Právní rámec kybernetické bezpečnosti
Kybernetická bezpečnost a robotika

Obsah

Úvod

Tato kapitola vychází ze zadání projektu výzkumu, vývoje a inovací s názvem „Aktuální kybernetické hrozby v České republice a jejich eliminace“. Reflektuje změny, kterými prošel v předmětné oblasti český právní řád do roku 2015. Jedná se zejména o přijetí zákona č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů („Zákon o kybernetické bezpečnosti“), jeho prováděcích předpisů, i vývoj v oblasti evropské právní úpravy a mezinárodních závazků České republiky v posledních letech.

Kapitola se zaměřuje na analýzu a dopady vyplývající z nově přijatého Zákona o kybernetické bezpečnosti a jeho prováděcích předpisů, jež nabyly účinnosti dne 1. ledna 2015, na povinné subjekty. V rámci analýzy byla provedena stručná komparace uvedených právních předpisů s úpravou ve vybraných státech Evropské unie, dále byl posouzen soulad české právní úpravy s návrhem Směrnice Evropského Parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii. Významnou kapitolu tvoří i část o kybernetické kriminalitě a boji proti ní, včetně možnosti právní ochrany před kybernetickým útokem podle mezinárodního práva veřejného. Závěrečná část kapitoly je věnována mezinárodní spolupráci a mezinárodním iniciativám v oblasti boje proti kybernetické kriminalitě.

Na základě provedené analýzy a komparace národní, evropské a mezinárodní právní úpravy byl vytvořen soubor podnětů a doporučení pro případné novelizace přijatých právních norem předpisů a náměty pro další rozvoj v oblasti kybernetické bezpečnosti v České republice.

Seznam zkratek

Zkratka	Definice
Bezpečnostní strategie	Bezpečnostní strategie České republiky z roku 2015
CERT	Computer Emergency Response Team / skupina pro reakci na počítačové hrozby dle návrhu Směrnice
ČR	Česká republika
IS	Informační systém
Enisa	Evropská agentura pro bezpečnost sítí a informací
EU	Evropská unie
IS KII	Informační systém kritické informační infrastruktury
Jednotné kontaktní místo	Jednotné kontaktní místo pro bezpečnost sítí a informačních systémů
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
Krizový zákon	Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů, ve znění pozdějších předpisů
KS	Komunikační systém
KS KII	Komunikační systém kritické informační infrastruktury
KYBERNETICKÝ PROSTOR	Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací
Nařízení o kritériích pro určení prvku KI	Novelizované nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění pozdějších předpisů
NATO	Severoatlantické aliance
NBÚ nebo Úřad	Národní bezpečnostní úřad
SR	Slovenská republika
Směrnice	Směrnice Evropského Parlamentu a Rady o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informací v Unii (návrh)
Středoevropská platforma	Středoevropská platforma kybernetické bezpečnosti
Trestní řád	Zákon č. č. 141/1961 Sb., o trestním řízení soudním (trestní řádu), ve znění pozdějších předpisů
Trestní zákoník	Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů
Velká Británie	Spojené království Velké Británie a Severního Irska
VIS	Významný informační systém

Zákon o kybernetické bezpečnosti nebo Zákon	zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů
Vyhláška o kybernetické bezpečnosti	Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti, ve znění pozdějších předpisů
Vyhláška o VIS	Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění pozdějších předpisů

1 Podněty pro právní regulaci, základy právní úpravy

Následující text shrnuje úpravu nově účinného Zákona o kybernetické bezpečnosti a jeho prováděcích předpisů, jakož i historický vývoj této komplexní právní úpravy, která je v rámci EU zcela ojedinělá. Obsahuje zákonnou úpravu povinných subjektů v oblasti kybernetické bezpečnosti, povinnosti, které jsou jim ukládány, a úkoly kontrolních a dozorových orgánů. Pro lepší orientaci je do textu zařazen i přehled sankcí, které hrozí v případě nedodržení zákonem uložených povinností a lhůt, v nichž musí být dané povinnosti splněny.

1.1 Důvody pro přijetí Zákona o kybernetické bezpečnosti a jeho prováděcích předpisů, stav právní úpravy před jejich přijetím

K nutnosti přijetí závazné právní úpravy regulující oblast kybernetické bezpečnosti přispěl zejména nárůst četnosti používání informačních technologií a závislosti společnosti a jejího fungování na nich. Tím vzrostlo nejenom riziko zneužívání těchto technologií, ale zvýšil se i počet kybernetických útoků. Útoky jsou čím dál častěji prováděny v podobě organizované kybernetické špionáže a terorismu. Útoky proti informačním technologiím mohou mít rozsáhlé dopady na činnost subjektů využívajících je ke své činnosti a mohou vést ke značným škodám. V případě útoku proti prvkům kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické informační systémy nebo informační systémy veřejné správy, může být ohrožena bezpečnost nebo dokonce i existence státu. Přijetí nové závazné právní úpravy bylo nezbytné také s ohledem na závazky České republiky vůči státům NATO a EU.

Oblast kybernetické bezpečnosti je jednou z klíčových oblastí bezpečnostního prostředí České republiky. Jak uvádí Bezpečnostní strategie, jedním ze strategických zájmů České republiky je prevence a potlačování bezpečnostních hrozeb, které ovlivňují bezpečnost České republiky a jejích spojenců.[1] Provedenou analýzou bezpečnostního prostředí České republiky byly v rámci Bezpečnostní strategie hrozba kybernetických útoků a ohrožení funkčnosti kritické infrastruktury zařazeny mezi nejzávažnější bezpečnostní hrozby.

Na Bezpečnostní strategii navázala Strategie pro oblast kybernetické bezpečnosti, která konstatovala, že hlavním cílem České republiky v této oblasti je ochrana komunikačních a informačních systémů před kybernetickými hrozbami a snížení potenciálních škod způsobených v případě útoků na tyto informační a komunikační systémy.

Před přijetím Zákona o kybernetické bezpečnosti však neexistovala v českém právním řádu žádná specifická komplexní právní regulace kybernetické bezpečnosti. Základní instituty byly zakotveny v Ústavním pořádku ČR, dílčích otázek se dotýkala úprava speciálních zákonů[2] a jejich prováděcích předpisů. Nadnárodní regulace byla dále obsažena jak v mezinárodních smlouvách, doporučeních a jiných dokumentech mezinárodních organizací, tak i v primárním právu, v nařízeních a směrnicích EU. Právní úprava obsažená v právních předpisech ČR účinná do konce roku 2014 řešila pouze některé dílčí aspekty kybernetické bezpečnosti, a to zejména formou individuální odpovědnosti za počítačové delikty nebo formou certifikace zabezpečení informačních a komunikačních systémů užívaných k nakládání s utajovanými informacemi.

Právní rámec nově zakotvený v Zákonu o kybernetické bezpečnosti je základním nástrojem pro naplnění cíle chránit kybernetické prostředí České republiky. Zákon vymezuje činnosti jednotlivých orgánů při koordinaci postupu veřejné moci v oblasti kybernetické bezpečnosti, zajišťuje základní organizační rámec kybernetické bezpečnosti, stanovuje minimální požadavky na určené subjekty k zajištění prevence,

[1] KOLEKTIV AUTORŮ POD VEDENÍM MINISTERSTVA ZAHRANIČNÍCH VĚCÍ ČR. Bezpečnostní strategie České republiky. Praha, Schváleno Vládou České republiky v únoru 2015. ISBN 978-80-7441-005-5

[2] Zákony uvedené v Důvodové zprávě ke Kybernetickému zákonu, v bodě 1.3

detekce, reakce a opatření, které mají vést ke zvýšení odolnosti jednotlivých komunikačních a informačních systémů před stále rostoucím počtem kybernetických útoků. Zákon nezavádí nové přístupy, ale vychází ze standardů a zavedené praxe v této oblasti, zejména z řady norem ISO 27000 a COBIT.

Deklarovaným přínosem nové právní úpravy je zajištění vysoké úrovně bezpečnosti významných informačních systémů, informačních systémů kritické informační infrastruktury a informačních systémů kritické komunikační infrastruktury, jejichž zabezpečení by mělo vést k jejich vyšší odolnosti vůči kybernetickým útokům a tím i k eliminaci materiálních škod a nefunkčnosti nebo nedostupnosti služeb, které jsou jejich prostřednictvím poskytovány. Navíc by mělo dojít k posílení dobré pověsti České republiky v oblasti zabezpečení ICT, což by v ideálním případě mohlo vést ke zvýšení atraktivity České republiky pro zahraniční a tuzemské investory a zabránění ztrátám, které by jinak vznikly během kybernetických incidentů.

Cílem Zákona je zavést fungující systém zajištění kybernetické bezpečnosti, který zahrnuje bezpečnostní opatření, detekce kybernetických bezpečnostních událostí, hlášení kybernetických bezpečnostních incidentů, systém opatření k reakci na kybernetický bezpečnostní incident a činnost dohledových pracovišť (národní CERT a vládní CERT).

1.2 Zákon o kybernetické bezpečnosti

Návrh Zákona o kybernetické bezpečnosti byl zpracován ředitelem NBÚ a předložen vládě 31. července 2013. Návrh Zákona o kybernetické bezpečnosti byl schválen Poslaneckou sněmovnou a Senátem Parlamentu ČR v červnu a červenci 2014. Dne 13. srpna 2014 byl schválený návrh podepsán prezidentem republiky a 29. srpna 2014 vyhlášen ve Sbírce zákonů v částce 75 pod číslem 181/2014 Sb. Zákon nabyl účinnosti dne 1. ledna 2015.

Nově účinný Zákon o kybernetické bezpečnosti je založen na třech pilířích, kterými jsou

- bezpečnostní opatření,
- hlášení kybernetických bezpečnostních incidentů a
- opatření Úřadu.

Hlavními zásadami zákona jsou

- snaha minimalizovat zásahy do práv soukromých subjektů,
- individuální odpovědnost každého subjektu za bezpečnost vlastní sítě a
- technologická neutralita.

Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Cílem Zákona je stanovit minimální požadavky na standardní zabezpečení kritické informační infrastruktury, kritické komunikační infrastruktury, významných informačních systémů a významných sítí a zajistit dohledovým pracovištím přehled o situaci v kybernetické bezpečnosti, a to tak, aby zásahy do soukromé sféry povinných subjektů byly co nejmenší. Právní úprava je co do struktury zpracovávaných dat o kybernetických bezpečnostních incidentech minimalistická. Má předcházet výskytu kybernetických bezpečnostních incidentů a v případě, že se takové incidenty vyskytnou, má zamezit tomu, aby ohrozily celkové fungování informačních a komunikačních systémů.

1.2.1 *Základní pojmy definované Zákonem*

Zákon o kybernetické bezpečnosti definuje několik základních pojmů:

Kritická informační infrastruktura	Prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti
Významný informační systém	Informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého může narušení bezpečnosti omezit nebo výrazně ohrozit výkon působnosti orgánů veřejné moci a **který není kritickou informační infrastrukturou**
Významná síť	Je síť elektronických komunikací, která zajišťuje přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťuje přímé připojení ke kritické informační infrastruktuře

1.2.2 *Narušení kybernetické bezpečnosti*

Zákon rozlišuje tyto druhy narušení kybernetické bezpečnosti:

Kybernetická bezpečnostní událost	**Kybernetický bezpečnostní incident**	**Stav kybernetického nebezpečí**
Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací	Je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události	Stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací; stav kybernetického nebezpečí je možné stanovit pouze v případě, že výše uvedené ohrožení bezpečnosti nelze odvrátit činností Úřadu; o vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Úřadu a tento stav se vyhlašuje na dobu nezbytně nutnou, nejdéle na 7 dnů; tato doba může být prodloužena, nejdéle však na 30 dnů

1.2.3 *Systém zajištění kybernetické bezpečnosti*

Systém zajištění kybernetické bezpečnosti je tvořen pomocí bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů, jejich následné evidence a provádění opatření k ochraně informačních systémů a služeb a sítí elektronických komunikací. Dodržování povinností uložených povinným subjektům Zákonem o kybernetické bezpečnosti je vynucováno ukládáním sankcí.

1.2.4 *Povinné subjekty*

Zákon ukládá povinnosti v oblasti kybernetické bezpečnosti jak osobám soukromého, tak veřejného práva. Stanovuje tři skupiny regulovaných subjektů a definuje jejich povinnosti.

Za správce komunikačního nebo informačního systému kritické informační infrastruktury je považován ten, kdo určuje účel zpracování informací a podmínky provozování komunikačního nebo informačního systému, typicky tedy jeho vlastník. Správci jsou tak například jednotlivá ministerstva nebo jiné ústřední správní úřady, ale budou jimi i provozovatelé prvků kritické infrastruktury dle Krizového zákona

a příslušného Nařízení o kritériích pro určení prvku KI. Správce v režimu Zákona je tedy subjekt odpovědný za plnění povinností stanovených Zákonem.

1.2.5 *Povinnosti uložené povinným subjektům*

Jak vyplývá z níže uvedené tabulky, ve stavu kybernetického nebezpečí je povinným subjektům uložen vyšší rozsah povinností.

Povinná osoba § 3	**Hlášení KBI § 8**	**Reaktivní opatření § 13**	**Oznámení kontaktních údajů a jejich změn § 16**
a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),		za stavu kybernetického nebezpečí a stavu nouze	národní CERT
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d)	národní CERT	za stavu kybernetického nebezpečí a stavu nouze	národní CERT
c) správce informačního systému KII	Úřad (vládní CERT)		Úřad (vládní CERT)
d) správce komunikačního systému KII	Úřad (vládní CERT)		Úřad (vládní CERT)
e) správce VIS	Úřad (vládní CERT)		Úřad (vládní CERT)

1.2.6 *Sankce ukládané povinným subjektům v případě nesplnění Zákonem uložených povinností*

V případě porušení povinností uložených povinným osobám a orgánům Zákonem mohou být uloženy sankce až do výše 100 000 Kč. Níže je uvedena tabulka obsahující správní delikty, kterých se může povinná osoba dopustit, a sankce, které za tyto delikty mohou být uloženy. V posledním řádku je pak uveden přestupek, kterého se může dopustit také osoba fyzická, a to jako zaměstnanec Úřadu.

Povinnost	**Sankce**
Oznámení kontaktních údajů a jejich změn (§ 16)	do výše 10 000 Kč
Zavádění a provádění bezpečnostních opatření a vedení bezpečnostní dokumentace (§ 4)	do výše 100 000 Kč
Detekce kybernetických bezpečnostních událostí	Žádná sankce
Hlášení KBI (§ 8)	do výše 100 000 Kč
Reaktivní opatření (§ 13)	do výše 100 000 Kč
Opatření obecné povahy - ochranné opatření (§ 14)	do výše 100 000 Kč
Splnění povinností uložených v bezpečnostním opatření (§ 24)	do výše 100 000 Kč
Povinnost mlčenlivosti zaměstnance vykonávajícího práci v Úřadu (§ 10)	do výše 50 000 Kč

Správní delikty podle Zákona o kybernetické bezpečnosti projednává Úřad. Právnická osoba za správní delikt neodpovídá, pokud prokáže, že vynaložila veškeré úsilí, které je možné požadovat, aby porušení právní povinnosti zabránila. Odpovědnost právnické osoby za správní delikt zaniká, jestliže Úřad o deliktu nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl správní delikt spáchán. Došlo-li k porušení povinností uložených Zákonem o kybernetické bezpečnosti při podnikání fyzické osoby nebo v přímé souvislosti s ním, použijí se ustanovení Zákona o kybernetické bezpečnosti o odpovědnosti a postihu právnické osoby.

1.2.7 *Bezpečnostní opatření*

Souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru, je **bezpečnostním opatřením**. Bezpečnostní opatření se dělí na

- opatření organizační a
- opatření technická.

Konkrétní opatření spadající do těchto skupin jsou vyjmenována v ustanoveních § 5 odst. 2 a 3 Zákona. Obsah bezpečnostních opatření, obsah a struktura bezpečnostní dokumentace a rozsah bezpečnostních opatření pro povinné subjekty je stanoven v prováděcích právních předpisech. Typy a kategorie incidentů a způsob jejich hlášení jsou obsaženy ve Vyhlášce o kybernetické bezpečnosti.

1.2.8 *Opatření*

Opatření jsou činnosti, jejichž provedení je nutné k ochraně informačních systémů, služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu. Opatřeními jsou

- varování,
- reaktivní opatření a
- ochranné opatření.

Provedení opatření je podle Zákona povinným subjektům uloženo Úřadem v rozhodnutí nebo opatření obecné povahy.

1.2.9 *Dohled a kontrola*

Provádění dohledu nad dodržováním povinností uložených povinným subjektům na základě Zákona zajišťují dvě dohledová pracoviště – pracoviště vládního CERTu, který provozuje Úřad jako součást Národního centra kybernetické bezpečnosti, a pracoviště národního CERTu, který bude provozován právnickou osobou soukromého práva a ke své činnosti bude oprávněn na základě veřejnoprávní smlouvy uzavřené s Úřadem. Tato právnická osoba bude vybrána v řízení o výběru žádosti podle správního řádu[3]. Národní CERT (roli národního CERTu plní v současné době tým CSIRT.CZ) je subjektem, vůči němuž své Zákonem stanovené povinnosti v oblasti kybernetické bezpečnosti plní zejména subjekty uvedené v ustanoveních §3 a) a b) Zákona.

[3] ustanovení § 146 zákona č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

Národní CERT nedisponuje dle Zákona nařizovacími pravomocemi, ale má fungovat jako metodická podpora subjektů, které projeví zájem o kolektivní ochranu před kybernetickými bezpečnostními incidenty. Díky své soukromoprávní povaze může Národní CERT využít skutečnosti, že jeho provozovatel jakožto soukromý subjekt má možnost v nepředvídatelných situacích reagovat operativně, činit vše, co mu není zákonem zakázáno a vytvořit nová řešení či technické postupy.

Vládní CERT působící jako součást Úřadu disponuje dle Zákona nařizovacími a sankčními pravomocemi a zajišťuje uplatňování státní moci v oblasti kybernetické bezpečnosti.

Důležitá je efektivní komunikace mezi oběma subjekty, která bude probíhat zejména formou výměny informací o řešení kybernetických bezpečnostních incidentů. Výhodou existence jednoho soukromoprávního a druhého veřejnoprávního subjektu je i to, že pro oba typy dohledových pracovišť existují specifické struktury spolupráce. K některým kolaborativním aktivitám mají přístup jen dohledová pracoviště mající charakter orgánů veřejné moci a k jiným naopak jen soukromoprávní subjekty.

Kontrolu v oblasti kybernetické bezpečnosti provádí Úřad. Úřad kontroluje, jak povinné subjekty plní jím uložené povinnosti, a to jak za standardních okolností, tak za stavu kybernetického nebezpečí. V případě, že Úřad při kontrole zjistí nedostatky, uloží kontrolovanému subjektu, aby je ve stanovené lhůtě odstranil. Zjistí-li Úřad, že IS KII, KS KII nebo VIS je pro závažné nedostatky bezprostředně ohrožen kybernetickým bezpečnostním incidentem, může kontrolovanému orgánu zakázat používání systému nebo jeho části do doby, než budou nedostatky odstraněny. Jedná se o zásadní zásah do činnosti povinných osob, který může za určitých okolností výrazně účinnější než samotné sankce uvedené v Zákoně.

Ve vztahu ke splnění požadavků stanovených Zákonem, lze předpokládat, že ve větších společnostech jsou již požadavky stanovené Zákonem alespoň částečně splněny. Lze však zároveň předpokládat, že v malých společnostech bude plnění požadavků komplikovanější; totéž platí ve vztahu k organizacím státní správy. Většina povinných subjektů ze soukromé sféry již v současné době významnou část požadavků na bezpečnost splňuje – v organizačních strukturách větších subjektů existují i role bezpečnostního správce nebo manažera. Ve vztahu k mnohým subjektům bude zejména nutné stanovit, kdo je za plnění povinností v oblasti kybernetické bezpečnosti odpovědný.

1.2.10 *Lhůty*

Dobu, kdy se na jednotlivé povinné subjekty začnou vztahovat povinnosti vyplývající ze Zákona o kybernetické bezpečnosti, stanovuje Zákon ve svých přechodných ustanoveních pro každou kategorii povinných subjektů rozdílně.

Povinný subjekt § 3	**Bezpečnostní opatření § 4**	**Hlášení KBI § 8**	**Oznámení kontaktních údajů a jejich změn § 16**
a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, pokud není orgánem nebo osobou podle písmene b),			národní CERT
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d)		národní CERT	národní CERT

1 rok (od nabytí účinnosti Zákona) **30 dnů** (od nabytí účinnosti Zákona)

a) správce informačního systému KII		Úřad (vládní CERT)	Úřad (vládní CERT)
b) správce komunikačního systému KII		Úřad (vládní CERT)	Úřad (vládní CERT)
c) správce VIS		Úřad (vládní CERT)	Úřad (vládní CERT)

1 rok
(od určení povinného subjektu)

30 dnů
(od určení povinného subjektu; od naplnění určujících kritérií VIS)

1.3 Prováděcí předpisy k Zákonu

Prováděcími předpisy Zákona o kybernetické bezpečnosti jsou:

- Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti („**Vyhláška o kybernetické bezpečnosti**"). Tato vyhláška nabyla účinnosti dne 1. ledna 2015.
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích **(„Vyhláška o VIS"**). Vyhlášky nabyla účinnosti dne 1. ledna 2015.
- Novelizované nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury („**Nařízení o kritériích pro určení prvku KI**"). Novelizované znění nařízení nabylo účinnosti dne 1. ledna 2015.

1.3.1 *Vyhláška o významných informačních systémech*

Bližší informace pro určení subjektů, které jsou správci významných informačních systémů podléhajícími povinnostem podle Zákona o kybernetické bezpečnosti, poskytuje Vyhláška o VIS[4]. Vymezení *významných informačních systémů* umožňuje stanovení přesného okruhu subjektů, od kterých bude vyžadováno plnění povinností stanovených v Zákoně, jejichž obsah a rozsah je detailněji specifikován ve Vyhlášce o VIS.

Mezi správce významných informačních systémů patří podle Vyhlášky o VIS *výhradně osoby veřejného práva*. Nejsou mezi ně zařazeny obce[5] a při výkonu působnosti obce ani hlavní město Praha. Informační systémy těchto subjektů nejsou zařazeny proto, že jejich funkčnost ovlivňuje menší počet osob, a jejichž poškození by vedlo ke vzniku méně rozsáhlých škod. Jejich zařazení mezi významné informační systémy, a s tím související plnění povinností podle Zákona, by mohlo být pro tyto subjekty nepřiměřenou zátěží. Tato zátěž by neodpovídala následkům, které by mohly v důsledku kybernetického útoku na takové informační systémy nastat.

Významné informační systémy se dle Vyhlášky o VIS budou určovat dvojím způsobem

- jedna skupina je taxativně vypočtena v příloze č. 1 Vyhlášky o VIS, a
- ostatní bude mít za úkol určit jejich správce dle ve Vyhlášce o VIS stanovených určujících kritérií.

Informační systémy uvedené v příloze č. 1 byly určeny jako významné na základě zjevného naplnění určujících kritérií stanovených vyhláškou. Změna názvu daného systému pak nebude mít vliv na jeho zařazení do této přílohy, či vyřazení z ní, bude-li i nadále plnit své původní funkce.

Určující kritéria se dělí na kritéria dopadová a oblastní. Pro stanovení informačního systému jako významného informačního systému je nutné, aby splnil jak **dopadová**, tak **oblastní určující kritéria**.

1.3.2 *Nařízení o kritériích pro určení prvku KI*

Kritéria pro určení prvku kritické informační infrastruktury se dělí na kritéria **průřezová** a **odvětvová** a jsou podmínkami, za jejichž splnění bude prvek určen prvkem kritické informační infrastruktury.

[4] Vyhláška naplňuje zmocňovací ustanovení v § 28 odst. 1 Zákona o kybernetické bezpečnosti, které slouží k provedení § 6 písm. d) Zákona o kybernetické bezpečnosti.
[5] Zákon č. 128/2000 Sb., o obcích (obecní zřízení), ve znění pozdějších předpisů.

V případě zařazení mezi prvky kritické informační infrastruktury musí prvek **splňovat kumulativně průřezová i odvětvová kritéria**.

Nově určeným správcům prvků kritické infrastruktury vzniknou povinnosti v souladu s Krizovým zákonem, zejména zpracování plánu krizové připravenosti prvku kritické infrastruktury a určení odpovědného bezpečnostního zaměstnance.

1.3.3 *Vyhláška o kybernetické bezpečnosti*

Vyhláška o kybernetické bezpečnosti[6] upravuje obsah bezpečnostních opatření a rozsah, v jakém jsou jednotlivé skupiny subjektů, na něž regulace Zákona o kybernetické bezpečnosti dopadá, povinny bezpečnostní opatření zavést a provádět. Dále reguluje rozsah a doporučenou strukturu bezpečnostní dokumentace. Vyhláška dále stanoví jednotlivé kategorie a typy kybernetických bezpečnostních incidentů, náležitosti a způsob jejich hlášení a vzor a formu oznámení kontaktních údajů, které jsou povinné subjekty povinny oznamovat vládnímu CERT, nebo národnímu CERT a základní náležitosti oznámení o provedení reaktivního opatření a jeho výsledku.

Vyhláška podrobně stanoví organizační a technická bezpečnostní opatření, která jsou subjekty uvedené v § 3 písm. c) až e) zákona o kybernetické bezpečnosti povinny zavést a provádět ve svých informačních a komunikačních systémech.

Jednotlivá bezpečnostní opatření vycházejí především z pravidel stanovených technickými normami řady ISO/IEC 27001[7)], které jsou upraveny tak, aby jejich zavedení a následné dodržování bylo proveditelné jak osobami soukromého práva, tak i orgány veřejné moci, za současného naplnění podmínky zajištění adekvátní úrovně zabezpečení vybraných informačních a komunikačních systémů.

Vyhláška o kybernetické bezpečnosti stanoví typy a kategorie i rozsah a způsob hlášení kybernetických bezpečnostních incidentů. Stanoví také, jaké náležitosti má mít oznámení o provedení reaktivních opatření a jaký byl jeho výsledek. Dále určí kategorizaci a typologii kybernetických bezpečnostních incidentů a náležitosti hlášení kybernetického bezpečnostního incidentu tak, aby již z tohoto hlášení byly Úřad nebo Národní centrum kybernetické bezpečnosti schopni na konkrétní kybernetický bezpečnostní incident reagovat.

Jedním z cílů nové právní úpravy je zavést u správců informačních a komunikační rámec ISMS[8] prostřednictvím požadavku na vytvoření rozsáhlé bezpečnostní dokumentace a určit odpovědnosti za oblast IT Security definováním bezpečnostních rolí, které mají být u správců informačních a komunikačních systémů KII zavedeny.

Vyhláška o kybernetické bezpečnosti specifikuje tyto jednotlivé role, kterými jsou manažer kybernetické bezpečnosti, architekt kybernetické bezpečnosti, auditor kybernetické bezpečnosti a garant aktiva.

---

[6] K vydání vyhlášky o kybernetické bezpečnosti je Úřad zmocněn ustanovením § 28 odst. 2 Zákona o kybernetické bezpečnosti k provedení § 6 písm. a) až c), § 8 odst. 4, § 13 odst. 4 a § 16 odst. 6 Zákona o kybernetické bezpečnosti.

[7)] Základním východiskem tvorby vyhlášky jsou normy ISO/IEC 27001:2013 – Informační technologie – Bezpečnostní techniky – Systém řízení bezpečnosti informací a ISO/IEC 27002:2013 – Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací, které odráží moderní pojetí dobré praxe řízení bezpečnosti informací.

[8] Information Security Management System – systém řízení bezpečnosti informací.

2 Unijní předpisy o zajištění kybernetické bezpečnosti

Text obsahuje analýzu úpravy kybernetické bezpečnosti v právu EU s důrazem na návrh Směrnice Evropského Parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, a na změny, kterými návrh Směrnice prošel, než byl přijat Evropským Parlamentem, a na posouzení rozdílů mezi úpravou navrhované Směrnice a českou právní úpravou.

2.1 Strategie pro kybernetickou bezpečnost a návrh Směrnice Evropského Parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii

V únoru 2013 přijala EU Strategii pro kybernetickou bezpečnost. V ní jsou definovány principy (ochrana základních práv, svobody projevu, osobních údajů a soukromí, přístup k internetu pro všechny, demokratická správa kybernetického prostředí a sdílená odpovědnost za zajištění ochrany), jejichž dodržování by mělo k udržení kybernetické bezpečnosti dopomoci. Strategie pro kybernetickou bezpečnost dále stanovila pět strategických priorit, kterých chce dodržováním výše uvedených principů dosáhnout.

Těmito prioritami jsou:

- dosažení kybernetické způsobilosti,
- redukce kybernetické kriminality,
- příprava politik k obraně proti kybernetickým útokům,
- vyvinutí průmyslových a technologických zdrojů pro kybernetickou bezpečnost,
- zavedení mezinárodní politiky pro kybernetickou bezpečnost, odrážející evropské hodnoty.

Za účelem zvýšení bezpečnosti sítí byl 7. února 2013 předložen k projednání návrh Směrnice Evropského Parlamentu a Rady o opatřeních k zajištění vysoké úrovně bezpečnosti sítí a informací v Unii („**Směrnice**“). Cílem návrhu Směrnice bylo zajistit, aby všechny členské státy přijaly národní strategii a plán spolupráce pro bezpečnost sítí a informací a tím zajistily alespoň minimální vyžadovaný stupeň jejich ochrany. Zároveň se předpokládá vznik spolupráce a koordinované výměny informací mezi členskými státy. Bude se vyžadovat také sdílení informací mezi soukromým a veřejným sektorem. Společnosti z klíčových odvětví[9] a orgány státní správy budou mít povinnost posuzovat rizika, kterým čelí a přijímat odpovídající opatření pro zajištění bezpečnosti sítí a informací. Dosavadní evropská právní úprava je silně fragmentovaná, upravuje oblast kybernetické bezpečnosti v nedostatečném rozsahu a jsou v ní mnohé mezery[10]. Podle dosavadních pravidel jsou k zavedení bezpečnostních opatření povinny pouze

[9] Dle návrhu Směrnice jsou klíčovými odvětvími bankovnictví, burza cenných papírů, výroba, přenos a distribuce energie, doprava (letecká, železniční, námořní), zdravotnictví, internetové služby a veřejná správa.

[10] Evropské předpisy, které v současné době upravují oblast kybernetické bezpečnosti, jsou tyto: Směrnice Evropského Parlamentu a Rady:

- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody;2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu),
- 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES,
- 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES,
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí,
- 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

telekomunikační společnosti a správci údajů. Pouze telekomunikační společnosti mají povinnost hlásit významné bezpečnostní incidenty. Nový návrh Směrnice stanovuje pravidla pro všechny vlastníky a správce kritické infrastruktury.

Směrnice má zajišťovat minimální míru bezpečnosti. Funguje-li v členských státech právní úprava zajišťující vyšší míru bezpečnosti, může i nadále zůstat v platnosti. Stejně tak jsou členské státy oprávněny přijmout novou úpravu zaručující vyšší bezpečnostní požadavky, než jsou požadavky stanovené ve Směrnici.

2.2 Stav procesu přijímáni Směrnice

Dne 13. března 2014 byl návrh Směrnice v prvním čtení schválen Evropským Parlamentem a 5. června 2014 proběhla v Radě EU debata týkající se návrhu Směrnice. Evropským Parlamentem projednaná Směrnice vychází z původního návrhu, oproti původnímu návrhu ale obsahuje mnohé změny, zejména zpřesňuje okolnosti, za kterých jsou povinné subjekty povinny plnit své povinnosti v oblasti kybernetické bezpečnosti. Dále se v návrhu mění vymezení povinných subjektů. Návrh pozměněný Evropským Parlamentem klade na povinné subjekty nižší administrativní zátěž a více dbá na ochranu jejich údajů. V rámci právního procesu bude dále nutné, aby návrh Směrnice byl schválen Radou EU. V případě přijetí Směrnice ve stávajícím znění budou mít členské státy povinnost přijmout a zveřejnit právní předpisy nezbytné pro dosažení souladu s ní nejpozději do jednoho a půl roku ode dne jejího přijetí.

Vzhledem ke skutečnosti, že se jedná pouze o návrh Směrnice, který se může v průběhu právního procesu dále změnit, a nikoli o přijatou a platnou úpravu, jsou všechny naše níže uvedené závěry pouze doporučeními vycházejícími z nám dostupného návrhu Směrnice.

2.3 Rozdíly mezi evropskou úpravou a Zákonem o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti je obsahově velmi podobný znění Směrnice. Původní návrh Směrnice stanovil úkoly povinných subjektů a členských států více rámcově, zatímco návrh Směrnice přijatý Evropským Parlamentem je více zpřesňující.

2.3.1 *Povinné subjekty*

Původní návrh Směrnice stanovil, že **povinnými subjekty budou** mimo jiné **klíčoví poskytovatelé služeb informační společnosti**, jak je stanoveno ve Směrnici 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti[11]. Jedná se o služby, které podporují následné služby informační společnosti, jako jsou například platformy pro elektronické obchodování, internetové platební brány, sociální sítě, vyhledavače, služby cloud computingu a obchody s aplikacemi. Narušení těchto služeb brání poskytování dalších služeb, pro něž jsou tyto služby klíčovými vstupy. Dle původního návrhu směrnice se požadavky na bezpečnost a povinnosti měly vztahovat též na orgány veřejné správy a provozovatele kritických infrastruktur, které jsou na informačních a komunikačních technologiích silně závislé a mají zásadní význam pro zachování životně důležitých ekonomických a společenských funkcí, jako je elektřina, plyn, doprava, úvěrové instituce, burzy cenných papírů a zdravotnictví. Demonstrativní výčet skupin subjektů je uveden v Příloze II návrhu Směrnice.

Nařízení Evropského parlamentu a Rady

- 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací ve znění nařízení č. 1007/2008,
- 1077/2011/ES kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.

[11] Úř. věst. L 204, 21.7.1998.s. 37.

Návrh přijatý Evropským Parlamentem („**Upravený návrh směrnice**“) obsahuje výrazné změny co do výčtu povinných subjektů. Oproti původnímu návrhu by se minimální požadavky na bezpečnost měly vztahovat pouze na zúžený okruh hospodářských subjektů. Podle Upraveného návrhu by Směrnice měla regulovat pouze kritickou infrastrukturu, která má zásadní význam pro zachování životně důležitých ekonomických a společenských činností v oblasti energetiky, dopravy, bankovnictví, infrastruktury, finančních trhů a zdravotnictví. Orgánům veřejné správy pověřené výkonem veřejné služby se pouze doporučuje ke správě a ochraně své vlastní sítě a informačních systémů přistupovat pečlivě, jinak se na ně Směrnice neaplikuje. Stejně jako v původním návrhu jsou z oblasti působnosti Směrnice vyloučeni výrobci hardware a vývojáři software – oproti původní verzi tedy nedošlo ke změně. Výstražná informační síť kritické infrastruktury (CIWIN) by se měla rozšířit i na hospodářské subjekty, na něž se vztahuje návrh směrnice.

Dle Upraveného návrhu by se Směrnice **neměla vztahovat na klíčové poskytovatele služeb** informační společnosti[12], kteří podporují následné služby informační společnosti, jako jsou například platformy pro elektronické obchodování, internetové platební brány, sociální sítě, vyhledavače, služby cloud computingu a obchody s aplikacemi. Aplikovatelnost Směrnice pro tyto subjekty byla uvedena v bodu 8 písm. a) článku 3 návrhu Směrnice (demonstrativní výčet povinných subjektů v první části Přílohy II návrhu Směrnice). Tyto části Směrnice byly nově zcela vypuštěny. Bod 8 písm. b) článku 3 návrhu Směrnice, který stanovuje použitelnost Směrnice pro subjekty v oblasti energetiky, dopravy, bankovnictví, zdravotnictví (v původním návrhu též obchodování s cennými papíry, které bylo v pozměněném návrhu odstraněno) byl dále rozšířen o oblasti infrastruktury finančních trhů, výměnných uzlů internetu a potravinového dodavatelského řetězce a o podmínky, aby jejich narušení nebo zničení mělo v členském státě v důsledku neschopnosti zachovat tyto funkce významný dopad a aby dotčená síť a dotčené informační systémy byly spojeny se základními službami provozovatele infrastruktury.

2.3.1.1 Diference mezi Zákonem a úpravami ve Směrnici

Na rozdíl od návrhu Směrnice český Zákon o kybernetické bezpečnosti[13] a jeho prováděcí předpisy stanoví, že se povinnosti v oblasti kybernetické bezpečnosti ukládají jak soukromým, tak veřejnoprávním subjektům. Co se týče aplikovatelnosti předpisu na veřejnoprávní povinné subjekty, však není česká právní úprava v rozporu ani s původním, ani s Upraveným návrhem Směrnice. Dle obou návrhů totiž členský stát může povinnosti povinných veřejnoprávních subjektů upravit podle uvážení.

Na rozdíl od návrhu Směrnice, který stanovuje pro všechny povinné subjekty stejný rozsah povinností, Zákon o kybernetické bezpečnosti rozlišuje povinné subjekty do pěti skupin, u nichž rozsah povinností diferencuje.

Dalším rozdílem oproti evropské úpravě je skutečnost, že dle původního návrhu i podle návrhu po provedení změn, se dle Směrnice budou považovat za povinné subjekty **provozovatelé kritických infrastruktur**, zatímco dle důvodové zprávy k Zákonu o kybernetické bezpečnosti budou v ČR povinnými subjekty ty, které fakticky určují účel příslušného systému a podmínky jeho provozování, typicky jeho vlastníci. V tomto ohledu by potenciálně mohlo docházet k rozdílnému označení povinných subjektů podle Směrnice a Zákona.

Vzhledem k tomu, že směrnice jsou právními akty stanovujícími cíl, který musejí všechny členské státy EU splnit, s tím, že každý členský stát se může rozhodnout, jakým způsobem tak učiní, lze dovodit, že

[12] Jak je stanoveno ve Směrnici 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů a předpisů pro služby informační společnosti, Úř. věst. L 204, 21.7.1998.s. 37.
[13] §3 Zákon o kybernetické bezpečnosti a dále Vyhláška o VIS a novelizované Nařízení 432/2010 Sb.

v případě přijetí Směrnice bude tato stanovovat cíl zajištění vysoké úrovně společné bezpečnosti sítí a informací v EU.

S ohledem na znění Zákona mohou v praxi vznikat výkladové obtíže v případě určování povinného subjektu, tj. správce IS nebo KS. Vlastník prvku kritické infrastruktury může být osobou odlišnou od provozovatele/vlastníka příslušného IS nebo KS. Případné výkladové nejasnosti bude nutné řešit v součinnosti s Úřadem.

2.3.2 *Kontrolní a dozorové orgány*

Upravený návrh Směrnice stanoví, že členský stát má možnost jmenovat více než jeden odpovědný orgán a povinnost určit jeden **civilní vnitrostátní orgán**, kterým bude například jeden z odpovědných orgánů, jako vnitrostátní **Jednotné kontaktní místo**. Měla by být zajištěna vzájemná spolupráce odpovědných orgánů a Jednotného kontaktního místa při plnění povinností stanovených Směrnicí. Přeshraniční spolupráci členských států by měla zajišťovat Jednotná kontaktní místa prostřednictvím sítě pro spolupráci. Oznámení o bezpečnostních incidentech by měla být sdělována jak odpovědným orgánům, tak Jednotnému kontaktnímu místu ve státě, kde byla základní služba narušena. Pokud by byly základní služby narušeny ve více než jednom členském státě, Jednotné kontaktní místo, které oznámení obdrželo, by mělo informovat ostatní dotčená Jednotná kontaktní místa.

Upravený návrh směrnice oproti původnímu návrhu Směrnice výrazně důkladněji chrání povinné subjekty v oblasti zveřejňování informací o bezpečnostních incidentech. Jednotné kontaktní místo smí dle Upraveného návrhu směrnice zveřejnit informaci o kybernetickém incidentu jen po konzultaci s odpovědným orgánem a v případě, že je k zamezení incidentu nebo k jeho vyřešení třeba, aby o něm měla veřejnost povědomí, nebo pokud dotčený povinný subjekt odmítl řešit závažnou strukturální slabinu spojenou s tímto incidentem. V každém případě je oznamující odpovědný orgán povinen zajistit, aby dotčený povinný subjekt měl možnost se k věci vyjádřit a aby rozhodnutí o zveřejnění bylo vyváženo veřejným zájmem. Podmínky pro zveřejnění informací o kybernetickém incidentu by se dle Upraveného návrhu směrnice výrazně zpřísnily. Česká právní úprava chrání povinné subjekty v ještě větší míře. Úřad může poskytovat údaje z evidence incidentů provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru. Právo zveřejňovat údaje o kybernetických incidentech ale není Úřadu přiznáno vůbec.

Dle Upraveného návrhu by Jednotná kontaktní místa měla převzít mnohé povinnosti, které dle původního návrhu připadaly odpovědným orgánům. Stanoveny jsou mimo jiné v čl. 8 odst. 3 návrhu Směrnice a jsou jimi například: šíření včasných varování týkajících se rizik a incidentů a zajišťování koordinované reakce. Jsou jim dány i nové úkoly, jako vyvíjení pokynů pro konkrétní kritéria pro jednotlivá odvětví ve spolupráci s agenturou ENISA. Upravený návrh směrnice výrazně posiluje spolupráci s agenturou ENISA a zajišťuje informovanost sítě pro spolupráci o výzkumu v oblasti bezpečnosti a jiných relevantních programech v rámci iniciativy Horizont 2020.

Pro každé odvětví uvedené v Příloze II Směrnice (energetika, doprava, výroba a dodávky vody, potravinový dodavatelský řetězec, výměnné uzly internetu, infrastruktura finančních trhů) by dle Upraveného návrhu směrnice měla být zřízena alespoň jedna skupina CERT odpovědná za řešení incidentů a rizik. Skupina CERT by mohla být zřízena v rámci odpovědného orgánu. Skupiny CERT by měly být podřízeny odpovědným orgánům, nebo Jednotným kontaktním místům, která budou přezkoumávat jejich pravomoci a účinnost jejich postupů při řešení incidentů. Skupiny CERT by měly být oprávněny k tomu, aby se účastnily a iniciovaly společná cvičení s jinými skupinami CERT z členských států i z nadnárodních institucí jako jsou NATO a OSN.

Sankce zůstaly v Upraveném návrhu Směrnici stejné, bylo však navrženo nové ustanovení, dle kterého členské státy zajistí, aby sankce byly ukládány jen v případě, že subjekt nesplnil své povinnosti záměrně, nebo v důsledku hrubé nedbalosti. Byly též výrazně omezeny pravomoci Komise – například byla zrušena

pravomoc přijímat akty v přenesené pravomoci v oblasti dostupnosti bezpečné vnitrostátní komunikační a informační infrastruktury a existence odpovídajících zdrojů umožňujících zapojení odpovědného orgánu a skupiny CERT do bezpečného systému sdílení informací a zrušena byla též možnost Komise vyzvat členský stát, aby poskytl veškeré relevantní informace o určitém riziku nebo incidentu. Členským státům se tak ponechává větší volnost vnitrostátní úpravy.

Zákon o kybernetické bezpečnosti je postaven na existenci Úřadu jako orgánu vykonávajícího kontrolu v oblasti kybernetické bezpečnosti. Směrnice odděluje existenci odpovědného orgánu a skupin CERT. Česká úprava kybernetické bezpečnosti svým přístupem odpovídá možnosti dané Upraveným návrhem směrnice, tj. mít více odpovědných orgánů a jeden z nich (národní CERT) určit jako Jednotné kontaktní místo. Český Zákon o kybernetické bezpečnosti uvádí, že jako součást Úřadu bude působit vládní CERT jako veřejnoprávní subjekt a dalším subjektem bude národní CERT, který bude fungovat jako Jednotné kontaktní místo. Jak Směrnice výslovně stanovuje, skupina CERT může být zřízena v rámci odpovědného orgánu. Národní CERT v tomto ohledu také splňuje požadavky kladené Směrnicí – je civilním orgánem a dle Zákona je jeho úkolem zajišťovat přeshraniční spolupráci s jinými Jednotnými kontaktními místy.

Ohledně sankcí původní návrh Směrnice upravoval pouze nutnost jejich přiměřenosti – přičemž sankce podle Zákona jistě nelze považovat za nepřiměřeně vysoké, Upravený návrh ale umožňuje jejich uložení pouze v případě, že povinný subjekt nesplnil své povinnosti vědomě nebo z hrubé nedbalosti. Sankce stanovené v Zákoně jsou povinným subjektům ukládány za správní delikty. Právnická osoba[14] za delikt neodpovídá, prokáže-li, že vynaložila veškeré úsilí, které je po ní možné požadovat, aby porušení právní povinnosti zabránila. Navíc správním deliktem je pouze nesplnění povinností uložených Úřadem nebo nenahlášení kontaktních údajů (pro subjekty dle §3 c) až e) také nezavedení a neprovádění bezpečnostních opatření a bezpečnostní dokumentace) – povinné subjekty tedy, v případě, že nesplní, nesplní buď úmyslně, nebo z hrubé nedbalosti.

[14] Došlo-li k porušení povinností uložených Zákonem o kybernetické bezpečnosti při podnikání fyzické osoby nebo v přímé souvislosti s ním, použijí se ustanovení Zákona o kybernetické bezpečnosti o odpovědnosti a postihu právnické osoby.

3 Kybernetické bezpečnost rámci EU a ve vybraných zemích

3.1 Regulace v rámci EU

Vývoj informačních komunikací, elektronických sítí a informačních systémů a vzrůstající závislost evropských společenství na něm s sebou přinesly rozvoj kybernetické kriminality, jako trestné činnosti, která je hrozbou jak pro občany a podniky, tak i pro státní orgány a další subjekty veřejného práva.

V lednu 2013 začalo na půdě EU fungovat Evropské centrum pro boj proti kybernetické kriminalitě („**Centrum**"). V jeho vytvoření hrála klíčovou roli Evropská komise. Předmětné středisko funguje v EU v rámci Evropského policejního úřadu – Europolu, které sídlí v nizozemském Haagu. Centrum zaměřuje svou činnost na ochranu fyzických a právnických osob před nezákonnými činnostmi na internetu prováděnými organizovanými zločineckými skupinami (zejména se bude jednat o oblasti podvodů v internetovém bankovnictví, nebo kybernetickou kriminalitu poškozující děti). „*Centrum bude při plnění svých úkolů a za účelem poskytování lepší podpory vyšetřovatelům, státním zástupcům a soudcům zabývajícím se kyberkriminalitou soustřeďovat jak informace z veřejně dostupných zdrojů, tak i ze soukromého sektoru, od policie a akademické obce. Nové centrum bude rovněž sloužit jako znalostní základna pro vnitrostátní policii v členských státech a sdruží evropské odborné kapacity a odbornou přípravu v této oblasti".*[15]

Situace v jednotlivých členských státech je hodnocena dle dostupných materiálů. Z tohoto důvodu je u některých zemí uvedeno více informací, které lze získat z veřejně dostupných zdrojů.

3.2 Regulace v některých členských státech EU

3.2.1 *Estonsko*

Jedním z evropských lídrů v oblasti kybernetické bezpečnosti je Estonsko, které bylo v roce 2007 postiženo sérií závažných kybernetických útoků. V návaznosti na ně přijalo Estonsko řadu kroků s cílem zvýšit a zajistit kybernetickou bezpečnost země. Poslední kybernetická strategie Estonska se vztahuje na období let 2014 až 2017. Estonská vláda na toto období vyčlenila 16 milionů Eur, většina z nich má být čerpána z evropských fondů. Strategie si klade za cíl odhalování rizik kybernetické bezpečnosti a obranu proti nim. Vzhledem k závislosti na elektronických systémech (e-state, e-volby, identifikační průkazy), se Estonsko stalo velice zranitelné. Kybernetická strategie se proto soustředí na zajištění kritické infrastruktury a významných systémů pomocí právního rámce, podporou mezinárodní spolupráce, zvyšováním povědomí o kybernetické bezpečnosti, zajišťováním profesionálů v oblasti kybernetické bezpečnosti, jakož i vývojem IT řešení pro zajištění kybernetické bezpečnosti.

Pro odhalování kybernetické kriminality byla v roce 2012 zřízena sekce pro odhalování kyberkriminality. V rámci této sekce byla zřízena i pozice webového policejního komisaře, jehož úkolem je také zvyšování povědomí veřejnosti o bezpečnosti internetu a ochrana dětí a mládeže online.

Jednou z nejdůležitějších aktivit v boji proti kyberkriminalitě a kyberterorismu, které se v Estonsku věnují, jsou kybernetická bezpečnostní cvičení, jejichž účelem mimo jiné je, prověření efektivnosti a dostatečnosti zavedených právních předpisů pro oblast kybernetické bezpečnosti. V roce 2012 zorganizovala estonská vláda unikátní kybernetické bezpečnostní cvičení „Kybernetická horečka"[16]. Od roku 2012 se v Estonsku

[15] http://europa.eu/rapid/press-release_IP-12-317_cs.htm
[16] http://www.riso.ee/en/content/cyber-security-0

pořádají kybernetická bezpečnostní cvičení NATO, přičemž Talin je Centrem Excelence NATO pro kybernetickou bezpečnost.

Estonsko pokračuje v boji proti kyberkriminalitě i v roce 2015 a připravuje založení policejní jednotky, která by se přímo věnovala problémům s kyberkriminalitou. Tato jednotka by měla působit jako součást Ústřední kriminální policie již od roku 2016.[17]

3.2.2 *Německo*

Oblast kybernetické bezpečnosti je nově ve Spolkové republice Německo komplexně upravena. Vedle toho jsou bezpečnost dat a ochrana informací okrajově upraveny v dalších spolkových zákonech[18].

Základním dokumentem pro oblast kybernetické bezpečnosti je Strategie kybernetické bezpečnosti schválená v únoru 2011, v níž spolková vláda definuje cíle pro kybernetickou bezpečnost. Strategie je zaměřena především na ochranu kritických informačních infrastruktur, ochranu informačních systémů v SRN, posílení bezpečnosti informačních systémů ve veřejné správě, zřízení Národního centra obrany proti kybernetickým útokům[19], zřízení Národní rady pro kybernetickou bezpečnost, jejímž úkolem je propojit IT management na spolkové úrovni s IT Radou pro plánování[20] a s oblastí kybernetické bezpečnosti na strategické a politické úrovni, efektivní ochranu proti zločinům páchaným v kybernetickém prostoru, efektivní akce k zajištění kybernetické bezpečnosti v Evropě i ve světě, používání spolehlivých a důvěryhodných informačních technologií, rozvíjení lidských zdrojů ve spolkových orgánech a rozvoj nástrojů na ochranu proti kybernetickým útokům.

První návrh zákona na zvýšení bezpečnosti informačních systémů byl předložen v březnu 2013. V důsledku změny vlády a odporu ekonomických subjektů ale nedošlo k jeho přijetí. Návrh zákona byl kritizován též z právního pohledu – jeho součástí například nebyla definice „provozovatelů kritické infrastruktury" nebo „významných bezpečnostních incidentů". Nesouhlas s navrhovanou úpravou spočíval v tom, že tyto pojmy jsou natolik důležité, že by měly být upraveny přímo v zákoně. Dále v zákoně nebyla uvedena možná omezení základních práv týkající se vlastnictví a výkonu povolání u provozovatelů kritické informační infrastruktury, jejichž uvedení je nutné podle německé Ústavy. Návrh zákona byl kritizován též společnostmi, na něž by kybernetický útok mohl být proveden.

Zákon na zvýšení bezpečnosti informačních systémů byl přijat v červenci roku 2015[21]. Stejně jako návrh zákona z roku 2013 je vytvořen ve formě novely stávajících právních předpisů,[22] do nichž je tímto zákonem doplněna regulace oblasti kybernetické bezpečnosti.

---

[17] http://www.baltictimes.com/estonian_police_to_create_cyber_crime_unit/

[18] Telekommunikationsgesetz z 22. června 2004 (BGBl. I S. 1190), ve znění pozdějších předisů
Urheberrechtsgesetz z 9. září 1965 (BGBl. I S. 1273), ve znění pozdějších předisů
Bundesdatenschutzgesetz ve znění oznámení ze dne 14. ledna 2003 (BGBl. I S. 66), ve znění pozdějších předpisů
Telemediengesetz z 26. února 2007 (BGBl. I S. 179), ve znění pozdějších předpisů
Gesetz über den Datenschutz bei Telediensten ze dne 11. června 1997 (BT-Drs. 13/7934)
BSI-Gesetz ze dne 14. srpna 2009 (BGBl. I S. 2821)

[19] Nationales *Cyber*-Abwehrzentrum – centrum obrany proti kybernetickým útokům

[20] IT Plannungsrat je radou, která má mandát umožnit závaznou spolupráci mezi vládou na federální úrovni, na státní úrovni a vládami lokálními v oblasti IT a e-government.

[21] http://www.itgovernance.eu/blog/new-german-cyber-security-law-to-protect-critical-infrastructure/

[22] BSI-Gesetz ze dne 14. srpna 2009 (BGBl. I, S. 2821)
Bundeskriminalamtgesetz ze dne 7. července 1997 (BGBl. I S. 1650)
Telemediengesetzes ze dne 26. února 2007 (BGBl. I S. 179)
Telekommunikationsgesetz ze dne 22. června 2004 (BGBl. I S. 1190)
Aussenwirtchaftsgsetz

Německý zákon, stejně jako český Zákon, přináší minimální úroveň bezpečnostních opatření, která by měla být povinnými subjekty zavedena. Na rozdíl od českého Zákona, budou mít provozovatelé kritické informační infrastruktury v Německu na provedení opatření na ochranu informačně-technických systémů k dispozici dva roky od účinnosti prováděcího předpisu, na základě kterého budou určeni jako provozovatelé kritické informační infrastruktury. Zákon také stanovuje povinnost provozovatelů kritické infrastruktury podrobit se každé dva roky bezpečnostnímu auditu, zkouškám a certifikacím a zprostředkovat jejich výsledky, včetně případných odhalených nedostatků, Spolkovému úřadu pro ochranu informační techniky („**Spolkový úřad**“). Spolkový úřad bude fungovat jako centrální dozorové místo pro provozovatele kritických infrastruktur. V případě, že by kybernetické incidenty mohly ohrozit funkčnost kritických informačních infrastruktur, bude jejich hlášení povinné. Subjekty, které incident nahlásí, mají právo zůstat v anonymitě. Tím by mělo být minimalizováno riziko ztráty dobré pověsti postižených subjektů.

Na rozdíl od českého Zákona, německý zákon se vztahuje pouze na ochranu informačních systémů kritické infrastruktury[23]. Povinnými subjekty tak nejsou správci významných informačních systémů, jak jsou definováni českou úpravou, ani poskytovatelé služby elektronických komunikací či orgány nebo osoby zajišťující významnou síť.

V roce 2009 byla schválena Národní strategie pro ochranu kritických infrastruktur KRITIS. Prvky kritické infrastruktury jsou v ní definovány jako organizace a zařízení s velkým významem pro státní společnost, jejichž narušení nebo výpadek by způsobily narušení dodávek, významné narušení veřejné bezpečnosti nebo jiné dramatické důsledky.

Sektory spadající do kritické infrastruktury jsou v SRN velmi podobné odvětvovým kritériím uvedeným v příloze č. 1 Nařízení. Na rozdíl od odvětvových kritérií Nařízení obsahuje německá regulace navíc sektor kritické infrastruktury „Média a kultura“. Od českých odvětvových kritérií se liší také tím, že oblast potravinářství obsahuje nejen potravinářskou výrobu, ale též obchod s potravinami. Takovou úpravu lze považovat za komplexnější. Do české úpravy by proto měla být zařazena oblast obchodu s potravinami. Německá úprava obsahuje též zařazení oblastí: zdravotní péče, léky a očkovací látky a laboratoře. Jak je patrné z níže uvedeného srovnání, obory spadající do kritické infrastruktury jsou v německé regulaci popsány mnohem šířeji než v českém Nařízení, následkem toho je skutečnost, že do některých oborů kritické infrastruktury (například elektřina nebo plyn) bude v SRN spadat větší počet subjektů.

3.2.3 *Slovensko*

Trestání počítačové kriminality je na Slovensku koncipováno úžeji než v České republice. Primárně tuto oblast upravuje § 247 zákona č. 300/2005 Z.z., Trestný zákon, ve znění pozdějších předpisů („**Slovenský trestní zákon**"). Podle tohoto ustanovení se trestá trestný čin poškození a zneužití záznamu na nosiči informací, který obsahuje dvě samostatné skutkové podstaty, tj. samotné poškození a zneužití záznamu a dále neoprávněný přístup do počítačového systému. Tato úprava s určitými rozdíly odpovídá ustanovením § 230 (Neoprávněný přístup k počítačovému systému a nosiči informací) a § 231 (Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat) českého Trestního zákoníku. Na rozdíl od české trestněprávní úpravy, Slovenský trestní zákon neupravuje trestný čin Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti, kdy takový trestný čin může spáchat například zaměstnanec porušením svých zákonných povinností z hrubé nedbalosti.

[23] Kritická infrastruktura ve smyslu zákona BSI-Gesetz ze dne 14. srpna 2009 (BGBl. I, S. 2821).

Další oblast počítačové kriminality na Slovensku lze potrestat podle ustanovení o Trestných činech proti průmyslovým právům a právu autorskému (§ 281 – § 283 Slovenského trestního zákona). Tato úprava s menšími odlišnostmi odpovídá české právní úpravě, na Slovensku je navíc přitěžující okolností podmiňující použití vyšší sazby skutečnost, když pachatel spáchá trestný čin porušování autorského práva prostřednictvím počítačového systému. V české právní úpravě je na rozdíl od slovenské úpravy přitěžující okolností skutečnost, kdy trestná činnost vykazuje znaky obchodní činnosti nebo jiného podnikání.

S počítačovou kriminalitou souvisí i trestná činnost v oblasti porušování soukromí a listovního tajemství, které zahrnuje i data a zprávy v elektronické podobě. Slovenská právní úprava poskytuje ochranu tajemství dopravovaných zpráv v ustanoveních §§ 196 až 198 Slovenského trestního zákona, česká navíc explicitně i ochranu listin a jiných dokumentů, v rámci toho i počítačových dat, uchovávaných v soukromí (§ 183 Trestního zákoníku).

Trestněprávní ochranu dopravnímu, telekomunikačnímu a informačnímu systému poskytuje v České republice ustanovení § 311 Teroristický útok. Na Slovensku obdobná trestněprávní ochrana chybí.

Obecně lze ke slovenské trestněprávní úpravě v oblasti kybernetické kriminality konstatovat, že oproti české trestněprávní regulaci, je méně podrobná a sankcionuje užší škálu protiprávního jednání. V případě protiprávného jednání, které má v České republice konkrétní skutkovou podstatu, je na Slovensku nutné aplikovat obecnější ustanovení, která daná jednání postihují. Například v případě trestného činu Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí by se na Slovensku s největší pravděpodobností použila skutková podstata ustanovení § 194 Porušování domovní svobody nebo § 194a Ochrana soukromí v obydlí Slovenského trestního zákona.

Úpravy **kybernetické bezpečnosti** se na Slovensku dotýká několik právních předpisů, nicméně pouze okrajově. Příprava komplexní právní úpravy pro oblast kybernetické bezpečnosti je jedním s cílů *Koncepcie kybernetickej bezpečnosti Slovenskej republiky.* Slovensko si klade za cíl stanovit úroveň minimálních bezpečnostních opatření a v té souvislosti i institucionální rámec pro výkon veřejné správy pro oblast kybernetické bezpečnosti. Další kroky v této oblasti by měly vést ke stanovení politiky kybernetické bezpečnosti, systému řízení kybernetické bezpečnosti, dosažení přiměřené míry kybernetické odolnosti SR, snížení míry kybernetické kriminality, zajištění trvalého rozvoje způsobilostí a technologických zdrojů kybernetické bezpečnosti SR.

Koncepce počítá s komplexní právní úpravou kybernetické bezpečnosti, jejíž příprava právě probíhá v podobě zákona o informační bezpečnosti.

Navrhovaný text slovenského zákona o informační bezpečnosti („**Návrh zákona o informační bezpečnosti**“) používá jinou terminologii, než zákon o kybernetické bezpečnosti (např. informační a počítačová bezpečnost, digitální a kybernetický prostor, atd.). Navrhovaná právní úprava informační bezpečnosti je zcela jinak koncipovaná, než česká úprava, která je přehledněji strukturována a pro povinné subjekty srozumitelnější. Na rozdíl od českého zákona by povinnými subjekty na Slovensku měli být i poskytovatelé služeb informační společnosti, tj. například společnosti provozující e-shopy.

Povinnost zavést bezpečnostní opatření stanovená v Návrhu zákona o informační bezpečnosti je závazná nejen pro provozovatele kritické infrastruktury, ale i pro povinné subjekty dle zákona o informačních systémech veřejné správy a poskytovatele služeb elektronických komunikací. Podle zákona o kybernetické bezpečnosti se tato povinnost vztahuje pouze na správce informačních a komunikačních systémů KII a správce VIS, tj. vybraných informačních systémů veřejné správy.

Převážná část zákona se věnuje informačním systémům veřejné správy, jejich vývoji, vytvoření a zavedení do provozu. V rámci toho se kategorizují informace a podle nich i informační systémy s ohledem na úroveň ochrany informací zpracovávaných těmito systémy. Podle kategorie informačního systému se použijí bezpečnostní opatření (bezpečnostní opatření základní úrovně, zvýšené úrovně, bezpečnostní opatření, kterými se zredukují rizika na akceptovatelnou úroveň). Co se ale těmito bezpečnostními

opatřeními konkrétně myslí, to už Návrh zákona o informační bezpečnosti neuvádí. Pouze u informačních systémů (§ 23/3 a 6) v případě bezpečnostního projektu odkazuje na výnos MF SR č. 55/2014 o standardech pro informační systémy veřejné správy a na ISO/IEC 27005.

Návrh zákona o informační bezpečnosti nedostatečně upravuje bezpečnostní opatření, které musí všechny povinné subjekty, kromě poskytovatelů služeb informační společnosti, zavést. Uvádí jenom jejich výčet bez dalšího konkretizování (např. určení kontaktní osoby pro nahlašování bezpečnostních incidentů, vypracování směrnice pro řešení bezpečnostních incidentů, atd.).

Na rozdíl od Zákona o kybernetické bezpečnosti, který se v ustanoveních § 11 a násl. věnuje opatřením v případě hrozby v oblasti kybernetické bezpečnosti nebo v případě kybernetického bezpečnostního incidentu, Návrh zákona o informační bezpečnosti tuto oblast neupravuje, neupravuje ani stav kybernetického nebezpečí. Návrh pouze okrajově řeší prevenci, reakci na vzniklé hrozby však věnuje minimum prostoru a to na nelogickém místě, u výčtu kompetencí orgánů státní správy, tj. Ministerstva financí SR.

Funkci národního a vládního CERTu by na Slovensku měl plnit útvar CSIRT, který je kontaktním místem jak soukromoprávních tak i veřejnoprávních subjektů.

V posledních ustanoveních návrhu zákona je upraven kritický informační systém a odkazuje u něj na ustanovení vztahující se na informační systémy veřejné správy, takže se těchto systému týkají stejná pravidla jako informačních systémů veřejné správy. Obdobná úroveň ochrany u KII a VIS funguje i v České republice.

Návrh zákona počítá s citelnými finančními sankcemi, když maximální sankce za porušení povinnosti zařadit jednotlivé informační systémy veřejné správy, které jsou v její působnosti, do některé z kategorií a zajistit jim přiměřenou ochranu, může dosáhnout až 500 000 EUR. Stejná pokuta hrozí i dodavateli informačního systému, pokud prokazatelně odstraní nebo zablokuje funkce informačního systému, které pak mohou umožnit nepozorovaný přístup do tohoto systému nebo k jeho údajům. Je na zvážení, jestli takto vysoké sankce, které míří i na veřejnoprávní subjekty, budou slovenskými státní orgány v případě porušení povinností efektivně vymáhat.

Kritickou infrastrukturu upravuje samostatný zákon č. 45/2011 Z.z. o kritickej infraštruktúre. Tento zákon uvádí výčet sektorů kritické infrastruktury a obecně vymezuje sektorová a průřezová kritéria, ty však blíže výslovně neupravuje. Právní úprava tudíž neobsahuje specifikaci těchto kritérií, jak je tomu v případě Nařízení o kritériích pro určení prvku KI v ČR, ale jenom způsob jejich stanovení. Tento koncept je s ohledem na ochranu kritické infrastruktury logičtější, vzhledem k tomu, že sektorová a průřezová kritéria nejsou stanovena veřejně a podléhají utajení. Slovenské Ministerstvo vnitra pak překládá návrh sektorových kritérií a ve spolupráci s jinými ministerstvy návrh průřezových kritérií, dále spravuje neveřejný centrální rejstřík prvků kritické infrastruktury.

Při srovnání odvětví kritické infrastruktury mezi slovenskou a českou úpravou najdeme mnohé rozdíly. Na Slovensku např. nejsou uvedeny odvětví *potravinářství a zemědělství*, *kybernetické bezpečnosti*, *finančního trhu a měny*, *nouzové služby*, jako (např. IZS a v rámci toho OPIS, ČHMÚ), *veřejné správy* (a v rámci toho např. oblast sociálního zabezpečení včetně příslušných IS a KS). Ve výčtu českých odvětví zas není uveden chemický a farmaceutický průmysl, hutnictví, důlní průmysl.

Slovenský provozovatel prvku KI má na rozdíl od toho českého nárok na finanční příspěvek na plnění svých povinností souvisejících s provedením bezpečnostních opatření na ochranu prvku KI. Finanční příspěvek poskytuje ústřední orgán v daném sektoru, tj. např. příslušné ministerstvo.

3.2.4 *Polsko*

Polsko v posledních letech čelilo několika útokům na kybernetickou bezpečnost, zejména se jedná o útok na webové stránky Sejmu[24], dolní komory Národního shromáždění, nebo útok na polské aerolinky LOT[25].

Právní **úprava kybernetické kriminality** a ochrany kyberprostoru je v Polsku zakotvena v dokumentech, jako je například Doktrína o ochraně kyberprostoru[26] nebo Zásady pro ochranu kyberprostoru.[27] Dílčí úpravu je také možné nalézt například v regulaci telekomunikací nebo finančního sektoru. V roce 2013 Polsko přijalo Strategii na ochranu kyberprostoru Polské republiky, která implementuje většinu doporučení, ale přesto ucelená právní úprava této problematiky dosud není kompletní.[28]

I přesto, že Polsko již čelilo několika kybernetickým útokům, kybernetická bezpečnost není prozatím součástí všeobecného vzdělávacího systému. Obsáhlejší kurzy, které je možné absolvovat v souvislosti s tímto tématem, jsou pouze součástí výcviku vybraných policejních vyšetřovatelů.

Mnohem podrobnější úprava existuje k otázce kritické infrastruktury. Orgánem, který má tuto oblast v Polsku na starosti, je Vládní centrum pro bezpečnost[29]. Hlavními předpisy upravujícími tuto oblast jsou zákon o krizovém řízení, nařízení o národním programu krizového řízení, nařízení o CIP plánech, nařízení o zprávě o hrozbách národní bezpečnosti a nařízení předsedy vlády ze dne 11. dubna 2011 o organizaci a provozu Vládního centra pro bezpečnost. Tyto předpisy upravují také důležité informační systémy v zemi a jejich fungování. V Polsku také působí dva týmy CERT, jeden od roku 1996 a druhý od roku 2008, který je zodpovědný za bezpečnost a koordinaci při útoku na polské vládní instituce a entity spojené s kritickou infrastrukturou.[30]

Polská úprava kritické infrastruktury se v zákoně o krizovém řízení podrobně věnuje podmínkám sestavení národního programu krizového řízení, důraz na tento program je kladen právě proto, že přímo upravuje podrobnější kritéria kritické infrastruktury. Tento program je pravidelně aktualizován a nesmí mít plánovací cyklus delší než dva roky. Na rozdíl od České republiky nejsou kritéria kritické infrastruktury veřejně přístupná[31], protože jsou přímo součástí národního programu. S ohledem na vývoj infrastruktury je nutné kritéria pravidelně aktualizovat. Tuto činnost vykonává podle nařízení předseda Vládního centra pro bezpečnost, který předkládá seznam kritérií ministrům a ředitelům vládních kanceláří, kteří následně poskytnou předsedovi návrhy na další kritéria kritické infrastruktury, která by mohla být zahrnuta do seznamu.

Zákon o krizovém řízení se také podrobně zabývá konkrétním postupem pří řešení situací ve vojvodstvích, kdy řízením a sestavením jednotlivých skupin ve vojvodství je pověřen vojvoda. Pravomoci a působnost vojvodství v této problematice je v zákoně o krizovém řízení poměrně obsáhle upravena.

3.2.5 *Spojené království Velké Británie a Severního Irska*

V roce 2011 byla vydána **Národní strategie kybernetické bezpečnosti**, v níž jsou stanoveny základní cíle, jichž by mělo být dosaženo do roku 2015.

Jsou jimi:

[24] http://byznys.lidovky.cz/hackeri-zautocili-na-vladni-weby-v-polsku-f1b-/media.aspx?c=A120122_003837_ln-media_ape.
[25] http://www.novinky.cz/zahranicni/evropa/372971-hackeri-napadli-polske-aerolinky-zpozdily-se-i-spoje-do-prahy.html.
[26] http://www.bbn.gov.pl/ftp/dok/01/DCB.pdf.
[27] https://mac.gov.pl/files/wp-content/uploads/2012/09/polityka-CBR-stan-na-18-09-2012-konsultacje-resortowe-.pdf.
[28] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_poland.pdf.
[29] http://rcb.gov.pl/eng/?page_id=74.
[30] http://cybersecurity.bsa.org/assets/PDFs/country_reports/cs_poland.pdf.
[31] http://www.niss.gov.ua/public/File/2013_table/1107_polish.pdf.

- dosažení výborné schopnosti Velké Británie čelit kybernetické kriminalitě a být jedním z nejbezpečnějších míst světa pro podnikání v kybernetickém prostoru;
- zvýšení odolnosti proti kybernetickým útokům a schopnost lepší ochrany svých zájmů v kybernetickém prostoru;
- vytvoření otevřeného a stabilního kybernetického prostoru, jehož užívání bude bezpečné pro širokou veřejnost;
- dosažení vysoké úrovně průřezových znalostí, dovedností a schopností, které jsou nutné k dosažení všech cílů v oblasti kybernetické bezpečnosti.

Zákon komplexně regulující oblast kybernetické bezpečnosti ve Velké Británii neexistuje; tato oblast je regulována podzákonnými právními předpisy, například výkladovými ustanoveními k Zákonu o komunikacích z roku 200332. Oblast kybernetické kriminality je regulována v Zákoně o zneužití počítačů, Zákoně o ochraně dat, Zákoně o podvodech a v Trestním zákoně.[33]

Ve Velké Británii je **národní infrastruktura** definována vládou jako zařízení, systémy, stránky a sítě důležité pro fungování země a dodávek základních služeb, na nichž závisí každodenní život ve Velké Británii.

Národní infrastruktura je rozdělena do devíti sektorů: komunikace, záchranné služby, energetika, finanční služby, potravinářství, vláda, zdraví, doprava a voda. Dále jsou zde uvedeny technologie, kde může být infrastruktura podporující dodávky základních služeb umístěna napříč několika sektory. Infrastruktura je kategorizována podle své hodnoty, či kritičnosti a podle rozsahu škod, které by způsobilo její narušení. Ne všechny součásti národní infrastruktury jsou kritické; kritickými součástmi jsou pouze ty, jejichž narušení či ztráta by měly významný vliv na poskytování základních služeb a vedly by k významným ekonomickým nebo sociálním důsledkům a ztrátám na životech.

Úroveň kritičnosti infrastruktury je specifikována ve Strategickém rámci a politickém prohlášení o zlepšení odolnosti kritické infrastruktury proti narušení přírodními riziky podle:

- vlivu na dodávky základních služeb;
- vlivu ztráty základních služeb na ekonomiku a život v zemi.

Dále musí být vzaty v úvahu:

- stupeň narušení základních služeb;
- rozsah jejich narušení;
- délka období, v němž narušení přetrvává.

Úroveň kritičnosti infrastruktury se rozpadá do pěti kategorií, od infrastruktury nejkritičtější, jejíž narušení by mělo katastrofické dopady na celou Velkou Británii, po infrastrukturu, důsledky jejíhož narušení by byly méně závažné. Jak je uvedeno ve srovnání níže, sektory služeb spadajících do národní infrastruktury ve Velké Británii a do kritické infrastruktury v České republice jsou stejné. Významnější rozdíly jsou až na úrovni sub-sektorů – například v oblasti potravin je v České republice upravena pouze jejich produkce, zatímco britská úprava obsahuje také jejich zpracování, dovoz, distribuci a maloobchodní prodej. V tomto směru považujeme britskou úpravu za vhodnější a pro budoucí českou právní úpravu bychom navrhli zařazení těchto dalších sub-sektorů pod sektor potravinářství.

Obor technologií uvedený ve srovnání jako součást sektorů Velké Británie je v české úpravě definován jako prvek kritické infrastruktury spadající do sektoru telekomunikačních a informačních služeb. Nařízení o kritériích pro určení prvku KI na rozdíl od britské vládní definice popisuje také jednotlivé obory spadající

[32] Ofcom guidance on security requirements in sections 105A to D of the Communications Act 2003.
[33] Computer Misuse Act (1990); Data Protection Act (1998); Fraud Act; Criminal Act (1977).

do sektorů národní infrastruktury, tyto detailní popisy podléhají ve Velké Británii režimu utajení, aby tak nedocházelo k exponování prvků kritické infrastruktury.

4 Kybernetická kriminalita

4.1 Kybernetická kriminalita v ČR

Vzhledem k rychlému vývoji v oblasti informačních technologií se dostala ochrana počítačových dat a systému před kybernetickými útoky do trestněprávních předpisů všech vyspělých zemí.

4.1.1 *Typologie kybernetických útoků*

Kybernetické útoky se diferencují podle různých kritérií. Jedním z nich je rozdělení podle motivace útočníka na **kyberkriminalitu**, která směřuje ke vlastnímu obohacení, **hacktivismus**, který upozorňuje na určitý problém formou apelu, **kybernetickou válku** směřující k poškození infrastruktury jiným státem či nestátním aktérem a **kybernetickou špionáž** sloužící k získání informací v obchodním či mezinárodním styku.[34]

Další rozdělení kybernetických útoků sleduje intenzitu či dopad těchto útoků. Rozlišuje se tak **porušení vnitřního nařízení**, například neopatrným nakládáním s přístupovými hesly, neaktualizování firemního bezpečnostního softwaru. **Porušením právní povinnosti** by například bylo nehlášení kybernetických bezpečnostních incidentů. Kyberkriminalita je dle tohoto kritéria trestná činnost směřující k získání vlastního prospěchu. **Kybernetický terorismus** ohrožuje chod (prvků) kritické informační infrastruktury nebo významných informačních systému kdy útočníkem je nestátní subjekt. Na druhou stranu u **kybernetické války** je útočníkem jiný stát, nástrojem útoku přitom nejsou zbraně. U všech těchto útoků se mohou používat stejné nástroje.[35]

V oblasti boje proti kybernetické kriminalitě je nutná nejenom kvalitní právní regulace kybernetické bezpečnosti, úprava trestního stíhání kybernetické kriminality, ale zejména detailnější vymezení působnosti orgánů činných v trestním řízení, tj. policie, státního zastupitelství a soudů.

Policie České republiky přímo na svých internetových stránkách obsahuje odkaz na hlášení kybernetických útoků. Podporuje i projekty týkající se bezpečnosti internetu, kterých je v současnosti celá řada.[36]

Pro úspěšné vyšetřování potírání kybernetické kriminality je nutné nejenom kvalitní technické zázemí orgánů činných v trestním řízení, ale i adekvátní vzdělávání policistů, státních zástupců a soudců specializujících se na tuto oblast. Dle dostupných informací žádné koncepční vzdělávání orgánů činných v trestním řízení neprobíhá. Nejsou ani formálně a organizačně vytvořené specializované týmy na jednotlivých úrovních trestního řízení.

4.1.2 *Úprava kybernetické kriminality v Trestním zákoníku*

Počítačová, nebo jak se nově zavedlo, kybernetická kriminalita, se v České republice začala postihovat v roce 2002 podle zákona č. 140/1961 Sb., trestního zákona, ve znění pozdějších předpisů. Příslušná právní úprava je nyní obsažena v Trestním zákoníku. Postihování kybernetické kriminality se oproti původní právní úpravě značně rozšířilo, čímž byl splněn závazek České republiky vyplývající z Úmluvy Rady Evropy o počítačové kriminalitě ze dne 23. listopadu 2001.

Dle aktuální právní úpravy lze ke kybernetické kriminalitě přiřadit následující trestné činy:

- § 182 – porušení tajemství dopravovaných zpráv,
- § 183 – porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,

[34] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti. *Revue pro právo a technologie*. 2013, **4**(8). ISSN 1805-2797.
[35] Ibid.
[36] *Bezpečný internet*. Dostupné také z: http://www.policie.cz/clanek/bezpecny-internet-270537.aspx.

- § 191 – šíření pornografie,
- § 192 – výroba a jiné nakládání s dětskou pornografií,
- § 230 – neoprávněný přístup k počítačovému systému a nosiči informací,
- § 231 – opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat,
- § 232 – poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti.

V kybernetickém prostoru lze spáchat i trestný čin *Spáchání teroristického útoku (§ 311 Trestního zákoníku)*. Je nutné upozornit na skutečnosti, že z výše uvedených trestných činů pouze u trestného činu *Teroristického útoku (§311 Trestního zákoníku)* lze spáchat trestný čin *Neoznámení trestného činu (§ 368 Trestního zákoníku)* a trestný čin *Nepřekažení trestného činu (§ 367 Trestního zákoníku)*. U trestného činu Teroristického útoku tedy existuje jak povinnost tento čin oznámit, tak i překazit jej.

Právnická osoba se může dopustit následujících trestných činů: Porušení tajemství dopravovaných správ (§ 182 Trestního zákoníku), Výroba a jiné nakládání s dětskou pornografií (§ 192 Trestního zákoníku), Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 Trestního zákoníku), Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 Trestního zákoníku), Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 Trestního zákoníku), Teroristický útok (§ 311 Trestního zákoníku).

Níže je uveden přehled skutkových podstat kybernetických trestných činů v užším smyslu.

§ 230 Neoprávněný přístup k počítačovému systému a nosiči informací

Ustanovení § 230 Trestního zákoníku obsahuje v odstavci 1 a 2 dvě samostatné skutkové podstaty přičemž zahrnuje pět různých jednání podle Úmluvy o počítačové kriminalitě.

První odstavec tohoto ustanovení sankcionuje již samotné prolomení bezpečnostních opatření, jejichž účelem je chránit důvěrnost počítačových dat a počítačového systémů (jejich částí), například hesla nebo firewallu. Patří sem například tzv. *hacking, spoofing.*

Tento trestný čin je úmyslný, tj. nelze jej spáchat z nedbalosti.

Druhý odstavec tohoto ustanovení sankcionuje neoprávněnou manipulaci s počítačovými daty, poté co pachatel získal přístup k počítačovému systému nebo nosiči informací. Tento přístup mohl získat jak neoprávněně tak i oprávněně, například zaměstnancem, který má jako administrátor IT přístup k počítačovému systému.

Trestným následkem pak je neoprávněné užití dat - *počítačová špionáž*, vymazání, jiné zničení, poškození, změna dat, atd. - *počítačová sabotáž.* Jde tedy o jednání, kdy se data buď odstraňují, nebo se snižuje jejich upotřebitelnost. Může se tak stát například prostřednictvím celé řady škodlivého softwaru (malware), tj. viry, červy a tzv. trojské koně. Za velmi nebezpečné útoky patřící do této skupiny jsou považovány útoky typu *DoS (denial-of-service)* nebo *DDos (distributed-denial-of-service)*.

Dalším z trestných následků je padělání nebo pozměnění dat, jde o obdobu padělání listin (např. změna výsledků testů přijímacího řízení v databázi informačního systému).

Trestné je i neoprávněné vložení dat, nebo učinění jiného zásahu do programového nebo technického vybavení počítače, které může například způsobit trvalé ochromení činnosti počítače, nefunkčnost některých programů, třeba i v důsledku počítačových virů.

I u druhé skutkové podstaty se jedná o úmyslný trestný čin, tj. nelze jej spáchat z nedbalosti.

Jednou ze zvlášť přitěžujících okolností pro použití vyšší trestní sazby za spáchání trestného činu podle ustanovení § 230, jak je uvedeno v odstavci 4, je způsobení vážné poruchy v činnosti orgánu státní správy, územní samosprávy, soudu, nebo jiného orgánu veřejné moci. Dalo by se říct, že toto ustanovení koresponduje vyšší míře ochrany, která je poskytovaná např. významným informačním systémům které

spravují orgány moci výkonné podle Zákona o kybernetické bezpečnosti. Vedle toho se vyšší trestní sazba použije i v případě způsobení vážné poruchy v činnosti právnické nebo fyzické osoby, která je podnikatelem. Zde lze naopak spatřovat zvýšenou ochranu povinných soukromoprávních subjektů dle Zákona o kybernetické bezpečnosti, a to např. subjektu zajišťujícího síť elektronických komunikací nebo správců kritické informační infrastruktury.[37]

Neoznámení ani nepřekažení trestného činu podle ustanovení § 230 Trestního zákoníku není trestné.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

Toto ustanovení kriminalizuje další z jednání uvedených v Úmluvě o počítačové kriminalitě.

Pro spáchání tohoto trestného činu je nutné naplnit současně dva znaky, a to úmysl spáchat trestný čin podle ustanovení § 182 odst. 1 písm. b), c) Trestního zákoníku nebo podle ustanovení § 230 odst. 1, 2 Trestního zákoníku a opatřit nebo přechovávat přístupové zařízení nebo heslo. Typicky se bude jednat o počítačový program, například *prolamovače hesel,* programy zjišťující otevřené porty počítače, tzv. *skenery*, programy odposlouchávající síťový provoz, tzv. *sniffer* (tímto způsobem je např. možné zachycení přenášených hesel). Dále programy typu *exploit*, které po zjištění slabiny systému tuto slabinu využívají.

I tento čin je činem úmyslným, tj. nelze jej spáchat z nedbalosti.

Vyšší trestní sazbu lze použít v případě přitěžujících okolností, kdy pachatel spáchal tento čin jako člen organizované skupiny, nebo získal-li pro sebe nebo pro jiného značný prospěch, tj. nejméně 500 000 Kč.

Ještě vyšší trestní sazbu lze použít v případě zvlášť přitěžující okolnosti, kdy pachatel pro sebe nebo jiného získal prospěch velkého rozsahu, tj. nejméně 5 000 000 Kč.

Neoznámení ani nepřekažení trestného činu podle § 231 Trestního zákoníku není trestné.[38]

§ 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti

Toto ustanovení jde nad rámec smluvních závazků ČR nebo práva EU, kdy sankcionuje i nedbalostní jednání zasahující do dat či do technického nebo programového vybavení počítače. Podmínkou pro spáchání tohoto trestného činu kumulativně jsou způsobení značné škody, tj. nejméně ve výši 500 000 Kč a kvalifikovaná nedbalost, tj. hrubá nedbalost[39]

Podmínkou je, aby jednání pachatel v hrubé nedbalosti bylo učiněno v souvislosti s porušením povinností vyplývajících ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté.

Toto ustanovení je obdobou trestného činu Porušení povinností při správě cizího majetku z nedbalosti (§ 221 Trestního zákoníku). Pachateli mohou být například zaměstnanci, vedoucí pracovníci, statutární

---

[37] Komentář k § 230 Z. ŠÁMALa kol. *Trestní zákoník. Komentář.*. 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.
[38] Komentář k § 231 Z. ŠÁMAL a kol. *Trestní zákoník. Komentář.* 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.
[39] § 16 odst. 2 Trestního zákoníku: Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.

orgány, IT ředitelé nebo osoby v obdobných pozicích u povinných subjektů podle Zákona o kybernetické bezpečnosti, pokud nesplní zákonem stanovené povinnosti, např., že nezavedou potřebná bezpečnostní opatření. Pokud by v takovém případě došlo ke kybernetickému útoku, kterému by jinak mohlo být zabráněno přijetím zákonem požadovaných bezpečnostních opatření, a vznikla by škoda buď samotnému povinnému subjektu, nebo třetím osobám, osoby odpovědné za zavedení bezpečnostních opatření by mohly být trestně stíhány. V popsaném případě by porušení povinností vyplývajících ze Zákona o kybernetické bezpečnosti zcela jistě znamenaly hrubou nedbalost ve vztahu k jednání, resp. nejednání pachatele.

Přitěžující okolností pro použití vyšší trestní sazby je způsobení škody velkého rozsahu, tj. nejméně 5 000 000 Kč.[40]

§ 182 Porušení tajemství dopravovaných zpráv

Toto ustanovení obsahuje dvě samostatné skutkové podstaty a mimo jiné sankcionuje i některá jednání související s kybernetickou kriminalitou, jež budou popsána níže.

Odstavec 1 slouží k ochraně proti úmyslnému porušení tajemství posílané zprávy například prostřednictvím sítě elektronických komunikací nebo neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, přiřaditelné k identifikovanému účastníku nebo uživateli. Jedná se především o ochranu zprávy datové, textové, hlasové (e-mail, písemná i hlasová konverzace pomocí Skype, ICQ, chat), zvukové (zvukový záznam, živý přenos, přenos pomocí telefonu - pevnou linkou, mobilním telefonem, přenos pomocí internetu atd.), obrazové (zachycené kamerou, fotoaparátem, webovou kamerou, kamerou telefonu atd.). Porušení tajemství nastane již samotným zásahem narušitele, například svévolným otevřením zprávy, odposlechem či vyslechnutím telefonického rozhovoru, aniž by se s obsahem zprávy seznámila třetí osoba. Porušení tajemství zahrnuje i vyzrazení obsahu zprávy, nezáleží ani na hodnotě obsahu zprávy pro adresáta.

V odstavci 2 se poskytuje ochrana proti prozrazení nebo využití tajemství, o němž se pachatel dozvěděl např. z přenosu prostřednictvím sítě elektronických komunikací, který nebyl určen jemu. Skutek musí být ale spáchán s úmyslem způsobit jinému škodu nebo opatřit sobě nebo jinému neoprávněný prospěch. Postihován zde bude pachatel, který se s tajemstvím zprávy obeznámil nikoliv neoprávněně, nebo také neúmyslně (například jako zaměstnanec fotoslužby zpracovávající zakázku na vyvolání filmu, zaměstnanec provozovatele počítačového systému), avšak tohoto tajemství dál prozradil nebo vyžil s cílem opatřit sobě nebo jinému neoprávněný prospěch.

Skutek lze spáchat jen úmyslně.

Zvláštní skutková podstata uvedená v odstavci 5 je vázána na pachatele, který musí být zaměstnancem provozovatele poštovních služeb, telekomunikačních služeb nebo počítačového systému anebo jinou osobu vykonávající komunikační činnosti. Tato jiná osoba může být jak fyzická tak i právnická, která jako podnikatel vykonává činnost v rámci elektronických komunikací, přičemž jde o jakoukoli činnost při komunikaci mezi lidmi, při které přichází do styku s listovním tajemstvím nebo jiným tajemstvím dopravovaných zpráv zajištěným na základě zabezpečení důvěrnosti komunikací v rámci služby elektronických komunikací nebo počítačového systému. Požaduje se, aby pachatel spáchal některý z výše uvedených činů, nebo je umožnil jeho spáchání, například umožnil někomu odposlech

[40] Komentář k § 232 Z. ŠÁMAL a kol. *Trestní zákoník. Komentář.* 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.

telefonických hovorů, neoprávněné osobě zjednal přístup k neveřejnému přenosu počítačových dat do počítačového systému či z něj. Dále postihuje pozměnění nebo potlačení dopravované nebo přenášené písemnosti nebo zprávy takovým zaměstnancem nebo jinou osobou. Může se jednat například o zásah do procesu doručování zpráv, do neveřejného přenosu počítačových dat, do telefonického hovoru).

K tomuto trestnému činu spáchanému v oblasti počítačové kriminality doposud není relevantní judikatura.[41]

§ 183 Porušení tajemství listin a jiných dokumentů uchovávaných v soukromí

Trestněprávní ochrana proti porušení tajemství listin se vztahuje i na počítačová data uchovávaná v soukromí. Pachatel se dopustí trestného činu tím, že je zveřejní, úmyslně a neoprávněně zpřístupní třetí osobě nebo jiným způsobem použije. Pod sankci je zde použití dokumentu v neprospěch poškozeného, k poškození jeho podnikání, k majetkovému poškození, k poškození v zaměstnání nebo ke svému obohacení nebo získání jiné výhody.

Pachatelem tohoto trestného činu může být pouze osoba fyzická, poškozeným nicméně i právnická osoba.

4.1.3 *Judikatura v oblasti kybernetické kriminality*

Rozhodovací činnost českých soudů v souvislosti s počítačovou kriminalitou nebyla v minulosti vždy jednotná. Soudy, zejména na nižších úrovních, často rozhodovaly téměř identické případy rozdílně. Tyto rozpory jsou způsobeny zejména tím, že se jedná o poměrně nový a dynamicky se vyvíjející právní obor, se kterým soudy, potažmo státní zástupci, nemají tolik zkušeností. Dalším důvodem je nedostatečná úprava této oblasti v zákoně č. 140/1961 Sb., trestního zákon, ve znění pozdějších předpisů a poměrně krátká účinnost Trestního zákoníku (od 1. ledna 2010), ve kterém jsou již nové trestné činy související s kybernetickou kriminalitou obsaženy. S tím souvisí i nízký počet soudních sporů, které v České republice musely soudy řešit. Důvodem není ale pouze krátká účinnost Trestního zákoníku. Poškozenými v těchto případech bývají totiž často banky či jiné finanční instituce, případně další veřejně exponované subjekty, které si zakládají na svém dobrém jménu a pověsti. Vyšetřování a s tím související medializace těchto případů většinou nejsou v zájmu těchto osob, takže se tyto situace snaží řešit interní cestou. Jak již bylo zmíněno výše, dalším problémem pro odhalování a trestání kybernetické kriminality je nízký počet odborníků (jak zkušených vyšetřovatelů, tak i státních zástupců a soudců), kteří se oblastí kybernetické bezpečnosti primárně zabývají. Přesto již nyní máme několik rozhodnutí Nejvyššího soudu, které je třeba uvést.

Nejvyšší soud ČR se v rozhodnutí 6 Tdo 1677/2011 zabýval v dovolání obviněného mimo další skutkové podstaty zejména trestným činem neoprávněného opatření, padělání nebo pozměnění platebního prostředku podle § 234 odst. 3 Trestního zákoníku. Obviněný v tomto případě neoprávněně získal přístup k přihlašovacím údajům jiných osob do tzv. internet bankingu. Tam se následně za pomoci těchto údajů přihlásil a zadal zde příkazy k úhradě, jejichž účelem bylo neoprávněně se obohatit. V dovolání se hájil tím, že pokud použil správné přihlašovací údaje a zadal příkazy k úhradě, nemohl se dopustit padělání platebního prostředku, jelikož ten byl vydán technicky správným způsobem. Podle jeho názoru se tedy nemohlo jednat o padělání. Nejvyšší soud s takovou obhajobou nesouhlasil a rozhodl, že *pokud je platební prostředek (v tomto případě příkaz k úhradě) vydán jinou než oprávněnou osobou (tj. majitele účtu) bez jejího vědomí, jde o prakticky totožný případ, jako kdyby padělal příkaz k úhradě na papírovém předtisku. Rozdíl je pouze v tom, že v tomto případě nenahradil podpis oprávněné osoby, ale využil jeho*

[41] Komentář k § 182 Z. ŠÁMAL a kol. *Trestní zákoník. Komentář.* 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.

internetové bankovnictví, do kterého se vlastník účtu musí přihlásit jedinečnými a tajnými přístupovými údaji, a toto jednání je fakticky rovno úspěšnému zfalšování jeho podpisu. O padělání se tedy v tomto případě jedná.

Trestné činy týkající se dětské pornografie mají podle Nejvyššího soudu také přesah do kybernetické kriminality, konkrétně se jedná o § 191 odst. 3 písm. b) a o § 192 odst. 3 písm. b) Trestního zákoníku. V těchto trestných činech se jedná o šíření pornografie a dětské pornografie, výše zmíněná ustanovení se konkrétně týkají šíření *tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobě účinným způsobem*. Soudy se ve své rozhodovací činnosti nemohly shodnout, zda lze šíření prostřednictvím elektronické pošty mezi tzv. e-mailovými schránkami subsumovat pod tato ustanovení, tedy zda lze o veřejně přístupnou síť nebo jiný obdobě účinný způsob. Nejvyšší soud byl tedy požádán nejvyšším státním zástupcem o vyjasnění této otázky pro budoucí rozhodovací činnost soudů nižších instancí. Podle Nejvyššího soudu *rozesílání pornografických děl takovýmto způsobem, tedy e-mailovými schránkami nenaplňuje znak „veřejně přístupná počítačová síť"*. Nicméně soud dále stanovil, že *pokud by se jednalo o rozesílání většímu počtu účastníků (zpravidla alespoň několik desítek), toto jednání naplňuje znak „jiným obdobně účinným způsobem"*.

Několik případů rozhodovací činnosti Nejvyššího soudu ČR se týkalo také porušení práva autorského v souvislosti s kybernetickou kriminalitou, zejména tzv. *embeddingu*. Podstatou této metody je umožnit jinému, aby měl přístup k určitému obsahu neoprávněně umístěnému na jiném místě v kybernetickém prostoru. Jednalo se o známé případy uživatelsky hojně navštěvovaných serverů (kinotip.cz, ulozto.cz a další), které touto metodou odkazovaly na nelegálně zveřejňovaná díla chráněná autorskými právy. Jejich obranu u soudu spočívala v tom, že díla chráněná autorským práva nebyla umisťována na jejich serverech, ale pouze na ně za použití metody embeddingu odkazovala. Nejvyšší soud ČR k tomuto jednání rozhodl, že *takovéto jednání je v rozporu s § 270 trestního zákoníku*, *je totiž v tomto konkrétním případě (embedding) bez významu, kdo umístil na internet (zveřejnil) daný obsah, ale podstatná je pouze okolnost, že pachatel zpřístupnil obsah chráněný autorským právem dalším osobám. Soud připustil, že pokud pachatel umístí na své internetové stránky pouze prostý odkaz na takovéto dílo (tedy pouze informaci, kde se takové dílo nachází, bez možnosti přímého přístupu – embeddingu), tak v takovémto případě se o porušení zákona nejedná.*

4.2 Regulace na úrovni Rady Evropy

4.2.1 *Úmluva o počítačové kriminalitě (2001)*

Úmluva o počítačové kriminalitě představuje mezi akty mezinárodního práva, které jsou v oblasti kybernetické kriminality implementovány, **nejzásadnější dokument**. Byla sjednána na půdě Rady Evropy v roce 2001, následně byla v Budapešti otevřena k podpisu. Česká republika tuto úmluvu podepsala v roce 2005 a ratifikovala v červenci 2013. Úmluva o počítačové kriminalitě je ve svém přístupu nejkomplexnější. Upravuje některé aspekty mezinárodní spolupráce a reguluje závazky hmotněprávní i procesně právní. Míra implementace závazků do českého Trestního zákona je patrná.

4.2.2 *Úmluva Rady Evropy o prevenci terorismu (2005)*

Úmluva Rady Evropy o prevenci terorismu je poměrně nový instrument, který má zvýšit úsilí smluvních stran při předcházení terorismu a to jak na národní úrovni, tak i pomocí mezinárodní spolupráce. Není to ale čistě preventivní dokument, v článcích 5 až 7 vymezuje nové skutkové podstaty, které se smluvní strany zavazují prohlásit za trestné. Tuto Úmluvu podepsali všichni členové Evropské unie, kromě České republiky. Proto nejsou její ustanovení a z nich plynoucí povinnosti v českém právním řádu implementovány. Znění českého trestního zákona však není se zněním této Úmluvy v rozporu. Z níže uvedené tabulky je patrné, která ustanovení Úmluvy lze pokrýt úpravou obsaženou v trestním zákoně.

4.3 Právní ochrana před kybernetickými útoky podle mezinárodního veřejného práva

V posledním období vzrostl v celosvětovém měřítku počet kybernetických útoků natolik, že podnítil diskuse o kybernetické válce. Pečlivému čtenáři ponecháváme k úvaze, nakolik taková „válka" naplňuje znaky definice ozbrojeného konfliktu, kterou poskytl mezinárodní trestní tribunál pro bývalou Jugoslávii v případu Duško Tadiče.42 Útoky se přitom dotýkají i některých subjektů v České republice, jako např. rozsáhlé útoky typu DDoS z počátku roku 2013, které vyřadily z provozu platební terminály českých bank.

4.3.1 *Kybernetický útok*

Tento klíčový pojem nemá definici právní, ani univerzálně přijímanou definici obecnou. Americké Ministerstvo obrany (*Department of Defense*) popisuje kybernetický útok prostřednictvím jeho cílů jako operaci užívající počítačové sítě za účelem přerušení, zhoršení kvality, potlačení nebo zničení informací v počítačích nebo počítačových sítích.[43] Označení obdobných incidentů za útoky se jeví jako do značné míry nepřesné, neboť mezinárodní právo veřejné spojuje pojem útok s ozbrojeným konfliktem.[44] Podle některých autorů je tento problém ale pouze virtuální a pojem kybernetický útok se ujal jako generální pojem veškerých kybernetických hrozeb namířených proti informačním systémům. Vlastní cíl útoku může být mimo informační systém, avšak zasažením systému dojde minimálně k ovlivnění cíle. Kybernetické útoky využívají provázanost systému, které tvoří síť telekomunikací, kde jednotlivé počítače vzájemně spolupracují, směňují data a umožňují spojení mezi jejich uživateli. Taková síť zařízení a telekomunikací, včetně probíhající interakce, komunikace a její obsahové složky, bývá označována jako **kybernetický prostor**.[45]

Mezi kybernetické útoky patří útok typu *Distributed Denail of Service* (DDoS), který má zpravidla vyřadit napadený informační systém z provozu nebo minimálně snížit jeho schopnosti. Útok spočívá v záměrném přetížení napadeného informačního systému tím, že se pachatel napojí na velké množství různých počítačů, které se slangově označují jako *„botnet"* nebo *„zombie",* a těm poté bez vědomí uživatele přikáže, aby zahltily požadavky cílový server. Systém napadený DDoS útokem se projevuje zejména neobvyklým zpomalením služby, nedostupnosti částí nebo celých webových stránek, extrémním nárůstem spamů apod.[46]

Většina kybernetických útoků přesahuje hranice států. DDoS útoky jsou zpravidla trestným činem podle českého práva, nicméně jejich pachatele se povětšinou nacházejí v zahraničí. K odhalení pachatele/ů bude zapotřebí součinnosti cizích států.[47]

4.3.2 *Kybernetický útok jako mezinárodní protiprávní chování – použití síly*

První a nejzásadnější otázka, kterou je nutné výkladem zodpovědět, zní: Kdy je kybernetický útok použitím síly podle čl. 2, odst. 4 Charty OSN? S trochou nadsázky můžeme odpovědět, že téměř nikdy.

---

[42] ICTY, Prosecutor v. Duško Tadić, Case No. IT-94-1-AR72, Appeals Chamber, Decision on the Defence Motion for Interlocutory Appeal on Jurisdiction, 2 October 1995, par. 70.
[43] The Joint Ciefs of Staff, joint pub. No. 3-13, Joint Doctrine for Information 1-9 (Oct. 9, 1998). Dostupné z: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, [2015-10-27].
[44] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie,* 2013, roč. 4, č. 8, s. 76. ISSN 1804-5383.
[45] SCHAAP, Maroj Arie J. Cyber Warfare operations: Development and use under International Law. Air Force Law Review. 2009, roč. 69. Str. 125 – 126.
[46] VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. Trestní právo. 2011, roč. 15, č. 1, 2011. Str. 12 – 13.
[47] SHACKELFORD, Scott J. From Nuclear War to Net War: Analogizing Cyber Attacks in Intemational Law . Berkeley Journal of International Law. 2009, roč. 27, č. 1. Str. 193 – 251.

Doposud nejvýznamnější výstup doktríny v této oblasti, Talinský manuál o aplikovatelnosti mezinárodní práva na kybernetické válčení, ve svém pravidlu 10 s jasným odkazem na čl. 2, odst. 4 Charty OSN stanoví: *„A cyber operation that constitutes a threat or use of force against the territorial integrity or political independence of any State, or that is in any other manner inconsistent with the purposes of the United Nations, is unlawful."*[48] Potíže zde může činit samotné určení, kdy použití síly směřuje proti územní celistvosti a politické nezávislosti státu nebo je uskutečněné způsobem odporujícím cílům OSN. Hned v pravidle následujícím Talinský manuál definuje, kdy je kybernetický útok použitím síly: *„A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."*[49]

Pro posouzení, zdali je určité jednání v kyberprostoru použitím síly, je tedy nutné posoudit rozsah takového jednání a jeho důsledky („scale and effects"). Tudíž jednání, které má zničit nebo poškodit objekt nebo zabít člověka, je podle Talinského manuálu bezesporu použití síly. Podle tohoto právního výkladu by ovšem útok prostřednictvím viru Stuxnet znamenal použití síly, a tudíž založil právo Íránu na sebeobranu, neboť hmatatelně došlo ke škodám. Útoky na Estonsko v roce 2007 zůstávají v tomto světle na sporné hranici, kde na jedné straně zůstává argument, že nikdo nebyl zraněn a hmotné škody lze obtížně vyčíslit. Na straně druhé leží srovnání DDoS útoku s vojenskou blokádou přístavu.

Nicméně mezinárodní společenství výklad, že v Estonsku a v Íránu došlo k použití síly, nepřijalo. Ani napadené státy neuplatnily právo na sebeobranu. A maiori ad minus (argument logického vykladu práva - "od menšího k většímu") tak jako použití síly nekvalifikujeme ani DDoS útoky proti České republice. Nad rámec uvedeného lze poznamenat, že Talinský manuál je obecně velmi restriktivní, co se týče aplikace **ius ad bellum** (právo na válku) na kybernetický prostor, zatímco ohledně **ius in bello** (právo ve válce) dochází k řadě hmatatelných závěrů. Tady i doktrína souhlasí, že ius in bello lze lépe aplikovat na kybernetické útoky. Rozdíly mezi konvenčním a kybernetickým válečnictvím spočívají v intenzitě, nikoliv v druhovém určení. Takže režim mezinárodního humanitárního práva, který upravuje válečnictví konvenční, může být efektivně aplikován i na kybernetické útoky.[50]

Řada autorů[51] při klasifikaci kybernetického útoku jako použití síly používá tzv. Schmittova kritéria[52], podle nichž lze některé útoky klasifikovat jako použití síly, jiné tohoto prahu nedosahují a jsou potom pouhým ekonomickým a politickým donucením. Schmitt jako tato kritéria určil **závažnost** (severity), **bezprostřednost** (immediacy), **přímost** (directness), **míru narušení či agresivitu** (invasiveness) a **měřitelnost následků** (measurability).

Samotná kritéria ale v tomto případě mohou být předmětem výkladu a rozdílného vnímání. Jaký útok tedy je a jaký není použitím síly, zůstává spornou otázkou. Jensen[53] podotýká, že rozvoj mezinárodního práva musí ještě pokročit, aby byl kybernetický útok rozeznáván jako použití síly a ozbrojený útok, který zakládá

[48] Předklad autorův: „Kybernetická operace, která zakládá hrozbu silou nebo použití síly proti územní celistvosti nebo politické nezávislosti státu, nebo která je jiným způsobem neslučitelná s cíli Spojených národů, je protiprávní."
[49] Předklad autorův: „Kybernetická operace zakládá použití síly, když jsou její rozsah a účinky srovnatelné s nekybernetickou operací dosahující úrovně použití síly."
[50] GERVAIS, M. Cyber Attacks and the Laws of War. Berkeley Journal of International Law. 2012, roč. 30, č. 2. Str. 579.
[51] GŘIVNA, Tomáš. POLČÁK, Radim (eds.). Kyberkriminalita a právo. Praha: Auditorium, 2008. ISBN 978- 80-903786-7-4. Str. 57 – 61. REMUS, Titiriga. Cyber-attacks and International law of armed conflicts; a "jus ad bellum" perspective. Journal of International Commercial Law and Technology. 2013, roč. 8, č. 3. Str. 179 – 189.
[52] SCHMITT, Michael. N. Computer Network Attack: The Normative Software. IN Yearbook of International Humanitarian Law. Roč. 4. Haag: TMC Asser Press, 2001. Str. 53 – 85.
[53] JENSEN, Eric Talbot. Computer Attacks on National Infrastructure: A Use of Force Invoking the Right of Self-Defense. Stanford Journal of International Law. 2002, roč. 28. Str. 207 – 240.

právo na sebeobranu. Obecně volá po tom, aby státy získaly právo na sebeobranu proti kybernetickému útoku nehledě na to, jestli je takovýto útok použitím síly nebo nikoli: „Whether initiated by an enemy's military, a terrorist organization, or an individual, CNAs [Computer Network Attacks] will be a serious and destabilizing force unless states are given the right to protect themselves with a proportionate response in self-defense, including anticipatory self-defense, even if the attack does not constitute an armed attack."[54]

Zkušeností také hovoří, že výklad Charty, včetně výkladu čl. 2, odst. 4, vždy podléhal mocenským vlivům, což se obzvlášť intenzivně projevovalo za studené války. Podle něj **kybernetický prostor** zůstane velmi nejistým právním terénem a výklad právních norem, které na něj lze aplikovat, se tak jako za studené války může podrobit potřebám velmocí. K obdobné úvaze vede I názor, že by kybernetické útoky mohly být za takovouto hrozbu označeny Radou bezpečnosti OSN podle čl. 39 Charty OSN. Rada bezpečnosti prakticky může označit za hrozbu cokoli, a tudíž záleží na jejích (stálých) členech – opět více či méně hegemonických státech.

Právo na obranu proti ozbrojenému útoku podle Charty OSN se tedy pravděpodobně nepoužije. Jak by se tedy touto formou napadený stát měl bránit? Talinský manuál opět používá případ Nikaragua[55] a pracuje s obyčejovou zásadou neintervenovat ve věcech cizího státu. Pokud tedy není kybernetický útok použitím síly, měl by být označen jako protiprávní intervence ve věcech cizího státu, případně také jako narušení suverenity. Zásada neintervenovat ve věcech cizího státu vyvstává jako nutný důsledek **rovnosti a nezávislosti suverénních států** a musí být považována za jeden ze základních principů mezinárodního práva.[56]

Lze konstatovat, že DDoS útok by sice z pohledu mezinárodního práva měl být kvalifikován spíše jako porušení suverenity a práva neintervenovat ve věcech cizího státu, nežli jako použití síly. Pokaždé je však nezbytné detailně posoudit konkrétní rozsah a následky útoku.

Zásadně problematickou otázkou zůstává, že jednotlivé části kybermnetického prostoru nelze teritorializovat – přiřadit konkrétním státům podle hardwaru, který se nachází v jejich působnosti. Přímou odpovědnost za kybernetický útok cizím státem, podle zásad mezinárodního práva, podmiňuje **přičitatelnost** tohoto útoku státu na základě testu efektivní kontroly. Prokazování efektivní kontroly státu nad kybernetickým útokem bude zpravidla velmi technicky komplikované. Judikatura i doktrína popisují povinnost státu varovat ostatní státy nedopustit zneužití vlastního území pro obdobné útoky, avšak je spíše otázkou skutkovou, zdali tento postup představuje efektivní řešení, kdy DDoS útok prochází územím několika států a nelze jeho původce odhalit. Takové situace evokuji k otázce, zda by nebylo lepším řešením vytvoření výlučných pravidel pro kybernetický prostor, např. práva na okamžitý kybernetický protiúder.

Otázka legality protiúderu je tedy stejně komplikovaná, jako otázka ilegality samotného prvotního kybernetického útoku. Při nedostatku použitelné právní úpravy tak vstupuje do hry otázka ospravedlnění, tedy legitimity takovýchto protiútoků. A s ní přichází obecně značná právní nejistota. Vzhledem k architektuře kybernetického prostoru není problém vytvořit falešný prvotní útok a následně drtivě zasáhnout nevinný stát – domnělého pachatele – protiúderem.

---

[54] Překlad autorův: Ať už zosnované nepřátelskou armádou, teroristickou skupinou nebo jednotlivcem, útoky na počítačovou síť budou závažnou a destabilizující silou, pokud státy nezískají právo bránit se proti nim přiměřenou sebeobrannou reakcí, včetně předstižné obrany, i když útok neobnáší ozbrojený útok.

[55] Pozn. autora: čl. 1 Ženevských úmluv ukládá smluvním stranám – skoro všem státům světa – povinnost nejen zachovávat, ale i zajišťovat zachovávání těchto úmluv za všech okolností. V roce 1986 ve svém rozsudku v případě *Nikaragua proti Spojeným státům* konstatoval Mezinárodní soudní dvůr (MSD), že závazek plynoucí z čl. 1 Ženevských úmluv má platnost mezinárodního obyčeje.

[56] JOYER, Christopher C. International Law in the 21st Century: Rules for Global Governance. London: Rowman and Littlefield, 2005. ISBN 0742500098. Str. 54

Otázkou zůstává, zdali tento právní stav přetrvá nebo státy své vzájemné vztahy v kyberprostoru více zregulují tak, aby zamezily jeho zneužívání. Vyvstane mezi státy a uživateli kyberprostoru nová společenská smlouva a přestane kybernetická anarchie. Neomezí ale tato regulace příliš svobodu jednotlivce v zájmu posílení státu? A co je podmínkou toho, aby státy takovouto regulaci přijaly?

Odborná veřejnost diskutuje o tom, zdali si společnost všechna nebezpečí této kybernetické anarchie neuvědomí příliš pozdě. Tedy až poté, co přijde kybernetický útok zatím nepoznaného rozsahu, s nedozírnými následky.

5 Mezinárodní spolupráce v boji s kybernetickým terorismem

5.1 Česká republika a mezinárodní spolupráce

Česká republika je členem **NATO**, **EU**, **OSN** a **Organizace pro bezpečnost a spolupráci v Evropě**, účastní se společných bezpečnostních aktivit i kybernetických cvičení. Stávající česká právní úprava je v mezinárodním měřítku považována za jednu z nejkomplexnějších a nejvyspělejších. Rovněž co se týče kybernetických cvičení, Česká republika obsazuje přední příčky úspěšnosti v obraně proti hrozbám a podílí se též na organizaci kybernetických cvičení.

5.2 Aktivity na úrovni Organizace Spojených Národů a NATO

5.2.1 *OSN*

Prvním spojeneckým svazkem pro kybernetickou bezpečnost zaštítěným OSN je Mezinárodní mnohostranné partnerství proti kybernetickým hrozbám[57] (IMPACT). IMPACT je od roku 2011 klíčovým partnerem Mezinárodní telekomunikační unie OSN (ITU) .[58]

IMPACT slouží jako politicky neutrální platforma proti kybernetickým hrozbám, kde se střetávají vlády členských států, soukromé subjekty a odborná veřejnost. Se 152 členskými zeměmi ITU-IMPACT, a také díky podpoře ze strany nejvýznamnějších ekonomických subjektů, akademické sféry i mezinárodních organizací, se partnerství IMPACT stalo největší světovou aliancí svého druhu.

Skupina vládních expertů OSN se shodla na zprávě o konsensu, která je důležitá pro udržení míru a stability mezi státy v této oblasti. Byla jím stanovena doporučení pro tvorbu norem, pravidel a principů odpovědného chování států v kybernetickém prostoru. Vládní experti pěti stálých členů Rady Bezpečnosti OSN a deseti kybernetických velmocí se shodli, že mezinárodní právo a principy práva státní odpovědnosti se použijí i pro aktivity států v kybernetickém prostoru.

Zpráva obsahuje tyto cíle:

- Výměna informací o národních politikách, best practices, rozhodovacích procesech a národních organizacích v oblasti kybernetické bezpečnosti. V roce 2012 si USA a v roce 2013 Německo vyměnily s Ruskem takzvané Bílé knihy o kybernetické obraně.59
- Vytváření dvoustranných nebo vícestranných konzultačních rámců pro zavedení opatření pro budování důvěry, například v rámci Ligy arabských států, Sdružení národů jihovýchodní Asie (ASEAN), Organizace pro bezpečnost a spolupráci v Evropě (OSCE), atd. Tyto rámce mohou obsahovat workshopy a cvičení prevence a zvládání kybernetických incidentů.
- Zvyšování úrovně sdílení informací a krizové komunikace mezi státy o kybernetických bezpečnostních incidentech na třech stupních: výměna technických informací o mallwaru a dalších škodlivých indikátorech bilaterálně mezi národními CERTy a uvnitř již existujících multilaterálních komunit CERT; výměna informací prostřednictvím již existujících nebo nově vytvořených kanálů krizového managementu a přijímání, evidence, analýza a sdílení včasných varování a dalších informací za účelem snížení zranitelnosti a rizika a dále prostřednictvím dialogů na politické úrovni a úrovni policie.
- Zvyšování spolupráce ke zjištění incidentů, které by mohly narušit systémy kritické infrastruktury, zejména ty, které jsou závislé na kontrolních mechanismech fungujících prostřednictvím ICT.

[57] International Multilateral Partnership Against Cyber Threats.
[58] International Telecommunication Union – agentura OSN specializující se na ICT.
[59] Jde o souhrnný koncepční rámec, který definuje a zdůvodňuje roli a funkce ozbrojených sil; jako součást státní bezpečnosti obsahuje plány zabezpečení proti kybernetickým útokům.

- Zvyšování mechanismů pro spolupráci v prosazování práva ke snížení počtu incidentů, které by mohly být kvalifikovány jako státní nepřátelské aktivity a které by mohly narušit mezinárodní bezpečnost.

V důsledku uvedeného mají členské státy a regionální organizace sadu doporučení pro spolupráci, prevenci konfliktů a budování důvěry. Koncem tohoto roku by se OSCE měla dohodnout na první sadě opatření pro budování důvěry.

5.2.2 *NATO*

Pro zvýšení kybernetické bezpečnosti a posílení obrany proti kybernetickým útokům byla na půdě NATO přijata nová posílená politika. Na summitu v září 2014, který se konal ve Walesu, byl spojenci schválen nový akční plán. Nová politika stanovuje, že obrana proti kybernetickým útokům je součástí klíčového úkolu kolektivní obrany NATO, potvrzuje, že mezinárodní právo je použitelné i v kybernetickém prostoru a zintenzivňuje spolupráci NATO s průmyslem. Hlavní prioritou je ochrana komunikačních systémů, které vlastní nebo provozuje NATO.

5.2.2.1 Hlavní aktivity NATO v oblasti kybernetické bezpečnosti

- Politika kybernetické obrany NATO;
- Asistence jednotlivým spojeneckým zemím;
- Zvyšování kapacity kybernetické obrany NATO;
- Spolupráce s partnery;
- Spolupráce s průmyslem.

Politika kybernetické obrany NATO je implementována jak politickými, armádními a technickými autoritami NATO, tak i jednotlivými spojeneckými zeměmi. Severoatlantická rada (NAC) zajišťuje politický dohled nad všemi aspekty implementace. NAC je informována o hlavních kybernetických incidentech a útocích a je nejdůležitější autoritou v krizovém managementu vztahujícím se ke kybernetické obraně.

Poprvé byla obrana proti kybernetickým útokům zmíněna v politické agendě NATO na pražském summitu v roce 2002. Po kybernetických útocích proti Estonským veřejným a soukromým institucím se v dubnu a květnu 2007 ministři obrany spojenců shodli, že v této oblasti bude nutné přijmout urgentní opatření. Jako výsledek přijalo NATO v lednu 2008 svou první politiku kybernetické obrany. Konflikt mezi Ruskem a Gruzií v létě roku 2008 ukázal, že kybernetické útoky mají potenciál stát se významnou součástí mezinárodního válečného stavu. Nový strategický koncept byl přijat na Lisabonském summitu v roce 2010 a v červnu 2012 byla založena Komunikační a informační agentura NATO (NCIA). V červnu 2014 schválili ministry obrany NATO novou politiku kybernetické bezpečnosti, která je nyní implementována. Na Waleském summitu v září 2014 spojenci schválili nový akční plán, který bude spolu s novou politikou přispívat k plnění klíčových úkolů aliance.

V souvislosti s obranou proti kybernetickým hrozbám řeší NATO otázku možnosti integrace kybernetických kapacit do jiných válečných operací a aktivit. Tato oblast zůstává relativně neprozkoumaná a hlavní výzvou je integrace kybernetiky do širšího strategického operačního konceptu, co se týče obrany i útoku.

5.2.2.2 Článek 5 Washingtonské deklarace

Otázkou je také samotný článek 5 Washingtonské deklarace.[60] Ze strany NATO by mělo dojít ke zpřesnění formulace tohoto článku, co se týče toho, jak bude fungovat závazek kolektivní obrany v momentě, kdy dojde ke kybernetickým útokům na USA. Mezi spojeneckými státy jsou velké rozdíly v úrovni rozvoje kybernetických kapacit (obrana, zpravodajské služby). Není tedy jasné, jak moc budou vyvinuté kybernetické velmoci muset odhalit a použít své kapacity.

5.3 Evropská agentura pro bezpečnost sítí a informací („Enisa“)

Enisa (European Network and Information Security Agency) byla založena Nařízením Evropského parlamentu a Rady č. 460/2004 z 10. března 2004, o založení Evropské agentury pro bezpečnost sítí a informací. Enisa je upravena též v pozměňovacích aktech – Nařízení Evropského parlamentu a Rady č. 1007/2008 a Nařízení Evropského parlamentu a Rady č. 580/2011.

Jejím cílem je zvýšit schopnost Evropské unie, členských států EU a soukromých subjektů předcházet a čelit problémům v oblasti bezpečnosti informací, má pomáhat EU také při sběru, analýze a rozšiřování údajů o bezpečnosti sítí a informací. Agentura navíc poskytuje asistenci a rady Evropskému Parlamentu, Komisi a členským státům a pomáhá Komisi s tvorbou evropských politik a s technickými přípravnými pracemi při novelizování a rozvoji evropské právní regulace v předmětné oblasti. Úkolem Enisa je také vykonávat a zvyšovat úroveň spolupráce mezi činiteli působícími ve veřejném i soukromém sektoru za účelem dosažení vysokého stupně bezpečnosti v EU, například organizovat kybernetická cvičení, školení, ekonomické analýzy, posouzení rizik a kampaně na zvýšení povědomí o kybernetické bezpečnosti. Enisa je nápomocna Komisi a zemím EU v dialogu s průmyslem, aby se věnovaly bezpečnostním otázkám technického a programového počítačového vybavení, sleduje vývoj norem pro produkty a služby v oblasti bezpečnosti sítí a informací a podporuje opatření pro posuzování a řízení rizik. Enisa formuluje své závěry, doporučení a poskytuje poradenství.

Enisa se skládá ze tří stálých orgánů a z ad hoc pracovních skupin. Prvním z nich je **správní rada**, jejímiž členy jsou zástupci členských států EU, Komise a zástupci hospodářských subjektů, vědeckých odborníků a spotřebitelů.

Dalším orgánem je **výkonný ředitel**, který je jmenován správní radou na základě seznamu kandidátů navržených Komisí. Výkonný ředitel vede Enisa a své povinnosti plní nezávisle.

Stálá skupina zastoupených zájmů je orgánem vytvořeným výkonným ředitelem. Skupina je složena ze zástupců společností působících v oblasti informačních a komunikačních technologií, vědeckých odborníků a spotřebitelů. Úkolem stálé skupiny zastoupených zájmů je poradenství výkonnému řediteli

[60] Smluvní strany se dohodly, že ozbrojený útok proti jedné nebo více z nich v Evropě nebo Severní Americe bude považován za útok proti všem, a proto se dohodly, že dojde-li k takovémuto ozbrojenému útoku, každá z nich, uplatňujíc právo na individuální nebo kolektivní sebeobranu uznané článkem 51 Charty OSN, pomůže smluvní straně nebo stranám takto napadeným tím, že neprodleně podnikne sama a v součinnosti s ostatními stranami takovou akci, jakou bude považovat za nutnou, včetně použití ozbrojené síly, s cílem obnovit a zachovat bezpečnost severoatlantického prostoru. Každý takový útok a veškerá opatření učiněna v jeho důsledku budou neprodleně oznámena Radě bezpečnosti. Tato opatření budou ukončena, jakmile Rada bezpečnosti přijme opatření nutná pro obnovení a zachování mezinárodního míru a bezpečnosti.

v souvislosti s výkonem jeho povinností, vypracovávání návrhu pracovního programu Enisa a v zajišťování komunikace s příslušnými subjekty o všech otázkách spojených s pracovním programem.

Výkonný ředitel ve spolupráci se stálou skupinou zastoupených zájmů vytváří **ad hoc pracovní skupiny** složené z odborníků. Ad hoc pracovní skupiny se zabývají řešením specifických technických a vědeckých otázek.

V roce 2014 a na počátku roku 2015 probíhá dosud největší cvičení kybernetické bezpečnosti Cyber Europe 2014, jehož se účastní více než 200 organizací a 400 odborníků z 29 evropských zemí. Cvičení simuluje rozsáhlou krizi týkající se kritických informačních infrastruktur a v jeho průběhu se zkoušejí postupy pro sdílení operativních informací o kybernetických krizích v Evropě a testují se standardní operativní postupy EU (EU-SOPS).[61] Toto cvičení se koná pravidelně a probíhá ve třech fázích během celého roku. **Technická fáze** zahrnuje zjišťování incidentů, jejich vyšetřování, zmírňování následků a výměny informací, **operativní/taktická fáze** se týká varování, hodnocení krizí, spolupráce a koordinace, poradenství a výměny informací na operativní úrovni a **strategická fáze** se zaměřuje na rozhodování a politické dopady incidentů.

Základním metodologickým přístupem v oblasti kybernetické bezpečnosti je model „Plan-Do-Check-Act“, který je užíván v případech, kdy jsou zaváděny nové přístupy a jsou potřebná vylepšení existujících modelů.

Čtyři fáze procesu „Plan-Do-Check-Act“ zahrnují:

- **Plan**: Zachycení a analýza problému.
- **Do**: Vyvinutí a testování potenciálního řešení.
- **Check**: Posouzení efektivity použitého řešení a analýza možností, jak by mohlo být vylepšeno.
- **Act**: Plná implementace vylepšeného řešení.

V současné době identifikovala Enisa tyto oblasti, v nichž je nutné zlepšit vzájemnou spolupráci: autentifikace, ukazatel automatického sdílení, posuzování shody, analýzy dat, mezinárodní aspekty, vlivy a sbližování, soukromí a vzájemné působení dodavatelských řetězců. V těchto oblastech se Enisa orientuje na vývoj nových standardů. Do budoucna se plánují změny v řízení Enisa a postupné navyšování zdrojů pro podporu jejího fungování a bude rozšířen rámec jejích úkolů. Má se stát klíčovou organizací v boji proti počítačové kriminalitě a koordinovat úsilí orgánů činných v trestním řízení a orgánů pro ochranu soukromí.

5.4 Středoevropská platforma kybernetické bezpečnosti

Středoevropská platforma kybernetické bezpečnosti („Středoevropská platforma“) byla založena v květnu 2013 na základě iniciativy Rakouska a České republiky. Jejím cílem je umožnění sdílení informací, osvědčených postupů, zkušeností a know-how v oblasti kybernetických hrozeb a v oblasti kybernetických útoků.

V květnu roku 2014 se uskutečnilo třetí setkání v rámci Středoevropské platformy ve Vídni. Sešli se zde zástupci vládních, národních a vojenských CSIRT týmů, národních bezpečnostních úřadů a národních center kybernetické bezpečnosti z České republiky, Slovenska, Polska, Maďarska a Rakouska. Proběhlo zhodnocení pokroku v dosavadní jednoleté spolupráci na poli kybernetické bezpečnosti, povědomí o kybernetické bezpečnosti a řízení rizik. Platforma usiluje také o zvýšení schopností svých členů prostřednictvím společného vzdělávání, cvičení a koordinace v oblasti vědy a výzkumu. Setkání se věnovala zejména posilování důvěry a výměně informací o situaci v daných zemích. V budoucnu budou

[61] Standardy, které přináší návody jak zvládat velké kybernetické bezpečnostní incidenty, které by se mohly vystupňovat v krizi.

diskutovány otázky vytvoření zabezpečených informačních kanálů. Prioritami setkání bylo přijetí pracovního programu Středoevropské platformy pro období nadcházejících tří let a dohoda o pravidlech a principech spolupráce v rámci Středoevropské platformy. Výsledky vídeňského setkání Středoevropské platformy byly testovány během prvního společného kybernetického cvičení, které proběhlo v červnu 2014.

Do budoucna plánuje Středoevropská platforma budování společného mezinárodního povědomí o kybernetické bezpečnosti a řízení rizik. Toho může být dosaženo prací na vzájemné důvěře a aktivací procesů spolupráce.

5.5 Talinský manuál

Talinský manuál je příručka publikovaná v dubnu roku 2013. Současné normy mezinárodního práva ozbrojeného konfliktu jsou podle něj uplatnitelné na oblast kybernetické války. Talinský manuál definuje, že jakákoli kybernetická operace, která zakládá hrozbu nebo použití síly, směřuje proti územní celistvosti a politické nezávislosti státu nebo je uskutečněna jiným způsobem odporujícím cílům OSN, je nezákonná. Kybernetický útok je použitím síly, pokud jeho rozsah a efekt je srovnatelný s nekybernetickými operacemi dosahujícími stupně použití síly. Z komentáře v Talinském manuálu lze usoudit, že tento dokument vnímá určitý software jako zbraň, čímž dává základ pro aplikaci článku 51 Charty OSN o obraně proti ozbrojenému útoku. Pro posouzení, zda je určité jednání v kyberprostoru použitím síly, je tedy nutné posoudit rozsah takového jednání a jeho důsledky. Jednání, které má zničit nebo poškodit objekt nebo zabít člověka, je podle Talinského manuálu použitím síly.

6 Návrhy de lege ferenda[62] v oblasti kybernetické bezpečnosti

6.1 Doporučení právních změn

6.1.1 *Úprava Zákona o kybernetické bezpečnosti a prováděcích předpisů*

6.1.1.1 Kritická (informační) infrastruktura a její průřezová a odvětvová kritéria

Svou podrobnou úpravou Nařízení o kritériích pro určení prvků KI přináší velmi přesná kritéria, dle kterých lze bez významnějších obtíží určit infrastrukturu, která je v České republice považována za kritickou. Tento přístup je v EU zcela ojedinělý. Standardně jiné členské státy (např. Německo, Velká Británie, Polsko) veřejně definují jenom odvětví nebo sektory, které obsahují prvky kritické infrastruktury, a tato odvětví blíže nespecifikují, nespecifikují ani významné informační systémy.

Skutečnost že Nařízení o kritériích pro určení prvků KI obsahuje detailní specifikaci jak průřezových kritérií, tak i odvětvových kritérií, může mít zcela zásadní negativní vliv na vlastníky prvků kritické infrastruktury, ale i na bezpečnost ČR. S ohledem na bezpečnost ČR je nutné v nejkratší možné době obsah Nařízení o kritériích pro určení prvků KI zrevidovat a kritéria v něm uvedená podřídit režimu utajení. Z uvedeného vyplývá následující doporučení:

- Zestručnění odvětvových kritérií tak, aby každá z definic obsahovala pouze jejich obecné vymezení namísto detailního popisu, dle něhož jsou prvky kritické infrastruktury České republiky bez větších obtíží identifikovatelné. Možné je například následující zestručnění přílohy Nařízení o kritériích pro určení KI:
  - Uvedení odvětví kritické infrastruktury (např. **energetika**);
  - Uvedení pododvětví (subsektorů) kritické infrastruktury (např. **elektřina, zemní plyn, ropa a ropné produkty**);
  - Neuvádět další bližší specifikaci.

S ohledem na výše uvedené porovnání právních úprav jiných států lze doporučit modifikaci okruhu odvětvových kritérií, průřezových kritérií, případně subsektorů, následujícím způsobem:

- V rámci rezortního připomínkového řízení k právní úpravě kybernetické bezpečnosti v roce 2014 a v rámci toho i novely Nařízení o kritériích pro určení prvků KI došlo k nastavení průřezového kritéria v odvětví IV. Zdravotnictví tak, že právní úprava se vztáhne pouze na nemocnice s počtem akutních lůžek alespoň 2500 pacientů. Tímto bylo dosaženo, že ani největší české nemocnice nejsou prvky kritické infrastruktury a ani jejich informační a komunikační systémy, jelikož žádná nemocnice s takovým počtem lůžek v ČR nedisponuje. V tomto ohledu by bylo vhodné snížit mezní hodnotu osob s následnou hospitalizací např. na kapacitu lůžek 800 tak, aby regulace pokrývala alespoň síť nejvýznamnějších českých nemocnic.[63]
- Zahrnutí odvětvového kritéria „obchod s potravinami“, „dodavatelský potravinový řetězec“, „zpracování, dovoz, distribuce a maloobchodní prodej“ do odvětví III. Potravinářství a zemědělství přílohy Nařízení o kritériích pro určení prvků KI, jak je tomu například v Německu a Velké Británii.

[62] Pozn, autora: označuje námět pro přípravu nové právní úpravy, diskusi o její potřebnosti a smyslu, popřípadě kritiku navrhovaných osnov koncipovaných či renovovaných zákonů.

[63] Ne všechny nemocnice zveřejňují aktuální data o počtech lůžek ve svých zařízeních; jako příklad nemocnic, které by dle našeho návrhu v budoucnu měly spadat do kritické infrastruktury, lze uvést fakultní nemocnice. U nemocnic, jejichž počet lůžek je zveřejněn, je tento uveden; vychází se přitom z dat zveřejněných portálem Ministerstva zdravotnictví ČR (http://ap.mzcr.cz/VyhledavaniDetail.aspx?p=F). Navrhovaná zařízení: Fakultní nemocnice Olomouc, Fakultní nemocnice Ostrava, Fakultní nemocnice Plzeň, Fakultní nemocnice u sv. Anny v Brně (964 lůžek), Fakultní nemocnice Brno, Fakultní nemocnice Hradec Králové (1360 lůžek), Fakultní nemocnice Královské Vinohrady (1279 lůžek), Fakultní nemocnice v Motole, Všeobecná fakultní nemocnice v Praze.

- Zahrnutí odvětvového kritéria „zdravotní péče, léků, očkovacích látek a laboratoří“ do odvětví IV. Zdravotnictví přílohy Nařízení o kritériích pro určení prvků KI, jak je tomu například v Německu.
- Zahrnutí odvětvového kritéria „veřejná kanalizace“ do odvětví II. Vodní hospodářství přílohy Nařízení o kritériích pro určení prvků KI, jak je tomu například v Německu.
- Zahrnutí odvětvového kritéria „chemický a farmaceutický průmysl, hutnictví, důlní průmysl“ do nového odvětví „Průmysl“, které by bylo začleněno do přílohy Nařízení o kritériích pro určení prvků KI, jak je tomu například na Slovensku.
- Začlenění nového odvětví „Média a kultura“ do přílohy Nařízení o kritériích pro určení prvků KI, jak je tomu například v Německu.
- S ohledem na připravovanou Směrnici je možné očekávat rozšíření výčtu dotčených subjektů například o klíčové poskytovatele služeb informační společnosti, jak je stanoveno v návrhu Směrnice (platformy pro elektronické obchodování, internetové platební brány, sociální sítě, vyhledavače, služby cloud computingu a obchody s aplikacemi) případně o oblasti infrastruktury finančních trhů, výměnných uzlů internetu a potravinového dodavatelského řetězce, jak vyplývá z Upraveného návrhu směrnice.

6.1.1.2 Významné informační systémy

Vyhláška o VIS obsahuje demonstrativní výčet VIS a tím i subjektů – orgánů veřejné moci, které jsou touto vyhláškou regulovány a na které vztahuje právní úprava Zákona. Ohledně veřejnosti seznamu VIS platí stejné připomínky jako u výčtu prvků kritické infrastruktury. Tento seznam, který tvoří přílohu č. 1 k Vyhlášce o VIS, by měl podléhat režimu utajení. Jinak tím dochází k ohrožení samotných VIS, ale i bezpečnosti ČR.

6.1.1.3 Zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti je ve vztahu k povinným subjektům koncipován značně benevolentně. Vedle nízkých sankcí neobsahuje ani způsob zveřejňování bezpečnostních incidentů, pokud je to ve veřejném zájmu. Návrh Směrnice se zveřejňováním za určitých podmínek počítá – je však nutné uvést, že nelze zhodnotit, v jakém konečném znění dojde ke schválení Směrnice.

Upravený návrh Směrnice totiž oproti původnímu návrhu výrazně důkladněji chrání povinné subjekty v oblasti zveřejňování informací o bezpečnostních incidentech. Jednotné kontaktní místo smí dle Upraveného návrhu směrnice zveřejnit informaci o kybernetickém incidentu jen po konzultaci s odpovědným orgánem a v případě, že je k zamezení incidentu nebo k jeho vyřešení třeba, aby o něm měla veřejnost povědomí. Zveřejnění by bylo rovněž možné, pokud by dotčený povinný subjekt odmítl řešit závažnou strukturální slabinu spojenou s tímto incidentem. Zveřejnění by v takovém případě zcela jistě sloužilo jako efektivní způsob sankcionování povinných subjektů, které své povinnosti odmítnou dodržovat.

V každém případě by dle Upraveného návrhu směrnice byl oznamující odpovědný orgán povinen zajistit, aby dotčený povinný subjekt měl možnost se k věci vyjádřit a aby rozhodnutí o zveřejnění bylo vyváženo veřejným zájmem. Česká právní úprava chrání povinné subjekty v ještě větší míře. Úřad může poskytovat údaje z evidence incidentů provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru. Právo zveřejňovat údaje o kybernetických incidentech ale není Úřadu přiznáno vůbec. Tento přístup sice vstřícný vůči povinným subjektům, nicméně za určitých okolností může působit značně v neprospěch celé společnosti. Bylo by tomu zejména tehdy, pokud by existoval objektivní zájem na tom, aby se informace o kybernetickém incidentu zveřejnily.

6.2 Doporučení strategií

Mimo právní změny lze doporučit řadu dalších aktivit a činností za účelem posíleni kybernetické bezpečnosti ČR.

Jednou z osvědčených aktivit je provádění kybernetických cvičení, která by mohla odhalit slabiny nové právní úpravy a umožnit tak přípravu změn v nejkratším možném čase.

Pro úspěšné vyšetřování a potírání kybernetické kriminality jsou nutné nejenom dostatečné finanční prostředky, ale i kvalitní technické a znalostní zázemí orgánů činných v trestním řízení. Jedná se zejména o adekvátní vzdělávání vyšetřovatelů trestných činů, státních zástupců a soudců. Bylo by vhodné, aby ve všech stadiích trestního řízení měly příslušné kapacity a dostatek znalostí, což povede ke zrychlení trestních řízení a zvýšení efektivity při odhalování a trestání deliktů.

Dle dostupných informací žádné koncepční vzdělávání orgánů činných v trestním řízení v oblasti kybernetické bezpečnosti neprobíhá. Nejsou ani formálně a organizačně vytvořené specializované týmy na jednotlivých úrovních trestního řízení, jak je tomu například v Estonsku. V rámci povinného vzdělávání soudců a státních zástupců by bylo vhodné otázky kybernetické bezpečnosti do vzdělávacích programů začlenit.

V neposlední řadě je nutné aktivně přistupovat i ke vzdělávání koncových uživatelů informačních technologií. V některých členských státech je vzdělávání v oblasti kybernetické bezpečnosti běžnou záležitostí již na základních školách. Nejvyššímu riziku páchání kyberkriminality jsou vystavovány zejména děti a senioři. Vzdělávání těchto rizikových skupin by měla být věnována zvláštní pozornosti.

Prevence bude v budoucnosti jedním z nejúčinnějších opatření v boji proti kyberkriminalitě. Z tohoto důvodu je nutné tuto oblast obzvláště rozvíjet.

Závěr

Tato kapitola byla zpracována v rámci zadání projektu výzkumu, vývoje a inovací s názvem „Aktuální kybernetické hrozby v České republice a jejich eliminace“. Reflektuje změny, kterými prošel český právní řád v oblasti regulace kybernetické bezpečnosti do června 2015. Věnuje procesu vzniku Zákona o kybernetické bezpečnosti, který je svou komplexností ojedinělým právním předpisem na území EU.

Text se zaměřuje na dopady vyplývající ze Zákona o kybernetické bezpečnosti a jeho prováděcích předpisů, jež nabyly účinnosti dne 1. ledna 2015, na povinné subjekty. V rámci kapitoly bylo provedeno porovnání uvedených právních předpisů s úpravou ve vybraných státech Evropské unie, dále byl posouzen soulad české právní úpravy s návrhem Směrnice. Podstatná část textu se věnuje problematice kybernetické kriminality a boje proti ní.

Na základě provedené analýzy a komparace národní, zahraniční (evropské) a mezinárodní právní úpravy byl vytvořen soubor podnětů a doporučení pro případné novelizace přijatých právních norem předpisů a náměty pro další rozvoj v oblasti kybernetické bezpečnosti v České republice.

Nejzásadnějším zjištěním je zejména ojedinělý přístup českého zákonodárce k detailní specifikaci kritérií pro určení prvku kritické infrastruktury a v rámci toho kritické informační infrastruktury v rámci veřejně přístupného právního předpisu. Konkrétní specifikace průřezových a odvětvových kritérií podléhají v jiných právních řádech režimu utajení. Obdobná situace je i u seznamu významných informačních systémů, který rovněž v jiných jurisdikcích není veřejně přístupný. V tomto ohledu je nutné českou právní úpravu modifikovat.

Výčet odvětvových kritérií pro určení prvků kritické infrastruktury je možné doplnit o další odvětví a sektory v návaznosti na provedenou komparaci s úpravami vybraných členských států EU, ale i s ohledem na připravovanou Směrnici.