekulatívneho predaja** zaregistrovanej domény práve tomuto známemu subjektu, a tým sa materiálne obohatiť, prípadne **parazitovať na jeho dobrej povesti.**



D) ĎALŠIE PREJAVY POČÍTAČOVEJ KRIMINALITY

- **Kybernetické vydieranie**
- **Šírenie poplašnej správy (hoax)**
- **Krádež identity (eiD)**
- **Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty**
- **Šírenie protizákonného obsahu (napr. detská pornografia, extrémistický materiál)**
- **Cyberstalking (virtuálne prenasledovanie)**
- **Počítačové vírusy**
- **Spam (nevyžiadaná pošta)**



ĎAKUJEM ZA POZORNOST.

