Tabulka č. 2 – Taxonomie kybernetických bezpečnostních incidentů

Skupina	Typ	Popis	BI	TČ	Kategorizace dle vyhlášky o kybernetické bezpečnosti	Doporučení	Rizika při realizaci protiopatření	Kategorizace dle trestního zákoníku	Znaky skutkové podstaty
Sběr informací	**Scanning**	Aktivní nebo pasivní shromažďování informací o informačních systémech a počítačových sítích, prostřednictvím kterého lze získat informace o zranitelnostech předmětných systémů	✓	✓				§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li scanning prováděn za účelem získání informací sloužících k sestavení postupu využitého následně k provedení neoprávněného přístupu k počítačovému systému či nosiči informací (§ 230), nebo k odposlechu datové komunikace (§ 182)
	Sniffing	Odposlouchávání všech protokolů, které počítač přijímá / odesílá pomocí počítačového programu, nebo hardwarového zařízení, takzvaného snifferu (používá se např. pro odposlouchávání přístupových jmen a hesel, čísel kreditních karet).	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je-li to prakticky možné, neznemožňovat okamžitě zařízení realizaci sniffingu - může být za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.	Pasivní analýza sniffovacího zařízení - zde v podstatě žádné riziko nehrozí. Představuje-li však sniffovací zařízení počítačový systém, který je opatřen bezpečnostním opatřením zamezujícím přístupu, mohla by analýza dat, ke kterým je získán přístup překonáním takového opatření, vést k naplnění znaků skutkové podstaty trestného činu dle § 230 TZ - Neoprávněný přístup k počítačovému systému a nosiči informací. Aktivní protiopatření s trasováním útočníka - běžné trasování a blokování komunikace by nemělo být problematické. Bude však postup vyžadovat přístup do šifrované komunikace, či bude-li přistupováno do	§ 182 - Porušení tajemství dopravovaných zpráv	Je-li odchytávána datová zpráva přenášená elektronickou sítí konkrétnímu uživateli, nebo jde-li o odchytávání datového přenosu do, z, nebo uvnitř počítačového systému
								§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Výroba, držení, nebo distribuce nástroje ke sniffingu v úmyslu spáchat TČ porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu k systému. Může jít také opatření hesla prostřednictvím sniffingu v úmyslu spáchat TČ neoprávněného přístupu k systému.
								§ 234 - Neoprávněné opatření, padělání a pozměnění platebního prostředku	Je-li prostřednictvím siffingu získán platební prostředek (platební karta, elektronické peníze apod.) bez souhlasu oprávněného držitele. Trestná je i příprava tohoto TČ.

							počítačového systému útočníka po překonání bezpečnostního opatření nebo za účelem získání dat, opět hrozní naplnění skutkových podstat trestných činů porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu do počítačového systému.		
	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 připadně 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
Škodlivý kód	**Virus, Trojan, Spyware**	Virus = typ malware, který se šíří z počítače na počítač tím, že se připojí k jiným aplikacím. Následně může působit nežádoucí a nebezpečnou činnost. Má v sobě obvykle zabudován mechanismus dalšího šíření či mutací. Trojský kůň = Program, který plní na první pohled nějakou užitečnou funkci, ale ve	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický	Je vhodné zajistit kopii škodlivého software, která může sloužit k další analýze jako zdroj důkazního materiálu a k identifikaci pachatele. Je-li to prakticky možné, nelikvidovat okamžitě malware z napadeného systému - může být	Anaýza malware - neměla by být problematická, pokud v rámci ní není malware šířen, nebo nezpůsobí škodu. Aktivní protiopatření s trasováním útočníka - běžné trasování a blokování útočníka by nemělo být problematické. Bude-li však postup vyžadovat přístup do šifrované komunikace, či bude-li přistupováno do	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Dochází-li prostřednictvím škodlivého software k neoprávněnému přístupu k systému po překonání bezpečnostního opatření, nebo je-li přístupem neoprávněně nakládáno s daty v napadeném systému.
								§ 209 - Podvod	Některé typy škodlivého software vyžadují zaslání finanční částky od uživatele například za účelem získání přístupu k jeho datům nebo jako pokutu za neoprávněné

		skutečnosti má ještě nějakou skrytou škodlivou funkci. Trojský kůň se sám nereplikuje, šíří se díky viditelně užitné funkci, kterou poskytuje. Spyware = program skrytě monitorující chování oprávněného uživatele počítače nebo systému. Svá zjištění tyto programy průběžně (např. při každém spuštění) zasílají subjektu, který program vytvořil, respektive distribuoval.			bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.	počítačového systému útočníka, nebo jiného napadeného, po překonání bezpečnostního opatření, nebo za účelem získání dat, opět hrozí naplnění skutkových podstat trestných činů porušení tajemství dopravovaných zpráv, nebo neoprávněného přístupu do počítačového systému.		užívání software - jde o takzvaný ransomware. Zpravidla lze tyto aktivity kvalifikovat jako podvod.
								§ 182 - Porušení tajemství dopravovaných zpráv	Některé typy malware mohou sloužit také k odposlechu komunikace napadeného systému, v takovém případě lze kvalifikovat dle § 182 TZ.
								§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li škodlivý software vyráběn, distribuován, nebo držen s úmyslem páchat jeho prostřednictvím TČ neoprávněného přístupu k počítačovému systému a nosiči informací.
	Distribuce	Distribuce škodlivého software prostřednictvím sítí, nebo datových nosičů, s cílem infikovat škodlivým kódem hostitelský systém.	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	Je vhodné zajistit kopii škodlivého software, která může sloužit k další analýze jako zdroj důkazního materiálu a k identifikaci pachatele. Je-li to prakticky možné, nelikvidovat okamžitě malware z napadeného systému - může být za běhu cenným zdrojem důkazního materiálu pro vyšetřování trestné činnosti.		§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Je-li škodlivý software vyráběn, distribuován, nebo držen s úmyslem páchat jeho prostřednictvím TČ neoprávněného přístupu k počítačovému systému a nosiči informací.
								§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Při distribuce malware dochází k neoprávněnému v kládání dat do počítačových systémů, lze tedy kvalifikovat jako TČ dle § 230 odst. 2 TZ
	C&C	Command and control je informační systém, ze kterého je řízeno fungování sítě zařízení infikovaných škodlivým software.	✓	✓	Může jít o kybernetický bezpečnostní incident způsobený škodlivým softwarem nebo kódem, nebo	Je vhodné informovat policii ještě před zneškodněním command and control centra. Je-li například	Snaha o nabourání do systému, který funguje jako command and control systém škodlivého botnetu, i za účelem zajištění bezpečnosti a dostupnosti spravovaných		

					kybernetický bezpečnostní incident způsobený kompromitací technických opatření. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti primárních aktiv.	hostováno na spravovaném zařízení nebo ve spravované sítí, může jeho monitoring významně přispět ke zjištění pachatele, nebo k lokalizaci poškozených systémů.	aktiv může být kvalifikována jako TČ dle § 230 TZ.		
Dostupnost	**DoS, DDoS**	Technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele a to útokem mnoha koordinovaných útočníků.	✓		Jde o typ ostatní kybernetického bezpečnostního incidentu způsobeného kybernetickým útokem. Jde o kybernetický bezpečnostní incident způsobující narušení dostupnosti aktiv.	Platí stejná doporučení jako u CandC	Distribuovanému útoku DoS jde zabránit efektivně v podstatě jedině zneškodněním CandC centra ovládaného útočníkem, jeho zpětné trasování a samotné zneškodnění předpokládá přístup obránce do počítačových systémů třetích stran, nebo útočníka, což lze kvalifikovat jako TČ dle § 230 TZ.	§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	K útoku DoS může docházet při využití explitu za účelem vyčerpání zdrojů napadeného systému, pak lze kvalifikovat dle § 230 odst. 1 písm. a), nebo pomocí zahlcení napadeného systému požadavky ze externích zařízení (například při využití botnetu), pak lze kvalifikovat dle § 230 odst. 1 písm. b)
	Sabotáž	Plánovaný útok cílený na poškození systému, přerušení procesu, nebo změnu či smazání informací.			Může jít o kybernetický bezpečnostní incident způsobený porušením organizačních opatření, nebo spojený s projevem trvale působících hrozeb. Jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti, dostupnosti či integrity aktiv.			§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Ať již jde o útok zvenčí nebo zevnitř organizace a nezávisle na tom, zda jde o vandalismus, nebo cílenou snahu poškodit systémy nebo datový přenost, lze vždy kvalifikovat některou ze skutkových podstat § 230 TZ.
								§ 232 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti	Je-li například za výskyt incidentu odpovědný správce který zanedbal svoje povinnosti a v té souvislosti umožnil vznik incidentu.

Pokus o průnik	**Využívání zranitelností**	Pokus o průnik do systému nebo sítě zneužitím zranitelností systému, jeho komponent, nebo sítí. K těmto pokusů může docházet pomocí exploitů, SQL injection, XSS, file inclusion apod.	✓	✓	Je-li průnik neúspěšný, jde toliko o kybernetickou bezpečnostní událost. Úspěšný průnik znamená kybernetický bezpečnostní incident způsobený překonáním bezpečnostního opatření, který způsobuje narušení důvěrnosti aktiv.			Shodně jako Průnik - ve stádiu pokusu	
	Pokus o přihlášení	Pokus o přihlášení do služby nebo získání přístupu k systému nebo síti. K těmto pokusům může docházet například při využití techniky brute force, slovníkového útoku, nebo odhadování hesla.	✓	✓	Pokud jde o neúspěšné přihlášení, jde toliko o kybernetickou bezpečnostní událost. Úspěšné přihlášení znamená kybernetický bezpečnostní incident způsobený překonáním bezpečnostního opatření, který způsobuje narušení důvěrnosti aktiv.			Shodně jako Průnik - ve stádiu pokusu	
Průnik	**Využívání zranitelností**	Průnik do systému nebo sítě realizovaný za zneužití zranitelností systému, jeho komponent, nebo sítě. K těmto útokům může docházet pomocí exploitů, SQL injection, XSS, file inclusion apod.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.			§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Všechny techniky takto mohou být kvalifikovány, buď při neoprávněném přístupu dochází k obcházení zabezpečení, nebo dochází k modifikaci nebo nakládání s daty systému.
								§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	I když je přístup neúspěšný, samotné využívání nástrojů při pokusu je dokonaný TČ dle § 231 TZ.

	Zneužití účtu	Průnik do systému nebo sítě prostřednictvím zneužití uživatelského nebo administrátorského účtu.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti či integrity aktiv.			§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Podaří-li se do systému vstoupit, nebo přidat, upravit, nebo smazat data.
								§ 231 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat	Podaří-li se získat přihlašovací údaje k systému za účelem páchání další trestné činnosti.
Informační bezpečnost	**Neautorizovaný přístup**	Neoprávněný přístup k určité sadě informací.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti aktiv.			§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Je-li překonáno bezpečnostní opatření.
	Neautorizovaná modifikace/smazání	Neautorizovaná změna nebo likvidace určité sady informací.	✓	✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu jde o kybernetický bezpečnostní incident způsobující narušení důvěrnosti, dostupnosti a integrity aktiv.			§ 230 - Neoprávněný přístup k počítačovému systému a nosiči informací	Vždy § 230 odst. 2 TZ.
Podvod	**Zneužití nebo neautorizované využití zdrojů**			✓	Podle příčiny může jít o kterýkoliv kybernetický bezpečnostní incident, podle dopadu může jít o kybernetický bezpečnostní incident způsobující				

					narušení dostupnosti a integrity aktiv.				
	Neoprávněné využití jména třetí strany				Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.			§ 268 Porušení práv k ochranné známce a jiným označením	
Škodlivý obsah	**Spam**	Hromadné rozesílání nevyžádaných zpráv elektronickými prostředky – nejčastěji elektronickou poštou.			Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.			Šíření spamu jako takové není trestným činem. Jeho obsah však může některé skutkové podstaty naplňovat, například v případech phishingu.	
	Duševní vlastnictví	Protiprávní užívání duševního vlastnictví - především šíření rozmnoženin autorských děl (audiovizuálních, software apod.), či jejich zpřístupňování.		✓	Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.			§ 270 Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi	
	Dětská pornografie, rasismus, schvalování násilí	Šíření závadného obsahu různého druhu, především zakázané pornografie, xenofobní a rasistické zprávy, podněcování k násilí apod.		✓	Nejde o kybernetický bezpečnostní incident - není narušena důvěrnost, integrita ani dostupnost systémů nebo sítí.			Hlava III. a hlava XIII.	Různé trestné činy - například šíření pornografie, výroba a jiné nakládání s dětskou pornografií, projev sympatií k hnutí směřujícímu k potlačení lidských práv apod.