CUSEC

Zodpovednostné vzťahy v kybernetickej bezpečnosti

Modul 5 – Kybernetická kriminalita
Časť 1

Mgr. Petra Dražová, PhD.

Doc. JUDr. Marek Kordík, PhD. LL.M.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Kompetenčné centrum pre reguláciu kybernetickej bezpečnosti, ochrany súkromia a kybernetickej kriminality
CUSEC

PRÁVNICKÁ FAKULTA
Univerzita Komenského
v Bratislave

Financované Európskou úniou Next GenerationEU prostredníctvom Plánu obnovy a odolnosti SR v rámci projektu pod číslom 17R05-04-V01-00002

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

CUSEC

Kybernetická kriminalita

Pojem kybernetická kriminalita 1/2

CUSEC

- 1984 – William Gibson v sci-fi románe Neuromancer spopularizoval pojem kyberpriestor (cyberspace), ktorý sám vymyslel
- poukaz na realitu zdanlivo oddelenú od „vonkajšieho sveta", vo vnútri internetu a ďalších počítačových sietí
- o štyri desaťročia neskôr = pretrvávajúca nejednotnosť pojmu kybernetická kriminalita

Spoločné črty:

- útoky sú páchané **na diaľku**, bez potreby fyzickej prítomnosti, resp. kontaktu s poškodeným
- zasahuje štáty, ekonomiku, občanov, pretože naše **životy a aktivity sú závislé od sietí a technológií**
- **medzinárodný presah**, bez ohľadu na štátne hranice, globálny fenomén
- územný dopad na **viaceré jurisdikcie**, druh trestnej činnosti, ktorá ovplyvňuje prostriedky IKT vo viacerých krajinách
- vyšetrovanie je zložité a náročné, pretože závisí od elektronických dôkazov, ktoré sú nestále (volatilné) a fragilné

CUSEC

Pojem kybernetická kriminalita 2/2

- kybernetická kriminalita, počítačová kriminalita, internetová kriminalita, e-kriminalita,
- gramatický výklad pojmu počítačová kriminalita by mohol viesť k nesprávnemu záveru, že táto nezahŕňa trestné činy páchané prostredníctvom mobilných zariadení či trestné činy páchané na internete
- všeobecná definícia: akákoľvek trestná činnosť, v rámci ktorej je počítač či iná informačná alebo komunikačná technológia v postavení nástroja, cieľa alebo prostriedku, t. j. **protiprávna činnosť, v ktorej je počítačový (informačný) systém nástrojom alebo cieľom, prípadne kombináciou**

Delenie kybernetickej kriminality

CUSEC

I. „CYBER – DEPENDENT" KRIMINALITA

- trestná činnosť „závislá" na prostriedkoch IKT
- „rýdza" kybernetická kriminalita v **užšom zmysle**
- TČ proti dôvernosti (C), dostupnosti (A) a celistvosti (I) počítačových (informačných) systémov a počítačových údajov (CIA trojuholník) – čl. 2 – 6 Budapeštianskeho Dohovoru
- technológia je **cieľom útoku**
- prítomný úmysel páchať ďalšie TČ
- príklady:
  - hacking,
  - distribúcia malvéru,
  - odchytávanie údajov (sniffing),
  - zásahy do systému, dát...

II. „CYBER – ENABLED" KRIMINALITA

- kybernetická kriminalita v **širšom význame**
- trestná činnosť „umožnená" technológiami, vyšší stupeň závažnosti svojim dosahom alebo rozsahom
- technológia predstavuje prostriedok, nástroj na spáchanie trestného činu
- technológia „napomáha" pri páchaní tradičných trestných činov

II.A Počítačové trestné činy (Computer-related offences)

- Čl. 7 – 8 Budapeštianskeho Dohovoru
- spravidla prítomný *dolus specialis* – finančný motív, osobná pomsta...
- trestné činy, pre spáchanie ktorých je použitie IKT podstatnou črtou *modus operandi*
- príklady:
  - podvody,
  - porušovanie práv duševného vlastníctva,
  - kyber-harassment, -stalking, -šikana...

II.B Trestné činy týkajúce sa obsahu (Content-related offences)

- trestné činy súvisiace s nezákonným obsahom
- príklady:
  - TČ detskej pornografie,
  - extrémistický, teroristický obsah...

III. „CYBER – SUPPORTED" KRIMINALITA

- v zásade nemožno hovoriť o kyberkriminalite per se, avšak ide o takú trestnú činnosť, na ktorej odhalenie a vyšetrenie je možné použiť rôzne údaje, v elektronickej podobe, ktoré po sebe zanechal páchateľ, príklady: obsahové údaje, prevádzkové údaje (prípad Pedro Bravo, Matej Čurko, Ján Kuciak)

Právna úprava kybernetickej kriminality

MEDZINÁRODNÉ PRÁVO

- **Dohovor o počítačovej kriminalite** (ďalej aj ako *„Budapeštiansky dohovor"*)
- **Prvý dodatkový protokol týkajúci sa trestnoprávneho postihu činov rasovej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov**
- **Druhý dodatkový protokol o posilnenej spolupráci a sprístupňovaní elektronických dôkazov**

PRÁVO EURÓPSKEJ ÚNIE

- Smernica Európskeho parlamentu a Rady 2013/40/EÚ z 12. augusta 2013 **o útokoch na informačné systémy, ktorou sa nahrádza rámcové rozhodnutie Rady 2005/222/SVV**
- Nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 **o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie**
- Smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, **ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní**

VNÚTROŠTÁTNE PRÁVO

- zákon č. 300/2005 Z. z. **Trestný zákon**
- zákon č. 301/2005 Z. z. **Trestný poriadok**
- zákon č. 91/2016 Z. z. **o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov**

Právna úprava kybernetickej kriminality Medzinárodné právo 1/2

- Budapeštiansky dohovor, ang. *Convention on Cybercrime*
  - prvý komplexný medzinárodnoprávny dokument v oblasti kybernetickej kriminality
  - Rada Európy (otvorenie na podpis v r. 2001)
  - 70 zmluvných strán (stav k 15.aprílu 2024)
  - pre Slovenskú republiku nadobudol platnosť dňa 1. mája 2008[1]
- Členenie: 4 kapitoly
  - Kapitola I: Použitie pojmov (počítačový systém, počítačové údaje, poskytovateľ služieb, prevádzkové údaje)
  - Kapitola II: Opatrenia, ktoré je potrebné prijať na vnútroštátnej úrovni

i. trestné právo hmotné
   - Hlava 1: Trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov (nezákonný prístup, nezákonné zachytenie údajov, zasahovanie do údajov, zasahovanie do systému, zneužitie zariadení)
   - Hlava 2: Počítačové trestné činy (falšovanie počítačových údajov, počítačový podvod)
   - Hlava 3. Trestné činy týkajúce sa obsahu (trestné činy týkajúce sa detskej pornografie)
   - Hlava 4: Trestné činy týkajúce sa porušenia autorských a príbuzných práv

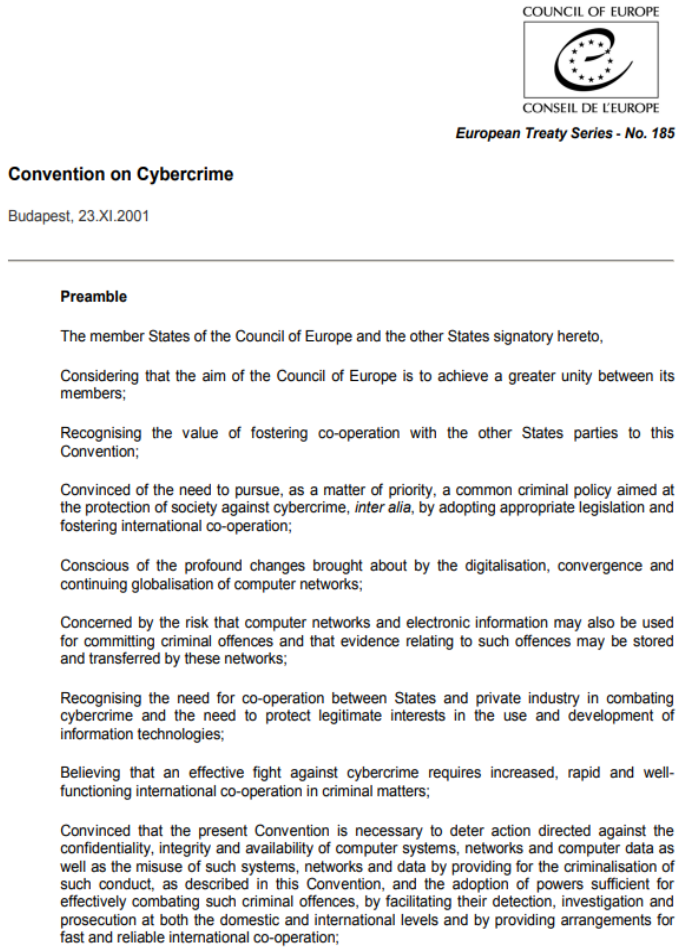
ii. procesné právo

  - Kapitola III: Medzinárodná spolupráca
  - Kapitola IV: Záverečné ustanovenia

1 Oznámenie Ministerstva zahraničných vecí Slovenskej republiky č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite

Právna úprava kybernetickej kriminality Medzinárodné právo 2/2

- Prvý dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa **kriminalizácie činov rasistickej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov** (2003)
  - pre Slovenskú republiku nadobudol platnosť dňa 1. októbra 2023[2]
- Druhý dodatkový Protokol k Dohovoru o počítačovej kriminalite **o posilnenej spolupráci a sprístupňovaní elektronických dôkazov** (2021)
  - Slovenská republika sa doposiaľ nestala signatárom
  - rozhodnutie Rady (EÚ) 2022/722 z 5. apríla 2022, ktorým sa členské štáty poverujú podpísať v záujme Európskej únie Druhý dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa posilnenej spolupráce a sprístupňovania elektronických dôkazov



COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

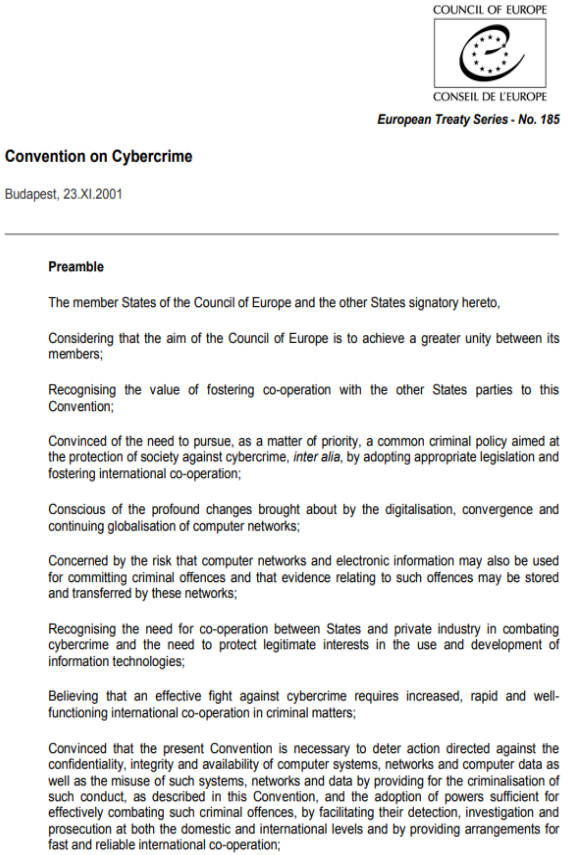
2 Oznámenie Ministerstva zahraničných vecí a európskych záležitostí Slovenskej republiky č. 382/2023 Z. z. k Dodatkovému protokolu k Dohovoru o počítačovej kriminalite týkajúci sa trestnoprávneho postihu činov rasovej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov

MEDZINÁRODNÉ PRÁVO 1/2

CUSEC

- **Dohovor o počítačovej kriminalite („Budapeštiansky dohovor“)**
  - otvorený na podpis v Budapešti 23.11.2001 (aj pre nečlenské štáty RE)
  - počet zmluvných strán (05/2025): 78
  - pre SR platný od 01.05.2008 (oznámenie MZV SR č. 137/2008 Z. z. o podpísaní Dohovoru o počítačovej kriminalite)
  - oddiel 2 (Procesné právo – čl. 14 -21)
  - čl. 14 (2) c) *„Ak článok 21 neustanovuje inak, každá strana uplatní právomoci a postupy uvedené v odseku 1 na zhromažďovanie dôkazov o trestnom čine v elektronickej forme.“*

- **Druhý dodatkový protokol k Budapeštianskemu dohovoru týkajúci sa posilnenej spolupráce a sprístupňovania elektronických dôkazov**
  - prijatý 17.11.2021 VM RE
  - otvorený na podpis 12.05.2022
  - počet signatárskych krajín (05/2025):47 / 2
  - uplatňovať sa začne až po 5 ratifikáciach (čl. 16 ods. 3)
  - rozhodnutie Rady (EÚ) zo 14.2.2023, ktorým sa ČŠ EÚ poverujú ratifikovať v záujme EÚ II. DP
  - SR sa doposiaľ nestala signatárom



COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

European Treaty Series - No. 185

Convention on Cybercrime

Budapest, 23.XI.2001

Preamble

The member States of the Council of Europe and the other States signatory hereto,

Considering that the aim of the Council of Europe is to achieve a greater unity between its members;

Recognising the value of fostering co-operation with the other States parties to this Convention;

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalisation, convergence and continuing globalisation of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;

Recognising the need for co-operation between States and private industry in combating cybercrime and the need to protect legitimate interests in the use and development of information technologies;

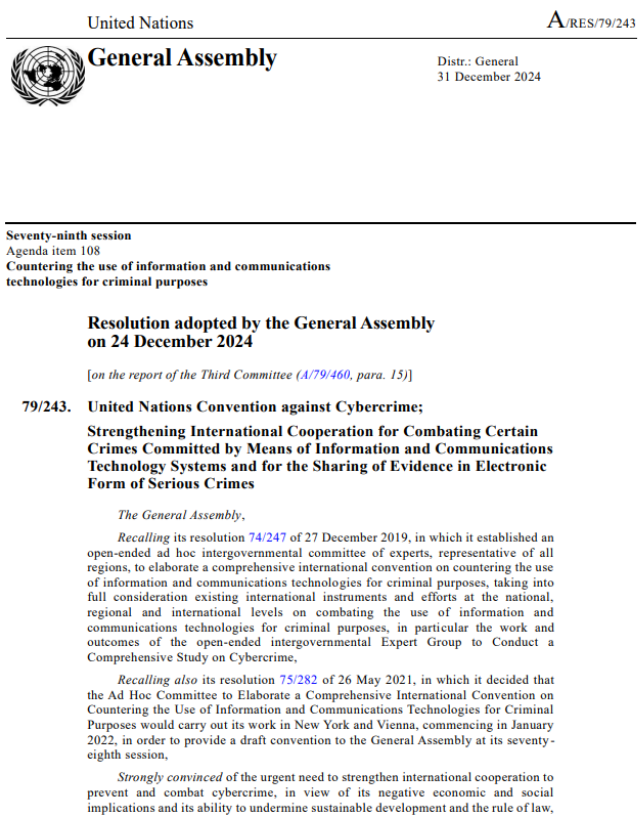
Believing that an effective fight against cybercrime requires increased, rapid and well-functioning international co-operation in criminal matters;

Convinced that the present Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels and by providing arrangements for fast and reliable international co-operation;

MEDZINÁRODNÉ PRÁVO 2/2

CUSEC

- **Dohovor OSN proti počítačovej kriminalite („Hanojský dohovor“)**
  - oficiálny názov: *United Nations Convention against Cybercrime*
  - prijatý dňa 24. decembra 2024 Valným zhromaždením OSN rezolúciou č. 79/243 v New York
  - zatiaľ nebol otvorený na podpis (očakávanie: v polovici r. 2025 – Hanoi (Vietnam)
  - záväznosť nadobudne 90. dňom po uložení 40. ratifikačnej listiny u Generálneho tajomníka OSN (t. j. ak bude ratifikovaný aspoň 40 ČS OSN)
  - čl. 23 ods. 2: *„Except as provided otherwise in this Convention, each State Party shall apply the powers and procedures referred to in paragraph 1 of this article to:*
    a) The criminal offences established in accordance with this Convention;
    b) Other criminal offences committed by means of an information and communications technology system; and
    c) The collection of evidence in electronic form of any criminal offence.“



United Nations A/RES/79/243

General Assembly

Distr.: General
31 December 2024

Seventy-ninth session
Agenda item 108
Countering the use of information and communications technologies for criminal purposes

Resolution adopted by the General Assembly on 24 December 2024

[*on the report of the Third Committee* (*A/79/460, para. 15*)]

79/243. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes

The General Assembly,

Recalling its resolution 74/247 of 27 December 2019, in which it established an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels on combating the use of information and communications technologies for criminal purposes, in particular the work and outcomes of the open-ended intergovernmental Expert Group to Conduct a Comprehensive Study on Cybercrime,

Recalling also its resolution 75/282 of 26 May 2021, in which it decided that the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes would carry out its work in New York and Vienna, commencing in January 2022, in order to provide a draft convention to the General Assembly at its seventy-eighth session,

Strongly convinced of the urgent need to strengthen international cooperation to prevent and combat cybercrime, in view of its negative economic and social implications and its ability to undermine sustainable development and the rule of law,

Vymedzenie základných pojmov

BUDAPEŠTIANSKY DOHOVOR	SMERNICA O ÚTOKOCH NA IS
Počítačový systém – čl. 1 písm. a) *„zariadenie alebo skupinu vzájomne prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré vykonávajú automatizované spracovávanie údajov na základe programu"*	**Informačný systém – čl. 2 písm. a)** *„je zariadenie alebo skupina navzájom prepojených alebo súvisiacich zariadení, z ktorých jedno alebo viaceré automaticky spracúvajú počítačové údaje podľa programu, ako aj počítačové údaje, ktoré toto zariadenie alebo skupina zariadení ukladá, spracúva, opätovne získava alebo prenáša na účely svojho fungovania, používania, ochrany a údržby"*
Počítačové údaje – čl. 1 písm. b) *„ záznam skutočností, informácií alebo pojmov vo forme, ktorá je vhodná na spracovanie v počítačovom systéme vrátane programu schopného spôsobiť, že počítačový systém vykoná určitú činnosť"*	**Počítačové údaje – čl.2 písm. b)** *„zastúpenia skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme vrátane programu, ktorý zabezpečí, aby informačný systém vykonal funkciu "*

Právna úprava kybernetickej kriminality
Právo Európskej únie

- *Primárne právo EÚ*
  - **čl. 83 ZFEÚ** – splnomocňujúce ustanovenie, podľa ktorého možno prostredníctvom smerníc ustanoviť minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v súvislosti s obzvlášť závažnou trestnou činnosťou s cezhraničným rozmerom
- *Sekundárne právo EÚ*
  - smernica 2013/40/EÚ **o útokoch na informačné systémy**
  - nariadenie Európskeho parlamentu a Rady (EÚ) 2023/1543 z 12. júla 2023 **o európskych príkazoch na predloženie elektronických dôkazov a európskych príkazoch na uchovanie elektronických dôkazov v trestnom konaní a na výkon trestu odňatia slobody v nadväznosti na trestné konanie**
  - smernica Európskeho parlamentu a Rady (EÚ) 2023/1544 z 12. júla 2023, **ktorou sa stanovujú harmonizované pravidlá určovania určených prevádzkarní a vymenúvania právnych zástupcov na účely zhromažďovania dôkazov v trestnom konaní**
  - smernica (EÚ) 2019/713 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu
  - smernica (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov
  - smernica 2011/92/EÚ o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii
  - smernica 2009/24/ES o právnej ochrane počítačových programov

CUSEC

Trestné právo hmotné:

- základy trestnej zodpovednosti,
- druhy trestov a podmienky pre ich ukladanie,
- druhy ochranných opatrení a podmienky pre ich ukladanie,
- skutkové podstaty trestných činov

- zákon č. 300/2005 Z. z. **Trestný zákon**
- zákon č. 91/2016 Z. z. **o trestnej zodpovednosti právnických osôb**
- zákon č. 221/2006 Z. z. **o výkone väzby**
- **o výkone trestu odňatia slobody** zákon č. 475/2005 Z. z.

Právna úprava kybernetickej kriminality Vnútroštátna právna úprava- všeobecná časť

- Páchateľ- všeobecný, t.j. každá trestne zodpovedná fyzická alebo právnická osoba.
- osoba inteligentná, uvedomujúca sa nebezpečnosť svojho konania, schopná využívať rôzne anonymizačné techniky s prvkami analytického myslenia v oblasti rizík, spojených najmä s oblasťou kybernetickej bezpečnosti.
- Počítačová kriminalita ako i jej páchatelia sa vyznačujú vysokou mierou latencie a anonymity, spravidla sa táto činnosť vykonáva za peniaze a trend posledných rokov je páchanie počítačovej kriminality ako „Crime as a Service" - profesionálnej služby za odplatu dodávanej klientele, ktorou môžu byť všetky formy organizovaných, zločineckých, teroristických skupín, alebo individuálnych entít, vrátane štátov, alebo ich predstaviteľov.

Právna úprava kybernetickej kriminality Vnútroštátna právna úprava- všeobecná časť

- Miesto činu- determinované §12 TZ. V zmysle tohto ustanovenia je miestom spáchania trestného činu každé miesto, na ktorom:
- páchateľ konal (subjektívna súvislosť), alebo
- nastal alebo podľa predstavy páchateľa mal nastať následok predpokladaný týmto zákonom. (objektívna súvislosť)
- Z uvedeného je zrejmé, že vzhľadom na dostupnosť spoľahlivých anonymizačných techník najmä lokalizačných údajov bude miesto, kde páchateľ konal známe, ak vôbec, v oveľa neskoršom štádiu trestného stíhania. Väčšina prípadov počítačových trestných činov sa posudzuje podľa miesta, kde nastal, alebo podľa predstavy páchateľa mal nastať škodlivý následok.
- Dištančné delikty

Právna úprava kybernetickej kriminality Vnútroštátna právna úprava- všeobecná časť

- Okolnosti vylučujúce protiprávnosť vo vzťahu k počítačovej kriminalite zohrávajú špecifickú úlohu a kvalifikáciu najmä s činnosťami na úseku kybernetickej bezpečnosti, akými sú analýzy rizík zraniteľnosti, najmä testovanie resp. penetračné testovanie podľa §20 ods. 1, písm. a) zákona o kybernetickej bezpečnosti, ako súčasti bezpečnostných opatrení . Aby v praxi takéto penetračné testovanie, v prípade vzniku škody, bolo možné označiť za okolnosti vylučujúce protiprávnosť podľa §27 a nasl. Trestného zákona musia byť splnené nasledovné predpoklady.

Právna úprava kybernetickej kriminality Vnútroštátna právna úprava- všeobecná časť

- Obete počítačovej kriminality v zmysle slovenskej právnej úpravy spĺňajú i definíciu obzvlášť zraniteľnej obete, najmä v prípadoch trestných činov detskej pornografie, nebezpečnému vyhrážaniu, či nebezpečnému prenasledovaniu, alebo nebezpečnému elektronickému obťažovaniu,
- Všetky procesné úkony s obzvlášť zraniteľnou obeťou by mali byť vykonávané ohľaduplne, citlivo a očtk by k nim mali pristupovať ako k neopakovateľným úkonom.
- Vo vzťahu k poškodeným trestného činu podvodu (v terminológií počítačovej kriminality tzv. SCAM) aplikačná prax rozvinula tzv. teóriu primeranej miery opatrnosti poškodeného. (R NS SR I2 Tdo V 21/2013

Právna úprava kybernetickej kriminality Vnútroštátna právna úprava- Osobitná časť

- zákon č. 300/2005 Z. z. **Trestný zákon**
- v dôsledku transpozície smernice 2013/40/EÚ o útokoch na informačné systémy bol s účinnosťou od 1. januára 2016 nahradený trestný čin poškodenia a zneužitia záznamu na nosiči informácií nasledujúcimi trestnými činmi:
  - **§ 247 TZ Neoprávnený prístup do počítačového systému**
  - **§ 247a TZ Neoprávnený zásah do počítačového systému**
  - **§ 247b TZ Neoprávnený zásah do počítačového údaja**
  - **§ 247c TZ Neoprávnené zachytávanie počítačových údajov**
  - **§ 247d TZ Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov**

- zákon č. 301/2005 Z. z. **Trestný poriadok**

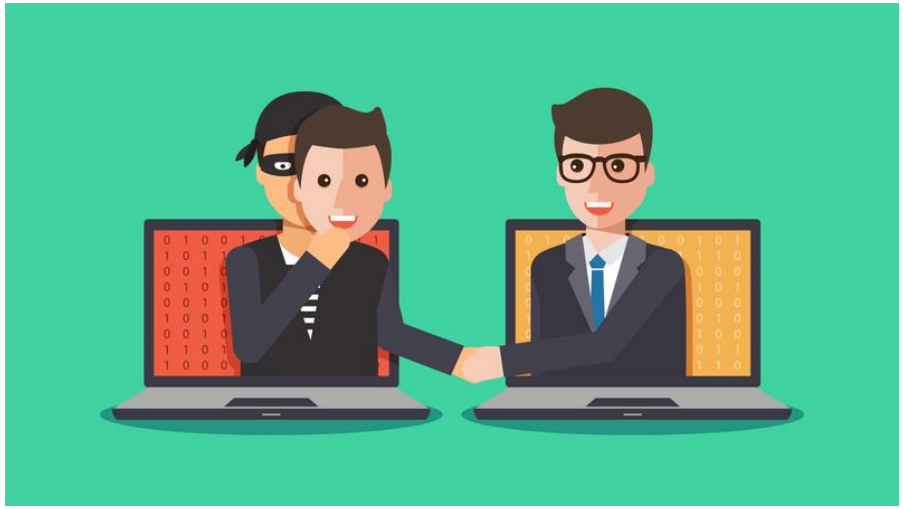
- zákon č. 91/2016 Z. z. **o trestnej zodpovednosti právnických osôb a o zmene a doplnení niektorých zákonov**

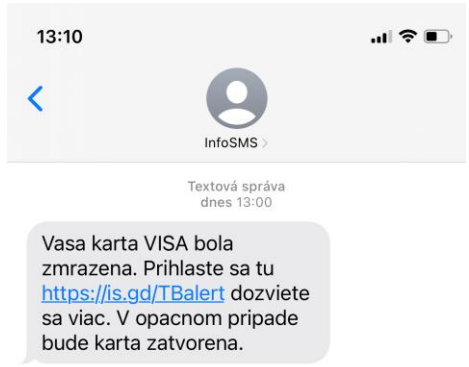
Dohovor o počítačovej kriminalite	Smernica 2013/40/EÚ o útokoch na informačné systémy	Trestný zákon
Čl.2 Nezákonný prístup	Čl. 3 Protiprávny prístup do informačných systémov	§ 247 Neoprávnený prístup do počítačového systému
Čl. 5 Zasahovanie do systému	Čl. 4 Protiprávny zásah do systému	§ 247a Neoprávnený zásah do počítačového systému
Čl.4 Zasahovanie do údajov	Čl. 5 Protiprávny zásah do údajov	§ 247b Neoprávnený zásah do počítačového údaja
Čl. 2 Nezákonné zachytenie údajov	Čl. 6 Protiprávne zachytávanie údajov	§ 247c Neoprávnené zachytávanie počítačových údajov
Čl.6 Zneužitie zariadení	Čl. 7 Nástroje na spáchanie trestných činov	§ 247d Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov

§ 247 TZ Neoprávnený prístup do počítačového systému 1/2

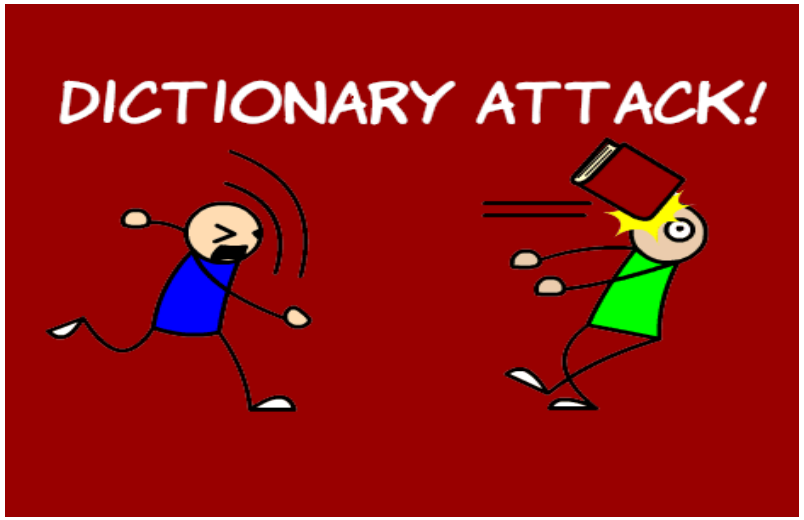
- **§ 247 ods. 1 TZ** *„Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.“*
  - Objekt: ochrana počítačového systému ako celku alebo ktorejkoľvek jeho časti (vrátane technického a programového vybavenia)
  - Objektívna stránka: prekonanie bezpečnostného opatrenia a získanie neoprávneného prístupu do počítačového systému alebo jeho časti
  - Subjekt: ktorákoľvek trestne zodpovedná osoba
  - Subjektívna stránka: úmyselné zavinenie
- spôsobenie škody sa teda v základnej skutkovej podstate **nevyžaduje**, spôsobenie aspoň značnej škody je však okolnosťou umožňujúcou použitie **vyššej trestnej sadzby**
- chránený záujem je porušený nielen vtedy, keď páchateľ prenáša alebo mení údaje v počítačovom systéme bez súhlasu oprávnenej osoby, ale aj vtedy, ak si páchateľ neoprávnene prehliada údaje v počítačovom systéme
- prekonaním bezpečnostného opatrenia je teda každé opatrenie spôsobilé zabrániť neoprávnenému prístupu k počítačovému systému, a teda aj k nosiču dát, napr. *prekonanie zabezpečenia pomocou skrytého HW* (zariadenie zaznamenávajúce všetky heslá, ktoré boli napísané použitím klávesnice, ktoré ich následne prenáša páchateľovi), *session hijacking…*
- vzhľadom na to, že tento TČ je v ods. 1 a ods. 2 **prečinom**, prichádza do úvahy uplatnenie **materiálneho korektívu** - treba skúmať, do akej miery bolo narušené súkromie užívateľa, čo bolo cieľom páchateľa, o aký systém ide (pracovný, súkromný) a pod.

§ 247 TZ Neoprávnený prístup do počítačového systému 2/2






```
[80][http-get-form] host: 192.168.100.155   login: admin   password: password
[80][http-get-form] host: 192.168.100.155   login: admin   password: p@ssword
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567890
[80][http-get-form] host: 192.168.100.155   login: admin   password: Password
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123456
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1234567
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12345678
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1q2w3e4r
[80][http-get-form] host: 192.168.100.155   login: admin   password: 123
[80][http-get-form] host: 192.168.100.155   login: admin   password: 1
[80][http-get-form] host: 192.168.100.155   login: admin   password: 12
1 of 1 target successfully completed, 12 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2017-07-27 15:28:24
```



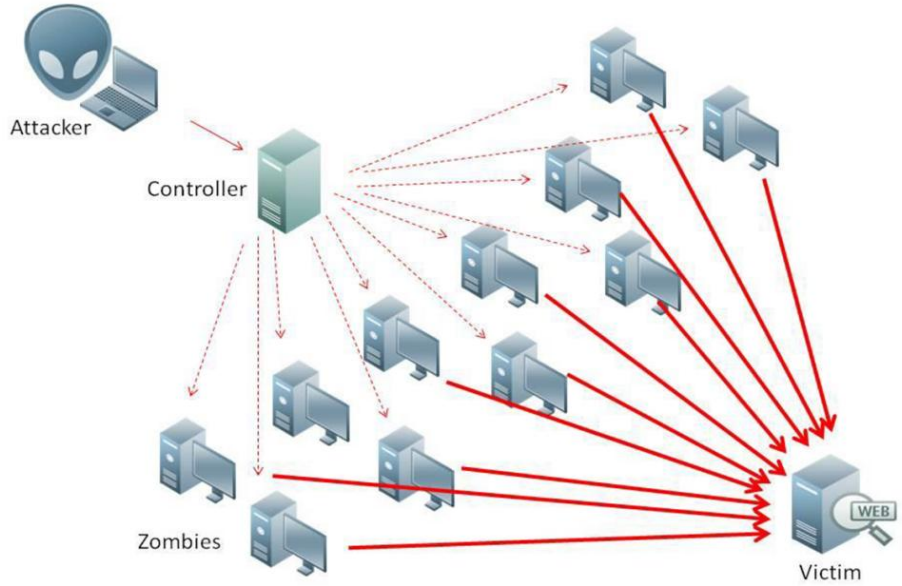
- hacking
- útoky „hrubou silou"
- slovníkové útoky...

§ 247a TZ Neoprávnený zásah do počítačového systému 1/2

- **§ 247a ods. 1 TZ** *„Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti* ***a)*** *neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo znneprístupnením počítačových údajov, alebo* ***b)*** *tým, že urobí neoprávnený zásah do technického alebo programového vybavenia počítača a získané informácie neoprávnene zničí, poškodí, vymaže, pozmení alebo zníži ich kvalitu, potrestá sa odňatím slobody na šesť mesiacov až tri roky.“*
  - Objekt: ochrana počítačového systému ako celku alebo ktorejkoľvek jeho časti pred neoprávneným zásahom
  - Objektívna stránka: alternatívne a) alebo b) v dôsledku čoho sa obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti
  - Subjekt: ktorákoľvek trestne zodpovedná osoba
  - Subjektívna stránka: úmyselné zavinenie
- chránený záujem je porušený vtedy, keď páchateľ koná niektorým z uvedených spôsobov, resp. kumulatívne
- spôsobenie škody sa v základnej skutkovej podstate **nevyžaduje**, spôsobenie aspoň značnej škody je však okolnosťou umožňujúcou použitie **vyššej trestnej sadzby**
- ide napr. využívanie tzv. botnetov, ktoré následne spôsobujú nežiaducu činnosť (SPAM, hosting škodlivých stránok)
- vzhľadom na to, že tento TČ je v ods. 1 **prečinom**, prichádza do úvahy uplatnenie **materiálneho korektívu**

§ 247 TZ Neoprávnený zásah do počítačového systému 2/2

Malware



DoS / DDoS attacks

§ 247b TZ Neoprávnený zásah do počítačového údaja 1/2

- § 247b ods. 1 TZ *„Kto úmyselne poškodí, vymaže, pozmení, potlačí alebo zneprístupní počítačové údaje alebo zhorší ich kvalitu v rámci počítačového systému alebo jeho časti, potrestá sa odňatím slobody na šesť mesiacov až tri roky.“*
  - Objekt: ochrana počítačového údaja, jeho integrita a riadne použitie pred zneužitím, zničením, zneprístupnením a pod.
  - Objektívna stránka: je naplnená poškodením, vymazaním, pozmenením, potlačením alebo zneprístupnením počítačového údaja, zhoršením jeho kvality alebo jeho časti
  - Subjekt: ktorákoľvek trestne zodpovedná osoba
  - Subjektívna stránka: úmyselné zavinenie
- spôsobenie škody sa teda v základnej skutkovej podstate **nevyžaduje**, spôsobenie aspoň značnej škody je však okolnosťou umožňujúcou použitie **vyššej trestnej sadzby**

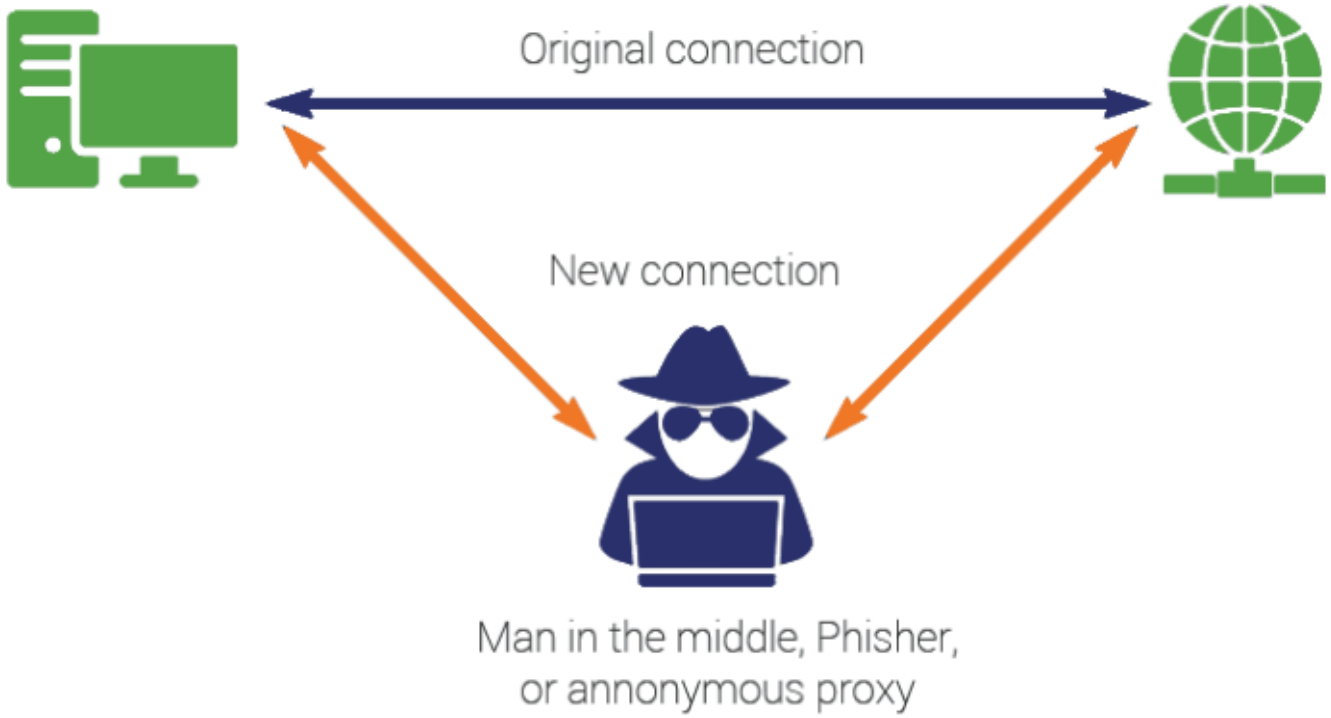
§ 247b TZ Neoprávnený zásah do počítačového údaja 2/2

Ransomware

§ 247c TZ Neoprávnené zachytávanie počítačových údajov 1/2

- **§ 247c ods. 1 TZ** *„Kto neoprávnene zachytáva počítačové údaje prostredníctvom technických prostriedkov, neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v jeho rámci vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje takéto počítačové údaje, potrestá sa odňatím slobody na šesť mesiacov až tri roky.“*
- **§ 247c ods. 2 TZ** *„Kto ako zamestnanec poskytovateľa elektronickej komunikačnej služby spácha čin uvedený v odseku 1 alebo inému úmyselne umožní spáchať taký čin, alebo pozmení alebo potlačí správu podanú prostredníctvom elektronickej komunikačnej služby, potrestá sa odňatím slobody na jeden rok až päť rokov.“*
  - Objekt: ochrana tajomstva informácie, ktorá je neverejne prenášaná z počítačového systému, do počítačového systému alebo v rámci neho
  - Objektívna stránka ad ods. 1: spočíva v neoprávnenom zachytávaní PC údajov prostredníctvom technických prostriedkov, neverejných prenosov PC údajov do PC systému, z neho alebo v jeho rámci, vrátane elektromagnetických emisií s PC systému, ktorý obsahuje takéto PC údaje
  - Objektívna stránka ad ods. 2: detto ako ods. 1 alebo v umožnení inému spáchať taký čin alebo v pozmenení alebo potlačení správy podanej prostredníctvom elektronickej komunikačnej služby
  - Subjekt ad ods. 1: všeobecný (ktorákoľvek trestne zodpovedná osoba)
  - Subjekt ad ods. 2: špeciálny (zamestnanec poskytovateľa elektronickej komunikačnej služby)
  - Subjektívna stránka: úmyselné zavinenie
- tento trestný čin spôsobuje obdobné porušenie súkromia pri komunikácii ako odpočúvanie či záznam telefonických rozhovorov medzi osobami
- spôsobenie škody v základných skutkových podstatách **nevyžaduje**, spôsobenie aspoň značnej škody je však okolnosťou umožňujúcou použitie **vyššej trestnej sadzby**

§ 247c TZ Neoprávnené zachytávanie počítačových údajov 2/2



Packet sniffing

§ 247d TZ Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov 1/2

- **§ 247d ods. 1 TZ** *„Kto v úmysle spáchať trestný čin neoprávneného prístupu do počítačového systému podľa **§ 247**, neoprávneného zásahu do počítačového systému podľa **§ 247a**, neoprávneného zásahu do počítačového údaja podľa **§ 247b** alebo neoprávneného zachytávania počítačových údajov podľa **§ 247c** vyrobí, dovezie, obstará, kúpi, predá, vymení, uvedie do obehu alebo akokoľvek sprístupní*
  ***a)** zariadenie vrátane počítačového programu vytvorené na neoprávnený prístup do počítačového systému alebo jeho časti, alebo*
  ***b)** počítačové heslo, prístupový kód alebo podobné údaje umožňujúce prístup do počítačového systému alebo jeho časti,*
  potrestá sa odňatím slobody až na dva roky."
- konanie popísané v skutkovej podstate má v zásade charakter prípravy na spáchanie trestného činu, no vzhľadom na to, že príprava je trestná iba vo vzťahu k zločinu, zákonodarca toto ustanovenie koncipoval ako samostatný tzv. **predčasne dokonaný trestný čin**

§ 247d TZ Výroba a držba prístupového zariadenia, hesla do počítačového systému alebo iných údajov 2/2

Kali Linux Tools

Podvod § 221 TZ

- Čl. 17, ods. 2, 2. veta Ústavy SR
- Trestný zákon (Osobitná časť – 4. hlava – Piaty diel – § 221-226)
- Zákon o trestnej zodpovednosti PO (§ 3 ZoTzPO)
- Objekt: poctivé plnenie záväzkov, pacta sunt servanda
- Subjekt: všeobecný
- Objektívna stránka: obohatenie sa/iného na škodu majetku uvedením niekoho do omylu, alebo využitím omylu iného a spôsobenie aspoň malej škody
- Subjektívna stránka: úmyselné zavinenie
- Primeraná miera opatrnosti (zo strany FI)
- Z hľadiska princípov, na ktorých je založený demokratický štát je neprijateľné, aby trestným postihom jedného účastníka súkromnoprávneho vzťahov bola nahradzovaná nevyhnutná miera opatrnosti druhého účastníka pri ochrane vlastných práv a majetkových záujmov. Trestným postihom nie je možné nahrádzať inštitút iných právnych odvetví, ktoré sú určené na ochranu majetkových práv a záujmov.(Uznesenie Najvyššieho súdu Slovenskej republiky, ev 11 TDO 1121/2012, z 14.3.2013)

Trendy – všeobecne

- Scenáre a *modus operandi* kopírujúce západnú Európu a silné ekonomiky;
- 6-9/12 mesiacov delay oproti západnej Európe;
- Narastajúci trend využívania informačných technológii;
- priame a konfrontačné;
- využívanie faktoru „cezhraničnosti“:
- zakladanie účtov, využívanie ICT služieb (najmä mobilný hlas, data, hosting)
- prevody PO z osôb/na osoby s občianstvom z ČR, AT, PL, HUN.
- jazyková príbuznosť a istota ČR, HUN.
- vojna na Ukrajine a rastúca ukrajinská komunita;

Trendy – modus operandi

- Narastajúci trend využívania informačných technológii s vyššou mierou sofistikácie;

  - CEO podvody
    - definícia;
    - *modus operandi* spravidla zahrňa „decision- makera" zo zahraničia (partner, CEO, CFO, šéf skupiny)

    - používania cudzieho jazyka vo vzťahu k SR;

    - cieľ na cezhraničné štruktúry a skupiny s viac úrovňovou štruktúrou riadenia;

    - vysoká miera autenticity v podkladových dokumentoch (hlavičky, tituly, adresy, loga podľa design manuálov);

    - deepfake (call-y, videá, online schôdzky);

LEGENDA „INVESTOR"

- Nátlakové techniky- teraz, hneď, okamžite je potrebné investovať, garancia 20-30% výnosu. Utvrdzovanie a fishing techniky.
- Spravidla telefonicky, osobný kontakt je skôr raritný
- Opätovné navolávanie, či poškodený už FIAT zmenil zas crypto.
- Hovory trvajú aj niekoľko hodín.
- Často spojený v druhom skutku, s časovým odstupom s legendou „policajt".
- Faktor hanby a ostychu.
- Ak sa používajú cryptomaty, často prítomný prostredník, ktorý „pomôže" s transakciou, spravidla odlišná osoba od volajúceho- veľmi často sami uvedení do omylu, podávajú TO pre nevyplatené provízie.
- Sunshine effect.
- Peak sa dosahuje koncom pracovného týždňa, resp. cez víkend, spravidla v poobedňajších /večerných hodinách.

LEGENDA „POLICAJT"

- Nátlakové techniky- teraz, hneď, okamžite je potrebné poslať crypto, FIAT na „policajný účet (často REVOLUT a následne zmena na crypto), pretože práver teraz prebieha krádež.
- Opätovné navolávanie, či poškodený už FIAT zmenil zas crypto.
- Hovory trvajú aj niekoľko hodín.
- Častá prítomnosť druhého volajúceho z „Centrálnej banky", povzbudzujúceho na prevod na crypto.
- Sunshine effect.
- Peak sa dosahuje koncom pracovného týždňa, resp. cez víkend, spravidla v poobedňajších /večerných hodinách.

CUSEC

LEGENDA „CRYPTO -INVESTOR"

- Nátlakové techniky- teraz, hneď, okamžite je potrebné investovať, garancia 20-30% výnosu.
- Profesionálny dizajn stránok a investičných dokumentov
- Vytvorenie a zapísanie stablecoinov do blockchainu, avšak s nulovou hodnotou
- Podvod spočíva v nákupe a následnom uvoľnení za poplatok
- Analógia s NFT

LEGENDA „INVESTOR" (ROMANCE SCAM)

- Nátlakové techniky- teraz, hneď, okamžite je potrebné investovať, garancia 20-30% výnosu. Utvrdzovanie a fishing techniky.
- Často aj osobné stretnutie.
- Medová pasca vo forme vytvorenia vzťahu obete k páchateľovi pod legendou „investora", vojaka, doktora.
- Dlhodobé konanie.
- Viacero platieb.
- Faktor hanby a ostychu.

ROZSAHOVO VEĽKÉ KRÁDEŽE CRYPTA

- Zatiaľ nie v SR,
- Vyhľadávanie systémových nedostatkoch, najmä cez interný podvod, koruptnuté prístupové údaje, medzery kybernetickej bezpečnosti bridge aplikácií.
- Napr. Bybit

ZBER ÚDAJOV A POMOC POŠKODENÝM

TO

7 kriminalistických otázok:

- **KTO? – popis páchateľa, nápomocná je akákoľvek identifikácia osoby, pattern (prízvuk, rečová vada, IP adresa, mail, textovka, tel. číslo, platobná karta).**
- **ČO?- popis samotného konania.**
- **KDE?- adresa crypto peňaženky, účet, platobná karta, mobilný telefón.KEDY? – Dátum a čas s indikáciou CEE časovej zóny, sunshine effect a určitosť pri zaisťovaní.**
- **PREČO?- motív alebo pohnútka.**
- **S KÝM?- spolupáchateľ, spolupáchatelia.**
- **S ČIM?- zariadenie, nástroj t.č., počítačový program, prelomené heslo.**

Všeobecne

Nové vzory podvodov prichádzajú do SR cca 6-12m od výskytu v Západnej Európe- čas pre vaších CO pripraviť sa, otestovať procesy, atď.

Najzraniteľnejší sú seniori, celosvetový problém.

PZ nedisponuje „červeným tlačítkom" na pozdržanie transakcie, sám poškodený musí jednať

Primeraná miera opatrnosti poškodeného (NS SR 12 Tdo V 21/2013)

Nátlakové trestné činy

- Vydieranie (§189 TZ)- plnenie za hrozbu spôsobenia vážnej ujmy
- Nebezpečné vyhrážanie (§360 TZ)- IBA hrozba spôsobenia vážnej ujmy
- Hrubý nátlak (§190 TZ)- hrozba spôsobenia vážnej ujmy za poskytnutie plnenia za služby vlastné alebo cudzieho.
- Nebezpečné prenasledovanie (36a0§)- dôvodná obava o život a zdravie v dôsledku prenasledovania (stalking)
- Nebezpečné elektronické obťažovanie (§360 TZ)- prenasledovanie, ktoré nespôsobí dôvodnú obavu o život a zdravie, iba podstatne zhorší kvalitu života, alebo **zverejnenie osobného prejavu, získaného so súhlasom osoby.**
- Úžera (§235 TZ)- manipulatívne techniky AI podľa čl. 5 Aktu o umelej inteligencií

Trestné činy porušujúce súkromie a tajomstvo privilegovaných správ.

- Ohrozenie obchodného, bankového, poštového telekomunikačného a daňového tajomstva (§264 TZ)- priemyselná špionáž rôznymi cyber technikami.

- Vyzvedačstvo, Ohrozenie utajovanej skutočnosti a Ohrozenie dôvernej a vyhradenej (§318 až §320 TZ a §353 TZ).- Vyzvedanie PT a T pre cudziu moc. Vyzvedanie PT a T pre inú osobu – aj z nedbanlivosti, Vyzvedanie D a V pre inú osobu.

- Ochrana súkromia v obydlí (§194a TZ) a Porušenie dôvernosti ústneho prejavu osobnej povahy (§377 TZ)- Povinnosť sledovať a zaznamenávať prejavy osobnej povahy v obydlí a sprístupnení záznamu, vs. Všeobecne. **Zverejnenie prejavu osobnej povahy získaného bez súhlasu osoby.**

Počítačové trestné činy súvisiace s obsahom

- Porušovanie autorských práv (§283 TZ) – extenzívna skutková podstata. Torrenty pre vlastnú potrebu, nie komerčnú nie je porušením autorských práv C-610/15 vo veci Stichting Brein proti Ziggo BV and XS4ALL Internet BV ('XS4ALL')

- Nebezpečné vyhrážanie (§360 TZ)- vznik dôvodnej obavy o život a zdravie vyhrážaním sa, bez extrémistického motívu. Silný prekrýv s priestupkom. Hate speech.

- Šírenie poplašnej správy (§361 TZ) – nepravdivá info, ktorá nepriaznivo zasahuje do života osôb. Nielen bombové maily ale i hoaxy a dezinformácie.

- Detská pornografia (§368-370TZ)- NCMEC reporty selektované na základe IP adries.

- Extrémizmus (§421-§424 TZ) propagácia hnutí smerujúcich k potláčaniu základných ľudských práv , výroba, prechovávanie extrém. materiálov, popieranie holokaustu.

Kybernetický terorizmus, záškodníctvo a medzinárodné zločiny (genocída, zločiny proti ľudskosti a vojnové zločiny)

- Všeobecné ohrozenie (§284 TZ), poškodzovanie všeobecne prospešného zariadenia (§§286 TZ), Záškodníctvo (§315 TZ) a Teroristický útok (419 TZ).- poškodzovanie (napr. cyber útokom) zariadenia/ infraštruktúry a ohrozenia života, zdravia, veľkej škody u skupiny osôb. Bez ohrozenia života a zdravia ide o poškodzovanie všeobecne prospešného zariadenia. Ohrozenie ústavnosti a obranyschopnosti SR- Záškodníctvo. Teroristický útok je koncipovaný širšie.

- Používanie zakázaného bojového prostriedku a nedovolené vedenie boja (§426TZ), Perzekúcia (§432TZ), Vojnové bezprávie (§433 TZ). Medzinárodné zločiny, ICC draft paper, ktorým sa kybernetické útoky budú stíhať ako medzinárodné zločiny, ak budú naplnené skutkové podstaty.

CUSEC

Ďakujeme za Vašu pozornosť!

Mgr. Petra Dražová, PhD.

Doc. JUDr. Marek Kordík, PhD. LL.M.

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY