DECT

MUNI LAW

Národní centrum kompetence pro kyberbezpečnost

e4j

TYPICKÉ SKUTKOVÉ PODSTATY KYBERKRIMINALITY

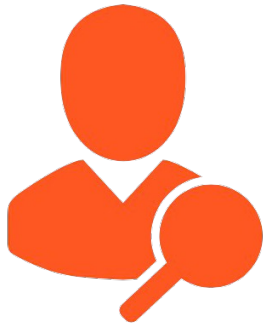
VÁCLAV STUPKA

PROBLEMATIKA KRIMINALIZACE

- Jurisdikční limity kriminalizace a přeshraniční charakter kyberprostoru
- Kriminalizaci stanovují státy nezávisle
- Vznik bezpečných přístavů
- Harmonizace prostřednictvím mezinárodních instrumentů
- Riziko zneužití procesních nástrojů, riziko kriminalizace legitimních aktivit
- Co je a není kyberkriminalita?

JAK KLASIFIKOVAT KYBERKRIMINALITU

- Obecně dva přístupy:
  - Kategorizace podle trestního práva hmotného
    - Skutkové podstaty
    - Menší granularita
    - Problém se statistikou
  - Kategorizace prostřednictvím kasifikace kybernetických bezpečnostních incidentů
    - Detailnější třídění
    - V souladu s reaitou
    - Neváže na skutkové podstaty
  - Kategorizace podle jiných kriterií



NEJOBVYKLEJŠÍ PRAKTIKY

- Hacking
- DoS
- Krádež identity
- Šíření virů
- Online podvody
- Softwarové pirátství
- Falšování
- Šíření škodlivého kódu
- Šíření Malware
- Phishing
- Spam
- Ransomware

VYUŽITÍ TAXONOMIÍ

- Různé přístupy
  - Klasifikace podle CIA triády
  - Klasifikace podle charakteru útočníka
  - Klasifikace pode charakteru útoku
- Neexistuje obecně přijímaná klasifikace
- ENISA/Europol taxonomie hraje v EU hlavní roli

Skupina	Typ
Sběr informací	Scanning
	Sniffing
	Phishing
Škodlivý kód	Virus, Trojan, Spyware
	Distribuce
	C&C
Dostupnost	DoS, DDoS
	Sabotáž
Pokus o průnik	Využívání zranitelností
	Pokus o přihlášení
Průnik	Využívání zranitelností
	Zneužití účtu
Informační bezpečnost	Neautorizovaný přístup
	Neautorizovaná modifikace/smazání
Podvod	Zneužití nebo neautorizované využití zdrojů
	Neoprávněné využití jména třetí strany
Škodlivý obsah	Spam
	Duševní vlastnictví
	Dětská pornografie, rasismus, schvalování násilí

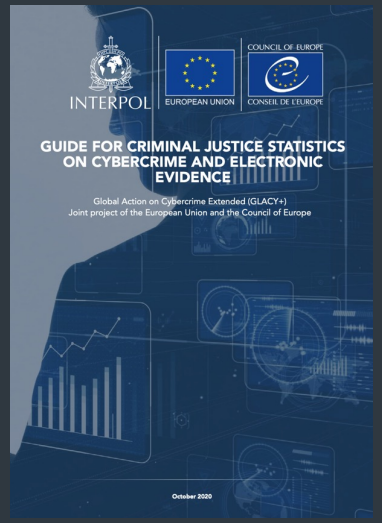
TAXONOMIE KBI

Postavena na taxonomii ENISA/Europol

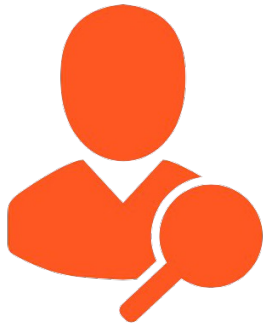
Vazba na skutkové podstaty

Vazba na mezinárodní instrumenty

Nedokonalá a nekompletní

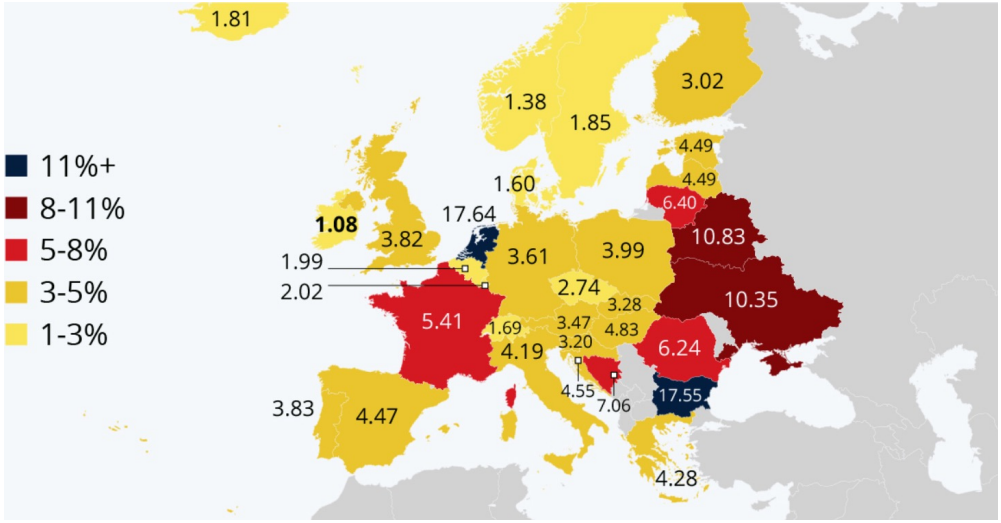


Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení	Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty	Využitelné důkazní prostředky
Phishing	Podvodná metoda, usilující o zcizování digitální identity uživatele, jeho přihlašovacích jmen, hesel, čísel bankovních karet a účtu apod. za účelem jejich následného zneužití (výběr hotovosti z konta, neoprávněný přístup k datům atd.). Vytvoření podvodné zprávy, šířené většinou elektronickou poštou, jež se snaží zmíněné údaje z uživatele vylákat.	✔	✔	Jde o typ ostatní kybernetického bezpečnostního incidentu způsobeného kybernetickým útokem. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.	Je vhodné zajistit obsah podvodných zpráv a služeb zajistit pokud možno včetně zdrojových kódů. Před znemožněním jejich provozu je vhodné kontaktovat PČR, která může zajistit vysledování přenosu zneužitých údajů a případně tak identifikovat pachatele.	Bude-li prováděna aktivní analýza s přístupem k útočníkovu systému, nebo systému hostujícímu podvodnou stránku, může dojít k naplnění znaků skutkové podstaty TČ dle § 230 TZ. Zajištění komunikace podvodné stránky, nebo poškozeného s útočníkem, může být rovněž vyhodnoceno jako zásah do telekomunikačního tajemství a jako TČ dle § 182 TZ.	§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Jsou-li prostřednictvím phishingu získávány přístupové údaje k přístupu do počítačového systému, nebo k nosiči informací za účelem spáchání trestných činů podle § 230 nebo § 182.	
							§ 209 - Podvod	Je-li poškozený uveden útočníkem v omyl, na základě kterého mu vznikne škoda - například bude útočník v rámci phishingu vyžadovat zaslání finanční hotovosti.	
							§ 234 - Neoprávněné opatření, padělání a pozměnění platebního prostředku	Jsou-li prostřednictvím phishingu získávány údaje o platebních kartách, nebo přístupové údaje do internetového bankovnictví	



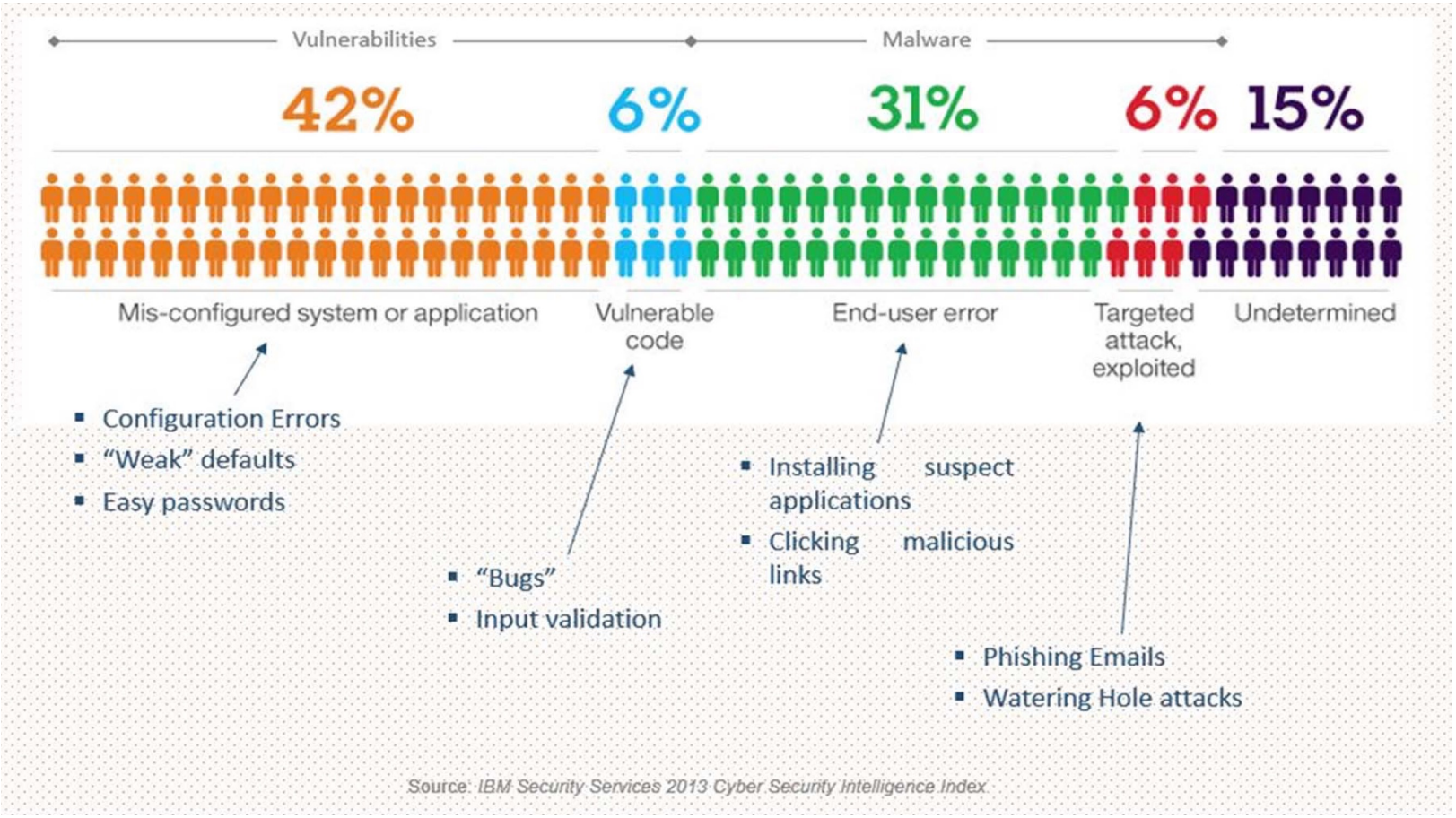
STATISTIKY V OBLASTI KYBERKRIMINALITY

- Omezená objektivita
- Problémy v detekci i klasifikaci
- Různá klasifikace různé výsledky



IKSP Institut pro kriminologii a sociální prevenci

ZDROJE


Vulnerabilities
Malware
42%
6%
31%
6%
15%
Mis-configured system or application
Vulnerable code
End-user error
Targeted attack, exploited
Undetermined
Configuration Errors
"Weak" defaults
Easy passwords
"Bugs"
Input validation
Installing suspect applications
Clicking malicious links
Phishing Emails
Watering Hole attacks
Source: IBM Security Services 2013 Cyber Security Intelligence Index

KATEGORIZACE KYBERKRIMINALITY

- Podle UNODC:
  - Útoky na CIA triádu
    - Hacking, MITM, DoS, etc.
  - Trestné činy související s počítačem
    - Podvod, vydírání, zneužití identity, spamming, duševní vlastnictví, poškozování osob a skupin
  - Trestné činy související s obsahem
    - Dětská pornografie (?)

KATEGORIZACE KYBERKRIMINALITY

Cyber-dependent

Může být páchána pouze prostřednictvím ICT

Dělení:

- ICT jako cíl
- ICT jako prostředek

Cyber-enabled

Tradiční činy páchané prostřednictvím ICT

Cyber-supported

Jen incidentální využití ICT k páchání trestných činů

CYBER-DEPENDENT

- Využití ICT může být předpokladem naplnění základní či kvalifikované skutkové podstaty
- Jednotlivé skutkové podstaty jsou rozmístěné po celé zvláštní části TZ
- Lze je rozdělit na
  - ty, které jsou namířené proti CIA triádě systémů
  - ty, které se páchají prostřednictvím systémů

OHROŽUJÍCÍ CIA TRIÁDU

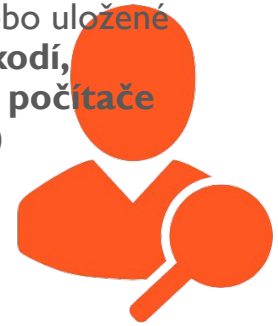
- **Porušení tajemství dopravovaných zpráv** (§ 182 TZ) - MITM, Sniffing, apod.
  - Kdo úmyslně **poruší tajemství datové**, textové, hlasové, zvukové či obrazové zprávy **posílané prostřednictvím sítě elektronických komunikací** a **přiřaditelné k identifikovanému účastníku** nebo uživateli, který zprávu přijímá, **nebo neveřejného přenosu počítačových dat** do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data (3 roky)
  - **Zaměstnanec** provozovatele poštovních služeb, **telekomunikační služby nebo počítačového systému** anebo kdokoli jiný vykonávající komunikační činnosti, který **spáchá nebo umožní dtto** [nebo] **pozmění nebo potlačí** […] zprávu podanou neveřejným přenosem počítačových dat, telefonicky, telegraficky nebo jiným podobným způsobem
- **Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí** (§ 183 TZ) – Hacking, zneužití přístupu apod.
  - Kdo **neoprávněně poruší tajemství** […] jiného záznamu, počítačových dat anebo jiného dokumentu uchovávaného v soukromí jiného tím, že je zveřejní, zpřístupní třetí osobě nebo je jiným způsobem použije (1 rok)

OHROŽUJÍCÍ CIA TRIÁDU

- **Neoprávněný přístup k počítačovému systému a nosiči informací** (§ 230 TZ) – Hacking, cracking, DoS, defacing, phishingové weby, šíření malware, apod.
  - Kdo **překoná bezpečnostní opatření**, a tím **neoprávněně získá přístup k počítačovému systému** nebo k jeho části (2 roky)
  - Kdo **zasáhne do** počítačového systému nebo k nosiči informací a neoprávněně **užije** data, data neoprávněně **vymaže** nebo jinak **zničí, poškodí, změní, potlačí**, sníží jejich kvalitu nebo **je učiní neupotřebitelnými**, **padělá nebo pozmění** data tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, nebo **neoprávněně vloží** data, nebo **učiní jiný zásah do programového nebo technického vybavení** počítače nebo jiného technického zařízení pro zpracování dat (3 roky)
  - […] v úmyslu **neoprávněně omezit funkčnost** počítačového systému nebo jiného technického zařízení pro zpracování dat (4 roky)
  - […] způsobí-li takovým činem **vážnou poruchu v činnosti** orgánu státní správy, územní samosprávy, soudu nebo jiného orgánu veřejné moci, nebo právnické nebo fyzické osoby, která je podnikatelem (5 let)

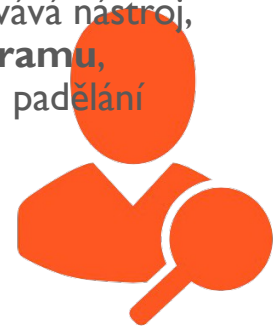
OHROŽUJÍCÍ CIA TRIÁDU

- **Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat** (§ 231 TZ)
  - Kdo **v úmyslu spáchat trestný čin** porušení tajemství dopravovaných zpráv podle nebo neoprávněného přístupu k počítačovému systému a nosiči informací **vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní**, sobě nebo jinému opatří nebo přechovává **zařízení** nebo jeho součást, **postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu**, vytvořený nebo přizpůsobený k **neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému** nebo k jeho části, nebo **počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek**, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části (2 roky)
- **Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti** (§ 232 TZ)
  - Kdo **z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání**, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté **data uložená v počítačovém systému** nebo na nosiči informací **zničí, poškodí, pozmění nebo učiní neupotřebitelnými**, nebo **učiní zásah do technického nebo programového vybavení počítače** nebo jiného technického zařízení pro zpracování dat, a tím **způsobí na cizím majetku značnou škodu** (6 měsíců)



OHROŽUJÍCÍ CIA TRIÁDU

- **Neoprávněné opatření, padělání a pozměnění platebního prostředku** (§ 234)
  - Kdo sobě nebo jinému **bez souhlasu** oprávněného držitele **opatří, zpřístupní, přijme nebo přechovává platební prostředek jiného**, zejména nepřenosnou platební kartu identifikovatelnou podle jména nebo čísla, elektronické peníze, příkaz k zúčtování, cestovní šek nebo záruční šekovou kartu (2 roky)
  - Kdo sobě nebo jinému **opatří, zpřístupní, přijme nebo přechovává padělaný nebo pozměněný platební prostředek** (5 let)
  - Zneužití (až 8 let)
  - Příprava je trestná!
- **Výroba a držení padělatelského náčiní** (§ 236)
  - Kdo **vyrobí, nabízí, prodá, zprostředkuje nebo jinak zpřístupní**, sobě nebo jinému opatří nebo přechovává nástroj, zařízení nebo jeho součást, postup, pomůcku **nebo jakýkoli jiný prostředek, včetně počítačového programu**, vytvořený nebo přizpůsobený k padělání nebo pozměnění peněz nebo prvků sloužících k ochraně peněz proti padělání anebo **vytvořený nebo přizpůsobený k padělání nebo pozměnění platebních prostředků**

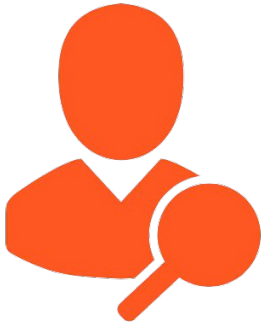


VYUŽÍVAJÍCÍ ICT

- Široká paleta skutkových podstat
- Mají jiný charakter při využití ICT
- Například:
  - **Výroba a jiné nakládání s dětskou pornografií** (§ 192 TZ), pokud jde o počítačové či elektronické dílo (+ šíření veřejnou počítačovou sítí, 2, 3/6 let)
  - **Porušení autorského práva** (§ 270 TZ), pokud je porušeno právo k počítačovému programu, databázi, nebo jinému dílu v elektronické podobě,
  - **Nebezpečné pronásledování** (§ 354 TZ) prostřednictvím elektronických prostředků
  - **Podvod** (§ 209 TZ), v případě páchání tohoto trestného činu v prostředí internetu (například phishing), apod.
  - **Vydírání** (§ 175 TZ) v případě ransomwarových kampaní
  - **Neoprávněné nakládání s osobními údaji** (§ 180 TZ) – například při získávání a obchodu s identitami

KVALIFIKOVANÉ SKUTKOVÉ PODSTATY

- Realizované prostřednictvím veřejně přístupné počítačové sítě
- Např.
  - neoprávněné nakládání s osobními údaji (§ 180 TZ),
  - pomluva (§ 184 TZ),
  - šíření pornografie (§ 191 TZ),
  - výroba a jiné nakládání s dětskou pornografií (§ 192 TZ),
  - šíření toxikomanie (§ 287 TZ),
  - propagace terorismu (§ 312e TZ),
  - vyhrožovaní teroristickým činem (§ 312f TZ),
  - křivé obvinění (§ 345 TZ),
  - násilí proti skupině obyvatel a proti jednotlivci (§ 352 TZ),
  - hanobení národa, rasy, etnické nebo jiné skupiny osob (§ 355 TZ),
  - podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod (§ 365 TZ),
  - založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka (§ 403 TZ),
  - podněcování útočné války (§ 407).



HARMONIZACE

- Sjednocení hmotněprávní úpravy
- Omezení bezpečných přístavů

By December 2023	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	34	*63%*	13	*24%*	7	*13%*
All Americas	35	23	*66%*	10	*29%*	2	*6%*
All Asia	42	20	*48%*	19	*45%*	3	*7%*
All Europe	48	46	*96%*	2	*4%*	0	*0%*
All Oceania	14	8	*57%*	4	*29%*	2	*14%*
All	**193**	**131**	***68%***	**48**	***25%***	**14**	***7%***

DÍKY ZA POZORNOST

STUPKA@NC3.CZ