KYBERNETICKÁ KRIMINALITA

Krkošková, Zachar

KYBERNETICKÁ KRIMINALITA

Definice:

Kriminalita namířena proti počítačům, jejich HW SW datům a sítím, nebo v ní vystupuje počítač pouze jako nástroj pro páchání trestného činu, případně počítačová síť a k ní připojená zařízen jsou prostřednictvím, v němž se taková činnost odehrává. (Jírovský)

Trestný čin související s technologiemi, počítači a internetem, který má za následek poškození majetku nebo osob. (Schell)

Kyberprostor je všudypřítomný, místně neomezený a velká část útoků má přeshraniční charakter

Vyšetřování Kyberkriminality

Pachatel: může se jím stát kdokoli vzhledem k dostupnosti technologií. Pachatel je označován jako Hacker.

Rogers hackery rozděluje do 8 kategorií

- Nováčci
- Cyber punks
- Vnitropodnikoví
- Drobní zlodějíčkové
- Autoři virů
- Stará hackerská garda
- profesionální zločinci
- Informační bojovníci

Motiv: Finanční zisk, pomsta, prosté hledání vzrušení, zvědavost, zábava, dobrodružství nebo šíření politického nebo ideologického přesvědčení.

Digitální důkazy: může být definován jako „jakákoli data uložená nebo přenesená za použití počítače, která podporují nebo vyvracejí teorii o tom, jak se čin stál, či která pomáhají vysvětlit záměry pachatele, nebo jeho alibi.“

Digitální počítačová stopa: je definována jako „jakákoliv informace s vypovídající hodnotou pro danou relevantní událost, uložená nebo přenášená v digitální podobě.“

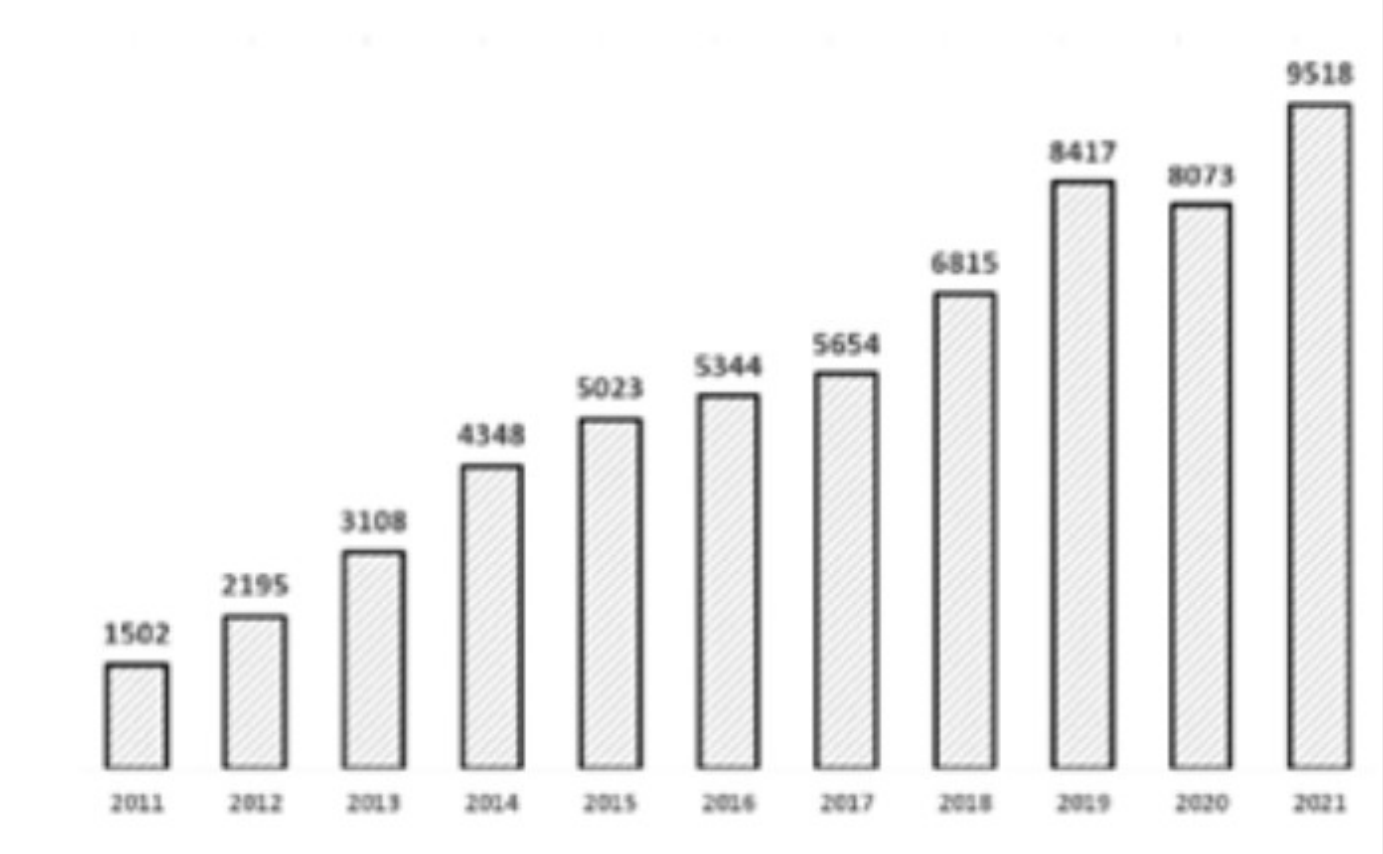
TRESTNÉ ČINY DLE TZ

- **TČ proti majetku**: podvod (§209 TZ), Neoprávněný přístup k počítačovému systému a nosiči informaci (§230 TZ), Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat §231TZ), Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§232 TZ)
- **TČ proti svobodě a právům na ochranu osobnosti, soukromí a listovního tajemství**
- **TČ proti ČR, cizímu státu a mezinárodní organizaci**
- **TČ proti lidské důstojnosti v sexuální oblasti**
- **TČ hospodářské**
- **TČ proti pořádku ve věcech veřejných**

CO SI POD TÍM KONKRÉTNĚJI PŘEDSTAVIT

- **Podvody** (e-shopy, inzerce, romance scam, phishing apod.)
- **Hacking** (neoprávněný vstup do počítačového systému a jeho zneužití)
- **podvodná žádost** o finance často prostřednictvím falešného profilu
- **Podvodné e-shopy** (často bývají zneužity značky známých společností jako je Alza, Česká pošta, Tesco atd.)
- **Mravnostní trestné činy** (týká se ohrožování výchovy dětí, dětské pornografie, navazování nedovolených kontaktů atd.)
- **Trestné činy proti autorskému právu** (neoprávněné sdílení hudby, filmů, softwaru)
- **Násilné projevy a hate crime** (vydírání, vyhrožování, nebezpečné pronásledování, šíření poplašné zprávy, extrémismus)

PODLE ZPRÁVY O STAVU VNITŘNÍ BEZPEČNOSTI A VEŘEJNÉHO POŘÁDKU V ČESKÉ REPUBLICE V ROCE 2021 (VE SROVNÁNÍ S ROKEM 2020) **TRESTNÁ ČINNOST SPÁCHANÁ PROSTŘEDNICTVÍM INTERNETU I JINÝCH SÍTÍ ZAZNAMENALA V ROCE 2021 NÁRŮST NA 9 518 SKUTKŮ (+1 445, +17,8 %).**



TRENDY V KYBERNETICKÉ KRIMINALITĚ

Běžná kriminalita se přesouvá do kyberprostoru

Tento trend značně urychlila pandemie covid-19, kvůli které se do kyberprostoru přesunula celá řada aktivit z reálného světa – jako je nakupování, vzdělávání, pracovní a osobní setkávání či volnočasové aktivity.

Legalizace výnosů z trestné činnosti a zametání stop prostřednictvím kryptoměn

Zpráva o činnosti Státního zastupitelství za rok 2021 uvádí, že: „Drtivá většina finančních prostředků pocházejících z kybernetické majetkové trestné činnosti je přeposílaná do zahraničních peněžních institucí nebo okamžitě převedena na některou z kryptoměn. Za uplynulé období lze pozorovat masivní využívání virtuálních měn (kryptoměn) jako prostředku k zametení stop a současně i k legalizaci výnosů z trestné činnosti.“

Častější případy sofistikovaných trestných činů

Stále častěji se objevují případy sofistikovaných trestných činů, k jejichž provedení je třeba expertních znalostí hackerů. Meziročně stoupl počet skutků tzv. hackingu (ve smyslu útoků na počítačové systémy s následným vydíráním) o 45 %. Tento jev souvisí s prováděním kybernetických útoků nabízejících, či poptávaných jako služba na darknetu.

Ministerstvo spravedlnosti
České republiky

INTERPOL

GENERÁLNÍ ŘEDITELSTVÍ NÁRODNÍ POLICIE

Ministerstvo civilní ochrany

PŘEDVOLÁNÍ K SOUDU

Pro výzkumné účely
(článek 331-1-22 trestního řádu)

Jsem pan Jan Švejnar, generální ředitel Národní policie a šéf Úřadu pro vyšetřování zločinů. Ve spolupráci s Evropskou policejní službou (**INTERPOL**) se na Vás obracím bezprostředně po odhalení kybernetického vniknutí (autorizovaného zejména ve vztahu k dětské pornografii, pornografickým stránkám, kyberpornografii), abych Vás informoval, že jste předmětem různých právních řízení:

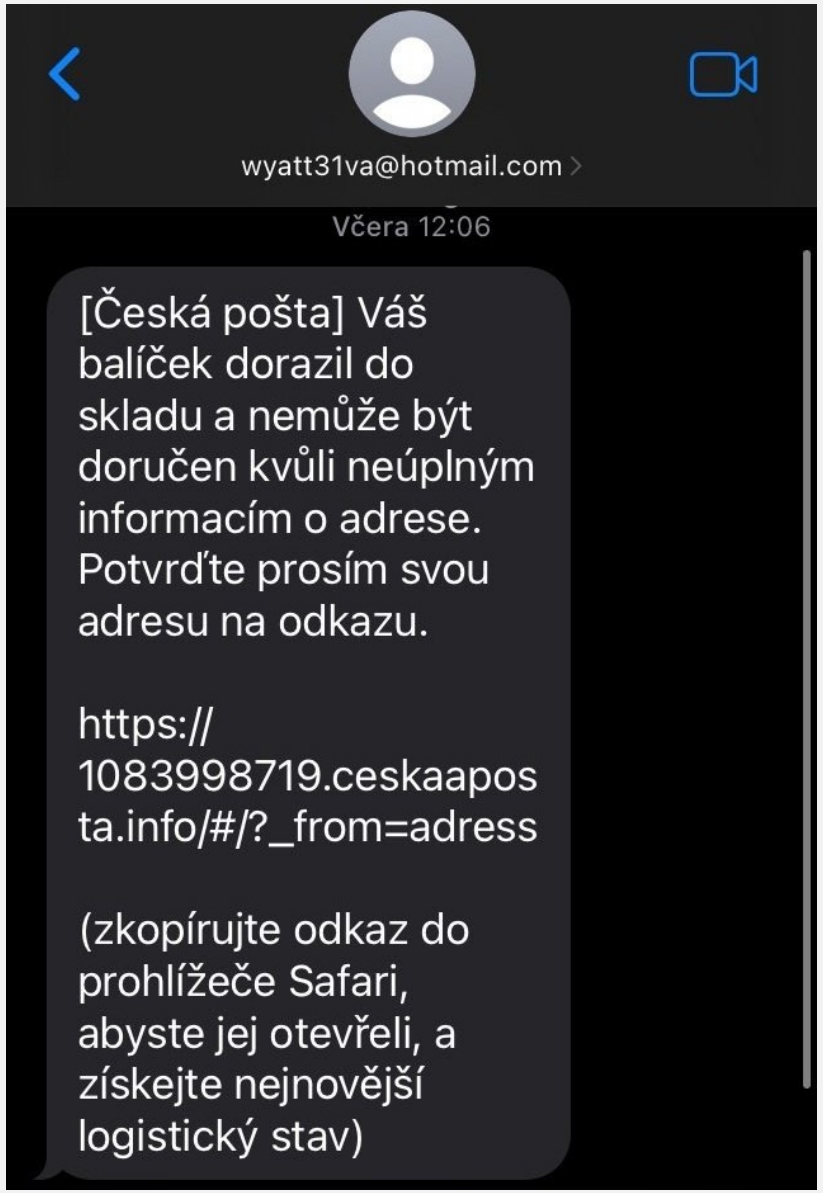
* **PORNOGRAFICKÉ STRÁNKY**
* **DĚTSKÁ PORNOGRAFIE**
* **KYBERPORNOGRAFIE**
* **NESLUŠNÉ OBNAŽOVÁNÍ**

Kontaktujte nás prosím e-mailem a napište nám své důvody, abychom je mohli zohlednit při posuzování sankce a to v přísně stanovené lhůtě 48 hodin.
Po uplynutí této doby zašleme naši zprávu panu Maroš Žilinka Cechům, státnímu zástupci, aby na vás mohl vydat zatykač a zapsat vás na seznam sexuálních delikventů.
Váš spis bude rovněž zveřejněn v médiích, aby se veřejnost a vaše rodina dozvěděla, co na počítači děláte.
Čekáme na vaši reakci, abychom mohli otevřít oznámení.

GENERÁLNÍ ŘEDITEL

Nyní jste varováni.

Gle Jan Švejnar
Generální ředitel Policie České republiky
a vedoucí Úřadu pro vyšetřování trestných činů
24 hodin denně, 7 dní v týdnu



CSSZ:
Davky a prispevky na vasem uctu aktivni.
Ziskat: https://e-cssz.pro/

Prispevek na bydleni od MPSV: https://mp-sv-cz1207.online

UPS: Váš balíček F85896565220 bude podléhat dodatečným celním poplatkům.
Aktualizujte doručení svého balíku prostřednictvím: https://paketovaktualizacia.com

MEZINÁRODNÍ DIMENZE

- Kyberprostor nezná hranice
- Zločinecké organizace
  - Podpora/tolerance států, na jejichž území sídlí
    - Rusko, Čína, Írán, KLDR
    - Výměnou je využití jejich služeb pro zájmy těchto států

NEJČASTĚJŠÍ TYPY AKTIVIT

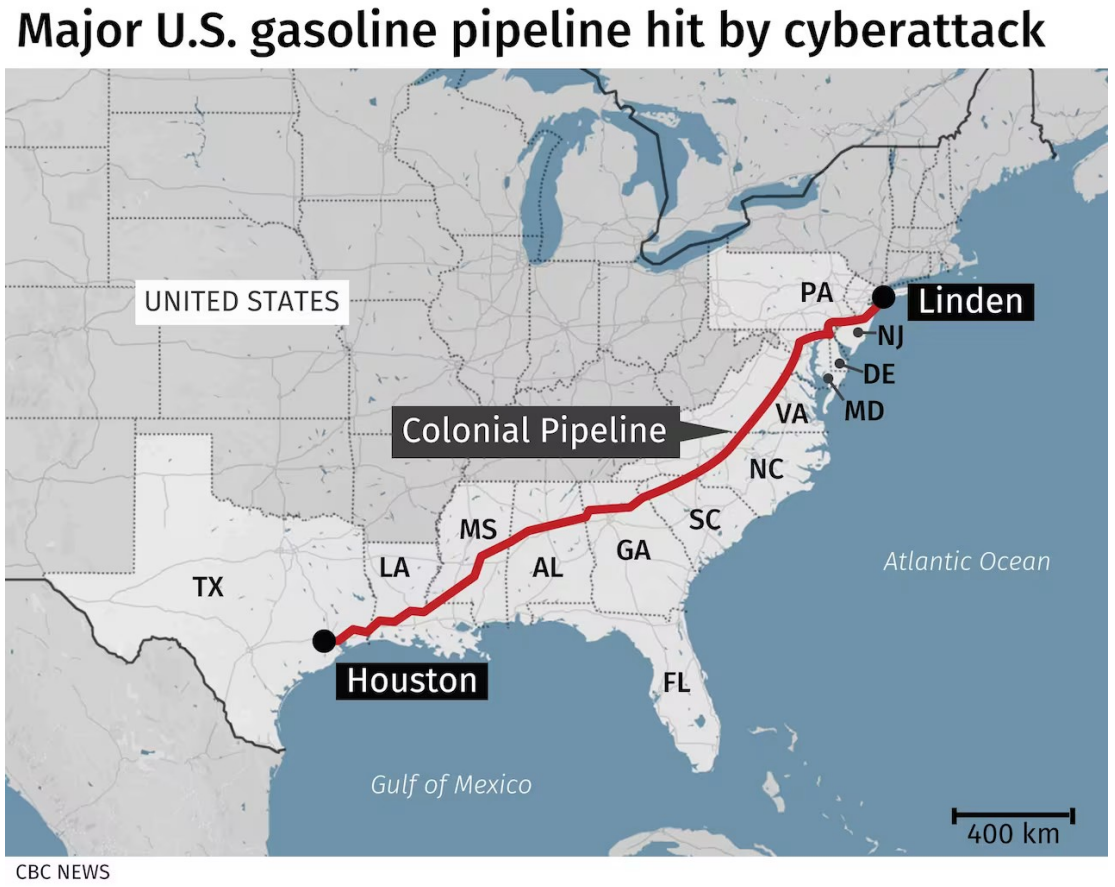
- Ransomwary
  - Ransomware jako služba
- Narušení integrity dat a jejich únik
  - Prodej získaných dat přes Dark Web
- Kyberkriminalita jako služba
  - Možnost zaplatit si službu a konkrétní typ útoku prostřednictvím kryptoměny
  - DDoS, botnety, ransomwary, politické cíle, špionáž, praní špinavých peněz …
- Kyberkriminalita využívána také pro zjednodušení/podporu ”klasické” organizované kriminality
  - Obchod a pašování lidí, zbraní, drog, zbraní…

COLONIAL PIPELINE 2021

- Paralýza dodávek pohonných hmot
- Zajišťuje cca 45 % spotřeby V a JV pobřeží USA
- Energetická síť jako součást kritické infrastruktury

UNOB 2023

- Terčem citlivá data – ukradena a následně zveřejněna
  - Data pracovníků, studentů, provozní dokumenty, faktury, zápisy z porad, finanční výkazy, ekonomické dokumenty, mailová komunikace



Zdroj: CBC News 2021

BOJ PROTI KYBERKRIMINALITĚ – NÁRODNÍ ÚROVEŇ

- Krajská ředitelství policie
- Národní centrála proti organizovanému zločinu (NCOZ) → 2022 Národní centrála proti terorismu, extremismu a kybernetické kriminalitě (NCTEKK)
- NÚKIB – poskytování pomoci zasaženým subjektům dle zákona o kybernetické bezpečnosti
  - GovCERT
- BIS, VZ, ÚZSI
- Důležitá je osvěta široké veřejnosti

BOJ PROTI KYBERKRIMINALITĚ – MEZINÁRODNÍ ÚROVEŇ

- Budapešťská úmluva o kyberkriminalitě
  - Rada Evropy 2004, 66 smluvních států + cca 80 % států světa na ni založilo své zákony upravující kyberkriminalitu
  - Kriminalizace určitého jednání
  - Zajištění procesních kroků a zajišťování elektronických důkazů
  - Přeshraniční a mezinárodní spolupráce – asi nejdůležitější vzhledem k charakteristikám kyberprostoru
  - Otevřena i státům, které nejsou součástí Rady Evropy

BOJ PROTI KYBERKRIMINALITĚ – MEZINÁRODNÍ ÚROVEŇ

- Snahy Ruska a dalších států o novou úmluvu v boji proti kyberkriminalitě
  - Založena Ad Hoc Committee on Cybercrime 2019
  - Cíl je vytvořit novou úmluvu nahrazující Budapešťskou – hlavní argument je a bylo nezapojení všech států světa, proto pod záštitou OSN
  - Kriminalizace určitého jednání – více obsáhlejší ALE návrhy obsahují i politické skutky
- Counter-ransomware initiative
  - Mezinárodní iniciativa na boj s ransomwarem
  - Nedávné společné prohlášení – zasažené vládní/státní instituce nebudou platit výkupné
  - ČR aktivním členem
- Spolupráce v rámci EUROPOL a INTERPOL

POUŽITÉ ZDROJE

- https://www.cbc.ca/news/business/pipeline-colonial-cyberattack-ransonware-1.6020315
- https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/
- https://www.keepersecurity.com/en_GB/how-much-is-my-information-worth-to-hacker-dark-web.html
- https://www.coe.int/en/web/cybercrime/the-budapest-convention
- https://www.csa.gov.sg/News-Events/News-Articles/2023/international-counter-ransomware-initiative-members-come-together-to-strongly-discourage-ransomware-payments
- https://counter-ransomware.org/briefingroom/5de1273d-a905-4e47-8d00-d2e0cdec578d
- https://www.unodc.org/e4j/zh/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html
- https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime-activities.html
- https://rm.coe.int/cyber-buda-benefits-6-december-2023-en/1680ada6a3
- https://ccdcoe.org/library/publications/battling-cybercrime-through-the-new-additional-protocol-to-the-budapest-convention/
- https://www.irozhlas.cz/zpravy-domov/unob-univerzita-obrany-kyberneticky-utok-hackeri_2309271200_kac
- https://dig.watch/processes/cybercrime-ad-hoc-committee

DĚKUJEME ZA POZORNOST