UNIVERZITA
PAVLA JOZEFA ŠAFÁRIKA
V KOŠICIACH

Financované
Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO
INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA
A INFORMATIZÁCIE
SLOVENSKEJ REPUBLIKY

KYBERNETICKÁ KRIMINALITA – HMOTNOPRÁVNE ASPEKTY

Meno a priezvisko

XX.XX.XXXX

OBSAH

1) Úvod do kybernetickej kriminality
2) Dohovor o počítačovej kriminalite
3) Právna úprava EÚ
4) Vnútroštátna právna úprava

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

ÚVOD DO KYBERNETICKEJ KRIMINALITY

VŠEOBECNE O KYBERKRIMINALITE

- **druh trestnej činnosti**
- dominantne zahŕňa prípady, kedy sú informačno-komunikačné technológie **prostriedkom na spáchanie inej trestnej činnosti**
- **rôzne motívy** ⇨ majetkový prospech a obohatenia sa na úkor iného až deklarovanie určitých postojov
- spravidla páchanie trestnej činnosti **mimo územia SR** (zo zahraničia, resp. prostredníctvom zahraničia) ⇨ **problematické dokazovanie**
- mimoriadne náročný proces preukázania a vyvodenia trestnoprávnej zodpovednosti

POJEM KYBERKRIMINALITY

- absentuje univerzálna právna definícia
- Smejkal: **trestná činnosť páchaná v kybernetickom priestore**
- Polčák: **akákoľvek protiprávna činnosť, v rámci ktorej je počítač či iná informačná alebo komunikačná technológia v postavení nástroja, cieľa alebo prostriedku;** možno rozlišovať:
  - ***a) cyber-dependent* kriminalitu** – trestná činnosť, ktorá môže byť spáchaná iba prostredníctvom počítačov, počítačových sietí alebo iných druhov IKT (napr. hacking, šírenie malvéru, DDoS útokov)
  - ***b) cyber-enabled* kriminalitu** – trestné činy, ktoré majú väčší dosah alebo rozsah vďaka využitiu IKT (detská pornografia, extrémizmus a iné formy nezákonného obsahu), ale môžu byť spáchané aj bez IKT
  - ***c) computer supported* kriminalitu** – IKT sa využíva v priebehu páchania trestnej činnosti iba príležitostne, ale spáchanie trestného činu uľahčuje (stalking, podvody, legalizácia výnosov z trestnej činnosti, obchodovanie s drogami)

KYBERKRIMINALITY V SR

2022

6. septembra 2022 17:37 Firmy Lesy SR

Štátne lesy zostali po hekerskom útoku bez systémov. Nemôžu predávať palivové drevo a padol im aj portál na kontrolu ťažby

IVAN HALUZA + Zapnúť články e-mailom

Ťažba dreva v lesoch. Ilustračné foto – TASR

2023

8.9.2023 13:59 | Bezpečnosť

Košická župa čelila kybernetickému útoku, elektronické služby úradu sú dočasne nefunkčné

Zdroj: Pixabay

Podobne ako v minulosti, aj tentoraz malo ísť o ransomvér.

2024

TREND Predplatiť

TREND.sk / Správy

Hekeri po útoku na kataster žiadajú vysoké výkupné, štát nemusí disponovať zálohami dát

Zdroj: Shutterstock

KYBERKRIMINALITA V SR

Trestný čin (paragraf, názov)	Zistené	Objasnené	% objasnenosti	Spôsobená škoda €
§ 201a Sexuálne zneužívanie	6	2	33,33	
§ 219 Neoprávnené vyrobenie a používanie platobného prostriedku, elektronických peňazí alebo inej platobnej karty	2116	457	21,6	5 953 000
§ 226 Neoprávnené obohatenie	9	2	22,22	76 000
§ 247 Neoprávnený prístup do počítačového systému	23	1	4,35	600 000
§ 247a Neoprávnený zásah do počítačového systému	8	–	0	15 000
§ 247b Neoprávnený zásah do počítačového údaja	5	–	0	10 000
§ 247c Neoprávnený prístup do počítačového systému	2	1	50	–
§ 247d Neoprávnené zachytávanie počítačových údajov	–	–	–	–
§ 283 Porušovanie autorského práva	44	9	20,45	1 848 000
§ 368 Výroba detskej pornografie	33	16	48,48	7 000
§ 369 Rozširovanie detskej pornografie	201	56	27,86	30 000
§ 370 Prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení	37	23	62,16	13 000
Spolu	**2 447**	**567**	**23,17**	**8 552 000**

Zdroj: Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2023
https://www.nbu.gov.sk/data/att/2855.pdf

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

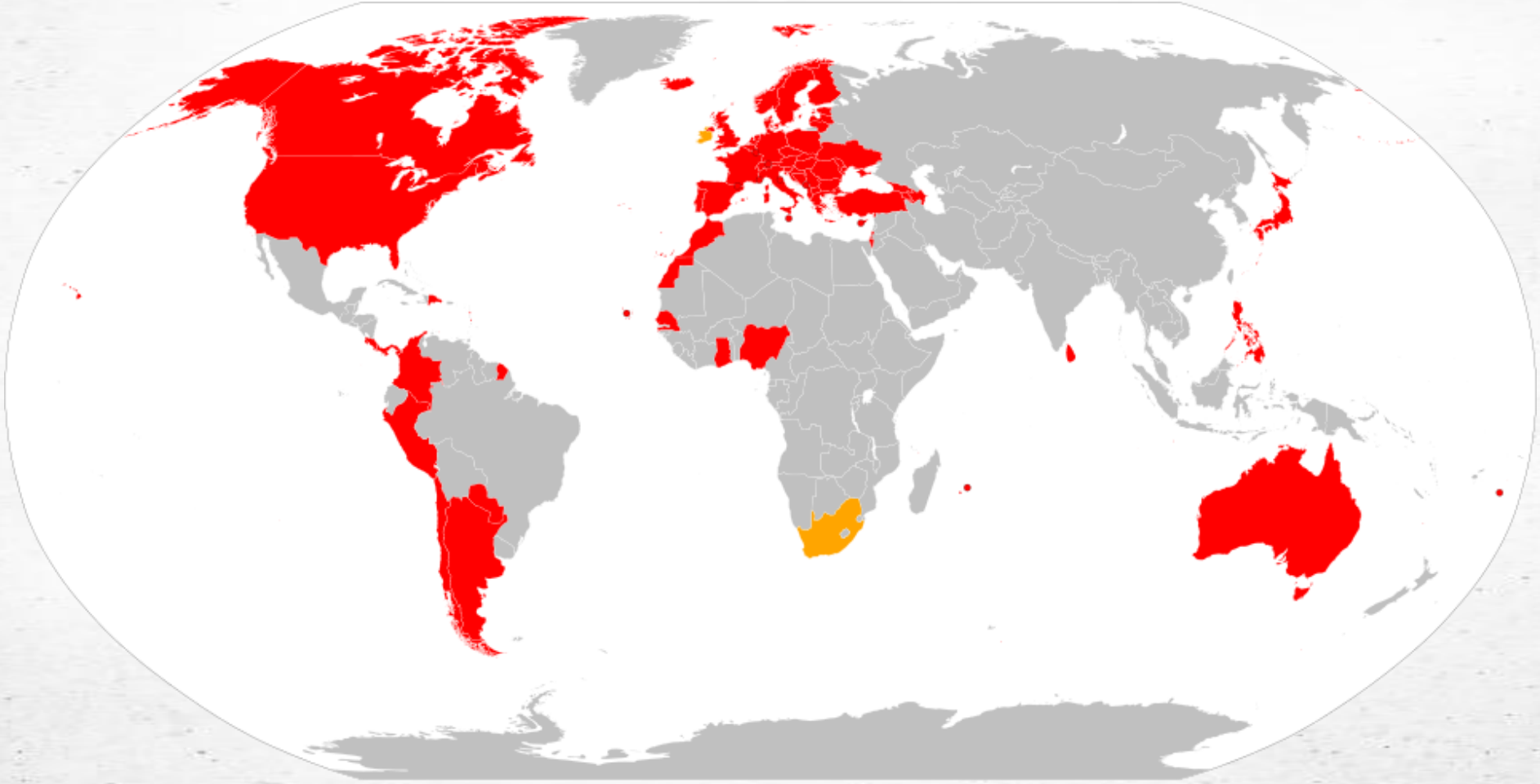
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

DOHOVOR O POČÍTAČOVEJ KRIMINALITE

MEDZINÁRODNÁ PRÁVNA ÚPRAVA

- **Dohovor o počítačovej kriminalite (Convention on Cybercrime)**
  - Budapešť, 2001 – Rada Európy
  - vymedzuje základné pojmy ako počítačový systém a počítačové údaje
  - ustanovuje **konania, ktoré by mali byť trestnoprávne stíhateľné vo všetkých signatárskych štátoch dohovoru** (kategórie trestných činov)
  - upravuje aj možnosť vyvodenia trestnoprávnej zodpovednosti voči PO
  - úprava vybraných procesných aspektov
  - medzinárodná spolupráca

DOHOVOR O POČÍTAČOVEJ KRIMINALITE – SIGNATÁRSKE ŠTÁTY



https://commons.wikimedia.org/wiki/File:Ratified_Convention_on_Cybercrime.svg

DOHOVOR O POČÍTAČOVEJ KRIMINALITE	
Trestné činy proti dôvernosti, hodnovernosti a dostupnosti počítačových údajov a systémov	
Nezákonný prístup (čl. 2)	neoprávnený prístup do počítačového systému ako celku alebo do jeho časti spáchaný úmyselne
Nezákonné zachytenie údajov (čl. 3)	neoprávnené zachytávanie neverejných prenosov počítačových údajov do počítačového systému, z neho alebo v rámci tohto systému vrátane elektromagnetických emisií z počítačového systému, ktorý obsahuje také počítačové údaje vykonané technickými prostriedkami spáchané úmyselne
Zasahovanie do údajov (čl. 4)	neoprávnené poškodenie, vymazanie, zhoršenie kvality, pozmenenie počítačových údajov alebo zamedzenie prístupu k nim spáchané úmyselne
Zasahovanie do systému (čl. 5)	neoprávnené závažné marenie funkčnosti počítačového systému vkladaním, prenášaním, poškodením, vymazaním, zhoršením, pozmenením počítačových údajov alebo zamedzením prístupu k nim spáchané úmyselne
Zneužitie zariadení (čl. 6)	konania uvedené ďalej, ak boli spáchané úmyselne a bez oprávnenia: a) výroba, predaj, obstarávanie na účely použitia, dovoz, distribúcia alebo iné sprístupnenie i. zariadenia vrátane počítačového programu vytvoreného alebo upraveného predovšetkým s cieľom spáchať niektorý z trestných činov vymedzených v článkoch 2 až 5, ii. počítačového hesla, prístupového kódu alebo podobných údajov, ktorých pomocou je možný prístup do počítačového systému ako celku alebo do niektorej jeho časti, s úmyslom ich použiť na spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5 a **b)** držba veci uvedenej v odseku 1 písm. a) bode i. alebo ii. s úmyslom ju použiť na spáchanie niektorého z trestných činov vymedzených v článkoch 2 až 5. Strana môže ustanoviť zákonom, že na založenie trestnej zodpovednosti sa vyžaduje držba viacerých takých vecí.

DOHOVOR O POČÍTAČOVEJ KRIMINALITE	
Počítačové trestné činy	
Falšovanie počítačových údajov (čl. 7)	vloženie, pozmenenie, vymazanie počítačových údajov alebo zamedzenie prístupu k nim, v ktorých dôsledku stratia údaje autentickosť, s úmyslom považovať ich za autentické alebo aby sa na základe nich ako autentických údajov konalo, na právne účely, bez ohľadu na to, či tieto údaje sú alebo nie sú priamo čitateľné alebo zrozumiteľné, ak boli spáchané úmyselne a bez oprávnenia
Počítačový podvod (čl. 8)	spôsobenie majetkovej ujmy inému **a)** vložením, pozmenením, vymazaním počítačových údajov alebo zamedzením prístupu k nim, **b)** zásahom do fungovania počítačového systému s podvodným alebo nečestným úmyslom neoprávnene získať pre seba alebo pre iného majetkový prospech, ak bolo spáchané úmyselne a bez oprávnenia

DOHOVOR O POČÍTAČOVEJ KRIMINALITE	
Trestné činy týkajúce sa obsahu	
Trestné činy týkajúce sa detskej pornografie (čl. 9)	konania uvedené ďalej, ak boli spáchané úmyselne a bez oprávnenia: **a)** výroba detskej pornografie na účely jej distribúcie počítačovým systémom, **b)** ponuka alebo sprístupnenie detskej pornografie počítačovým systémom, **c)** distribúcia alebo prenos detskej pornografie počítačovým systémom, **d)** zaobstaranie detskej pornografie počítačovým systémom pre seba alebo pre iného, **e)** držba detskej pornografie v počítačovom systéme alebo na pamäťovom nosiči počítačových údajov. Pojem „detská pornografia“ zahŕňa pornografický materiál, ktorý zobrazuje **a)** maloletú osobu zúčastnenú na zjavnom sexuálnom správaní, **b)** osobu, ktorá sa zdá byť maloletá a ktorá sa zúčastňuje na zjavnom sexuálnom správaní, **c)** realistické zobrazenia maloletej osoby zúčastnenej na zjavnom sexuálnom správaní. Pojem „maloletá osoba“ zahŕňa všetky osoby mladšie ako 18 rokov. Strana však môže určiť nižšiu vekovú hranicu, ktorá nesmie prekročiť hranicu 16 rokov.

DOHOVOR O POČÍTAČOVEJ KRIMINALITE	
Trestné činy týkajúce sa porušenia autorských a príbuzných práv	
Trestné činy týkajúce sa porušenia autorských a príbuzných práv (čl. 10)	1. **porušenie autorského práva** vymedzeného právnym poriadkom tejto strany v súlade so záväzkami, ktoré prijala podľa Parížskeho aktu z 24. júla 1971, ktorým sa mení Bernský dohovor o ochrane literárnych a umeleckých diel, Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o autorskom práve, okrem osobnostných práv priznaných týmito dohovormi, ak tieto činy boli spáchané úmyselne, v obchodnom meradle a prostredníctvom počítačového systému 2. **porušenie príbuzných práv**, ako ich vymedzuje jej právny poriadok v súlade so záväzkami, ktoré prijala podľa Medzinárodného dohovoru o ochrane výkonných umelcov, výrobcov zvukových záznamov a rozhlasových organizácií (Rímsky dohovor), Dohody o obchodných aspektoch práv na duševné vlastníctvo a Zmluvy Svetovej organizácie duševného vlastníctva (WIPO) o výkonoch a zvukových záznamoch, okrem osobnostných práv priznaných týmito dohovormi, ak tieto činy boli spáchané úmyselne, v obchodnom meradle a prostredníctvom počítačového systému

MEDZINÁRODNÁ PRÁVNA ÚPRAVA

- **I. Dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa trestnoprávneho postihu činov rasovej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov**
  - rozširuje katalóg trestných činov o trestnoprávny postih činov rasovej a xenofóbnej povahy spáchaných prostredníctvom počítačových systémov
  - na účely tohto protokolu sa „**rasovým a xenofóbnym materiálom**“ rozumie *každý písomný materiál, každé obrazové alebo iné znázornenie myšlienok alebo teórií, ktoré obhajuje, podporuje alebo podnecuje nenávisť, diskrimináciu alebo násilie proti ktorémukoľvek jednotlivcovi alebo skupine jednotlivcov z dôvodu rasy, farby pleti, pôvodu alebo národnej či etnickej príslušnosti, ako aj náboženstva, pokiaľ sa použije ako zámienka pre ktorýkoľvek z týchto faktorov*

I. DODATKOVÝ PROTOKOL K DOHOVORU O POČÍTAČOVEJ KRIMINALITE	
Šírenie rasových a xenofóbnych materiálov prostredníctvom počítačových systémov (čl. 3)	distribúcia alebo iné sprístupňovanie rasového a xenofóbneho materiálu prostredníctvom počítačového systému, ak sú spáchané úmyselne a neoprávnene
Rasovo a xenofóbne motivované vyhrážanie (čl. 4)	vyhrážanie sa prostredníctvom počítačového systému spáchaním závažného trestného činu upraveného vo vnútroštátnom právnom poriadku, (i) proti jednotlivcom z dôvodu príslušnosti k skupine odlišujúcej sa rasou, farbou pleti, pôvodom alebo národnou a etnickou príslušnosťou ako aj náboženstvom, pokiaľ sa použije ako zámienka pre ktorýkoľvek z týchto faktorov, alebo (ii) proti skupine jednotlivcov, ktorá sa odlišuje niektorou z týchto charakteristík ak sú spáchané úmyselne a neoprávnene
Rasovo a xenofóbne motivované urážanie (čl. 5)	verejné urážanie (i) osôb z dôvodu ich príslušnosti k skupine odlišujúcej sa rasou, farbou pleti, pôvodom alebo príslušnosti k národnosti alebo etnickej skupine ako aj náboženstva, ak sa použije ako zámienka pre ktorýkoľvek z týchto dôvodov alebo (ii) skupiny osôb, ktoré sa odlišujú niektorou z týchto charakteristík; prostredníctvom počítačového systému ak sú spáchané úmyselne a neoprávnene
Popieranie, hrubé zľahčovanie, schvaľovanie alebo ospravedlňovanie zločinov proti ľudskosti (čl. 6)	verejné rozširovanie alebo iné sprístupňovanie materiálu, ktorý popiera, hrubo zľahčuje, schvaľuje alebo ospravedlňuje zločin genocídy alebo zločiny proti ľudskosti, ktoré ako také ustanovujú a uznávajú právoplatné a záväzné rozhodnutia Medzinárodného vojenského tribunálu zriadeného na základe Londýnskej dohody z 8. augusta 1945 alebo ktoréhokoľvek iného medzinárodného súdu zriadeného na základe relevantných medzinárodných právnych nástrojov, ktorého jurisdikciu príslušná strana uznáva, prostredníctvom počítačového systému, ak sú spáchané úmyselne a neoprávnene

MEDZINÁRODNÁ PRÁVNA ÚPRAVA

II. Dodatkový protokol k Dohovoru o počítačovej kriminalite týkajúci sa posilnenej spolupráce a sprístupňovania elektronických dôkazov

- cieľom je posilniť spoluprácu v oblasti počítačovej kriminality a získavania dôkazov o trestných činoch v elektronickej forme na účely konkrétneho vyšetrovania alebo trestného konania
- **potreba zvýšenej a efektívnejšej spolupráce medzi štátmi a súkromným sektorom** a potreba väčšej jasnosti a právnej istoty pre poskytovateľov služieb a iné subjekty, pokiaľ ide o okolnosti, za ktorých môžu reagovať na žiadosti OČTK o sprístupnenie elektronických dôkazov
- **účinná cezhraničná spolupráca na účely trestnej justície**, a to aj medzi orgánmi verejného sektora a subjektmi súkromného sektora, si vyžaduje účinné podmienky a **silné záruky na ochranu základných práv**
    - keďže elektronické dôkazy sa často týkajú osobných údajov, protokol obsahuje aj silné záruky na ochranu súkromia a osobných údajov

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

PRÁVNA ÚPRAVA EÚ

ZMLUVA O FUNGOVANÍ EÚ

- **čl. 83 Zmluvy o fungovaní EÚ** ⇨ možnosť prijatia **minimálnych pravidiel týkajúcich sa vymedzenia trestných činov a sankcií v oblastiach obzvlášť závažnej trestnej činnosti** s cezhraničným rozmerom vyplývajúcim z povahy alebo dôsledkov týchto trestných činov alebo z osobitnej potreby bojovať proti nim na spoločnom základe
- tieto oblasti zahŕňajú aj **počítačovú kriminalitu**

SMERNICA 2013/40/EÚ

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

- ustanovuje minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti útokov na informačné systémy

„**informačný systém**“ 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**“ sú zastúpenia skutočností, informácií alebo pojmov vo forme vhodnej na spracovanie v informačnom systéme vrátane programu, ktorý zabezpečí, aby informačný systém vykonal funkciu

SMERNICA 2013/40/EÚ O ÚTOKOCH NA INFORMAČNÉ SYSTÉMY	
Protiprávny prístup do informačných systémov (čl. 3)	úmyselné získanie prístupu do celého informačného systému alebo akejkoľvek jeho časti bez oprávnenia, ak bolo spáchané porušením bezpečnostného opatrenia
Protiprávny zásah do systému (čl. 4)	úmyselné závažné bránenie fungovaniu informačného systému alebo prerušenie jeho fungovania vložením počítačových údajov, prenosom, poškodením, vymazaním, zhoršením, pozmenením alebo potlačením takýchto údajov alebo ich zneprístupnením bez oprávnenia
Protiprávny zásah do údajov (čl. 5)	úmyselné vymazanie, poškodenie, zhoršenie, pozmenenie, potlačenie počítačových údajov v informačnom systéme alebo zneprístupnenie takýchto údajov bez oprávnenia
Protiprávne zachytávanie údajov (čl. 6)	úmyselné zachytávanie údajov prostredníctvom technických prostriedkov, neverejného prenosu počítačových údajov do informačného systému, z informačného systému alebo v rámci neho vrátane elektromagnetického vysielania z informačného systému nesúceho takéto počítačové údaje, ak je spáchané bez oprávnenia

SMERNICA 2013/40/EÚ O ÚTOKOCH NA INFORMAČNÉ SYSTÉMY	
Nástroje na spáchanie trestných činov (čl. 7)	úmyselná výroba, predaj, obstarávanie na použitie, dovoz, distribúcia alebo akékoľvek sprístupnenie nasledujúcich nástrojov, ak je spáchaná bez oprávnenia a so zámerom, že sa uvedené nástroje použijú na spáchanie akéhokoľvek z trestných činov uvedených v článkoch 3 až 6, a to aspoň v prípadoch, ktoré nie sú menej závažné: a) počítačový program určený alebo primárne prispôsobený na spáchanie akýchkoľvek trestných činov uvedených v článkoch 3 až 6 b) počítačové heslo, prístupový kód alebo podobné údaje, ktorými je možné získať prístup k celému informačnému systému alebo akejkoľvek jeho časti

SMERNICA 2013/40/EÚ - SANKCIE

- požiadavka na uloženie **účinných, primeraných a odrádzajúcich sankcií** za TČ uvedené v článkoch 3 až 8
- stanovenie **hornej hranice sadzby trestu odňatia slobody (TOS):**

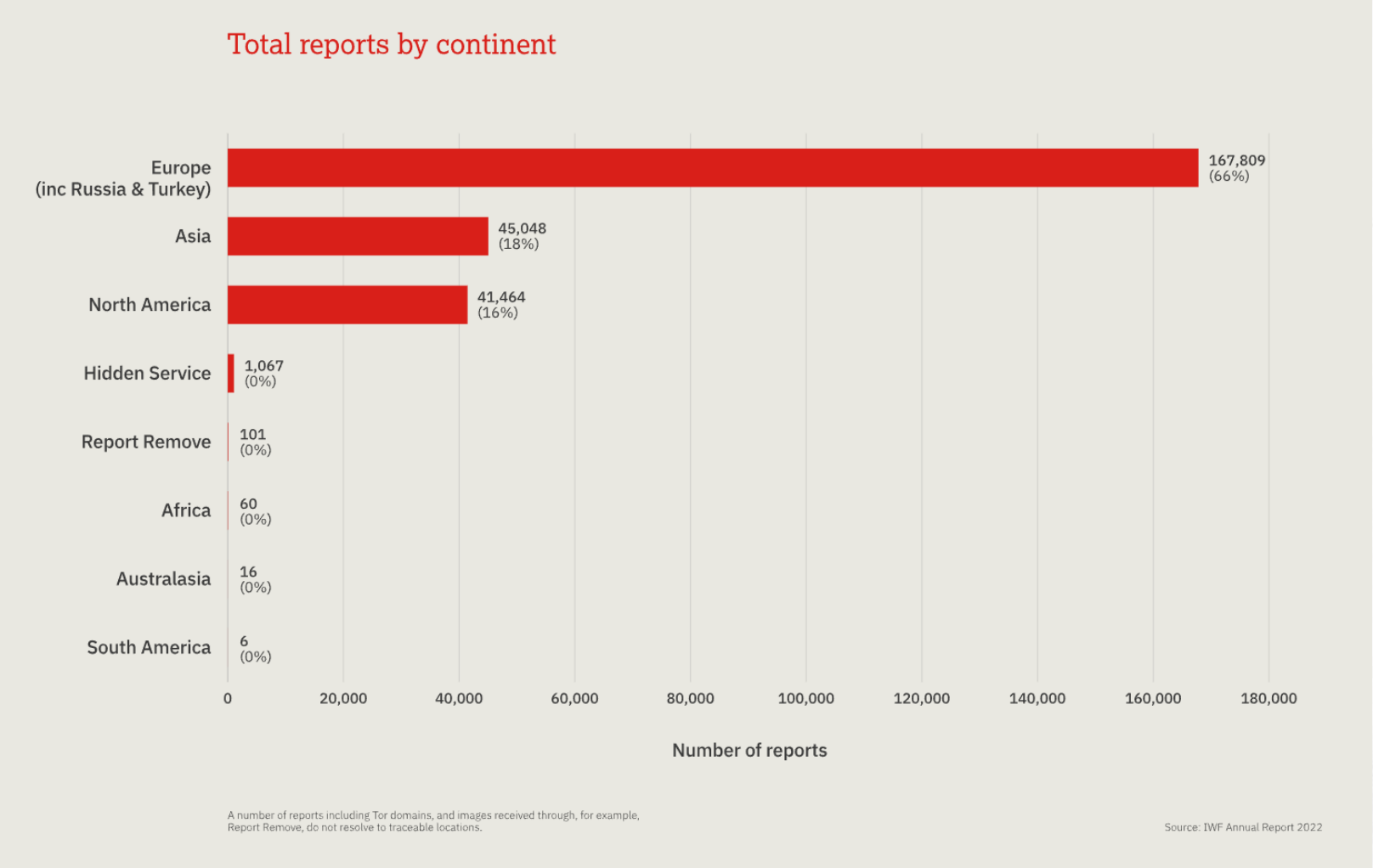
Kategória TČ	**Horná hranica sadzby TOS**
TČ uvedené v čl. 3 až 7	**najmenej dva roky**, a to aspoň v prípadoch, ktoré nie sú menej závažné
TČ uvedené v čl. 4 a 5, pokiaľ boli spáchané úmyselne	**najmenej tri roky** v prípade, ak bolo postihnuté veľké množstvo informačných systémov použitím nástroja uvedeného v článku 7, ktorý bol primárne určený alebo prispôsobený na tento účel
TČ uvedené v čl. 4 a 5	**najmenej päť rokov**, ak: a) boli spáchané v rámci zločineckej organizácie b) spôsobili závažnú škodu alebo c) boli spáchané na informačnom systéme kritickej infraštruktúry

SMERNICA 2019/713/EÚ

Smernica Európskeho parlamentu a Rady (EÚ) 2019/713 zo 17. apríla 2019 o boji proti podvodom s bezhotovostnými platobnými prostriedkami a proti ich falšovaniu a pozmeňovaniu, ktorou sa nahrádza rámcové rozhodnutie Rady 2001/413/SVV

- stanovuje minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti podvodov s bezhotovostnými platobnými prostriedkami a ich falšovania a pozmeňovania
- relevantný je najmä čl. 6, ktorý upravuje **podvody súvisiace s informačnými systémami** ⇨ vykonanie alebo spôsobenie prevodu peňazí, peňažnej hodnoty alebo virtuálnej meny, ktorým sa inej osobe spôsobí nezákonná majetková ujma v úmysle zadovážiť pre seba alebo pre iného neoprávnený prospech, bolo trestným činom, ak je spáchané úmyselne tým, že sa:
  a) neoprávnene zamedzí fungovaniu informačného systému alebo zasiahne do jeho fungovania
  b) neoprávnene vložia, pozmenia, vymažú, prenesú alebo potlačia počítačové údaje
    - horná hranica trestnej sadzby TOS ⇨ **najmenej tri roky**

DETSKÁ PORNOGRAFIA



SMERNICA 2011/93/EÚ

Smernica Európskeho parlamentu a Rady 2011/93/EÚ z 13. decembra 2011 o boji proti sexuálnemu zneužívaniu a sexuálnemu vykorisťovaniu detí a proti detskej pornografii

• ustanovuje minimálne pravidlá týkajúce sa vymedzenia trestných činov a sankcií v oblasti sexuálneho zneužívania a sexuálneho vykorisťovania detí, detskej pornografie a kontaktovania detí na sexuálne účely a zavádza ustanovenia na posilnenie prevencie tejto trestnej činnosti a ochrany jej obetí

• detskou pornografiou sa podľa čl. 2 písm. c) Smernice 2011/92/EÚ rozumie:

a) *„každý materiál, ktorý vizuálne zobrazuje dieťa zapojené do skutočného alebo simulovaného jednoznačne sexuálneho konania;*

b) každé zobrazenie pohlavných orgánov dieťaťa primárne určené na sexuálne účely;

c) každý materiál, ktorý vizuálne zobrazuje akúkoľvek osobu vyzerajúcu ako dieťa zapojenú do skutočného alebo simulovaného jednoznačne sexuálneho konania alebo každé zobrazenie pohlavných orgánov akejkoľvek osoby vyzerajúcej ako dieťa primárne určené na sexuálne účely, alebo

d) realistické snímky dieťaťa zapojeného do jednoznačne sexuálneho konania alebo realistické snímky pohlavných orgánov dieťaťa primárne určené na sexuálne účely.“

SMERNICA 2011/93/EÚ

Čl. 5 - Trestné činy súvisiace s detskou pornografiou

- za trestný čin sa považuje najmä:
  a) vedomé získavanie prístupu k detskej pornografii pomocou informačných a komunikačných technológií ⇨ horná hranica TOS najmenej 1 rok
  b) distribúcia, šírenie alebo ďalšie postupovanie detskej pornografie ⇨ horná hranica TOS najmenej 2 roky
  c) ponúkanie, dodávanie alebo sprístupňovanie detskej pornografie ⇨ horná hranica TOS najmenej 2 roky
  d) výroba detskej pornografie ⇨ horná hranica TOS najmenej 3 roky

SMERNICA 2011/93/EÚ

Čl. 6 – Kontaktovanie detí na účely ich sexuálneho zneužitia

- za trestný čin sa považuje toto úmyselné konanie: návrh dospelej osoby, uskutočnený pomocou informačných a komunikačných technológií, na stretnutie s dieťaťom, ktoré nedosiahlo vek, v ktorom je spôsobilé dať súhlas na pohlavný styk, s cieľom spáchať niektorý z trestných činov uvedených v článku 3 ods. 4 a článku 5 ods. 6, ak po tomto návrhu nasledovali faktické činy vedúce k takémuto stretnutiu
- horná hranica TOS ⇨ najmenej jeden rok

NÁVRH NARIADENIA EURÓPSKEHO PARLAMENTU A RADY, KTORÝM SA STANOVUJÚ PRAVIDLÁ PREDCHÁDZANIA SEXUÁLNEMU ZNEUŽÍVANIU DETÍ A BOJA PROTI NEMU (2022)

- majú sa ustanoviť jednotné pravidlá na riešenie zneužívania služieb informačnej spoločnosti na účely sexuálneho zneužívania detí online na vnútornom trhu
- navrhované povinnosti:
  a) posudzovanie rizika
  b) zmierňovanie rizika
  c) podávanie správ o rizikách
  d) povinnosti obchodov so softvérovými aplikáciami
  e) povinnosti týkajúce sa zisťovania
  f) oznamovacie povinnosti
  g) povinnosti týkajúce sa odstraňovania
  h) povinnosti týkajúce sa blokovania
- navrhuje sa zriadenie **Európskeho centra pre prevenciu sexuálneho zneužívania detí a boj proti nemu**

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

VNÚTROŠTÁTNA PRÁVNA ÚPRAVA

POČÍTAČOVÉ TRESTNÉ ČINY I.

§ 247 TZ: Neoprávnený prístup do počítačového systému

Kto prekoná bezpečnostné opatrenie, a tým získa neoprávnený prístup do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.

§ 247a TZ: Neoprávnený zásah do počítačového systému

Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti

a) neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením 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.

POČÍTAČOVÉ TRESTNÉ ČINY II.

§ 247b TZ: Neoprávnený zásah do počítačového údaja

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.

§ 247c TZ: Neoprávnené zachytávanie počítačových údajov

1. 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 až na dva roky.
2. 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 šesť mesiacov až tri roky.

POČÍTAČOVÉ TRESTNÉ ČINY II.

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

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.

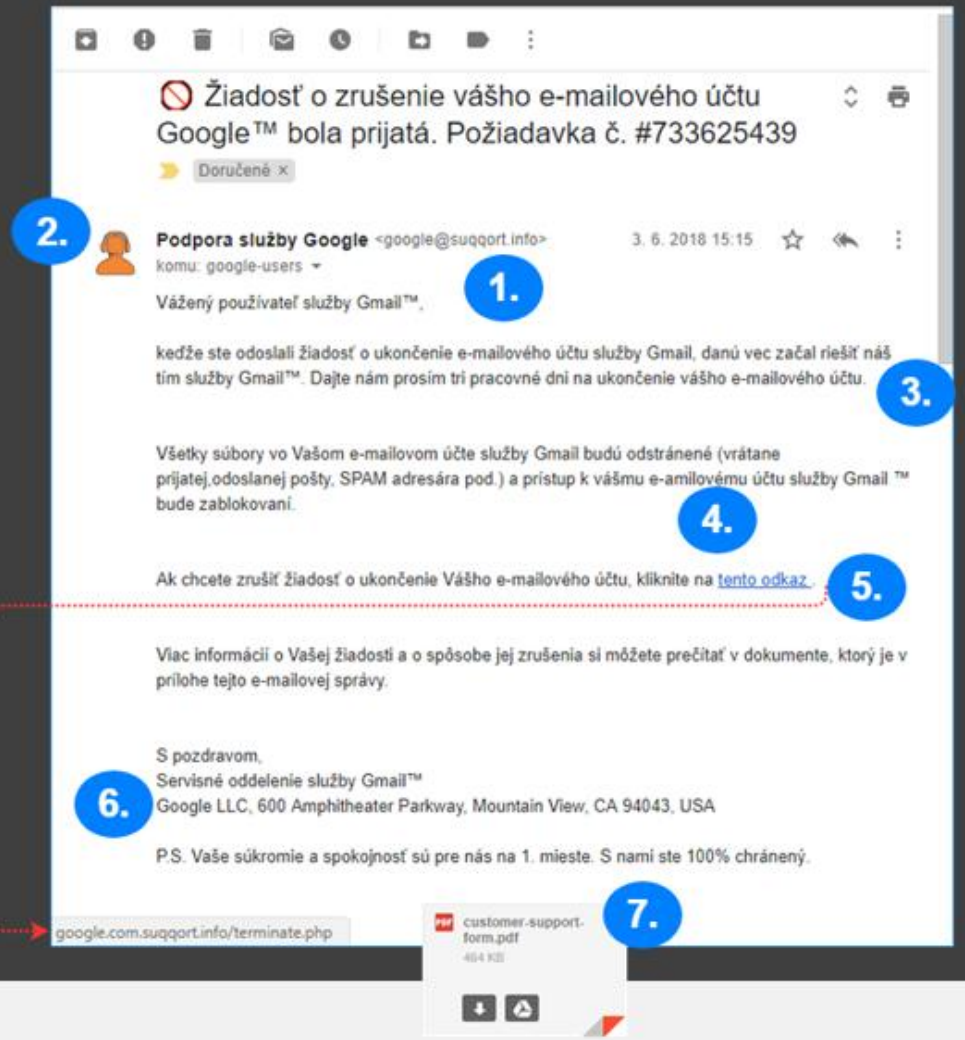
NEOPRÁVNENÝ PRÍSTUP DO POČÍTAČOVÉHO SYSTÉMU

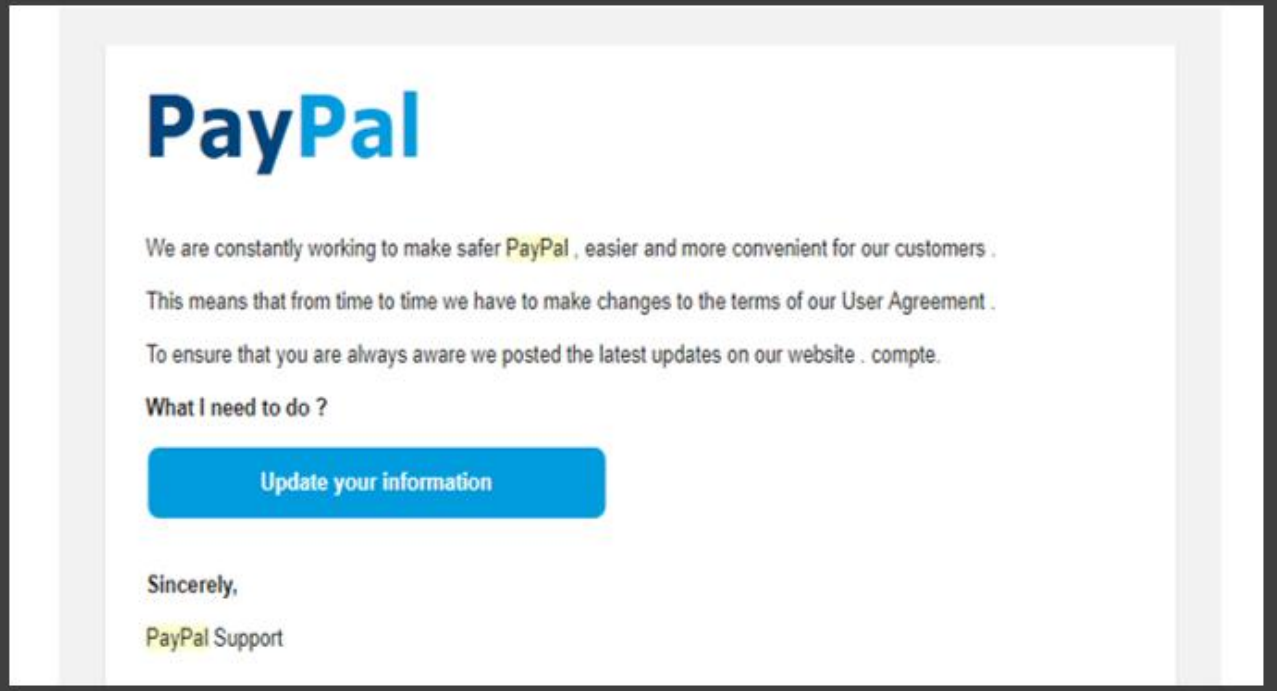
- **§ 247 (1) TZ:** Kto **prekoná bezpečnostné opatrenie**, a tým získa **neoprávnený prístup** do počítačového systému alebo jeho časti, potrestá sa odňatím slobody až na dva roky.
  - prekoná bezpečnostné opatrenie = napr. skúšaním prihlasovacích údajov, session hijacking (https://www.owasp.org/index.php/Session_hijacking_attack)
  - **informačný systém** ⇨ „funkčný celok zabezpečujúci cieľavedomú a systematickú informačnú činnosť prostredníctvom technických prostriedkov a programových prostriedkov, ktoré sú súčasťou informačného systému alebo ktoré informačnému systému poskytuje iný informačný systém.“ (Zákon č. 275/2006 Z. z. o informačných systémoch verejnej správy a o zmene a doplnení niektorých zákonov.)


```
File  Edit  View  Search  Terminal  Help
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC2" - 40 of 958 [chil
d 12]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "W3SVC3" - 41 of 958 [chil
d 9]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "WEB-INF" - 42 of 958 [chi
ld 3]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "msfadmin" - 43 of 958 [ch
ild 15]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_admin" - 44 of 958 [chil
d 14]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "_pages" - 45 of 958 [chil
d 5]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "a" - 46 of 958 [child 6]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aa" - 47 of 958 [child 8]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "aaa" - 48 of 958 [child 1
1]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "abc" - 49 of 958 [child 4
]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "about" - 50 of 958 [child
 2]
[ATTEMPT] target 192.168.1.101 - login "admin" - pass "academic" - 51 of 958 [ch
ild 0]
```

Neoprávnený prístup do počítačového systému (II.)

Útok hrubou silou / slovníkový útok





Neoprávnený prístup do počítačového systému (III.)

Sociálne inžinierstvo

NEOPRÁVNENÝ PRÍSTUP DO POČÍTAČOVÉHO SYSTÉMU

- Súd: Okresný súd Považská Bystrica
- Spisová značka: 2T/25/2015
- Identifikačné číslo súdneho spisu: 3715010050
- Dátum vydania rozhodnutia: 03. 03. 2015
- Podstata:
  - neoprávnene pripojil do počítačového systému spoločnosti počítačový Wifi router zn. Belkin
  - za pomoci nezisteného softvéru si vytvoril počítačový program na generovanie vstupných hesiel do pokladničného systému Progress
  - vnikol do pokladničného systému U. upravil ceny azakúpil presne nezistený tovar v sume najmenej 3.130,- Eur
  - pokračovací prečin poškodenia a zneužitia záznamu na nosiči informácii podľa § 247 ods. 1 TZ
  - peňažný trest 1.000 €

NEOPRÁVNENÝ PRÍSTUP DO POČÍTAČOVÉHO SYSTÉMU

- Súd: Okresný súd Levice
- Spisová značka: 4T/79/2019
- Identifikačné číslo súdneho spisu: 4319010786
- Dátum vydania rozhodnutia: 08. 08. 2019
- Podstata:
  - prostredníctvom svojho mobilného telefónu sa cez internet bez vedomia a súhlasu poškodenej I. D. prihlásil pomocou pravého hesla „K. XXXX“ ktoré mu nesprístupnila, do jej profilu na sociálnej sieti Facebook
  - zverejnil na ňom dve súkromné videá z roku 2018 s intímnym obsahom, na ktorých je zachytená obnažená poškodená I. D.
  - následne tieto videá rozposlal širokej verejnosti cca 135 priateľom na sociálnej sieti,
  - čím jej vážnym spôsobom narušil súkromie, bežný život a vystavil ju týmto spôsobom zosmiešneniu, ktoré ju doposiaľ prenasleduje,
  - prečin **neoprávneného prístupu do počítačového systému** podľa § 247 ods. 1 TZ v súbehu s prečinom **poškodzovania cudzích práv** podľa § 376 TZ
  - peňažný trest 500 €

NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO SYSTÉMU

- **§ 247a (1) TZ:**
- Kto **obmedzí** alebo **preruší fungovanie počítačového systému** alebo jeho časti
- **neoprávneným** vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením **počítačových údajov**, alebo
- 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.

Príklady:

- napr. Malware – rootkit
- napr. DoS (Denial of Service), DDoS (Distributed Denial of Service) útoky

NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO SYSTÉMU

- Súd: Okresný súd Vranov nad Topľou
- Spisová značka: 2T/51/2019
- Identifikačné číslo súdneho spisu: 8819010593
- Dátum vydania rozhodnutia: 30. 10. 2019
- Podstata:
  - v úmysle a za účelom obmedziť a prerušiť funkčnosť **digitálneho tachografu**, sťa by počítačového systému, dal do vozidla prídavné sofistikované zariadenie ovplyvňujúce funkčnosť digitálneho tachografu vozidla a to potlačením signálu snímača
  - pohybu, ktoré je aktivované z kabíny vodiča a to päťkrát zošliapnutím plynového pedála, v dôsledku čoho bolo možné po piatich zošliapnutiach plynového pedála vyradiť digitálny tachograf vozidla z činnosti
  - prečin **neoprávneného zásahu do počítačového systému** podľa § 247a ods. 1 písm. a) a b) TZ
  - peňažný trest 1.000 €

NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO ÚDAJA

- **§ 247b (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.

- **zneprístupní počítačové údaje -** napr. Malware – ransomware
- ochrana integrity údajov
- nie je nutné, aby bola spôsobená škoda => postačí zmena, poškodenie ...

NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO ÚDAJA

- Súd: Okresný súd Levice
- Spisová značka: 4T/19/2021
- Identifikačné číslo súdneho spisu: 4321010147
- Dátum vydania rozhodnutia: 17. 06. 2021
- Podstata:
  - zo svojho mobilného telefónu prostredníctvom znalosti pravých prihlasovacích údajov v rozsahu mena a hesla bez vedomia a súhlasu W. B. opakovane prihlásil do jej účtu na sociálnej sieti Facebook,
  - kde si prečítal jej súkromné správy, do svojho mobilného telefónu si stiahol jej intímne fotografie, ktoré v jej mene prostredníctvom súkromných správ rozposlal ich spoločným známym,
  - Po čom opakovane zmenil jej prihlasovacie údaje, v dôsledku čoho bola W. B. nútená vytvoriť si nový účet
  - požadoval za každé vymazanie jednej fotografie intímny styk, stretnutie a obnovenie vzájomného spolužitia, inak ich rozpošle ďalším osobám a zverejní ich na sociálnej sieti Facebook,

NEOPRÁVNENÝ ZÁSAH DO POČÍTAČOVÉHO ÚDAJA

- Súd: Okresný súd Levice
- Spisová značka: 4T/19/2021
- Identifikačné číslo súdneho spisu: 4321010147
- Dátum vydania rozhodnutia: 17. 06. 2021
- Podstata:
  - prekonal bezpečnostné opatrenie a tým získal neoprávnene prístup do počítačového systému a úmyselne pozmenil počítačové údaje v rámci počítačového systému
  - prečin **neoprávneného prístupu do počítačového systému** podľa § 247 ods. 1 TZ v súbehu s prečinom **neoprávneného zásahu do počítačového údaja** podľa § 247b ods. 1 TZ
  - **zločin vydierania** podľa § 189 odsek 1, odsek 2 písmeno b) TZ
  - Trest odňatia slobody v trvaní 3 rokov (podmienečne odložený + probačný dohľad)

VÝROBA A DRŽBA PRÍSTUPOVÉHO ZARIADENIA, HESLA DO POČÍTAČOVÉHO SYSTÉMU ALEBO INÝCH ÚDAJOV

- tento TČ je len prečin (horná hranica trestnej sadzby do 5 rokov)
- predstavuje prípravu pre ostatne trestné činy
- napr. použitie nástrojov v Kali Linuxe (musí byť motív spáchať počítačové trestné činy § 247 - § 247c)
- THC-Hydra (https://tools.kali.org/password-attacks/hydra)
- testovanie hesiel
- §247 - Neoprávnený prístup do počítačového systému
- Hping (https://www.binarytides.com/tcp-syn-flood-dos-attack-with-hping/)
- TCP SYN útok (DoS útok)
- §247a - Neoprávnený zásah do počítačového systému

KCKB UPJS

UNIVERZITA PAVLA JOZEFA ŠAFÁRIKA V KOŠICIACH

Financované Európskou úniou NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

Ďakujem za pozornosť

laura.rozenfeldova@upjs.sk

https://cyberawareness.sk