Cyber Security: Theory and Practice

Book · December 2015

DOI: 10.13140/RG.2.1.4052.3922

CITATIONS
0

READS
1,804

8 authors, including:

Petr Hrůza
Univerzita Obrany
16 PUBLICATIONS **24** CITATIONS
SEE PROFILE

Martin Hromada
Tomas Bata University in Zlín
158 PUBLICATIONS **871** CITATIONS
SEE PROFILE

Leopold Skoruša
Univerzita Obrany
11 PUBLICATIONS **3** CITATIONS
SEE PROFILE

KYBERNETICKÁ BEZPEČNOST
TEORIE A PRAXE

Martin HROMADA
Petr HRŮZA
Josef KADERKA
Oldřich LUŇÁČEK
Miroslav NEČAS
Bohumil PTÁČEK
Leopold SKORUŠA
Richard SLOŽIL

Vydavatelství Powerprint, Praha

2015

Kybernetická bezpečnost - Teorie a praxe

Martin HROMADA

Petr HRŮZA

Josef KADERKA

Oldřich LUŇÁČEK

Miroslav NEČAS

Bohumil PTÁČEK

Leopold SKORUŠA

Richard SLOŽIL

1. vydání, Brno 2015

Vydavatelství Powerprint, Praha

Recenzenti: prof. Ing. Zdeněk DVOŘÁK, Ph.D.

prof. Ing. Jaroslav ČECHÁK, Ph.D.

doc. Ing. Luděk LUKÁŠ, CSc.

ISBN 978-80-87994-72-6

OBSAH

ÚVOD

Kybernetická bezpečnost je v poslední době často skloňovaným tématem. Rizika spojená se zabezpečením vlastních dat a systémů se dotýkají nejen velkých firem s cenným know-how, ale prakticky každého běžného uživatele informačních technologií (IT).

Svět IT a především internetu je pro řadu uživatelů světem bez jasně daných pravidel a základních záruk. Je to svět, kde je možné existovat pod smyšlenou identitou nebo si vytvořit identitu novou, eventuálně popřít své činy a spoléhat se na anonymitu, nepostižitelnost a nedokazatelnost.

Tato odborná publikace 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.

Úvodní kapitoly se zaměřují 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. Funkčnost kritické informační infrastruktury je v současnosti jedním ze základních a důležitých

předpokladů hospodářského růstu a ekonomického rozvoje vůbec. Daňové odvody z příjmů z nich generovaných, jsou nezanedbatelným zdrojem příjmů státní pokladny, hned vedle příjmů tvořených daňovými odvody z oblasti energetiky či bankovnictví. Kritická informační infrastruktura vytváří podmínky pro fungování informační společnosti a patří mezi dynamické, rychle se měnící a vyvíjející oblasti lidské činnosti. Vývoj v této oblasti infrastruktury pomáhá postupně odstraňovat časoprostorové hranice, a to jak hranice mezi regiony, jednotlivými státy i kontinenty.

Informace o zranitelnostech a bezpečnostních děrách počítačových systémů jsou artiklem výhodného obchodu, jsou veřejně za úplatu nabízeny služby vedoucí k průnikům do systémů, ke krádežím dat, k vylupování e-mailových schránek a podobné nekalé činnosti. Naopak orgány činné v trestním řízení jsou díky převažující anonymitě pachatelů způsobenou absencí geografických internetových hranic a různorodostí společenských a právních systémů při páchání kybernetických trestných činů naprosto bezmocné. Způsobů odhalování kybernetické kriminality a nástrojů k tomu používaných je nepřeberné množství. Samostatný specialista, který je využívá ke své práci, volí především z těch finančně dostupných. Není však pravidlem, že čím dražší nástroj, tím lepší. Samozřejmě, že větší organizace má lepší finanční potenciál a tím i širší možnosti volby. Každý z nástrojů má svá specifika, má své výhody a nevýhody. Proto jsme tuto problematiku zařadili do publikace k lepšímu objasnění a pochopení způsobů odhalování kybernetické kriminality a nástrojů k tomu používaných.

V další části si publikace klade za cíl především identifikovat, popsat současnou situaci v oblasti kritické informační infrastruktury v ČR. V teoretické úrovni zhodnotit a identifikovat postavení poskytovatelů služeb elektronických komunikací ve vztahu k předmětným právním úpravám, a zvláště pak s vazbou na kybernetický zákon a na kritickou (informační) infrastrukturu.

Veškerá aktiva, která jsou uložena v informačních a komunikačních systémech, nebo jsou spravována pomocí řídicích systémů, jsou nepřetržitě ohrožována převážně neviditelnými kybernetickými útoky. Kompromitace nebo ztráta aktiv může mít pro organizaci fatální následky. Čím je hodnota aktiv a rizika jejich ztráty nebo zneužití vyšší, tím je nutné vytvoření silnějšího

týmu s větším rozsahem poskytovaných služeb. Všechna rozhodnutí managementu mají konkrétní návaznost na management rizik. Myšlení a jednání manažerů musí být proto založeno na vědomí, že řízení organizace a její procesů na všech úrovních, je svou podstatou neustálým předcházením rizik. Právě volbou vhodných metod pro posouzení rizik se zmiňujeme v kapitole analýza rizik.

Následující kapitola si klade za cíl seznámit čtenáře v minimální míře s některými specializovanými tématy technického charakteru, nahlíží do světa správy počítačových sítí a to prostřednictvím dvou vybraných témat. Oběma se prolíná externí směrovací protokol BGP, který je ve velkých sítích používán. První téma je zasvěceno popisu jedné z možností obrany před útokem označovaným jako distribuované odepření služeb a druhé téma pak ukazuje případ narušení funkce významné části světového Internetu, zapříčiněné malým tuzemským poskytovatele internetového připojení.

Dalším významným kladem publikace je šetření psychologického profilu útočníka, kterého je možné charakterizovat z několika úhlů pohledu na jeho osobnost, strukturu a hlavně motivaci jeho činnosti. Naopak bylo také zkoumáno ověření struktury osobnosti odborníků pracujících v oblasti informačních technologií. Celý proces diagnostického šetření byl zaměřen na zjištění osobnostních předpokladů osob pro práci v oblasti informačních technologií. Výsledkem je návrh souboru testů.

Kybernetický bezpečnostní tým má pro organizaci klíčový význam. Kompromitace nebo ztráta aktiv může mít pro organizaci fatální následky. Při plánování zavedení procesů kybernetické bezpečnosti a vytvoření příslušných rolí, je nutné vycházet z hodnocení aktiv a analýzy rizik. Výstupem pak právě může být nutnost vytvoření týmu kybernetické bezpečnosti.

Na závěr publikace se autoři zaměřili na popularizaci kybernetické bezpečnosti, která by se měla ubírat směrem k dětem, dospívající mládeži a v neposlední řadě také k seniorům. Počet uživatelů informačních a komunikačních technologií mezi seniory má stoupající tendenci. A právě senioři mnohdy akceptují nebezpečné jednání druhých osob bez jakéhokoliv podezření, že by je to mohlo ohrozit.

1 PRÁVNÍ RÁMEC KYBERNETICKÉ BEZPEČNOSTI

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 Podněty pro právní regulaci, základy právní úpravy

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 a 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, detekce, reakce a opatření, které mají vést ke zvýšení odolnosti jednotlivých komunikačních a informačních

[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

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 ke snížení úrovně 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 (Informačních a komunikačních technologiích), 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 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].

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 [1].

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].

1.2.2 Narušení kybernetické bezpečnosti

Druhy narušení kybernetické bezpečnosti:

Kybernetická bezpečnostní událost - Událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací [1].

Kybernetický bezpečnostní incident - Je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události [1].

Stav kybernetického nebezpečí - 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 vyhlásit 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].

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 tabulky číslo 1, ve stavu kybernetického nebezpečí je povinným subjektům uložen vyšší rozsah povinností.

Tab. 1. Povinnosti uložené povinným subjektům

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 číslo 2 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 [1].

Tab. 2. Povinnosti a sankce ukládané povinným subjektům

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
- ochranná 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 [1].

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.

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

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 [1].

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.

Tab. 3. Lhůty pro chování povinných subjektů

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			• národní CERT

orgánem nebo osobou podle písmene b),			
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 [2].

- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích **(„Vyhláška o VIS“**). Vyhlášky nabyla účinnosti dne 1. ledna 2015 [3].
- 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 [3].

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

- jedna skupina je taxativně vypočtena v příloze č. 1 Vyhlášky o VIS,

[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.

- 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. 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

[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.

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 [4].

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

[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.

definováním bezpečnostních rolí, které mají být u správců informačních a komunikačních systémů KII zavedeny [4].

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

1.4 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 [5].

1.4.1 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 je 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

[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.

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.

k zavedení bezpečnostních opatření povinny pouze 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.

1.4.2 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 dále uvedené závěry pouze doporučeními vycházejícími z nám dostupného návrhu Směrnice.

1.4.3 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.

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.

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)

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

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.

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.

---

[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.

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 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.

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 [1].

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.

1.5 Kybernetické bezpečnost rámci EU a ve vybraných zemích

Při posuzování kybernetické bezpečnosti v rámci EU jsme se soustředili pouze na evropské lídry v oblasti kybernetické bezpečnosti.

1.5.1 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,*

[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.

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.

1.5.2 Regulace v některých členských státech EU

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.

[15] http://europa.eu/rapid/press-release_IP-12-317_cs.htm

Důležitou aktivitou 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 pořádají kybernetická bezpečnostní cvičení NATO, přičemž v Talinu 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]

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],

[16] http://www.riso.ee/en/content/cyber-security-0
[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 předpisů 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

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.

Německý zákon, stejně jako český zákon, přináší minimální úroveň bezpečnostních opatření, která by měla být povinnými subjekty zavedena.

---

[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

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

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

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 následně 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.

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.

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, a také 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.

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.

[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.

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 při řešení situací ve vojvodstvích, kdy řízením a sestavením jednotlivých skupin

[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.

ve vojvodství je pověřen vojvoda. Pravomoci a působnost vojvodství v této problematice je v zákoně o krizovém řízení poměrně obsáhle upravena.

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:

- 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 2003[32]. 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.

---

[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).

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

2 KYBERNETICKÁ KRIMINALITA

Pro kyberprostor je typická interakce, globalita a sdílení dat. Ale také rizika útoků anonymních pachatelů v různé podobě.

2.1 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.

2.1.1 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 [7].

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 [7].

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.

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.

2.1.2 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,
- § 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).

Dále 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.[34]

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

[34]Komentář k § 230 Z. ŠÁMALa kol. *Trestní zákoník. Komentář.*. 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.

§ 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.[35]

§ 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

[35]Komentář k § 231 Z. ŠÁMAL a kol. *Trestní zákoník. Komentář.* 2. vydání. Nakladatelství C. H. Beck, 2012. ISBN 978-80-7400-428-5.

činu kumulativně jsou způsobení značné škody, tj. nejméně ve výši 500 000 Kč a kvalifikovaná nedbalost, tj. hrubá nedbalost[36]

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 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.[37]

§ 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.

---

[36] § 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.

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

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 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.[38]

§ 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.

2.1.3 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

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

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 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.*

2.2 Regulace na úrovni Rady Evropy

Mezi akty mezinárodního práva, které jsou v oblasti kybernetické kriminality implementovány na úrovni Rady Evropy, lze zařadit Úmluvu o počítačové kriminalitě a Úmluvu Rady Evropy o prevenci terorismu.

2.2.1 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.

2.2.2 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 následně uvedeného textu je patrné, která ustanovení Úmluvy lze pokrýt úpravou obsaženou v trestním zákoně.

2.3 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.39 Útoky se přitom dotýkají

[39] 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.

i některých subjektů v České republice, jako např. rozsáhlé útoky typu DDoS z počátku roku 2013, které vyřadily z provozu platební terminály českých bank.

2.3.1 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.[40] Označení obdobných incidentů za útoky se jeví jako do značné míry nepřesné, neboť mezinárodní právo veřejné spojuje pojem útok s ozbrojeným konfliktem [7]. 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**.[41]

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

[40] 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].
[41] SCHAAP, Maroj Arie J. Cyber Warfare operations: Development and use under International Law. Air Force, Law Review. 2009, roč. 69. Str. 125 – 126.

neobvyklým zpomalením služby, nedostupnosti částí nebo celých webových stránek, extrémním nárůstem spamů apod. [8].

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.[42]

2.3.2 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. 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.*“[43] 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.“*[44]

---

[42] 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.

[43] 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.“

[44] Předklad autorův: „Kybernetická operace zakládá použití síly, když jsou její rozsah a účinky srovnatelné s nekybernetickou operací dosahující úrovně použití síly.“

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 Iránu 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 nepřijalo výklad, že v Estonsku a v Iránu došlo k použití síly. 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.[45]

Řada autorů[46] při klasifikaci kybernetického útoku jako použití síly používá tzv. Schmittova kritéria[47], podle nichž lze některé útoky klasifikovat jako použití síly, jiné tohoto prahu nedosahují a jsou potom pouhým ekonomickým

[45] GERVAIS, M. Cyber Attacks and the Laws of War. Berkeley Journal of International Law. 2012, roč. 30, č. 2. Str. 579.
[46] 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.
[47] 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.

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[48] podotýká, že rozvoj mezinárodního práva musí ještě pokročit, aby byl kybernetický útok rozeznáván jako použití síly a ozbrojený útok, který zakládá 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."[49]

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

[48] 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.

[49] 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.

bránit? Talinský manuál opět používá případ Nikaragua[50] 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.[51]

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 kybernetického 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 vedou 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

[50] 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.

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

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.

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.

3 MEZINÁRODNÍ SPOLUPRÁCE V BOJI S KYBERNETICKÝM TERORISMEM

Stávající česká právní úprava je v mezinárodním měřítku považována za jednu z nejkomplexnějších a nejvyspělejších.

3.1 Česká republika a mezinárodní spolupráce

Česká republika je členem **NATO** (Severoatlantická aliance - North Atlantic Treaty Organization), **EU**, **OSN** a **Organizace pro bezpečnost a spolupráci v Evropě**, účastní se společných bezpečnostních aktivit i kybernetických cvičení. Rovněž co se týče kybernetických cvičení, Česká republika obsazuje přední příčky úspěšnosti v obraně proti hrozbám a podílí se též na organizaci kybernetických cvičení.

3.2 Aktivity na úrovni Organizace Spojených Národů a Severoatlantické aliance

V následující části jsou analyzovány aktivity z hlediska bezpečnosti u dvou nejdůležitějších mezinárodních organizací, jichž je Česká republika aktivním článkem.

3.2.1 OSN

Prvním spojeneckým svazkem pro kybernetickou bezpečnost zaštítěným OSN je Mezinárodní mnohostranné partnerství proti kybernetickým hrozbám[52] (IMPACT). IMPACT je od roku 2011 klíčovým partnerem Mezinárodní telekomunikační unie OSN (ITU).[53]

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

[52] International Multilateral Partnership Against Cyber Threats.
[53] International Telecommunication Union – agentura OSN specializující se na ICT.

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.[54]
- 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

[54] Jde o souhrnný koncepční rámec, který definuje a zdůvodňuje roli a funkce ozbrojených sil; jako součást státní bezpečnosti obsahuje plány zabezpečení proti kybernetickým útokům.

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.
- 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.

3.2.2 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.

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.

Článek 5 Washingtonské deklarace

Otázkou je také samotný článek 5 Washingtonské deklarace.[55] Ze strany NATO by mělo dojít ke zpřesnění formulace tohoto článku, co se týče toho,

[55] 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.

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.

3.3 Evropská agentura pro bezpečnost sítí a informací

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 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).[56] 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,

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

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.

3.4 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 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.

3.5 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.

3.6 Dílčí závěr ke kapitolám 1 - 3

Tyto kapitoly byly zpracovány v rámci zadání projektu výzkumu, vývoje a inovací s názvem „Aktuální kybernetické hrozby v České republice a jejich eliminace“. Reflektují změny, kterými prošel český právní řád v oblasti

regulace kybernetické bezpečnosti do června 2015. Věnuji se 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 kapitol 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.

4 NÁVRHY DE LEGE FERENDA V OBLASTI KYBERNETICKÉ BEZPEČNOSTI

Pokud chceme prognózovat další vývoj v oblasti boje s kybernetickou kriminalitou, nesmíme zapomínat i na vývoj právní úpravy v předmětné oblasti života společnosti.

4.1 Úprava Zákona o kybernetické bezpečnosti a prováděcích předpisů

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 sub-sektorů, 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.[57]

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.

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.

---

[57] 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 „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.

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.

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.

4.2 Doporučení

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.

5 METODY A NÁSTROJE BOJE S KYBERNETICKOU KRIMINALITOU

Pro potírání kybernetické kriminality je znalost platné právní úpravy v boji s kybernetickou kriminalitou bezpodmínečnou nutností.

5.1 Právní hlediska

V evropském měřítku se mezi ní především řadí akční plánu eEurope a Úmluva o počítačové kriminalitě. Úmluva definuje základní pojmy, stanovuje opatření, která je nutno provést na vnitrostátní úrovni, definuje počítačové trestné činy, trestné činy týkající se obsahu, porušování autorských práv, odpovědnost a sankce, řeší procesní právo, nutná opatření k definování povinnosti ukládat a předkládat potřebné provozní údaje z počítačových systémů, zakotvení pravomocí konat při řešení počítačové kriminality, řeší zásady mezinárodní spolupráce, vzájemné pomoci a výměny údajů. Česká republika je signatářem těchto právních předpisů a významnou část zakotvila do svých zákonů. Dále z národní legislativy se jedná především o trestní zákoník č.40/2009 Sb., který v sobě také zahrnuje podstatnou část ze zmiňované Úmluvy. Dalším důležitým právním předpisem je zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a prováděcí právní předpisy k zákonu č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Dále pro orgány a osoby činné v řešení kybernetické kriminality jsou důležité znalosti národní legislativy k ochraně údajů a soukromí, duševního vlastnictví, před nezákonným a škodlivým obsahem apod. Bohužel náš legislativní rámec není ucelený a některé právní normy zcela chybí. Například ty, které by podrobně definovaly postupy při zajišťování digitálních stop a jejich forenzní analýze. Doba si podobné právní předpisy vyžaduje, proto lze předpokládat, že se jich již brzy také dočkáme.

5.2 Objekty zkoumání

Práce specialisty je procesně podobná, jako v případě klasických trestních činů, nároky na jeho znalosti a jeho pracovní postupy jsou však mírně odlišné. Řešitel případů kybernetické kriminality musí počítat s fakty, které nejsou zvyklostí ve fyzickém prostředí. Zvláště to jsou neviditelné a v čase nestálé

digitální stopy, velká a převážně nezvratná anonymita pachatelů kybernetických trestných činů, prostředí bez přesně definovaných geografických hranic, častá nedostupnost některých důkazních materiálů, obtížně vyčíslitelné škody a podobně. V případě kybernetické kriminality je zkoumána digitální charakteristika místa činu, zjišťují se fakta o stavu před a po trestném činu, o přístupových právech a možnostech jejich zneužití, o tom, zda byly splněny všechny zákonné podmínky pro zajištění bezpečnosti dat, údajů, soukromí, duševního vlastnictví, ochrany před škodlivým obsahem apod. Mezi objekty zkoumání jsou zahrnuty počítače, informační systémy, datové sítě a jejich aktivní prvky a také prvky kybernetické bezpečnosti datových sítí a informačních systémů. Ve všech těchto bodech mohou ležet cenné informace, potřebné pro objasnění činu kybernetické kriminality. Specifickými objekty zkoumání jsou dnes již také stále více oblíbená nejrůznější mobilní zařízení. Mohou být jak majetkem organizace, tak soukromé. Jsou-li taková soukromá zařízení používána v datových sítích organizace, pokud je bezpečnostní politiky povolují, mluvíme pak o zařízeních typu BYOD, z anglického výrazu Bring Your Own Device.

Druhou skupinou objektů zkoumání jsou nástroje pachatele. Samozřejmě jen v případě, že pachatel byl odhalen a jeho nástroje, které k činu použil, jsou fyzicky dostupné. Takovými nástroji mohou být stolní počítač, notebook, tablet, nebo jiné mobilní zařízení. Pachatel může vlastnit nebo ovládat celou síť napadených počítačů, takzvaný botnet, který také nemusí ovládat přímo, ale přes dálkově spravovaný řídící počítač. S tím vším je nutné při odhalování jeho činů počítat. Místem, kde pachatel ukryl hledané informace a zcizená data, jsou mimo vnitřních pevných disků nebo vložených paměťových karet u pachatelových zařízení také nejrůznější externí úložiště. Mohou to být připojitelné USB disky a paměťová média, ale i síťová NAS (z anglického Network Attached Storage) a stále více oblíbená vzdálená cloudová úložiště. I ty je nutné zahrnou mezi potenciální objekty zkoumání. Důležitá je proto rozvaha. Neuvážené kroky z neznalosti, ale i pouhého opomenutí mohou znamenat nevratnou ztrátu cenných digitálních stop a důkazního materiálu. Rychlým odpojením jak pachatelova, tak napadených zařízení od napájení nebo počítačové sítě nebudou stopy po činu zakonzervovány, naopak bude velká část digitálních stop ztracena. Je proto na uvážení bezpečnostního manažera organizace a povolaného specialisty, co je větším rizikem.

Zda je důležitější okamžitě zabránit dalšímu zcizování dat, případně šíření škodlivého malware z napadeného počítače, nebo zajistit veškeré možné digitální stopy o kybernetickém kriminálním činu.

5.3 Metody a úkony objasňování

Odhalování kybernetické kriminality je souhrnem metod, postupů a nástrojů, které vedou k cíli bádání. Jejich cílem je trestnou činnost potvrdit nebo vyvrátit. Tyto metody zkoumání kybernetických trestných činů vychází ze závažnosti a způsobů provedení vlastního činu a případ od případu se liší. Aby bylo možné zvolit nejlepší a nejúčinnější metodu, je nutné co nejdříve získat co nejvíce informací o činu samotném a pak zvolit metodu, či kombinaci metod, aby byla zajištěna objektivita, rychlost a úplnost šetření.

Data, která jsou zkoumána, dělíme do tří oblastí podle jejich dostupnosti:

- Aktivní data – jednoduše dostupná v běžných adresářích.
- Skrytá data – data, která byla smazána či poškozena částečným přepsáním novými daty, jsou to také data, která byla zneviditelněna nebo znepřístupněna některým druhem ochrany, například šifrováním. K takovým datům je velmi obtížný přístup, což je jak časově velmi náročné, tak náročné na vědomosti specialistů provádějících šetření.
- Archivovaná data – data uložena v externích úložištích mimo vlastní počítač, či systém.

Výběr vhodné metody pro odhalování a vyšetřování případů kybernetické kriminality nejdříve významně ovlivní fakt, zda počítač byl cílem nebo nástrojem kybernetického kriminálního činu.

V případě, kdy počítač byl cílem, je důležitý každý krok vedoucí k zajištění co nejkvalitnějších informací o provedeném činu a jeho úspěšnosti. Jak již bylo uvedeno, v žádném případě není nejlepším řešením okamžité vypnutí počítače, přestože hrozí další zneužívání tohoto zařízení. Takto lze totiž nenávratně přijít o cenné informace, které jsou uloženy například v operační paměti, v registrech počítače, v připojených externích úložištích apod. Než se přistoupí k vypnutí nebo restartování počítače, a to i za účelem vytvoření bitové kopie jeho pevných disků, je třeba nejdříve vyčíst i všechny dočasné

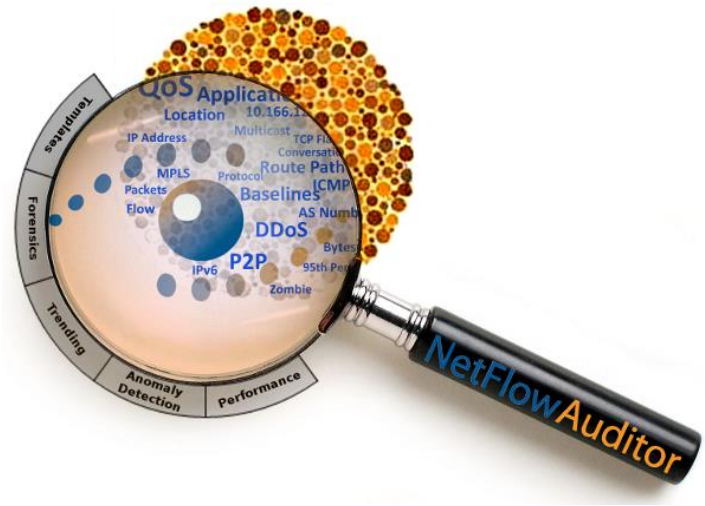
informace. To lze provést buď automatizovaně pomocí speciálních programů, nebo ručně s použitím systémových příkazů. Velkou chybou je také spuštění kontroly takového zařízení, například pomocí antivirového programu. Spuštěním kontrolního programu lze zapříčinit nechtěnou modifikaci dat. Jestliže všechny kroky k zálohování dočasných informací na externí úložiště, nikoliv na zkoumaný objekt (!), byly provedeny, tak teprve poté je možné počítač vypnout. Zavedení pomocného operačního systému se provádí výhradně z externích jednotek USB nebo vnitřní čtecí jednotky CD / DVD. Dále je potřebný program, který je schopen vytvořit přesnou bitovou kopii, tj. obraz zájmových disků. Jedině kopie identická s originálem pevného disku zaručí objektivitu šetření. Takové kopie se vytváří hned dvě. První bude pracovní a bude sloužit pro vlastní bádání a druhá bude záložní. Ze záložní kopie lze kdykoliv vytvořit novou pracovní kopii, pro případ, že předchozí byla při zkoumání modifikována nebo poškozena. S originálním systémem napadeného počítače forenzní analytik profesionál nikdy nepracuje. Způsob vytváření bitové kopie a některá další pravidla a doporučení pro forenzní analýzu digitálních dat je zakotveno v mezinárodně platných standardech, například v ISO/IEC 27037.

V situaci, kdy je pachatel známý a je i dostupný počítač, který byl nástrojem kybernetického kriminálního činu, postupuje se obdobně. V tomto případě není tak akutní hrozba dalšího působení škodlivé činnosti, jako v případě napadeného zřízení. Pokud však kybernetický útok ze zajištěného zařízení stále probíhá, je vhodné nejdříve zajistit co nejvíce informací a digitálních stop a teprve ho zastavit. V zařízení budou hledány stopy po způsobu spáchání trestného činu, po použitých nástrojích a zcizených datech. Opět je nutné před vypnutím počítače zajistit informace, které jsou uloženy v dočasných úložištích. Dále lze předpokládat, že pachatel zabezpečil svá datová úložiště například šifrováním, a proto je nutné nejdříve všechna nyní připojená externí úložiště, jako například USB, ale i ta vzdálená síťová a cloudová, řádně prozkoumat. Po jejich odpojení při vypnutí počítače již nemusí být dostupná pro absenci jejich přihlašovacích údajů. Také z operační paměti lze vyčíst další důležité informace, proto je nutné provést její výpis. To stejné platí i v případě systémových registrů. Důležité jsou informace o připojovaných paměťových médiích a discích. Přínosné mohou být i informace o běžících procesech. Z důvodu objektivity bádání je opět důležité dodržet zásadu, že na

originální diskové úložiště pachatelova počítače není možné zapisovat žádná data a nad originálním systémem nelze spouštět žádné investigativní programy a nástroje, které by jakýmkoliv způsobem modifikovaly data. Teprve po zajištění všech těchto digitálních stop může být pachatelův počítač vypnut a lze přistoupit k vytvoření přesné bitové kopie. Opět minimálně ve dvou shodných verzích, pracovní a záložní.

Specialista se však nemůže zaměřit jen na nástroj nebo objekt činu. Důležité je i vyhledání digitálních stop v okolí počítače, v datové síti. Předpokládáme, že pachatel před samotným činem prováděl činnost vedoucí k získání informací a skryté kroky nutné k jeho vlastnímu provedení. Musel tak po sobě zanechat mnoho zdánlivě neviditelných digitálních stop. Při hlubší analýze je takové stopy možné vyčíst jak z bezpečnostních prvků sítě, tak i z logů dalších síťových prvků, například z prvků informačního, komunikačního nebo řídicího systému nebo jen z okolních počítačů připojených k téže síti. Výhodou je, pokud u organizace působí kybernetický bezpečnostní tým typu SOC, CERT, CSIRT a podobně. V takovém případě lze i využít služeb specialistů takového týmu při spolupráci na zajištění digitálních stop po činnosti pachatele.

Jak bylo zmíněné, na datové síti je mnoho zařízení, která mohou uchovávat velké množství nejrůznějších digitálních stop. Trasováním možné cesty pachatelových paketů k objektu jeho činu lze sestavit mapu zařízení, u kterých je vhodné se pokusit vyčíst potřebné informace. Mezi taková zařízení patří například předřazené firewally, které mohly odmítat neúspěšné pokusy pachatele o průnik. Pokud jsou k tomu nakonfigurovány, tak i tyto informace po určitou dobu uchovávají ve svém logu. Dále to jsou bezpečnostní síťové senzory typu IDS/IPS , či NetFlow, které jsou pro detekci a mapování závadné činnosti přímo určeny. Senzory IDS / IPS pracují s pravidly, která jsou do jejich konfigurací vkládána. I v případě, že bezpečnostní tým neidentifikoval závadnou činnost, mohou úložiště senzorů obsahovat důležité záznamy, které lze dodatečně získat. V případě senzorů typu NetFlow lze při znalosti informací o pachateli rozkrýt informace o jeho komunikaci a o skrytých anomáliích datového toku. Také logy aktivních prvků sítě a informačních, komunikačních, či řídicích systémů mohly zaznamenat fragmenty jednotlivých pokusů. Provozovatelé těchto systémů tak mohou také být nápomocni při objasňování pachatelova činu.



Obr. 1. NetFlow Auditor pro analýzy

(zdroj www.netflowauditor.com)

Při zajišťování digitálních stop se používá metoda zkoumání informací z každého zdroje samostatně, a to připojením se na webové rozhraní zařízení, nebo automatizovaně, je-li v síti dostupný analytický nástroj typu SIEM (z anglického Security Information and Event Management). Nástroj slouží pro agregaci a korelaci informací. Uložené informace pak lze zpětnými dotazy analyzovat. Důležité je přitom správné vymezení časového úseku, kdy byly pachatelovy činy provedeny. To zjednoduší vyhledávání, sníží se objem prohledávaných dat a prováděné operace se výrazně urychlí.

Cílem kybernetického kriminálního činu dnes nemusí být jen počítač, informační, komunikační nebo řídicí systém, ale také mobilní zařízení, jako je telefon nebo tablet. Trh neustále žádá nové a nové modely a jejich rychlý vývoj nedrží krok s rozvojem bezpečnosti. Nová mobilní zařízení tak obsahují veliké množství zneužitelných bezpečnostních děr, kterých lze využít k průniku do zařízení a k získání cenných informací. Útoky na mobilní zařízení se rychle množí a objasňování takových činů není nijak jednoduchou záležitostí. Jak bylo již zmíněno, při forenzní analýze není přípustná modifikace originálních datových úložišť. V případě mobilních zařízení není možné toto vždy zcela zajistit. Je to způsobeno nutností instalace podpůrných aplikací, bez kterých jsou některé úkony obtížné, či nemožné. Mobilní

zařízení obvykle mají dva druhy paměťových úložišť. Vnitřní, které je typu NAND Flash a vnější, kterým je vkládaná paměťová karta. I zde je u obou typů před vlastním zajišťováním digitálních stop je také nutné vytvořit jejich přesné bitové kopie. Úplná záloha paměťové karty se provede bez větších problémů. Jinak je tomu v případě vnitřní paměti, kdy je zapotřebí specializovaných nástrojů, které však většinou vyžadují instalaci podpůrné aplikace do vlastního zařízení. Tím však může dojít k modifikaci například některých sice smazaných, ale ještě obnovitelných digitálních stop. Díky tomu je třeba předem dobře uvážit výběr vhodné metody a vybrat optimální nástroje. Pomocí nich pak lze vyčíst velké množství informací, jako jsou informace o mobilním zařízení, uložené kontakty, přehledy hovorů, zprávy SMS a MMS, obrázky, videa a zvukové soubory, informace z kalendáře, adresářová struktura, obnovit některé smazané soubory. Mimo to lze vyčíst informace z aplikací pro komunikaci na sociálních sítích, z webových prohlížečů, emailových klientů, z navigací a map a podobně. Výběr vhodného nástroje pro bádání je odvislý i od použitého souborového systému. Některé novější nástroje již nemusí podporovat starší souborové systémy. Existují také programy, které umožní prohlížení celých obrazů úložišť mobilních zařízení v počítačích s operačním systémem MS Windows, Linux a MAC. Pro analýzu je výhodnější mobilní zařízení, u kterého byl již dříve učiněn zásah do uživatelských práv typu ROOT. To umožní jednodušší a hlubší přístup. Tento zásah lze sice provést dodatečně, je však nutné počítat se skutečností, že to s sebou přináší i riziko zničení některých digitálních stop, případně i kolaps celého zařízení. Tuto činnost proto nemá provádět zvídavý laik, ale vyškolený specialista.

Veškeré zajištěné digitální stopy, jejich korelace a podrobná analýza složí k vytvoření obrazu o činnosti pachatele. Ne všechny informace a stopy však jsou pozitivní. Mohou se vyskytnout i informace takzvaně falešně pozitivní (z anglického false positive), které odvádí pozornost na nesprávnou cestu. Při odhalování kybernetické kriminality se díky umělé inteligenci zařízení s tím setkáváme velmi často. Je pak na řešiteli, aby takové informace odfiltroval a nedal se jimi zmást.

5.4 Nástroje pro zajištění digitálních stop a forenzní analýzy

Nástroje pro jednotlivé úkony a činnosti specialisty při zajišťování digitálních stop a objasňování kybernetické kriminality se volí dle jejich dostupnosti a účinnosti. Komerční nástroje práci zjednodušují a zrychlují, přinášejí však určitou finanční zátěž jak při pořízení, tak při technické podpoře jejich použití. Úroveň podpory ze strany výrobce při aktualizacích programového vybavení i případný pozáruční servis je adekvátně zpoplatněn. Volně dostupným nástrojům většinou chybí pravidelné aktualizace programu i ovladačů a výrazné je i riziko ukončení projektu a z toho plynoucí nutnost přechodu na jiný produkt. To vše může přinést mimo komplikací i nové nároky jak na finanční prostředky, tak na personál a jeho školení.

Příklady Volně dostupných nástrojů pro vytváření přesné bitové kopie:

- Program „dd“ operačního systému Linux. Jedná se o základní program pro nízkoúrovňové kopírování a konverzi surových dat, s jeho pomocí jsou ze zařízení čteny 2 kB bloky a přečtená data se zapisují do souboru s příponou „iso“. Tento volný program vyžaduje znalost OS Linux. Nevýhodou je nutnost vlastnit vhodné hardwarové komponenty pro připojení pevných disků.

- Clonezilla je jednoduše ovladatelný program pro vytváření bitových kopií a jejich klonování, vyznačuje se širokou škálou podporovaných souborových systémů a různých formátů rozdělení disku. Pracuje i se šifrovanými disky. Splňuje podmínku samostatné zavedení systému mimo kopírovaný počítač. Jeho zdrojový kód je volně přístupný na webu jeho vývojářů. Program Clonezilla je licencován GNU General Public License (GPL) verze 2. Nelze k němu však od vývojářů získat žádné potřebné hardwarové komponenty. Jejich pořízení je záležitostí uživatele.

Ke komerčním produktům se řadí například následující nástroje:

- RAC DEAS – jedná se o jednoduchý tuzemský produkt, který byl vyvinut ve Znaleckém ústavu RAC. Je to linuxová Live distribuce, která obsahuje dva nástroje pro vytváření forenzních bitových kopií disků. Nástroje FTK a Libewf. Produkt je intuitivní a není náročný na znalosti jeho obsluhy a práci s ním zvládne i zaškolená osoba.

- Tableau TD2U KIT – komerční produkt, forenzní duplikátor s rozhraním USB 2.0, 3.0, SATA, IDE SAS, s pracovní rychlostí přesahující 15GB/min a s jednoduchým ovládáním. Práce s ním se skládá jen ze základních úkonů. Vyžaduje jen připojení pevných disků na správná rozhraní a spuštění kopírování. Zároveň lze vytvářet více kopií na různé pevné disky připojené na jeho výstupní rozhraní. Obsahuje potřebný hardware.

- FTK imager – komerční produkt. Kromě jiného obsahuje jednoduchý postup pro výběr vstupního a výstupního zařízení pro přesné kopírování pevných disků. Softwarový nástroj patří k nejoblíbenějším pro zajišťování digitálních důkazů a stop. Není náročný na obsluhu a je obsahem i jiných forenzních produktů.

- Acronis True Image – softwarový produkt, který umožňuje vytvářet kopie disků a zálohy počítačů. Zálohy lze podle varianty programu ukládat i do cloudových úložišť. Běží pod OS Windows a MAC a podporuje jejich poslední verze.

- Symantec Ghost Solution Suite – další z komerčních produktů, který umožňuje vytvářet bitové kopie pevných disků. Není to však samostatný program, ale součást celého programového balíku.

Příklady některých komerčních nástrojů pro forenzní analýzy:

- EnCase Forensic - jedná se o mohutný forenzní analytický nástroj, který umí zpracovat velké objemy dat v přijatelném čase. Podporuje mnoho OS a aplikací a zařízení. Poradí si s mobilními zařízeními, vyjímatelnými médii, pevnými disky apod. Vyškolený specialista je schopen vytvářet vlastní dotazy a filtry pro vyhledávání digitálních stop a důkazů. Umožňuje vytváření výstupních zpráv, reportů. Od jeho výkonu je odvislá i jeho cena. Nutností je vyškolení specialistů a pravidelné doplňování jejich znalostí.

- FTK Forensic Toolkit – je dalším celosvětově rozšířeným komerčním nástrojem pro digitální forenzní analýzy. Je mohutný, rychlý a stabilní, s intuitivní obsluhou pro vyškolené specialisty. Umožňuje propojit různé

zdroje dat, jako počítače, pevné disky, mobilní zařízení, vzdálená úložiště a další a v nich sbírat digitální stopy.

- Evidence Center 2015 – ve srovnání s předchozími nástroji jednodušší, umožňující vyhledávat a zajišťovat digitální stopy na počítači, jak na pevném disku, tak v dočasných úložištích. Je zároveň určen i pro mobilní zařízení se systémy iOS, Anfdroid a Blackberry.

- NUIX – komerční produkt k vyhledání a vizualizaci kritických faktů v zajištěných digitálních důkazech. Určen pro zpracování dat z počítačů, mobilních zařízení, digitálních médií a jejich bitových kopií.

5.5 Nástroje pro analýzu mobilních zařízení

Jedná se o nástroje, pomocí kterých lze vyextrahovat potřebné digitální stopy z chytrých mobilních telefonů, tabletů, GPS a jiných mobilních zařízení a podrobně je analyzovat. Nástroje dokáží obejít hesla, přístupové kódy i ochranu gestem. Pracují s běžnými operačními systémy typu iOS, Android a Blackberry, s vnitřními NAND pamětmi i vloženými paměťovými kartami. Konstrukčně lze nástroje rozdělit do dvou oblastí. Na komplexní řešení, která obsahují jak software, tak potřebný hardware, včetně kabeláží a potřebných konektorů a na samostatné softwarové produkty, vyžadující instalaci na počítač nebo notebook. Co do schopností se jednotlivá řešení liší jen velmi nepatrně. Výhodou a parametrem ovlivňujícími výběr proto zřejmě bude úroveň jazykové lokalizace do mateřského jazyka, dostupnost lokální podpory a nabízené příslušenství.

Příklady některých takových nástrojů:

- XRY Complete - je komerční softwarový produkt určený pro instalaci na zařízení s operačním systémem MS Windows a umožňuje zajišťování digitálních stop na logické úrovni extrakcí z paměti telefonu, jejich analýzu a tvorbu výstupních reportů. Zvládá možnou obnovu smazaných a jinak nedostupných dat. Existuje několik variant tohoto produktu, včetně kompletu s výbavou potřebných konektorů.

- MOBILedit Forensic – jedná se o tuzemský komerční softwarový produkt, který zvládá prohlížení, vyhledávání a načtení dat z velkého

množství modelů mobilních telefonů. Umí obejít hesla a jiné druhy zabezpečení přístupu k zařízení s různým operačním systémem. Mimo základních informací o telefonu, o obsahu zpráv SMS a MMS, historii volání, GPS poloze, údajích z poznámek a kalendářů, si poradí s daty z aplikací pro komunikaci na sociálních sítích a připojení externích úložišť. Obsluha je jednoduchá a intuitivní.

- UFED – komerční komplexní mobilní řešení, určen k extrakci, dekódování a analýze digitálních stop z mobilních zařízení. Podporuje velké množství mobilních zařízení a obsahuje sadu potřebných konektorů. Obsluha je jednoduchá a intuitivní.

- Oxygen Forensic Suite - je komerční softwarové řešení pro vyhledávání a analýzu digitálních stop z mobilních zařízení. Z jejich systému i aplikací. Obchází ochranu hesly, kódy i gesty, i v případě iOS. Je schopno extrahovat digitální stopy, provádět jejich analýzy a generovat reporty. Umí provádět obnovu smazaných a ještě dostupných souborů. Umožňuje získat data z připojovaných iCloudových úložišť. Podporuje velké množství mobilních zařízení.

5.6 Metody vytěžování dat z otevřených zdrojů

Metody vytěžování dat z otevřených zdrojů slouží k identifikaci informací o kybernetických hrozbách. Využívá analytické nástroje s cílem efektivně vytěžovat nestrukturovaná data za účelem:

- identifikace nových informací o kybernetických hrozbách,
- řešení či vyšetřování kybernetických incidentů,
- realizace opatření a protiopatření,
- uchovávání a sdílení informací a znalostí.

Jedná se o proces systematického využívání informací o kybernetických hrozbách za účelem získávání znalostní potřebných pro ochranu kritické informační infrastruktury. Obdobné postupy však mohou být využity v oblasti zajišťování kybernetické bezpečnosti obecně. Vstupem do procesu jsou data a informace umožňující sledovat a vyhodnocovat:

- **aktivity, motivace a záměry útočníků** představující pro kritickou infrastrukturu současnou či potenciální hrozbu přímou či nepřímou,

- **zranitelnosti systémů kritické informační infrastruktury** a metody útoků, kterými tyto zranitelnosti mohou být využity**,**
- **události a incidenty**, které mohou signalizovat cílené a organizované útoky na kritickou informační infrastrukturu.

Výstupem analýzy nestrukturovaných dat jsou podklady pro konkrétní osoby či týmy (tzv. zpravodajské produkty), které jim pomáhají v jejich činnosti, zejména jde o následující druhy výstupů:

- **personalizovaný monitoring** poskytující fakta či signály o hrozbách,
- **analytická zpráva** odpovídající na otázky související s rozhodováním o strategii přijímání dlouhodobých opatření a protiopatření,
- **znalostní báze** sloužící pro uchovávání a sdílení získaných poznatků a znalostí.

Využitím profesionálních nástrojů pro analýzu nestrukturovaných dat je možné redukovat pracnost a časovou náročnost získávání a zpracování informací o kybernetických hrozbách a usnadnit sdílení získaných informací znalostí a poznatků. Díky tomu lze:

- zvýšit účelnost a účinnost nákladů na kvalifikovaný personál,
- udržovat a zvyšovat kvalifikaci odborníků na kybernetickou bezpečnost,
- snáze eliminovat kybernetická rizika a jejich dopady.

V rámci projektu „Aktuální kybernetické hrozby a jejich eliminace“ byly využity pro analýzu dat z otevřených zdrojů nástroje společnosti TOVEK.

5.6.1 Zdroje dat

Oblastí kybernetické bezpečnosti se zabývá řada otevřených zdrojů. Doporučit lze následující:

V českém jazyce

csirt - *https://www.csirt.cz/news/*
govcertcz - *http://www.govcert.cz/cs/informacni-servis/*

V anglickém jazyce

National Vulnerability Database NIST - *https://nvd.nist.gov/home.cfm* ***Softpedia*** - *http://news.softpedia.com/cat/Security/Hacking-News/*

Twitter *- https://twitter.com/ - pouze vybrané hashtagy (#cybersecurity, #hack, #hacker, #cyberrisk, #sqlinjection, #infosec, #sec, #vulnerability)*

Cyber Security Caucus *- http://cybersecuritycaucus.com/feed/*

Hackmageddon.com *- http://hackmageddon.com/feed/*

Help Net Security *- http://feeds2.feedburner.com/HelpNetSecurity*

OSVDB *- http://blog.osvdb.org/feed/*

US-CERT Alerts *- http://www.us-cert.gov/ncas/alerts.xml*

US-CERT Bulletins *- http://www.us-cert.gov/ncas/bulletins.xml*

Zone-H.org Special Defacements *- http://www.zone-h.org/rss/specialdefacements*

Analytické vyhledávání

Prvním krokem analýzy je vyhledání informací, které jsou relevantní řešenému tématu. Dotaz lze položit do jednoho nebo více zdrojů dat a to i ve více jazycích zároveň. Dotaz lze zadat:

- Výčtem klíčových slov
- Úryvkem volného textu
- Výběrem dokumentu pro hledání podobných
- Využitím dotazovacího jazyku Tovek – ve formě Tovek Query
- Ve formě aktivní mapy poznatků (Tovek Query rozšířený o komentáře a poznámky).

5.6.2 Dotazovací jazyk Tovek

Jedno ze zásadních vlastností použité fulltextové technologie je pokročilý dotazovací jazyk, který umožňuje formulovat expertní dotazy (Tovek Query) a aktivní mapy poznatků takovým způsobem, aby byly vyhledány pouze relevantní dokumenty. Dotazovací jazyk se využívá nejen pro hledání, ale rovněž pro definování pravidel (tzv. Tovek Query) pro automatické doručování dokumentů a kategorizaci. Obsahuje následující skupiny operátorů:

Pojmové operátory

Pojmové operátory jsou základní stavební kameny dotazů a definují, jaké pojmy se mají v dokumentech vyhledávat.

.word	slouží k vyhledání dokumentů, které obsahují jeden nebo více výskytů určitého pojmu v uvedeném mluvnickém tvaru
.stem	umožňuje vyhledat dokumenty obsahující určitý pojem v jakémkoli jeho mluvnickém tvaru, chování operátoru lze upřesnit konfigurací fulltextového jádra, chová se buď jako operátor *.beststem* a nebo jako operátor *.multistem*
.beststem	hledá dokumenty obsahující slova, která jsou jazykovým modulem převedena na stejný základní tvar jako zadané slovo, vrací-li tento modul více než jeden základní tvar, pak tento operátor vybere pouze ten tvar, který je zadanému slovu nejpodobnější
.multistem	hledá dokumenty obsahující slova, která jsou jazykovým modulem převedena na jakýkoliv ze základních tvarů vypočítaných pro zadané slovo
.wildcard	najde dokumenty, které obsahují jeden nebo více pojmů, které odpovídají zadanému regulárnímu výrazu
.typo/n	vyhledá dokumenty, které obsahují pojmy lišící se od zadaného pojmu maximálně o daný počet chyb
.thesaurus	slouží k vyhledání dokumentů obsahujících jakýkoli mluvnický tvar zadaného pojmu nebo jeho příbuzných pojmů
.soundex	umožňuje nalézt dokumenty obsahující jakýkoliv tvar pojmů znějících podobně jako zadaný pojem (vhodné zejména pro angličtinu)
.range	vyhledá dokumenty obsahující pojmy v daném rozsahu

Konceptuální operátory

Konceptuální operátory spojují jednotlivé dotazy do větších celků:

.best	slouží k nalezení dokumentů, které vyhovují alespoň jednomu poddotazu uvedenému jako parametr operátoru, skóre dokumentu je tím vyšší, čím více poddotazům odpovídá

.and	najde dokumenty, které vyhovují všem poddotazům uvedeným jako parametr operátoru
.or	najde dokumenty, které vyhovují alespoň jednomu poddotazu uvedenému jako parametr operátoru
.all	vyhodnocuje dokumenty stejně jako operátor *.and*, ale nepočítá skóre, a je díky tomu rychlejší
.any	vyhodnocuje dokumenty stejně jako operátor *.or*, ale nepočítá skóre a je díky tomu rychlejší

Poziční operátory

Poziční operátory vyhodnocují dokumenty nejen na základě samotného výskytu pojmů, ale i na jejich konkrétní pozici:

.near/n	slouží k nalezení dokumentů, které vyhovují všem dotazům uvedeným jako parametr operátoru, jejichž výskyty se nacházejí do maximální uvedené vzdálenosti, operátor *.near* podporuje několik způsobů vážení dokumentů, přičemž standardně je skóre dokumentů tím vyšší, čím blíže u sebe se jednotlivé výskyty nacházejí
.paragraph	tento operátor vyhodnocuje dokumenty stejně jako *.near/n*, kde n je délka odstavce, která je standardně nastavená na hodnotu 64
.sentence	tento operátor vyhodnocuje dokumenty jako *.near/n*, kde n je délka věty, která je standardně nastavená na hodnotu 16
.phrase	umožňuje nalézt dokumenty obsahující frázi složenou z výskytů jednotlivých dotazů uvedených jako parametr operátoru, nejčastěji se používá k vyhledání dokumentů obsahujících frázi složenou z několika konkrétních pojmů, příp. jejich stemů

Relační operátory

Relační operátory slouží k nastavování podmínek pro netokenizovaná pole dokumentu (tokenizace je vysvětlena v příručce Tovek: Fulltextové jádro, Příručka administrátora). Typicky se jedná o pole obsahující datum, číslo nebo řetězcovou konstantu:

.contains	umožňuje nalézt dokumenty, kde hodnota pole obsahuje určitý řetězec znaků
.matches	najde dokumenty, kde je hodnota pole shodná s uvedeným vzorem
.starts	najde dokumenty, kde hodnota pole začíná určitým řetězcem
.substring	vyhledá dokumenty, které v daném poli obsahují uvedený řetězec
.ends	najde dokumenty, kde hodnota pole končí uvedeným řetězcem
<	najde dokumenty, kde je hodnota pole menší než uvedená hodnota
<=	najde dokumenty, kde je hodnota pole menší nebo rovna uvedené hodnotě
=	najde dokumenty, kde je hodnota pole rovna uvedené hodnotě
!=	najde dokumenty, kde je hodnota pole různá od uvedené hodnoty
>=	najde dokumenty, kde je hodnota pole větší nebo rovna uvedené hodnotě
>	najde dokumenty, kde je hodnota pole větší než uvedená hodnota

Pokročilé operátory

Dotazovací jazyk podporuje následující pokročilé operátory:

.topic	umožňuje využít dotazy uložené v indexu, nebo definovaná lokálně v rámci určitého dotazu
.freetext	pomocí operátoru freetext lze specifikovat dotaz volným textem
.in	definuje v jaké zóně dokumentu, případně v jakém tokenizovaném poli, se má dotaz vyhodnocovat
.like	najde dokumenty podobné uvedenému dokumentu
.entity	najde dokumenty obsahující daný typ entity případně konkrétní entitu

Modifikátory

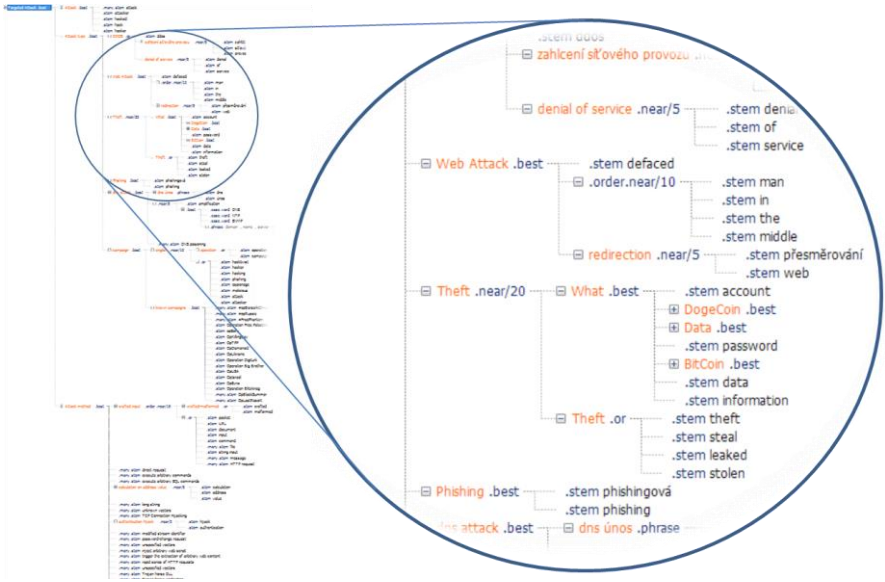
Modifikátory upravují nebo upřesňují význam operátorů. Dotazovací jazyk obsahuje následující modifikátory:

.case	lze použít s některými pojmovými operátory, omezuje vyhledávání pouze na pojmy, které se shodují i ve velikosti písmen
.many	nastavuje výpočet skóre dokumentu, kdy je zohledněn počet výskytů hledaných pojmů, čím více výskytů dokument obsahuje, tím vyšší je skóre
.not	umožňuje nalézt všechny dokumenty, které nevyhovují určitému dotazu
.order	určuje, že se jednotlivé parametry operátoru musí v dokumentu vyskytovat ve stejném pořadí, ve kterém jsou uvedeny v dotazu
.count/n	určuje minimální nebo maximální počet výskytů daného poddotazu v dokumentu
.lang/id	definuje jazyk všech parametrů daného operátoru
[číslo]	koeficient váhy umožňuje ovlivnit výsledné skóre přiřazené dokumentu při vyhodnocování dotazu, jednotlivé části dotazu mohou mít různé koeficienty váhy a tak různě přispívat k celkové váze dokumentu
[jméno]	pojmenování části dotazu, díky kterému se lze následně na danou část dotazu odkazovat pomocí operátoru *.topic*

[jméno/číslo] je-li třeba operátor pojmenovat a zároveň změnit jeho koeficient váhy, zapíší se oba tyto údaje do hranatých závorek oddělených lomítkem

Tovek Query a aktivní mapa poznatků

V rámci projektu „Aktuální kybernetické hrozby a jejich eliminace“ byly využívány zejména expertní dotazy ve formě Tovek Query (Obr. 2) s využitím dotazovacího jazyka Tovek. Dotazování touto formou umožňuje definovat dotaz tak, aby byly vyhledány relevantní informace s minimem chyb I. druhu (nezařazení relevantního dokumentu do seznamu výsledků hledání, anglicky false negative) i II. druhu (zařazení dokumentu, který není relevantní, anglicky false positive).



Obr. 2: Tovek Query *(zdroj vlastní)*

K vytváření expertních dotazů byl využit nástrojTovek Query Editor, který umožňuje sestavovat dotaz ve formě stromu včetně možnosti pojmenovávat jednotlivé větve dotazu a přiřazovat jim váhy. Tovek Query není jen výčtem klíčových slov, ale popisuje určité téma z více pohledů a ve více jazycích. Například dotaz k tématu „Cílený útok“ obsahuje kromě klíčových slov „útok, attack“ rovněž definování různých typů útoku (phishing, krádež, útok na web atd.) a různých metod útoku (SQL injection, crafted/malformed input, trojan horse atd.).

Seznam výsledků

Seznam výsledků hledání (Obr. 3) obsahuje dokumenty, které jsou vyhodnoceny jako relevantní k položenému dotazu. Primárně je seznam tříděn podle skóre dokumentů a obsahuje vybraná metadata dokumentů, např. titulek, datum, extrahované entity či skóre kontextových dotazů. Uživatel může zvolit, která metadata budou zobrazená v určitém seznamu výsledků. Podle metadat lze výsledky řadit, filtrovat a seskupovat.

Skóre	Date	Title	E_hackergr	ddos útok	dns útok	Kampaň	krádež	Phishing	útok na web
92	2013-05-08	OpUSA: Fake Leaks, Small Website Defacements, ...	Afghan Cyber Army, Anonymous, Izz ad-Din al-Qassa...	100	0	61	0	50	50
91	2013-11-17	Security Brief: Jeremy Hammond, Japan, TPP, Lin...	Anonymous, LulzSec hackers	100	0	71	50	0	0
90	2014-04-07	OpIsrael: Anonymous Hackers Target Websites of...	Anonymous	100	0	63	0	50	50
90	2014-04-07	OpIsrael: Anonymous Hackers Target Websites of...	Anonymous	100	0	63	0	50	50
87	2014-02-09	Security Brief: Telecoms Company Hacks, Sochi Ol...	Anonymous, NullCrew, RedHack, Syrian Electronic Army	100	0	0	50	50	50
87	2014-02-09	Security Brief: Telecoms Company Hacks, Sochi Ol...	Anonymous, NullCrew, RedHack, Syrian Electronic Army	100	0	0	50	50	50
87	2013-04-08	Hacktivists Target over 100,000 Israeli Sites, Offic...	AnonGhost, Anonymous	100	0	62	0	0	50
86	2014-02-21	Forbes and the Syrian Electronic Army Provide Mo...	Syrian Electronic Army	0	0	47	50	50	0
86	2014-02-21	Forbes and the Syrian Electronic Army Provide Mo...	Syrian Electronic Army	0	0	47	50	50	0
86	2013-12-29	2013 Security Brief: NSA Spying, Adobe Hack, Chi...	Syrian Electronic Army	100	0	50	0	0	0

Obr. 3: Seznam výsledků *(zdroj vlastní)*

Zobrazení dokumentu

Tovek Tools zobrazují náhled textu dokumentu (Obr. 4) s podsvícením nalezených slov (modře) a automaticky extrahovaných entit (ostatní barvy). Díky použití Tovek Query, který popisuje širší kontext daného tématu, jsou automaticky zvýrazněny důležité části dokumentu. Originál dokumentu lze otevřít z původního umístění, v tomto případě však není podsvícení dostupné.

name: Security Brief: Jeremy Hammond, Japan, TPP, Linux Malware - Softpedia
keywords: security brief, TPP, Linux malware, arrested, hacktivism
desc: In case you haven
date: 2013-11-17
link: http://news.softpedia.com/news/Security-Brief-Jeremy-Hammond-Japan-TPP-Linux-Malware-400949.shtml

The main events of the week between November 11 - November 17, 2013

Check out this week"s most important stories

In case you haven't been online much over the past week, here's your chance to catch up on some reading. One of this week's most important events was the sentencing of LulzSec and Anonymous hacktivist Jeremy Hammond . Much to the dismay of his supporters, Hammond has been sentenced to 10 years in prison and 3 years of supervised release. Just before the sentencing, the hacker made a statement in which he revealed some interesting things regarding his hacking activities and the way the US government had tricked hacktivists into doing its dirty work. According to Hammond, the FBI tricked them into hacking the websites of foreign government through Sabu, who at the time was working as an informant. Another hacktivism-related story is the one of the FBI memo obtained by Reuters. Apparently, the agency is warning US government organizations that their systems might have been breached over the past year by Anonymous hackers. The list includes the Department of Energy, the Army, the Department of Health and Human Services, and possibly several others. The attacks appear to be tied to the case of British man Lauri Love, who was recently arrested and charged. Some other interesting stories are related to Japan. Local media has reported that a total of 33 anti-nuclear citizens groups have been the target of a coordinated email-based denial-of-service (DOS) attack. The targeted organizations were sent a total of 2.53 million emails in the course of less than two months. In the meantime, Anonymous hacktivists have set their sights on the Japanese government in a campaign called OpKillingBay. The hackers

Obr. 4: Zobrazení dokumentu *(zdroj vlastní)*

Export dat

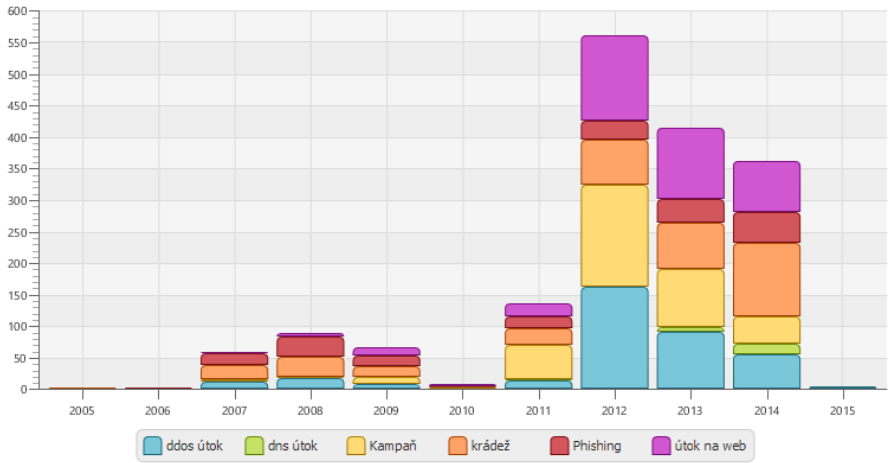
Tovek Tools umožňují snadno kopírovat data ze seznamu výsledků pomocí schránky a exportovat je v xml, html či txt formátu a zaslat je vybraným příjemcům.

5.6.3 Obsahová a kontextová analýza

Tovek Tools byly v rámci projektu využity k obsahové a kontextové analýze dokumentů z externích zdrojů. Výsledky této analýzy byly využity v několika oblastech: vytvoření databáze útočníků a skupin útočníků, vytvoření pravidel pro extrakci zranitelností a typů útoků, identifikace informací pro profily útočníků, definování pravidel pro automatickou kategorizaci informací z externích zdrojů dle témat ontologie a další.

Souhrny

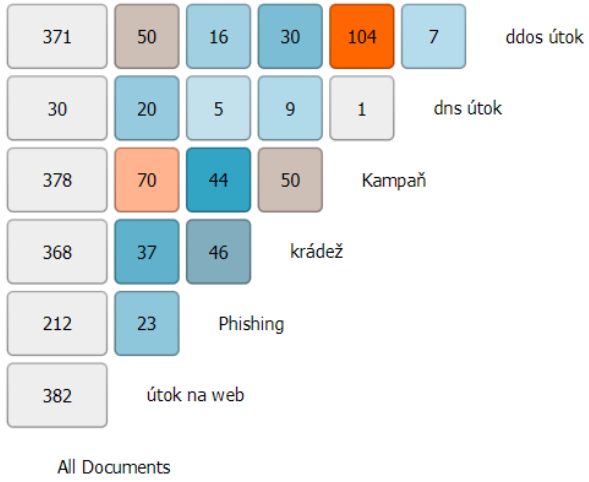
Tovek Tools umožňují zobrazovat souhrnné informace o nalezených dokumentech v podobě časového grafu, koláčových grafů, tabulek nebo mraků témat. Pomocí souhrnů lze dokumenty snadno filtrovat. Využívány byly zejména v kombinaci s kontextovou analýzou (Obr. 5) pro identifikaci časových trendů v oblasti typů útoků či zranitelností.



Obr. 5: Vývoj vybraných typů útoků v čase *(zdroj vlastní)*

Kontextová analýza

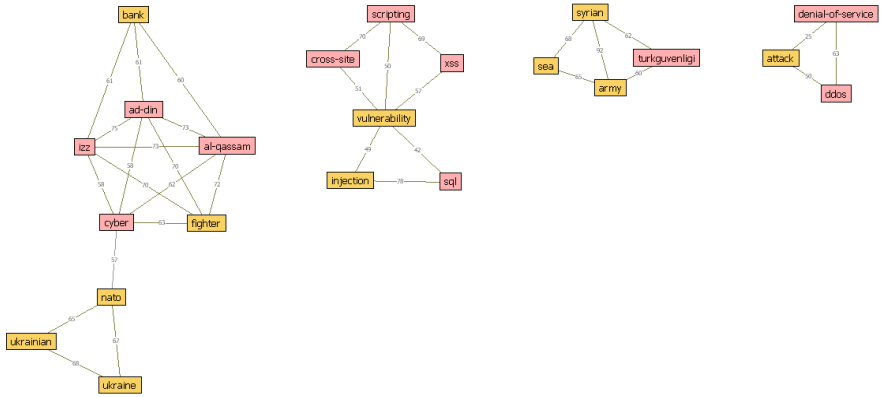
Modul InfoRating umožňuje nad seznamem výsledků provádět kontextovou analýzu. Výsledkem je kontextová matice zobrazující vztahy mezi tématy, která jsou definována kontextovými dotazy. V rámci projektu byla kontextová analýza využita pro generování personalizovaných reportů s křížovými referencemi a pro ladění expertních dotazů ve formě Tovek Query.



Obr. 6: Kontextová matice: vybrané typy útoků *(zdroj vlastní)*

Obsahová analýza

Modul Harvester umožňuje v souboru dokumentů automaticky identifikovat důležitá témata a indikovat jejich trend. Harvester kombinuje statistické metody s lingvistickou analýzou. Zobrazuje významná klíčová slova a vztahy mezi nimi. Umožňuje zobrazit okolí vybraných slov a dokumenty, ve kterých se vyskytují. V rámci projektu byl využit zejména při návrhu expertních dotazů a kategorizačních pravidel a při analýze většího objemu neznámých dat.



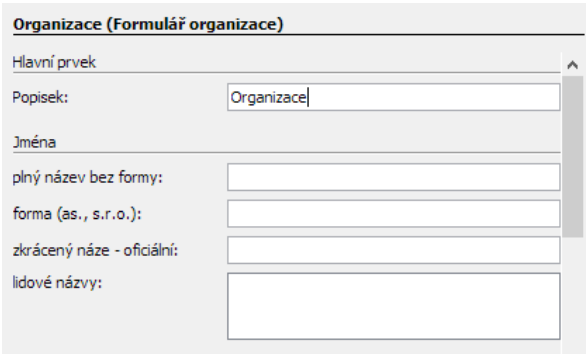
Obr. 7: Obsahová analýza v produktu Harvester *(zdroj vlastní)*

5.6.4 Uchovávání poznatků a znalostí

Poznatky získané analýzou nestrukturovaných dat je důležité uchovávat, opakovaně využívat a sdílet. Poznatky jsou uchovány v expertních dotazech a aktivních mapách poznatků. Tovek Tools rovněž umožňují uchovávat poznatky v šablonách dotazů, projektech a znalostní bázi.

Šablony dotazů

Šablony dotazů slouží pro hledání osob, organizací a dalších objektů. Šablona dotazu obsahuje logiku, dle které je ze zadaných údajů o objektu automaticky vygenerován dotaz. Předpřipravené šablony dotazů (Obr. 8) mohou využívat uživatelé, kteří mají věcnou znalost určité problematiky, ale nevládnou pokročilou znalostí dotazovacího jazyka. Lze také automaticky plnit daty ze znalostní báze či z jiných systémů, které obsahují informace o zájmových subjektech či objektech, a využívat je například pro automatizovaný monitoring informací.



Obr. 8: Šablona dotazu *(zdroj vlastní)*

Projekty

Projekty slouží k uložení dotazů, vyhledaných dokumentů a výsledků analýz. Jsou uloženy lokálně, lze exportovat a sdílet s dalšími uživateli Tovek Tools. Výhodou sdílení dotazů je to, že zpravidla neobsahují citlivé informace (ty obsahují až vyhledané dokumenty).

Znalostní báze

Vybrané dotazy, vytvořené v rámci analýzy, jsou ukládány do znalostní báze ve formě Tovek Query). Tyto dotazy umožňují automatizovaně dohledávat

informace k jednotlivým tématům ve znalostní bázi. Díky tomu jsou snadno dostupné dalším uživatelům.

5.7 Dílčí závěr

Způsobů odhalování kybernetické kriminality a nástrojů k tomu používaných je nepřeberné množství. Samostatný specialista, který je využívá ke své práci, volí především z těch finančně dostupných. Není však pravidlem, že čím dražší nástroj, tím lepší. Samozřejmě, že větší organizace má lepší finanční potenciál a tím i širší možnosti volby. Každý z nástrojů má svá specifika, má své výhody a nevýhody. Ne všechny nabízené funkce musí být využity. Naopak provozní a případná servisní podpora je nutností a její úroveň by měla být jedním z rozhodujících faktorů při výběru vhodného nástroje. Výhodou je vždy, pokud specialista, který čin objasňuje, může požádat o spolupráci kybernetický bezpečnostní tým, který vlastní jak potřebné bezpečnostní nástroje, tak disponuje potřebnými odbornými znalostmi. Je-li to navíc tým, který zajišťuje bezpečnost právě v místě, kde byl čin spáchán, pak tým disponuje i podrobnou znalostí prostředí. To vše usnadní a zrychlí objasňování činu a přinese větší množství zajištěných digitálních stop.

Mimo činnosti vedoucí k zajištění digitálních stop a informací o pachateli kybernetického trestného činu, o způsobu provedení, závažnosti a jeho dalších dopadech, je také vhodné se zabývat i informacemi o napadené straně. Tím, jak bylo napadené zařízení užíváno a zda uživatel nebo provozovatel svou nedbalostí nezapříčinil nebo neusnadnil provedení pachatelova činu. Týká se to případů, kdy je používán nelegální software, není pravidelně prováděno doporučené bezpečnostní záplatování, neprobíhají aktualizace operačního systému a používaného programového vybavení, není použit vhodný antivirový program nebo antivirový program není pravidelně aktualizován. Dále případů, kdy důležitá data a přístup k nim není dostatečně chráněn alespoň pomocí hesel, tato hesla nejsou dostatečně silná, nebo s nimi není patřičným způsobem nakládáno, tato data nejsou pravidelně zálohována, kdy u organizací neexistují bezpečnostní politiky a plány obnovy dat i systémů po kritických stavech a další podobná pochybení. To vše dává výsledný obraz o spáchaném činu kybernetické kriminality.

Cílem kybernetické trestné činnosti však nemusí být jen počítač soukromého uživatele, firmy nebo instituce, ale může to být i část informačního,

komunikačního nebo řídicího systému důležitého prvku kritické infrastruktury. Pod vlivem posledních teroristických událostí je nutné mít na zřeteli, jak zranitelné takové systémy jsou, jaké zásadní škody by takový útok mohl napáchat a jak obtížné by bylo objasnění činu samotného. Informace o zranitelnostech a bezpečnostních děrách počítačových systémů jsou artiklem výhodného obchodu, jsou veřejně za úplatu nabízeny služby vedoucí k průnikům do systémů, ke krádežím dat, k vylupování e-mailových schránek a podobné nekalé činnosti. Naopak orgány činné v trestním řízení jsou díky převažující anonymitě pachatelů způsobenou absencí geografických internetových hranic a různorodostí společenských a právních systémů při páchání kybernetických trestných činů naprosto bezmocné. Neexistuje jednotná mezinárodní právní legislativa umožňující útočníky vypátrat, natož postihnout. V takovém světě je nutné spoléhat především na vlastní připravenost a odolnost počítačových systémů a aktiv v nich uložených. Útočníci jsou ve výhodě díky faktoru překvapení a možného zaskočení druhé strany, tak z hlediska pro ně výhodného poměru nákladů na kybernetický útok a ochranu před ním. S minimálními náklady tak mohou způsobit obrovské škody na majetku i na lidských životech. Jejich útoky mohou být skryté a dlouhodobé a zachytit je a objasnit může být velmi obtížné. Prioritní a zásadní investice vedoucí k potlačování kybernetické kriminality proto nemá být do technologií, ale do personálu a jeho odborného vzdělávání.

6 POŽADAVKY NA PROVOZOVATELE KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

Existuje celá řada rizik, byť i vzdálených, které mohou způsobit i zánik civilizace. Musíme vzít na vědomí nejenom rizika, které ovlivňují vývoj ve světě a mají globální nebo kontinentální působnost, ale i národní a územní rizika. Nemůžeme přehlížet ani existenci ekonomických rizik a rizik, které ovlivňují ekonomický rozvoj zemí, podnikatelských subjektů a malých živnostníků. A nakonec tu je celá řada rizik, které mohou zásadním způsobem ovlivnit život každého člověka, rodiny a společnosti. Rizika tu vždy byly, jsou a budou a nelze je přehlížet, opomíjet, bagatelizovat ani ignorovat. Činnosti člověka jsou ohrožovány nežádoucími jevy, proti kterým se při každé činnosti snaží různými způsoby chránit. Stejně tomu tak je i u společností. Každá společnost se snaží chránit své aktivity proti nežádoucím jevům. Tato ochrana vstupuje do systému řízení každé společnosti a představuje její nedílnou součást.

6.1 Požadavky na provozovatele kritické informační infrastruktury ze zákona č. 240/200 Sb.

Krizové řízení je základem pro zajištění obrany a bezpečnosti státu. Je mnohem složitější a rozsáhlejší, než se na první pohled zdá. Nezabývá se jenom bezpečnostními riziky, ale i všemi dalšími riziky. Činnost související s krizovým řízením se nedotýká pouze orgánů krizového řízení, ale každého občana, firmy, podniku, společnosti, každého orgánu státní správy a samosprávy a všech ostatních prvků bezpečnostního systému státu a všech prvků kritické infrastruktury.

Prioritou krizového řízení je v první řadě ochrana zdraví a život občanů, která stojí jednoznačně nad všemi úkoly v mírovém životě. Další důležité úkoly jsou: ochrana kritické infrastruktury, ochrana majetku a životního prostředí. Cílem je potom realizace úkolů a opatření k zajištění ochrany zdraví, života osob, majetku, životního prostředí, zajištění obrany a bezpečnosti a zajištění trvale udržitelného rozvoje.

Definice některých vybraných pojmů podle zákona č. 240/2000 Sb., o krizovém řízení

Krizové řízení je souhrn řídících činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s:

- přípravou na krizové situace a jejich řešením, nebo
- ochranou kritické infrastruktury.

Na krizové řízení je možno pohlížet z hlediska užšího nebo širšího významu tohoto pojmu. V širším významu se realizují opatření v oblasti obnovy a prevence, v užším významu se realizují opatření v oblasti přípravy (zejména krizové plánování), řešení krizové situace a likvidačních prací.

Krizová situace je mimořádná událost, kdy dochází ke škodlivému působení sil a jevů vyvolaných činností člověka, přírodními vlivy a různými haváriemi, které ohrožují život, zdraví, majetek nebo životní prostředí a vyžadují provedení záchranných a likvidačních prací, kdy dochází k narušení kritické infrastruktury nebo k jinému nebezpečí, při nichž je vyhlášen stav nebezpečí, nouzový stav nebo stav ohrožení státu (krizový stav).

Krizová opatření jsou organizační nebo technická opatření určená k řešení krizové situace a odstranění jejích následků (mohou zasahovat i do práv a povinností osob).

Kritická infrastruktura – prvek kritické infrastruktury nebo systém prvků kritické infrastruktury. V případě narušení jejich funkcí by to mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob a ekonomiky státu.

Prvek kritické infrastruktury může být zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, která jsou určeny podle průřezových a odvětvových kritérií.

Subjektem kritické infrastruktury pak se rozumí provozovatel prvku kritické infrastruktury.

Ochrana kritické infrastruktury je soubor opatření, která jsou zaměřena na snížení rizika narušení funkce prvku kritické infrastruktury.

K zabezpečení služeb a hodnocení krizové situace v oblasti elektronických komunikací je zpracován typový plán pro typ krizové situace. Narušení poskytování veřejně dostupných služeb elektronických komunikací velkého rozsahu.

Typový plán obsahuje:

1. příčiny vzniku a trvání krizových situací;
2. scénář vývoje krizových situací;
3. dopady krizových situací na životy a poškození zdraví osob, zničení nebo poškození majetku;
4. poškození životního prostředí;
5. ekonomické dopady;
6. sociální dopady;
7. mezinárodní dopady atd.;
8. podmínky (předpoklady pro řešení krizových situací);
9. omezení (překážky) pro řešení krizových situací;
10. doporučené typové postupy, zásady a opatření v komunikačních systémech při řešení krizových situací a organizační údaje [9,18].

Zvláštní skutečnost - údaje z oblasti krizového řízení, které by v případě zneužití mohly vést k znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu právnické osoby nebo fyzické osoby vykonávající podnikatelskou nebo jinou obdobnou činnost podle zvláštních právních předpisů, pokud tyto údaje nejsou utajovanými informacemi.

6.2 Činnosti a povinnosti související s posuzováním, hodnocením a určováním prvků kritické infrastruktury

Problematika kritické infrastruktury (dále jen "KI") byla do právního řádu ČR začleněna úpravou zákona č. 240/200 Sb., o krizovém řízení. Důvodem byla nutnost implementace směrnice Rady č. 2008/114/ES o určování a označování

evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

KI včetně její ochrany svým charakterem patří do oblasti zachování základních funkcí státu a ochrany obyvatelstva. Zákon definuje KI jako prvek nebo systém prvků, jejichž narušení funkce by mělo vážný dopad na bezpečnost státu, zabezpečení základních životních potřeb, zdraví osob nebo ekonomiku státu. Prvky jsou určeny podle stanovených průřezových a odvětvových kritérií.

Jedním z předpokladů pro určení prvku KI je uplatnění odvětvových a průřezových kritérií. Odvětvová kritéria definují a stanovují jednotlivé gesční ústřední správní úřady (ministerstva). Ministerstvo vnitra (MV), které je gestorem celé této oblasti, jež předkládá vládě ČR ke schválení (nařízení vlády).

S kritickou infrastrukturou souvisí tedy pojmy:

a) **průřezová kritéria** - soubor hledisek pro posuzování závažnosti vlivu narušení funkce prvku KI s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně vážný ekonomický dopad nebo dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života;

b) **odvětvová kritéria** - jsou technické nebo provozní hodnoty k určování prvku KI v jednotlivě daných odvětvích.

Ministerstva a jiné ústřední správní úřady:

- navrhují odvětvová kritéria (za elektronické komunikace je to MPO ve spolupráci s ČTÚ - za krizové řízení);
- určují opatřením obecné povahy prvky KI (pouze v případě, kdy provozovatelem není organizační složka státu – jednoduše řečeno „prvky soukromých subjektů“) a informují MV jako gestora v této oblasti o této skutečnosti;
- v případě, kdy prvek je organizační složkou státu – splňuje kritéria, je na základě návrhu odpovědných ministerstev zařazen MV do seznamů prvků KI;

- kontrolují plány krizové připravenosti subjektů kritické infrastruktury a ochranu prvků kritické infrastruktury a ukládají opatření k nápravě nedostatků.

Kritéria pro výběr prvků kritické infrastruktury jsou stanovena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb.

Nařízení vlády č. 432/2010 Sb., se dotýkalo oblasti krizového řízení a řešení krizových situací jako jsou: přírodní katastrofy, průmyslové havárie a další [18].

Nařízení č. 315/2014 Sb., doplňuje původní nařízení v oblasti VI. Komunikační a informační systémy o část „G – oblast kybernetické bezpečnosti“., která souvisí, resp. se dotýká i všech původních částí oblasti č. VI., a navíc může zasáhnout i do dalších stanovených odvětvových kritérií.

Průřezová a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb.

Průřezová kritéria pro určení prvku kritické infrastruktury:

a) Oběti s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin.
b) Ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu.
c) Dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

Odvětvová kritéria pro určení prvku kritické infrastruktury související s oblastí komunikačních a informačních systémů jsou uvedena v kapitole VI - Komunikační a informační systémy:

A. Technologické prvky pevné sítě elektronických komunikací zahrnují centrum řízení a podpory sítě, řídící, mezinárodní a tranzitní ústředny, datové centrum a telekomunikační vedení.
B. Technologické prvky mobilní sítě elektronických komunikací zahrnují centrum řízení a podpory sítě, ústřednu mobilní sítě,

základnovou řídící jednotku sítě pokrývající strategickou lokalitu, základnovou stanici sítě pokrývající strategickou lokalitu a datové centrum sítě.

C. Technologické prvky sítí pro rozhlasové a televizní vysílání.
D. Technologické prvky pro satelitní komunikaci.
E. Technologické prvky pro poštovní služby.
F. Technologické prvky informačních systémů zahrnují řídící a datové centrum, síť elektronických komunikací a technologický prvkem zajišťující provoz registru doménových jmen "CZ" a zabezpečení provozu domény nejvyšší úrovně "CZ".
G. Oblast kybernetické bezpečnosti.
H. Informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahující 8 hodin.
I. Komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahující 8 hodin.
J. Informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách.
K. Komunikační systém, zajišťující připojení nebo propojení prvku KI, s kapacitou garantovaného datového přenosu nejméně 1Gbit/s.
L. Odvětvová kritéria pro určení prvku KI uvedená v písmenech A až F se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňující tato kritéria nezbytná pro zajištění kybernetické bezpečnosti.

V návaznosti na kritéria vyplývající z nařízení vlády č. 432/2010 Sb., část VI. Komunikační a informační systémy byly dle písm. a až f definovány jako subjekty kritické infrastruktury všichni operátoři?. Prvky a subjekty byly určeny opatřením obecné povahy [18].

Komunikační infrastruktura zastává v systému kritické infrastruktury státu důležitou úlohu. Zajišťuje komunikaci mezi prvky, resp. subjekty kritické infrastruktury státu, které tyto prvky provozují. Bez této komunikace by nebyla možná koordinace činností při záchranných pracích a eliminace

důsledků přírodních katastrof nebo včasné zajištění dodávek potřebných materiálů, technologií, pohonných hmot a maziv (PHM) a potravin, vody na místa, kde jsou zapotřebí. Komunikace je také velmi důležitá pro předávání informací mezi krizovými štáby, jejich členy a mezi výkonnými oddíly (hasiči, záchranáři, vojáci a další složky). Bez zajištěné komunikace se nedostanou důležité informace z postižených míst do krizových štábů a bez těchto informací nelze učinit dobrá rozhodnutí. Pokud se správná rozhodnutí nedostanou v pravý čas na správné místo, může mít toto selhání katastrofální následky pro obyvatelstvo a způsobit významné škody na majetku či dalších prvcích kritické infrastruktury státu.

Povinnosti určených subjektů kritické infrastruktury

V zákoně byly určeným prvkům kritické infrastruktury definovány také povinnosti. Vzhledem k uvedenému muselo být vymezeno, kdo bude za splnění těchto povinností odpovídat.

Zpracovávají plán krizové připravenosti subjektů kritické infrastruktury a ochranu prvků kritické infrastruktury.

Odpovídají za ochranu prvku kritické infrastruktury.

Musí umožnit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu vykonání kontroly plánu krizové připravenosti subjektu kritické infrastruktury a ochrany prvku kritické infrastruktury.

Plány krizové připravenosti subjektu kritické infrastruktury na základě nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., (plány krizové připravenosti subjektu kritické infrastruktury - § 17a, § 18), obsahují 3 části:

Základní – vymezení předmětu činnosti právnické nebo podnikající fyzické osoby, úkoly a opatření, které jsou důvodem pro zpracování plánu; charakteristiku krizového řízení, přehled a hodnocení možných zdrojů rizik a analýzy ohrožení a jejich možný dopad na činnost právnické nebo podnikající fyzické osoby; seznam prvků kritické infrastruktury; identifikaci možných ohrožení funkce prvku kritické infrastruktury;

Operativní – náležitosti zaměřené na ochranu funkce prvku kritické infrastruktury a stanovení opatření na jeho ochranu – způsob zabezpečení akceschopnosti k provedení krizových opatření; postupy řešení krizových

situací identifikovaných v analýze ohrožení; přehled spojení na příslušné orgány krizového řízení, apod.,

Pomocnou – náležitosti zaměřené na ochranu funkce prvku kritické infrastruktury – přehled právních předpisů použitých k přípravě na mimořádné události, krizové situace a jejich řešení; přehled uzavřených smluv k zajištění provedení opatření; geografické podklady a další dokumenty související s připraveností na mimořádné události a krizové situace a jejich řešení.

Již několikrát byl zmíněn pojem ochrana kritické infrastruktury. Zákon ji pojímá jako soubor činností a opatření, která povedou ke snížení rizika narušení funkce prvku kritické infrastruktury (plánovací dokumentace). Ochranná opatření musí vycházet z analýzy rizik ohrožující konkrétní prvek KI. Hlavním kritériem je posouzení zranitelnosti a možný dopad na činnosti prvku kritické infrastruktury. Systém ochrany musí být vytvořen na základě analýzy bezpečnostních hrozeb a rizik. Analýza pak definuje chráněná aktiva subjektu a identifikuje bezpečnostní hrozby. Na základě odhadu pravděpodobného projevení se hrozby a stanovení míry bezpečnostního rizika je jednotlivým bezpečnostním rizikům přiřazena pravděpodobnost jejich výskytu.

Základním opatřením subjektu KI pro stanovení a řízení komplexní bezpečnosti je bezpečnostní politika obsahující základní řídící a organizační předpis, který stanoví systém bezpečnosti, odpovědnost za její realizaci, vazby mezi jednotlivými prvky bezpečnosti, druhy a rámcový rozsah jednotlivých bezpečnostních opatření.

6.3 Bezpečnostní opatření ochrany kritické infrastruktury

Důležitou součástí systému ochrany kritické infrastruktury je zajištění bezpečnostních opatření k její ochraně. Bezpečnostní opatření řešíme v době, kdy má organizace ujasněny otázky definování kritické infrastruktury, resp. jejích jednotlivých prvků, to znamená, kdy víme, co máme chránit a proti čemu. Do úvahy je nezbytné vzít především ekonomické hledisko nákladů na opatření a to nejen ve vztahu k investicím, ale také k provozním nákladům na jejich funkčnost a udržování.

Bezpečnostním opatřením ochrany kritické infrastruktury se rozumí ucelený systém navzájem propojených opatření implementovaných s cílem zajistit

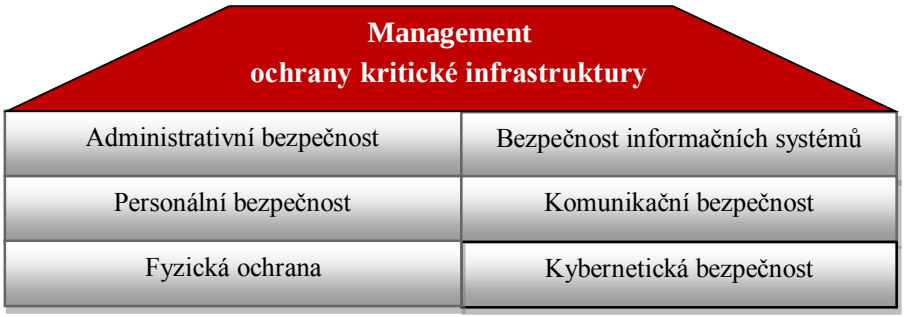
ochranu prvků kritické infrastruktury proti všem známým bezpečnostním rizikům. Opatření jsou zaměřená na ochranu proti vnějším rizikům. Jejich implementace je ovlivněna podmínkami jednotlivých odvětví kritické infrastruktury, která mají úzkou návaznost na provozní a technologickou bezpečnost. V praxi se tento přístup uplatňuje rozdílným způsobem zajištění prvků kritické infrastruktury.

Bezpečnostní opatření rozdělujeme na stálá a odstupňovaná [6].

- **Stálá bezpečnostní opatření** určují nezbytné investice do bezpečnosti a bezpečnostních prostředků, jejichž použití je kdykoliv opodstatněné. Tato oblast zahrnuje informace týkající se obecných opatření, jako jsou technická opatření (včetně instalace prostředků pro detekci, kontrolu přístupu, ochranu a prevenci); organizační opatření (včetně postupů varování a řešení krizí); kontrolní a ověřovací opatření; komunikace; zvyšování informovanosti a odborná příprava; bezpečnost informačních systémů.
- **Odstupňovaná bezpečnostní opatření** mohou být aktivována podle různého stupně rizika a ohrožení. Může to být například při zhoršení bezpečnostní situace, předpoklad teroristického útoku nebo válečného konfliktu. Odstupňovaná bezpečnostní opatření jsou naplánována a připravena za běžné situace. Aktivace se zpravidla provádí až při získání informací o možnosti napadení (př. aktivace záložních komunikačních kanálů, zajištění nebo posílení místního výkonu fyzické ochrany a podobně). Některé důležité objekty mohou být při zvýšené úrovni rizika střeženy ozbrojenými sbory.

6.3.1 Druhy bezpečnostních opatření pro ochranu kritické infrastruktury

Mezi základní druhy bezpečnostních opatření ochrany kritické infrastruktury patří:



Obr. 9. Schéma bezpečnostního systému ochrany KI *(zdroj [22])*

Jak již bylo uvedeno, bezpečnostní opatření ochrany kritické infrastruktury jsou popsaná v Plánu krizové připravenosti subjektu kritické infrastruktury. Součástí popisu jednotlivých bezpečnostních opatření musí být jejich úroveň (kvalita opatření) a rozsah počet prvků, jejich popis, umístění, apod.).

Uvedené informace a postupy se netýkají jenom a pouze oblasti kritické infrastruktury z pohledu krizového zákona. Některé další prvky (postupy) se již prolínají i s požadavky a postupy využívané i v oblasti kybernetické bezpečnosti.

6.3.2 Popis jednotlivých oblastí:

Management ochrany kritické infrastruktury je integrovaný systém řízení ochrany kritické infrastruktury. Zahrnuje nejen koncepci ochrany kritické infrastruktury ale i celý systém řízení (tj. bezpečnostní management kritické infrastruktury, postup implementace ochrany kritické infrastruktury, bezpečnostní dokumentaci, vzdělávání a proces životního cyklu bezpečnostního systému). Důležitou součástí managementu ochrany kritické infrastruktury jsou postupy při řešení jednotlivých typů mimořádných událostí a krizových situací.

Administrativní bezpečnost - souhrn opatření, která stanovují pravidla manipulace s dokumenty, popisují funkci kritické infrastruktury, a které je

nutné chránit před neoprávněnými osobami, a dokumenty popisující bezpečnostní opatření ochrany kritické infrastruktury. Do opatření administrativní bezpečnosti se zahrnuje také manipulace s médii, na kterých jsou tyto dokumenty ukládány.

Personální bezpečnost – patří mezi nejvýznamnější bezpečnostní opatření. Představuje výběr spolehlivých osob, které budou zajišťovat provoz prvků kritické infrastruktury a jejich bezpečnost, dále jejich vzdělávání a periodické ověřování jejich spolehlivosti vykonávat tyto funkce.

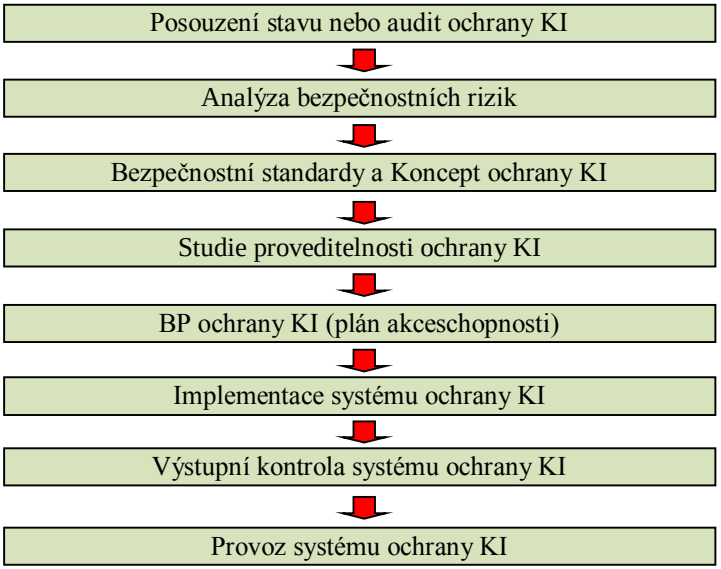
Bezpečnost informačních systémů tvoří systém opatření, jejichž cílem je zajistit důvěrnost, integritu a dostupnost informací, s nimiž tyto systémy nakládají, a odpovědnost správy a uživatele za jejich činnost v informačním systému a dále je podporován je rámcem opatření určených k ochraně řídicích a regulačních systémů prvků kritické infrastruktury. Součástí jsou také opatření bezpečnosti informačních systémů, které obsahují informace o ochraně kritické infrastruktury a také kryptografická ochrana. Bezpečnost informačních systémů kritické infrastruktury je založena na přísné bezpečnostní politice a periodickém ověřování úrovně bezpečnosti.

Komunikační bezpečnost se dotýká bezpečnosti přenosových cest využívaných pro řízení a regulaci funkčnosti prvků kritické infrastruktury. Součástí komunikační bezpečnosti je rovněž ochrana přenosových cest informačních systémů, které obsahují informace o ochraně kritické infrastruktury.

Kybernetická bezpečnost představuje systém opatření proti hrozbám kybernetické kriminality a kybernetického terorismu.

Fyzická ochrana - představuje systém opatření fyzické ostrahy technického zabezpečení a režimových opatření. Úroveň a rozsah opatření fyzické ochrany mohou být pro jednotlivé prvky kritické infrastruktury rozdílné.

6.3.3 Postup implementace bezpečnostních opatření kritické infrastruktury



Obr. 10. Možný postup implementace opatření. *(zdroj [22])*

Posouzení stavu ochrany KI

Jedním z kroků implementace bezpečnostních opatření ochrany kritické infrastruktury je posouzení jejich stávající úrovně nebo bezpečnostní audit. Posouzení řeší shodu s platným standardem a specifikuje doporučení pro odstranění neshod a posuzuje kvalitu opatření a ověřuje jejich funkčnost. Rozhodnutí, zda provést posouzení nebo audit bezpečnostních opatření, závisí především na těchto okolnostech:

- stav a systémovost bezpečnostních opatření;
- existence bezpečnostních standardů pro jednotlivá bezpečnostní opatření;
- etapa implementace bezpečnostního systému;
- existence výstupů z předchozích posouzení a auditů;
- zranitelnost kritické infrastruktury.

Analýza bezpečnostních rizik

Další krokem je vždy provedení analýzy bezpečnostních rizik nebo jejich aktualizace pro celý systém kritické infrastruktury i její jednotlivé prvky.

Analýza rizik musí definovat běžná rizika a zvýšená bezpečnostní rizika a měla by být provedena podle obecně uznávané metody ověřené při jiných aplikacích. Je vždy žádoucí, aby výstupy řešení byly verifikovány na základě expertního posouzení. Následně je nezbytné posoudit, zda jsou jednotlivé oblasti bezpečnostních opatření a jednotlivá opatření dostatečná pro analyzovanou úroveň bezpečnostního rizika.

Koncepce ochrany KI

Bezpečnostní opatření tvoří navzájem propojený bezpečnostní systém, který musí být budován podle jednotné koncepce a řízen z jednoho místa. Výchozím strategickým dokumentem v oblasti ochrany kritické infrastruktury by měla být Koncepce ochrany kritické infrastruktury, která by měla vycházet z analýzy bezpečnostních rizik a bezpečnostní politiky organizace. Součástí jsou bezpečnostní standardy. Pokud nejsou bezpečnostní standardy vydány, pak musí být zpracovány jako interní bezpečnostní norma provozovatele kritické infrastruktury. Je rámcem, který popisuje jednotlivé oblasti bezpečnostních opatření:

- základní cíle;
- odpovědnost za implementaci koncepce;
- popis současného stavu ochrany KI;
- popis očekávaného stavu ochrany KI;
- bezpečnostní standardy ochrany KI;
- bezpečnostní management ochrany KI;
- ochranu informací opatření ochrany KI;
- požadavky na výběr dodavatelů ochrany KI;
- rámcový harmonogram implementace koncepce ochrany KI.

Součástí koncepce ochrany KI jsou bezpečnostní standardy, které specifikují minimální úroveň ochrany pro jednotlivé kategorie objektů a druhy bezpečnostních opatření. Základem je kategorizace objektů, která je založena na významu prvků kritické infrastruktury v systému a rizikovosti. Ke každé kategorii jsou pak přiřazeny konkrétní požadavky na bezpečnostní opatření. Bezpečnostní standardy jsou základem optimalizace bezpečnostních opatření. Je vhodné, aby standardy zahrnovaly také požadavky na bezpečnostní technologie, a musí být zpracovány pro běžná bezpečnostní rizika a zvýšenou úroveň bezpečnostních rizik.

Studie proveditelnosti ochrany KI

Následujícím krokem při implementaci bezpečnostních opatření je studie proveditelnosti ochrany kritické infrastruktury. Zpracovává s cílem navrhnout systém bezpečnostních opatření pro konkrétní objekty. Nejčastěji se studie proveditelnosti zpracovávají pro opatření fyzické ochrany, řeší rozsah bezpečnostních opatření a musí specifikovat náklady na zavedení bezpečnostních opatření a na jejich provoz. Součástí je rovněž harmonogram implementace bezpečnostních opatření pro konkrétní objekty. Studie je pak podkladem pro projektování bezpečnostních systémů nebo součástí zadávací dokumentace pro výběr dodavatele bezpečnostních opatření.

Bezpečnostní projekt ochrany KI

Bezpečnostní projekt ochrany KI je v terminologii krizového řízení také nazýván Plánem akceschopnosti. Ten může být zapracován do operativní části Plánu krizové připravenosti subjektu kritické infrastruktury nebo je zde jen stručně popsán a tvoří samostatný dokument, který je doložen v přílohách plánu. Obsahuje podrobný popis bezpečnostních opatření, která jsou rozpracována pro jednotlivé prvky kritické infrastruktury a která jsou odstupňována pro běžnou a zvýšenou úroveň bezpečnostních rizik. Dále obsahuje odpovědnost za funkčnost bezpečnostních opatření a způsob provádění jejich kontrol, popisuje postupy ochrany při jednotlivých druzích ohrožení kritické infrastruktury včetně obnovy bezpečnostních opatření v případě jejich narušení. Do bezpečnostního projektu jsou zahrnuta také bezpečnostní opatření, která nejsou doposud implementována, a jejich doplnění vyplynulo z analýzy bezpečnostních rizik. K těmto opatřením je doložen harmonogram jejich implementace.

Implementace ochrany KI

Implementace je fáze zavádění jednotlivých bezpečnostních opatření do „života“. Zahrnuje výběr dodavatelů bezpečnostních opatření, řízení a monitoring jejich dodávek, školení pracovníků, kteří se budou na ochraně kritické infrastruktury podílet a aktivaci jednotlivých opatření, včetně zkušebního provozu. Forma ověření shody implementačních bezpečnostních opatření s bezpečnostním projektem je výstupní bezpečnostní audit.

Provoz systému ochrany KI

Provoz systému ochrany kritické infrastruktury představuje fázi, která navazuje na implementaci. V rámci provozu je nezbytné zajistit veškeré funkce bezpečnostních opatření deklarované v bezpečnostním projektu. Součástí provozu je ověřování funkčnosti bezpečnostních opatření a jejich zdokonalování. Provoz systému je nutné zajistit při běžné i zvýšené úrovni bezpečnostních rizik. Pozornost je nutné věnovat také managementu bezpečnostních incidentů a funkčnosti bezpečnostních opatření při nich. Postupy při řešení jednotlivých typů ohrožení je nezbytné nejen nastavit a proškolit, ale také procvičovat a zdokonalovat [11].

6.4 Požadavky pro provozovatele kritické informační infrastruktury vyplývající ze zákona č. 181/2014 Sb.

Oblast kybernetické bezpečnosti nabývá neustále na novém významu. Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného a odolného kyberprostoru v ČR, a to jak pro subjekty veřejného a soukromého sektoru, tak pro širokou veřejnost. Kybernetická bezpečnost pomáhá identifikovat, hodnotit a řešit hrozby v kyberprostoru, snižovat kybernetická rizika a eliminovat dopady kybernetických útoků, informační kriminality, terorismu a kybernetické špionáže ve smyslu posilování důvěrnosti, integrity a dostupnosti dat, systémů a dalších prvků informační a komunikační infrastruktury. Velmi zjednodušeně lze říci, že kybernetická bezpečnost je bezpečnost informací v digitální podobě a to od okamžiku jejich pořízení, během přenosu, zpracování až po uložení. Informace mají být chráněny proti odcizení, kompromitaci, modifikaci v celém svém životním cyklu [1].

Kyberprostor je virtuální, nehmotný prostor uvnitř elektronické komunikační sítě a zahrnuje veškeré dění, všechny prostory, veškeré zapojené entity, definice, práva, povinnosti, vazby a také množinu sítí více či méně od internetu oddělených. Pokud hovoříme o kybernetické bezpečnosti, pak se naše snahy o tuto bezpečnost mnohdy z velké části odehrávají právě v kyberprostoru. Důvod je jednoduchý, události odehrávající se v kyberprostoru, mají mnohdy více či méně závažné a někdy i fatální důsledky v reálném prostoru. Stačí si představit výpadek mobilní sítě.

S ohledem na rychlý technický pokrok se dostáváme do situace, kdy žijeme ve dvou světech, v reálném světě a virtuálním světě (kyberprostoru). V kyberprostoru dochází k vytváření množství subprostorů, které se řídí vlastními pravidly. Virtuální svět je mnohem hůře předvídatelný, mnohem hůře kontrolovatelný, mnohem hůře uchopitelný. I přesto je to prostředí, na kterém jsme naprosto dobrovolně závislí. A čím je společnost vyspělejší, tím, je závislost větší.

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Závislost veřejného a soukromého sektoru i zbytku společnosti na informačních a komunikačních technologiích se stává stále zřetelnější. Ochrana informací a jejich sdílení je v dnešní době zásadní pro bezpečnost obyvatelstva, ekonomiku státu a bezpečnost průmyslových provozů.

6.5 Dílčí závěr

Informační a komunikační bezpečnost, řízení rizik, krizové řízení a kritická infrastruktura, zachování kontinuity apod. jsou vzájemně propojené problematiky, které vedou k tomu, aby byla organizace připravena na řešení případných krizových situací, aby byla náležitě chráněna před hrozbami, které mohou takové krizové situace vyvolávat, a aby zachovala kontinuitu své činnosti i za nepříznivých okolností. Provozovatel prvku kritické infrastruktury odpovídá za jejich ochranu a to znamená, že všechny své činnosti musí mít zaměřené na zajištění funkčnosti, nepřetržitosti a celistvosti kritické infrastruktury s cílem zabránit hrozbě, riziku nebo zranitelnosti, zmírnit je a neutralizovat.

Současné nastavené právní podmínky a požadavky resp. povinnosti kladené na provozovatele informačních a komunikačních technologií dávají záruku zabezpečení vybudovaných hodnost, zajištění bezpečnosti nejenom ve státní sféře, ale i soukromé a schopnost lépe čelit novým a sofistikovanějším hrozbám. Zlepšování úrovně informační bezpečnosti ve státních institucích bude realizováno mimo jiné zaváděním systému řízení informační bezpečnosti – ISMS [16].

Bezpečné a spolehlivé fungování informačních a komunikačních technologií (ICT) je nezbytné pro fungování státních i veřejných struktur a je jedním ze základních předpokladů prosperity a trvalého ekonomického růstu Neustále roste podíl lidských činností a produkce přímo či nepřímo závislé na

fungování ICT. Sítě a online služby musí být nejenom bezpečné a odolné, ale také spolehlivé. Celá společnost musí zvyšovat svoje aktivity zaměřené na oblast bezpečnosti a spolehlivosti ICT. Nezbytnou součástí funkce systému ochrany kritické infrastruktury je zavedení ověřování účinnosti opatření přijímaných k její ochraně.

7 ANALÝZA RIZIK

Člověk a lidské jednání je ovlivňováno především obavou o svůj život, život blízkých a pocitem ohrožení majetku. Na vytváření stabilního bezpečného prostředí má zásadní vliv lidské chování v čase a místě. V souvislosti s tím je tedy osobním zájmem každého dodržovat sobě vlastní míru bezpečnosti v závislosti na úrovni svého poznání k udržení osobní potřeby žít bezpečně. Tato potřeba, tedy její míra, je dána individuálně, a proto nelze hovořit o pevné stabilitě bezpečnosti ve společnosti, kde je základním článkem vždy jednotlivec s demokraticky danými možnostmi. Procesy spojené s lidskými pohnutkami nelze přesně zachytit, jsou však vyhledávány inovativní metody nebo aplikace osvědčených nástrojů používaného ve strukturách jiných odvětví, které jsou aplikovány do oblastí, kde doposud použity nebyly. Cílem těchto metod je alespoň částečně zpřesnit a identifikovat rizika spojená s procesními scénáři, tedy fenomény lidského jednání.

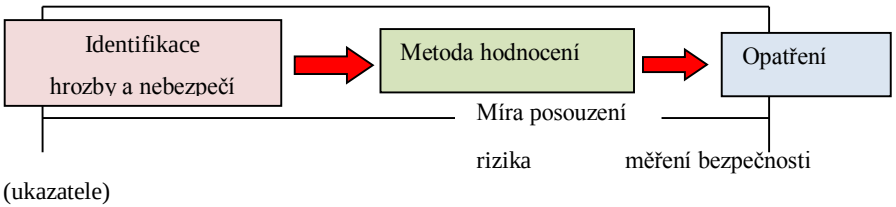
Komplexnost bezpečnosti (angl. safety) vychází z toho, že se jedná o soubor opatření k ochraně a rozvoji lidského systému, při kterém je stanovena přijatelná pravděpodobnost vzniku újmy na chráněných zájmech.

7.1 Metodiky hodnocení rizik

Pro analýzu a hodnocení rizik je v současné době k dispozici řada metodik a postupů i softwarových nástrojů. Jsou to postupy, které přispívají k rozvoji poznání a jsou velmi důležité v praxi. Slouží pro potřeby řízení a tvoří podklady pro rozhodovací proces. Je zapotřebí nejprve vyhodnotit, zda údaje a data, která jsou k dispozici, mají vypovídací hodnotu z hlediska rizik a zda jsou tato data použitelná u vybrané metodiky. Z toho vyplývá, že pracovní postupy musí respektovat určité požadavky, které zaručují správné a kvalifikované rozhodování a proaktivní řízení, které je nejlepším nástrojem pro zajištění ochrany, bezpečnosti a rozvoje státu či organizace.

Hodnocení rizik je možno provést jen na základě konkrétních, pravdivých a ověřených datových souborů o dané živelní pohromě, nehodě, havárii, útoku apod., které platí pro fyzikálně správně definovaný prostor či území a pro fyzikálně správně definovaný časový interval. Cílem je zajistit rozhodování ve prospěch věci. Proto musí být používán otestovaný soubor kritérií, který zaručuje objektivitu, nezávislost a nezaujatost hodnocení. V řadě případů jsou

posuzované problémy komplexní nebo mají mnoho nejistot a neurčitostí, což způsobuje, že je třeba použít multikriteriální expertní metody [11].



Obr. 11. Metodika vyhodnocení rizika *zdroj [22])*

Proto každý manažer musí z hlediska žádoucího cíle hodnocení rizik nejprve vyhodnotit, zda jsou splněny předpoklady předmětné metodiky, poté musí zhodnotit, zda jeho datové soubory mají vypovídací hodnotu, jejíž rizika chce sledovat. Teprve poté je možno provést výpočet. Interpretaci výsledků výpočtu lze provést v rozsahu, který je určen metodou, ale i osobní invencí a úsudkem řešitelů daných praxí a znalosti oboru. Jednotlivé metody analýzy rizik jsou tedy jen pomocným nástrojem posuzovatele., který vychází ze svých praktických zkušeností, předpisů a statistických údajů. Je prospěšné, pokud se na analýze rizik podílí více posuzovatelů za účelem srovnání a vyhodnocení výsledků.

Vzhledem ke složitosti a rozmanitosti vzniku živelních pohrom, nehod, havárií, útoků apod. na jedné straně a kvality, vypovídací schopnosti a homogenity dostupných datových souborů na straně druhé, není možno vypracovat žádné obecné pokyny pro stanovení rizik.

Vždy je třeba nejprve provést odborné posouzení:

- vstupních dat;
- požadavků a předpokladů určité metodiky;
- konkrétního cíle analýzy a hodnocení rizik;

a na základě tohoto posouzení provést výběr vhodného postupu.

Výběr vhodné metodiky určení rizik závisí na tom, zda:

- známe nebo můžeme stanovit rozložení živelních pohrom, nehod, havárií, útoků apod. v prostoru a v čase a můžeme spočítat četnostní rozložení živelních pohrom, nehod, havárií, útoků apod. (počet

vs. velikost) pro určité území a zvolený časový interval, dále vypočítat a zmapovat ohrožení;

- známe nebo můžeme stanovit rozložení dopadů živelních pohrom, nehod, havárií, útoků apod., stanovit scénáře dopadů ve variantním provedení a pravděpodobnosti jejich výskytů.

Základní metody pro stanovení rizik

Každá z existujících metod pro stanovení rizik, včetně těch dále uvedených, byla generována pro určitý specifický problém, proto jednotlivá paradigma nejsou vzájemně porovnatelná. Charakteristika obvykle používaných postupu pro stanovení rizik je podle [10, 18] následující:

1. Check List - CA (kontrolní seznam)

Kontrolní seznam je postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek (check list) jsou zpravidla generovány na základě seznamu charakteristik sledovaného systému nebo činností, které souvisejí se systémem a potenciálními dopady, selháním prvků systému a vznikem škod. Mají formu souboru otázek nebo témat, které je nezbytné brát při identifikaci do úvahy. Postupovat by se mělo definováním požadavků a norem; na tomto základě vytvořit soubor otázek orientovaných na nedostatky a rozdíly ve srovnání se standardem. Jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout různou relativní důležitost parametru (váhu) v rámci daného souboru.

2. Safety Review (bezpečnostní prohlídka)

Prohlídky resp. kontroly jsou zaměřené na posouzení stavu bezpečnosti provozů a procesů a lze je považovat za jedny z prvních metod posuzování nebezpečných situací a rizik. Jedná se v podstatě o fyzickou prohlídku zařízení, která může být uskutečňována expertním týmem nebo jednotlivcem. V případě nového provozu, se jedná o posuzování dokumentace ještě před zahájení výstavby či spuštění provozu. Tato prohlídka má za cíl identifikaci podmínek a okolností, které můžou vést k nehodě a tím k následkům a ohrožení zdraví lidí, poškození životného prostředí nebo majetku.

3. What – If Analysis (analýza toho, co se stane když)

Tato metoda je založena na určité formě brainstormingu, při kterém kvalifikovaný expertní tým prověřuje formou dotazů a odpovědí neočekávané události, které se můžou v procesu výroby vyskytnout. Identifikují se zde možná selhání a jejich následky formou tvořivých pracovních porad, kterých se zúčastňuje vybraná skupina expertů s cílem odhadnout následky vzniklého stavu či situace a samozřejmě návrh opatření a doporučení pro jejich prevenci a řešení. Prověřování se může týkat budov, energetického systému, surovin, produktů, skladů, prostředí provozu, pracovních postupů či provozní bezpečnosti. Pro relevanci výstupů a výsledků této studie je důležitá znalost procesů, kvalita expertního týmu, aplikační zkušenost týmu a další skutečnosti. Není to vnitřně strukturovaná technika jako některé jiné (např. HAZOP a FMEA). Namísto toho po analytikovi požaduje, aby přizpůsobil základní koncept šetření určitému účelu.

4. Preliminary Hazard Analysis – PHA (předběžná analýza ohrožení)

Předběžná analýza ohrožení – též kvantifikace zdrojů rizik je postup na vyhledávání nebezpečných stavů či nouzových situací, jejich příčin a dopadů a na jejich zařazení do kategorií dle předem stanovených kritérií. Koncept PHA ve své podstatě představuje soubor různých technik, vhodných pro posouzení rizika. V souhrnu se nejčastěji pod touto zkratkou jedná o následující techniky posuzování: what-if; what-if/checklist; hazard and operability (HAZOP) analysis; failure mode and effectsanalysis (FMEA); faulttreeanalysis; kombinace těchto metod; ekvivalentní alternativní metody

5. Process Quantitative Risk Analysis - QRA (analýza kvantitativních rizik procesu)

Kvantitativní hodnocení rizika se používá pro stanovení rizika při provozu, manipulaci, transportu a skladování nebezpečných látek. Kvantitativně se riziko hodnotí v případech, kdy se nebezpečné látky nacházejí na určitém konkrétním místě (průmyslová oblast, dopravní komunikace) v takovém množství, že mohou ohrožovat okolí. Analýza kvantitativních rizik procesu je koncept, který rozšiřuje kvalitativní (zpravidla verbální) metody hodnocení rizik o číselné hodnoty. Algoritmus využívá kombinaci (propojení) s jinými známými koncepty a směřuje k zavedení kritérií pro rozhodovací proces,

potřebnou strategii a programy k efektivnímu zvládání (řízení) rizika. Vyžaduje náročnou databázi a počítačovou podporu.

6. Hazard Operation Process – HAZOP (analýza ohrožení a provozuschopnosti)

HAZOP je postup založený na pravděpodobnostním hodnocení ohrožení a z nich plynoucích rizik. Jde o týmovou expertní multi-oborovou metodu. Hlavním cílem analýzy je identifikace scénářů potenciálního rizika. Využitím metody hazard analysis je vyhodnocen nebezpečný stav, který byl odhalen studiem provozuschopnosti. Výstupem a výsledkem je často kvalitativní parametr, vzhledem k absenci potřebných vstupních údajů. Kvantitativní vyhodnocení je možné realizovat pomocí metody logického stromu, který se skládá z objevených primárních příčin, jejich vzájemných závislostí a logických pravidel. HAZOP analýza může být použita i pro posouzení předběžného návrhu technologického procesu, či konečného návrhu projektu. Často se využívá i při vyhodnocování různých variant modifikací v zařízení či jako nástroj na zkoumání havarijních situací, které se v minulosti vyskytli. Identifikované neplánované nebo nepřijatelné dopady jsou formulovány v závěrečném doporučení, které směřuje ke zlepšení procesu.

7. Event Tree Analysis – ETA (analýza stromu událostí)

Analýza stromu událostí je postup, který sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Metoda ETA je graficky statistická metoda. Jedná se o induktivní systematický postup rozvíjející iniciační událost postupnými logickými kroky, kterými se berou do úvahy tzv. bezpečnostní funkce systému spolu s jejich úspěšností. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Výsledkem je logický graf rozvoje iniciační události a pravděpodobnostní hodnocení scénářů s ohledem na různé možné následky. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu. Vyhodnocením se získávají pravděpodobnosti uvažovaných konečných stavů. Takto je možné stanovit pravděpodobnost postupnosti poruch a navrhnou úpravy vedoucí ke zlepšení:

8. Failure Mode and Effect Analysis – FMEA (analýza selhání a jejich dopadů)

Jedná se o významnou metodu pro identifikaci nebezpečí v průmyslových zařízeních. Analýza selhání a jejich dopadů je postup založený na rozboru způsobů selhání a jejich důsledků, který umožňuje hledání dopadů a příčin na základě systematicky a strukturovaně vymezených selhání zařízení.

Metoda FMEA slouží ke kontrole jednotlivých prvku projektového návrhu systému a jeho provozu, u kterých jsou neustále rostoucí požadavky na spolehlivost a kvalitu výrobků či procesů, kde je velké množství komponentů a subsystémů či tlak na ekonomizaci procesů. Představuje metodu tvrdého, určitého typu, kde se předpokládá kvantitativní přístup řešení. Vyžaduje aplikaci počítačové techniky, speciální výpočetní program, náročnou a cíleně zaměřenou databázi.

9. Fault Tree Analysis – FTA (analýza stromu poruch)

Metoda stromu poruch byla vyvinuta pro potřeby elektrotechniky, rozvíjená v letectvu a široké uplatnění našla v jaderné energetice. Analýza stromu poruch je postup založený na systematickém zpětném rozboru událostí za využití řetězce příčin, které mohou vést k vybrané vrcholové události. Metoda FTA je graficky analytická popř. graficky statistická metoda. Názorné zobrazení stromu poruch představuje rozvětvený graf s dohodnutou symbolikou a popisem. Sestavení stromu poruch má řadu kroků, přičemž se vychází z vrcholové události, kterou analyzujeme. V dalších krocích se hledají určitá varovné znamení, že vrcholová událost nastane v jednotlivých subsystémech. Důležitým krokem je posouzení logického vztahu mezi iniciačními událostmi a vrcholovou událostí. Náročnost této metody souvisí s přípravnou fází, kde je potřebné vyřešit velké množství úkolů (přesně stanovit vrcholovou událost, stanovit přesné podmínky a okolnosti, která musí nastat, aby taková událost vznikla, stanovit fyzikální hranice systému a jiné).

10. Human Reliability Analysis – HRA (analýza lidské spolehlivosti)

Analýza lidské spolehlivosti je postup na posouzení vlivu lidského činitele na výskyt pohrom, nehod, havárií, útoků apod. či některých jejich dopadů. Koncept analýzy lidské spolehlivosti HRA směřuje k systematickému posouzení lidského faktoru (Human Factors) a lidské chyby (Human Error).

Ve své podstatě přísluší do zastřešující kategorie konceptu předběžného posuzování PHA. Zahrnuje přístupy mikro ergonomické (vztah „člověk-stroj“) a makro ergonomické (vztah systému „člověk-technologie“). Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Uplatnění metody HRA musí vždy tvořit integrovaný problém bezpečnosti provozu a lidského faktoru v mezních situacích různých havarijních scénářů, tzn. paralelně a nezávisle s další metodou rizikové analýzy.

11. Fuzzy Set and Verbal Verdict Method – FL-VV (metoda mlhavé logiky verbálních výroku)

Metoda mlhavé logiky a verbálních výroků je metoda založená na jazykové proměnné. Jde o více kriteriální metodu rozhodovací analýzy z kategorie měkkého, mlhavého typu. Opírá se o teorii mlhavých množin a může být aplikována v různých obměnách, jednak samostatně s přímým výstupem priorit, anebo jako stupnice v pomocných bodech, namísto standardní verbálně-numerické stupnice v relativních jednotkách, tj. ve spojení s metodou TUKP – Totálního ukazatele kvality prostředí (možnost uplatnění axiomatické teorie kardinálního užitku). Umožňuje aplikaci jednotlivcem i v kolektivu.

12. Relative Ranking – RR (relativní klasifikace)

Relativní klasifikace je ve skutečnosti spíš analytická strategie než jednoduchá dobře definovaná analytická metoda. Tato strategie umožňuje analytikům porovnat vlastnosti několika procesů nebo činností a určit tak, zda tyto procesy nebo činnosti mají natolik nebezpečné charakteristiky, že to analytiky opravňuje k další podrobnější studii. Relativní klasifikace může být použita rovněž pro srovnání několika návrhů umístění procesu nebo zařízení a zajistit tak informace o tom, která z alternativ je nejlepší nebo méně nebezpečná. Tato porovnání jsou založena na číselných srovnáních, která reprezentují relativní úroveň významnosti každého zdroje rizika.

13. Causes and Consequences Analysis - CCA (analýza příčin a dopadů)

Analýza příčin a dopadů je směs analýzy stromu poruch a analýzy stromu událostí. Největší předností CCA je její použití jako komunikačního prostředku: diagram příčin a dopadů zobrazuje vztahy mezi koncovými stavy

nehody (nepřijatelnými dopady) a jejich základními příčinami. Protože grafická forma, jež kombinuje jak strom poruch, tak strom událostí do stejného diagramu, může být hodně detailní, užívá se tato technika obvykle nejvíce v případech, kdy logika poruch analyzovaných nehod je poměrně jednoduchá. Jak už napovídá název, účelem analýzy příčin a dopadů je odhalit základní příčiny a dopady možných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod.

14. Probabilistic Safety Assessment – PSA (metoda pravděpodobnostního hodnocení)

Metoda stanovuje příspěvky jednotlivých zranitelných částí k celkové zranitelnosti celého systému. Tato technologie se používá např. k modelování scénářů hypotetických jaderných havárií, které vedou k tavení aktivní zóny a k odhadnutí četnosti takových havárií. V zemích OECD byly doposud zpracovány stovky studií PSA. Metodika PSA se skládá z: pochopení systému jaderného zařízení a ze shromáždění relevantních dat o jeho chování při provozu; identifikace iniciačních událostí a stavu poškození jaderného zařízení; modelování systému a řetězců událostí pomocí metodiky založené na logickém stromu; hodnocení vztahů mezi událostmi a lidskými činnostmi; vytvoření databáze dokumentující spolehlivost systému a komponent.

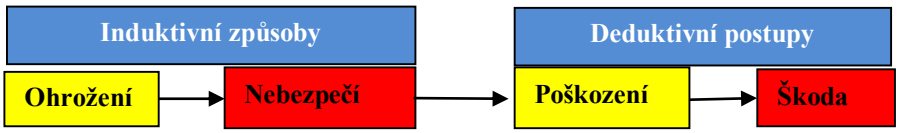
Všeobecně se v odborné praxi přijímá, že při použití metodiky, která není všeobecně známá, je nutno použitou metodiku důkladně popsat a popř. ji na příkladu srovnat s některou ze známých metodik.

Počítačová podpora a softwarové produkty

V dnešní době velkého rozvoje informačních technologií (IT) je k dispozici mnoho (několik set až tisíc) softwarových produktů, zaměřených na hodnocení rizik; všeobecně známých je asi patnáct. Softwarové produkty jsou založeny na fyzikálních modelech jednodušších či složitějších, což pochopitelně předurčuje lepší či horší správnost a spolehlivost výsledků. Většinu z existujících software, popsaných v odborné literatuře lze použít jen k hodnocení určitých typových případů. Interpretaci výsledků lze provést pouze v rozsahu, který je určen předpoklady metody a modelu, kterým software odpovídá.

Před použitím softwarového produktu, je třeba provést analýzu stejného typu, jako byla zmíněna výše u výběru metodik stanovení rizik. Analýza rizik je nezbytná pro stanovení přijímaného rizika i nepřijatelného rizika, Na základě těchto faktů stát používá k zajištění udržitelného rozvoje nástroje označovaného jako řízení rizik a řízení bezpečnosti, které zajišťují odstranění, zmenšení či alespoň zmírnění zjištěných nepřijatelných rizik opatřeními technickými, právními, výchovnými, ekonomickými a organizačními [9].

Riziko závisí, co se týká jeho snižování, na ochranných opatřeních, nebo jinak řečeno na inovaci chráněného systému, kterou můžeme toto riziko snižovat nebo jej dělit. Riziko je nejistota násobená nežádoucími následky. Nebezpečím je vlastnost předmětu či situace s potenciálem pro vytvoření škody. Bezpečnost lze obecně definovat jako agregovaný popis determinantů, které je potřeba udržovat v akceptovatelných mezích klidového stavu, nebo také, že bezpečnost je stav, při kterém vznik újmy na životech a zdraví lidí, majetku, životním prostředí, společnosti a kritické infrastruktuře má přijatelnou pravděpodobnost. Při posuzování ochrany objektu kritické infrastruktury je nutné identifikovat řetězec „**ohrožení-nebezpeční-poškození-škod**a“.

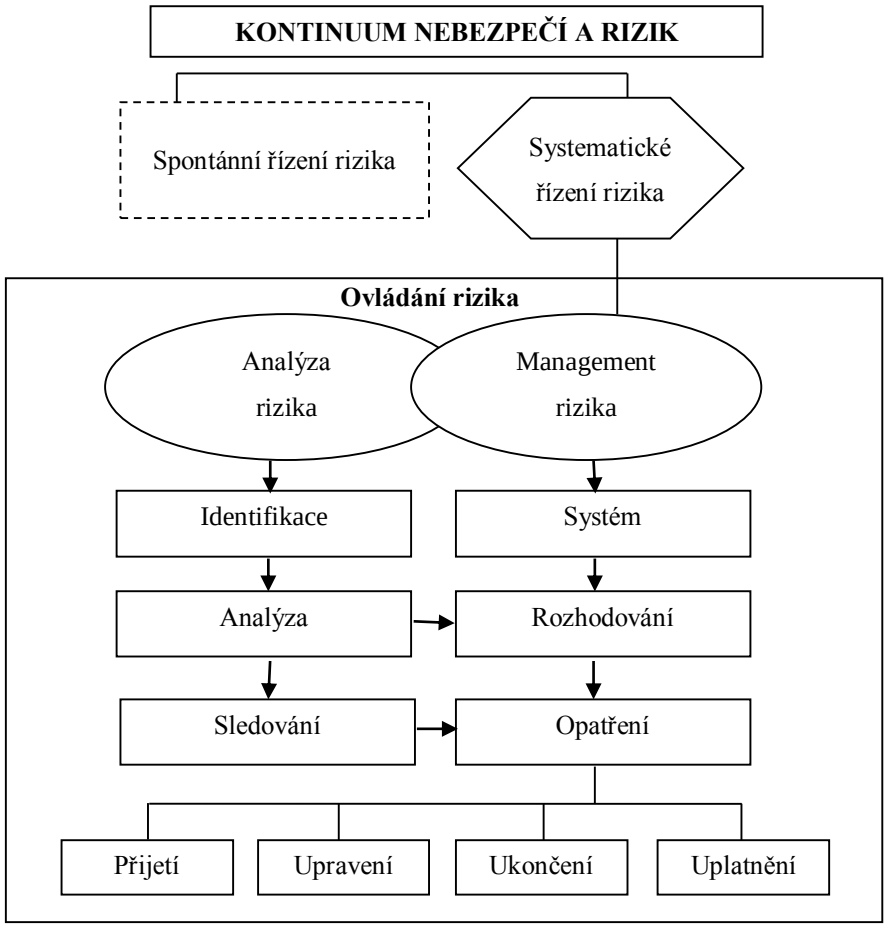


Obr. 12. Vzájemný vztah jednotlivých subjektů. *(zdroj [22])*

Následuje stanovení vhodné metody analýzy a výpočet rizika, včetně verifikace výsledků. Poté posuzujeme rizika podle stupnice, vybíráme optimální řešení k minimalizaci rizika a zavádíme nová opatření (technická nebo organizační), školení personálu, popřípadě doplnění pojištění a přijetí akceptovatelného nezbytného rizika.

Poté, co jsou vybrána opatření k optimalizaci systému do praxe, následuje management rizik, kam patří monitorování rizik, přezkoumávání a přehodnocování rizik a přizpůsobení hodnocení rizik změnám, které nastaly za nových podmínek. Úspěšné zavedení procesu řízení rizik vyžaduje rozdělení odpovědnosti. V modelu „Plánuj – Dělej – Kontroluj – Jednej“ (Plan-Do-Check-Act = PDCA). Při posuzování projektu bezpečnosti objektu

kritické infrastruktury nebo organizace vycházíme ze tří fází. V primární fázi zjišťujeme stav systému, stav prostředí a formulujeme záměry a bezpečnostní politiku organizace. Ve fázi sekundární přistupujeme k analýze rizika a na ni navazuje fáze terciální, ve které je realizováno plánování a sestavení směrnic a předpisů.



Obr. 13. Blokové schéma – kontinuum nebezpečí a rizik *(zdroj [11])*

Prvním krokem analýzy je stanovení aktiv, tedy co má být chráněno, Dále před čím se chráníme (útok, únos, loupež) a jakým způsobem ochranu zajistit. Je nutno posoudit, jak veliká je pravděpodobnost, že v konkrétním případě (místo, čas, osoby, okolnosti, apod.) vzniknou následky a jaké velké a nákladné mohou být? Každá z existujících metod pro stanovení rizik byla

vytvořena pro specifický problém. Metodik pro analýzu a hodnocení rizik je celá řada a přibývají další. Tyto metody lze aplikovat případně i na jiné objekty, vždy však s ohledem na původní účel. Kritérium výběru metod byla jejich dostupnost a rozšíření jejich aplikace v současné bezpečnostní praxi.

Posuzování hodnoty aktiva je založeno na velikosti škody způsobené zničením či ztrátou aktiva. Obvykle se při stanovení hodnoty aktiva vychází z jeho nákladových charakteristik, mohou to být ale i charakteristiky výnosové (pokud aktivum přináší dobře identifikovatelné zisky či jiné přínosy). Následuje identifikace rizik, která se provádí tak, že se vybírají ta, která by mohly ohrozit alespoň jedno z aktiv. Každé riziko se hodnotí vůči každému aktivu samostatně. Je vhodné nejdříve provádět orientační analýzu rizik pro následné rozhodování o volbě metody pro následnou vlastní „velkou" analýzu rizik konkrétního objektu kritické infrastruktury.

Primárně je tedy provedena orientační analýza rizik za účelem posouzení, který z objektů je klíčový z hlediska kritické infrastruktury a který je vystaven značným rizikům. Pro tyto objekty se následně provede detailní analýza rizik.

Poté následuje detailní hodnocení identifikovatelných rizik s následným určením jejich pořadí podle závažnosti jejich vlivu na aktivitu objektu.

Při vlastní analýze rizik se vychází z toho, že metody analýzy rizika mimo jiné dělíme na analýzy kvalitativní, semikvantitativní a kvantitativní.

Kvalitativní metody se vyznačují tím, že rizika jsou vyjádřena v určitém rozsahu (například jsou obodována <1 až 10>, nebo určena pravděpodobností <0;1> nebo slovně). Kvalitativní metody jsou jednodušší a rychlejší, ale více subjektivní.

Kvantitativní metody jsou založeny zpravidla na metodickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu a jsou mnohem přesnější.

Semikvantitativní metody doplňují kvalitativní hodnocení bodovými hodnotami. Cílem je vytvořit bodové škály, které jsou detailnější a potenciál verifikace mezi objekty je vyšší než u kvalitativní analýzy. Při identifikaci rizik postupujeme na základě stanovených cílů a rizika identifikujeme nejdříve z hlediska procesního, tedy vyhledáváme rizika způsobená lidským faktorem, která považujeme za mnohem nebezpečnější než následná rizika

identifikována z hlediska strukturálního (konstrukčního), způsobená především technickou nebo strukturální chybou [11].

7.2 Stupnice hodnocení důležitosti rizik

Kritické (Kategorie A)

komponenty, při jejichž výpadku, omezení nebo jakémkoli případně velmi krátkém přerušení dojde k zásadnímu ohrožení klíčových zájmů organizace a ke vzniku škod velkého rozsahu. Kritické komponenty je třeba zajišťovat nepřetržitě nebo jen s velmi omezenými výpadky, přičemž musí být tato maximální přípustná doba výpadku stanovena.

Nezbytné (Kategorie B)

Komponenty, při jejichž výpadku, omezení nebo přerušení na delší dobu se tyto komponenty stávají kritickými a může dojít k vážnému ohrožení zájmů organizace. V době nedostupnosti, nefunkčnosti nebo přerušení nezbytných komponent může mít organizace vážné problémy. Nezbytné komponenty musí být obnoveny co nejdříve, ovšem nejpozději do doby, kdy získají plně charakter kritických komponent, přitom tato doba musí být definována.

Zbytné (Kategorie C)

Komponenty, u kterých ani delší výpadek, nedostupnost, nefunkčnost nebo přerušení nezpůsobí organizace vážné problémy. Obnovení zbytných komponent je prováděno až po zajištění komponent kritických a nezbytných s tím, že musí být provedeno nejpozději do doby, která je stanovena. Některé zbytné komponenty mohou být dočasně po delší dobu zastoupeny jinými komponentami [23].

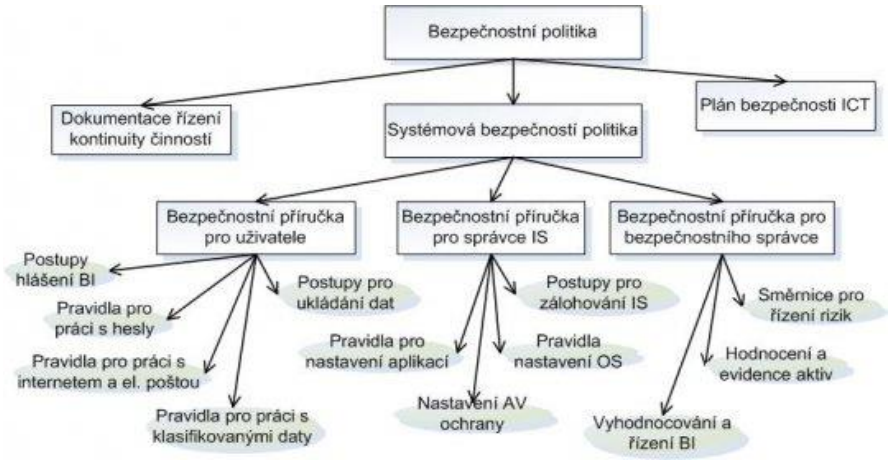
7.3 Procesy a bezpečnostní dokumentace

V rámci systému řízení informační bezpečnosti je třeba definovat a dokumentovat řadu základních bezpečnostních pravidel a procesů. Bezpečnostní politiky patří k základním dokumentům, které definují strategii informační bezpečnosti a základní pravidla v organizaci.

Další navazující dokumenty pak upravují a upřesňují metodiky dílčích oblastí a procesů bezpečnosti. Navazující bezpečnostní dokumentace tedy popisuje procesy bezpečnosti zpracování informací a správy IS, stanovuje a definuje

jednotlivé procesy, definuje role, jejich odpovědnosti a povinnosti při vykonávání daných procesů. Definuje základní postupy řízení bezpečnosti a postupy k dosažení cílů stanovených bezpečnostní politikou.

Součástí základní bezpečnostní dokumentace/dokumentace procesů bezpečnosti informací může být množina několika návazných bezpečnostních dokumentů, jejich rozdělení si organizace může definovat dle svých konkrétních potřeb, například takto:



Obr. 14. Schéma struktury bezpečnostní dokumentace. *(zdroj [22])*

Navazující bezpečnostní předpisy, směrnice a příručky se detailně věnují těm oblastem, které nejsou dosud kompletně vyřešeny, např. v bezpečnostní politice.

Dokumenty jsou vytvářeny v souladu i s další v organizaci již existující bezpečnostní dokumentací, dále například v souladu se stanovenými pravidly na řízení dokumentace podle implementovaného systému řízení jakosti (ISO 9001) apod. Veškeré dokumenty jsou začleněny do stávající struktury interní dokumentace organizace (směrnice, nařízení, předpisy, pracovní postupy atd.).

Navazující bezpečnostní předpisy konkretizují pracovní postupy a zásady práce v informačním systému a do detailu se věnují těm oblastem, které nejsou dosud kompletně vyřešeny, např. již v Bezpečnostní politice IS.

Mezi hlavní přínosy bezpečnostní dokumentace patří:

- Jednoznačné stanovení povinností a odpovědností uživatelů IS organizace.
- Všichni pracovníci budou znát konkrétní odpovědnosti a povinnosti při práci s informačním systémem.
- Zvýší se bezpečnostní povědomí uživatelů o informační bezpečnosti.
- Sníží se riziko úniku dat, např. prostřednictvím emailové komunikace apod.
- Omezení „absolutní moci" administrátorů a správců.
- Snadnější zajištění zastupitelnosti klíčových pracovníků (administrátorů, správců).

Konkrétně se může se jednat např. o:

Plán bezpečnosti ICT/Plán implementace - popis a definice bezpečnostního opatření, které je vhodná zavést do prostředí IS organizace. Množina bezpečnostních opatření vyplývá ze zjištěných bezpečnostních rizik daného IS, typicky při Analýze rizik IS. Plán bezpečnosti stanovuje ke každému bezpečnostnímu opatření harmonogram, který definuje prioritu, náklady a časovou náročnost implementace bezpečnostního opatření. Bezpečnostní opatření (v plánu bezpečnosti ICT projekty) se týkají nejen zavedení technických bezpečnostních opatření, ale i organizačních a personálních opatření.

Bezpečnostní příručka/Směrnice pro uživatele ICT – shrnuje povinnosti a odpovědnosti uživatelů z pohledu informační bezpečnosti při používání ICT organizace.

Bezpečnostní příručka/Směrnice pro administrátory IS/správce sítě/správce AV ochrany/správce zálohování, resp. pro jednotlivé pracovníky útvaru IT - obsahuje požadavky na činnost administrátorů při správě ICT v organizaci.

Bezpečnostní příručka/Směrnice pro bezpečnostního správce – jsou zde popsány jednotlivé činnosti zabezpečované bezpečnostním správcem ICT, jeho povinnosti, odpovědnosti a oprávnění při řešení otázek spojených s informační bezpečností.

Pokyny a návody/Pracovní postupy – definují jednotlivé postupy, povinnosti a práva při práci s prostředky ICT, potažmo s informačním systémem, př. pokyny a návody pro:

- používání elektronické pošty;
- práci s hesly;
- šifrování a práci s klíči/certifikáty;
- práci s notebooky;
- ukládání a zálohování dat;
- používání internetu; atd.

Technická dokumentace – týkající se například nastavení informačního systému, pravidel firewallu, obsahující zálohovací plán, administrátorský deník, provozní záznamy atd. [19].

Při tvorbě dokumentace využíváme svých dlouholetých zkušeností při budování systémů řízení informační bezpečnosti a detailního provádění úloh s tím spojených (analýzy rizik, analýzy současného stavu, technické a penetrační testy, návrh bezpečné infrastruktury, vytváření bezpečnostní dokumentace, tvorba havarijních plánů a plánů kontinuity) [15].

Dokumentace klíčových bezpečnostních procesů a opatření je jedním z důležitých prvků řízení informační bezpečnosti organizace. V duchu hesla „co je psáno, to je dáno“ představuje dokumentovaná bezpečnostní politika nebo bezpečnostní pravidla pro uživatele určitý závazek pro organizaci, její zaměstnance, případně i pro dodavatele a další subjekty, které vstupují do interakce s informačním systémem organizace.

7.4 Dílčí závěr

Každé podnikání je spojeno s permanentní přítomností nejrůznějších hrozeb. Předpokladem stability a adaptability jsou neustálé změny, které jsou vždy spojeny s riziky a to vnitřními i vnějšími.

Všechna rozhodnutí managementu mají konkrétní návaznost na management rizik. Myšlení a jednání manažerů musí být proto založeno na vědomí, že řízení organizace a její procesů na všech úrovních, je svou podstatou neustálým předcházením rizik. Prioritou by rovněž mělo být zabezpečení kritických interních serverů a použití zálohování a obnovy dat. Společnosti

také potřebují transparentnost celé strategie a odpovídající znalosti, aby mohly na hrozby reagovat rychle.

Volba vhodných metod pro posouzení rizik vychází z výsledku fáze stanovení kontextu. Záleží na typu projektu, jeho rizikovosti a důležitosti pro podnik. O použití expertní metody také rozhodují časové a nákladové nároky na její realizaci. Každý projekt je jiný, a proto se může stát, že po použití zvolených metod dojde k přehodnocení rizikovosti projektu. Některé z metod pro analýzu rizik lze použít taktéž pro identifikaci, hodnocení a náměty ošetření rizik. Při posuzování rizik se používají běžné manažerské techniky jako brainstorming, poučení z historických dat, studium dokumentace, strukturované rozhovory, diskuse s experty, dotazníky atd. Existuje řada standardů sjednocující pojmy, pravidla a praktiky z oblasti projektového managementu. Ty poskytují rozdílné úhly pohledu na řízení projektu, základní filosofii však zachovávají stejnou.

Současná doba je dynamická, rychlá. Projekty jsou omezovány jak ve zdrojích, tak v čase. V těchto podmínkách změn a nejistot vytváří jednu z konkurenčních výhod úroveň metodiky managementu rizik. Je nezbytné umět identifikovat nejistoty už při plánování projektu, a jimi vyvolaná rizika pak v průběhu realizace aktivně řídit. Účinné praktikování managementu projektových rizik, jakožto součásti projektového řízení, znamená propojení ověřených nástrojů a technik se systémovým myšlením.

8 BEZPEČNOSTNÍ POLITIKA

Každá organizace, bez ohledu na její zaměření, je při výkonu svých činností plně závislá na svých zaměstnancích. Nezbytnou součástí základních manažerských plánů jsou i úvahy o tom, jak chránit aktiva organizace. Jediná možnost je vytvoření systému řízení bezpečnosti informací. Organizace výměny informací při splnění stanovených cílů, strategií a politik hierarchicky rozvrstvuje oblast řešení bezpečnosti od úrovně celé společnosti až po jednotlivé chráněné oblasti – personální, informační a fyzickou. Aktiva organizace mají svoji hodnotu a jsou ve většině případů pro ni z hlediska jejího fungování kritická. V případě ztráty nebo závažného poškození některých aktiv tak může dojít i k ukončení činnosti organizace, a tím ke značným finančním ztrátám.

Slouží k zajištění přehledu o zavedených bezpečnostních opatřeních, obsahuje rozsáhlý výčet dokumentů, které jsou orgány a osoby (§ 3, písm. c) až e) zákona o kybernetické bezpečnosti) povinny o zavedených bezpečnostních opatřeních vést (jmenný výčet dokumentů; obecná struktura – přesné dodržení není regulováno), ale v případě nedodržení doporučené struktury musí regulované osoby dokládat, že vedou bezpečnostní dokumentaci alespoň v rozsahu stanoveném vyhláškou o kybernetické bezpečnosti. Sumarizuje požadovanou dokumentaci aplikovaných bezpečnostních opatření pro VIS a KII. Je úzce spojeno s přílohou č. 4 vyhlášky a obsahuje doporučenou strukturu dokumentů. Pro KII je navíc požadováno udržování záznamů o tom, jaké činnosti byly v rámci řízení kybernetické bezpečnosti prováděny a jejich výsledků.

Prokázání certifikace – uvedené ustanovení reaguje na situaci, kdy se orgán nebo osoba rozhodne VIS nebo KII certifikovat podle normy ISO/IEC 27001. Požadavky zajišťují, aby NBÚ zůstala schopnost udržet přehled o rozsahu realizovaných opatření a efektivnosti certifikovaného systému řízení bezpečnosti informací. Pokud orgán nebo osoba podle § 3, písm. c) až e) zákona o kybernetické bezpečnosti prokáže certifikaci systému řízení bezpečnosti informací a doloží požadované dokumenty, má se za to, že splňuje povinnost uvedenou v § 4 zákona o kybernetické bezpečnosti – byla zavedena bezpečnostní opatření a provádí se.

Bezpečnostní politika organizace musí navazovat na globální bezpečnostní politiku státu a tvoří jeden ze základních pilířů, na kterém stojí systém řízení informační bezpečnosti. Jedním ze základních kroků je její definice. Pokud tyto kroky nejsou oficiálním způsobem jednoznačně definovány jako základní parametry, např. povinnosti a odpovědnosti klíčových rolí pracovníků organizace, může být následně celý systém budován nesystematicky, neefektivně a naprosto neúčelně. Pevný a stabilní systém řízení musí proto být vybudován na stabilních základech.

Bezpečnostní politika informačních a komunikačních technologií definuje základní bezpečnostní požadavky a nařízení, které mají za cíl zajistit ochranu a bezpečnost informací v organizaci. Určuje rámec informační bezpečnosti organizace a po jejím schválení je závazná pro všechny pracovníky a je směrodatná i pro všechny externí subjekty, které přicházejí do kontaktu s ICT službami organizace. Musí být v souladu s politikou celé organizace, definuje základní strategii, cíle, postoje, role, odpovědnosti a zásady týkající se činností spojených s informační bezpečností. Vychází z existujících a platných interních směrnic a politik, které rozvíjí s ohledem na aplikovatelnost bezpečnostní dokumentace do prostředí organizace. Reflektuje závěry získané z analýz rizik IS a definuje mechanismy zajišťující efektivní řízení informační bezpečnosti. Je podkladem pro budování nižších a specifických stupňů bezpečnostní dokumentace.

Informační systém organizace (jak státní, tak soukromé firmy) představuje souhrn nejrůznějších aktiv (cokoliv, co má pro organizaci nějakou hodnotu) jako jsou data, služby a hmotný majetek. Ztráta aktiv nebo jejich poškození či dokonce odcizení představuje pro každou organizaci nejrůznější rizika jako např. omezení fungování, porušení legislativních předpisů nebo ztrátu dobrého jména. Bezpečnostní politika je tedy zásadním dokumentem pro minimalizaci uvedených rizik. Stanovuje celkový záměr a směr formálně vyjádřený vedením organizace, základní bezpečnostní cíle a definuje postupy k jejich dosažení. Další nezbytnou součástí bezpečnostní politiky je stanovení rolí a odpovědnosti v informačním systému organizace. Nutnou podmínkou úspěšné implementace systému řízení bezpečnosti, je nezbytná zainteresovanost nejvyššího vedení organizace.

Bezpečnost informačního systému je nutno chápat komplexně, proto je zapotřebí, aby bezpečnostní politika řešila řízení bezpečnosti v celé organizaci, ne jenom v její části. To samozřejmě nevylučuje existenci dílčích bezpečnostních směrnic pro jednotlivé části informačního systému.

8.1 Hlavní přínosy bezpečnostní politiky

- Bezpečnostní politika přináší do organizace jasně formulované základní principy řízení informační bezpečnosti.
- Všichni pracovníci musí znát své základní odpovědnosti a povinnosti při práci s informace a ICT.
- Jsou definovány základní požadavky na chování vnějších subjektů, např. dodavatelů v prostředí informačního systému organizace.
- Zvýší se bezpečnostní povědomí uživatelů o informační bezpečnosti.
- Omezení „absolutní moci“ administrátorů a správců.
- Zavedením bezpečnostní politiky se zvyšuje kredit organizace u obchodních parterů a spolupracujících subjektů.
- Bezpečnostní politika je vypracována na základě současných nejlepších norem a standardů používaných v oblasti bezpečnosti.
- Bezpečnostní politika organizace je koncepční nástroj pro podporu, rozvoj a použití nástrojů a procesů v informační oblasti (jedná se např. o umožňující koncepce v rezortu obrany) [23].
- Bezpečnostní politika v prostředí organizace musí být zavedena tak, aby maximálně plnila svou funkci a zároveň byla efektivním nástrojem pro prosazování zásad informační bezpečnosti.

8.2 Tvorba bezpečnostní politiky

Systém řízení bezpečnosti je nedílnou součástí systému řízení organizace a představuje zejména plnění manažerských funkcí. Na začátku jeho tvorby se jedná o stanovení bezpečnostních požadavků. Nejobecnější formou těchto požadavků jsou správně stanovené bezpečnostní cíle, které vycházejí z činnosti organizace (např. obchodních), legislativy, smluv a interních požadavků. Jsou-li jasní cíle, je třeba vytyčit strategii ukazující principy a rámcové postupy pro jejich dosažení.

Pro vypracování bezpečnostní politiky organizace existuje několik různých přístupů. Jedním z nich a obecně nejrozšířenější je vypracovat dokument v souladu s normou ISO/IEC 27001 – Systémy managementu bezpečnosti informací a na základě normy ISO/IEC 27002 – Informační technologie-Soubor postupů pro řízení informační bezpečnosti. V současné době je tento přístup jeden z nejlepších pohledů na řízení bezpečnosti ICT v organizaci.

Dokument bezpečnostní politika – politika bezpečnosti informací je vytvořen jako základní písemný dokument vedení organizace, obsahující představu o způsobu řešení bezpečnosti a základní požadavky na jednotlivé bezpečnostní oblasti celého informačního systému organizace. Při tvorbě bezpečnostních politik vycházíme z předpokladu, že jejich obsah musí zapadat do života organizace, musí se dotýkat každého v organizaci. Vlastní zpracování dokumentu vychází z podmínek a potřeb jednotlivých organizací a řídí se platnou legislativou, metodikami a standardy jako např. ISO/IEC 27002.

Základním úkolem je sestavení seznamu všech aktiv organizace, čímž rozumíme hmotný a nehmotný majetek, data, poskytované nebo čerpané služby [17].

Každá položka na zpracovaném seznamu aktiv je následně ohodnocena a jsou u ní posouzeny dopady v případě její ztráty, poškození nebo nedostupnosti. Na základě tohoto hodnocení jsou přijímána konkrétní opatření, která mají za cíl zabránit nežádoucím incidentům. Tato činnost se nazývá analýza rizik. Je nezbytné vysvětlit pojem incident, resp. bezpečnostní incident. Dle ISO/IEC TR 18044:2004 je bezpečnostní incident definován jako jedna nebo více nežádoucích nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnostních informací. Analýzou rizik je pak myšleno systematické využívání informací pro odhad rizika určení jeho zdrojů. Správné stanovení bezpečnostních rizik vůči aktivům dané organizace vytváří podklad pro identifikaci odpovídajících přiměřených bezpečnostních opatření. Postupy vedoucí k ohodnocení rizik (přes stanovení hodnot aktiv) k velikosti hrozeb a zranitelnosti jsou určující pro výslednou formulaci bezpečnostní politiky.

Na základě zpracované analýzy rizik pak organizace vypracovává konkrétní interní směrnice, kde definuje postupy po snižování rizik a postupy pro obnovení provozu informačního systému nebo jeho zasažených částí při havarijních situacích.

8.3 Obsah bezpečnostní politiky

V rámci bezpečnostní politiky je ustavena bezpečnostní komise, která je odpovědná za řízení bezpečnosti organizace a která dále odpovídá za udržování bezpečnostní politiky v aktuálním stavu a kontroluje plnění požadavků kladených na bezpečnost. Přílohou bezpečnostní politiky je provozně bezpečnostní dokumentace – systémová příručka, příručka bezpečnostního správce, příručka uživatele.

Bezpečnostní politiku můžeme formulovat v rámci jednoho dokumentu nebo několika dokumentů. Obsahem bezpečnostní politiky jsou následující oblasti, resp. kapitoly:

Bezpečnostní politika; organizační bezpečnost, klasifikace a řízení aktiv; personální bezpečnost; fyzická bezpečnost; bezpečnost prostředí; řízení komunikací a provozu; řízení přístupu; vývoj a údržba systémů; zvládání bezpečnostních incidentů; řízení kontinuity činností; zajištění shody.

8.4 Základní principy zpracování bezpečnostní politiky, struktura a přínosy

Základní principy zpracování bezpečnostní politiky, její struktura a přínosy lze chápat z několika pohledů.

8.4.1 Formulace bezpečnostní politiky na základě

- všech platných dokumentů organizace, které se vztahují k bezpečnosti jako např. BOZP, PO, ochrana zabezpečení vstupů, apod., nebo dalších dokumentů;
- systémových bezpečnostních požadavků;
- výsledků analýz rizik;
- bezpečnostních požadavků vyplývajících v zákonech, vyhláškách, normách, předpisech a standardech.

8.4.2 Struktura zahrnuje

- stanovení účelu bezpečnostní politiky;
- definice požadované úrovně bezpečnosti;
- definice odpovědnosti za klasifikaci dat, přístupových práv;
- definice odpovědnosti jednotlivých článků organizační struktury při řízení bezpečnosti ICT;
- normy chování zaměstnanců (vč. právních a etických) aspektů);
- plány a postupy při budování ICT v obecné rovině;
- definice úrovní zabezpečení a míry odolnosti v jednotlivých oblastech bezpečnosti (organizační, personální, technická);
- podmínky auditu.

8.4.3 Přínosy vytvoření bezpečnostní politiky v organizaci definují

- jasné formulace základních principů řízení informační bezpečnosti;
- znalost základních odpovědností a povinností při práci s informacemi a ICT u všech pracovníků;
- definice základních požadavků na chování vnějších subjektů v prostředí informačního systému organizace;
- zvýšení kreditu organizace u partnerů a spolupracujících subjektů;
- využití nejlepších norem a standardů používaných v oblasti bezpečnosti.

8.5 Bezpečnostní projekt

Požadavky na řešení bezpečnostní politiky v organizaci dává bezpečnostní projekt. Činnosti spojené s bezpečnostním projektem spočívají v nalezení a v popisu realizace stanovených bezpečnostních opatření. Technická opatření je nutné promítnout do bezpečnostní architektury IT organizace, což znamená najít jednotlivé komponenty IT infrastruktury a na ně navázat jednotlivá požadovaná bezpečnostní opatření. Netechnická opatření (fyzická, personální, procedurální) jsou aplikována formou směrnic. Výstupy z bezpečnostního projektu popisují, jak jsou bezpečnostní architekturou realizovány a implementovány bezpečnostní požadavky z bezpečnostní politiky a jak jsou vytvořeny podpůrné procedury k jejich prosazení. Zpracované bezpečnostní příručky pro uživatele a správce pak dávají detailní návod pro obsluhu,

nastavení a údržbu bezpečnostních mechanismů. Důležitou součástí bezpečnostního projektu je rozpracování vhodné řídící bezpečnostní struktury organizace, spolu s vydefinováním základních rolí, odpovědností a povinností v systému řízení bezpečnosti, včetně vhodné klasifikace aktiv organizace.

Vazba organizační normy na základní manažerské činnosti organizace je zajištěna nadřazenou bezpečnostní politikou informací, která zavazuje vedení organizace bezpečnost řídit a spravovat.

Obnova funkčnosti IT systémů organizace - klíčový dokument bezpečnostního projektu, který poskytuje rámcový návod na řešení havarijních situací v organizaci s pomocí rozpracovaného systému detailních a průběžně aktualizovaných havarijní/nouzových plánů jednotlivých informačních systémů. Základy nouzového plánování mají přímou vazbu na bezpečnostní politiku, protože jsou spojeny s identifikovanými cennými aktivy a odvozeny od míry rizika, které jim hrozí.

Manuál zvládání bezpečnostních incidentů – slouží k řešení bezpečnostních incidentů v organizaci, a který definuje bezpečnostní incident a popisuje činnosti zúčastněných na jeho identifikaci, lokalizaci, zvládnutí a vyšetření.

Kromě uvedené bezpečnostní projekt obsahuje výčet a přiřazení netechnických bezpečnostních opatření zejména organizačního charakteru, která směřují do příslušných útvarů organizace (personální bezpečnost, fyzická bezpečnost, provozní a vývojová bezpečnost).

8.6 Implementace řešení bezpečnosti

Tato činnost představuje především manažerskou snahu, kdy se organizace snaží implementací přeměnit bezpečnostní projekt ve fungující bezpečnostní systém. Jednoduše popsáno – jde o to, jakým způsobem bezpečnostní projekt (technickou a netechnickou část) zavést do každodenního fungování organizace. Celá činnost musí být v rámci organizace dobře koordinována a vedena. Implementace bezpečnostního projektu představuje komplexní, rozsáhlou činnost, znatelně zasahující do běžného každodenního fungování organizace. Vlastní implementace končí provedením akceptačních bezpečnostních testů, které mají za úkol přesvědčit a dokumentovat, že požadovaná technická opatření byla implementována správně, v požadovaném rozsahu a plně v souladu s bezpečnostní dokumentací.

Nepřetržitý a rychlý pokrok v oblasti ICT přináší stále nové příležitosti pro společnost, ale spolu s tím i nové bezpečnostní výzvy. Kombinace rostoucí závislosti na ICT, např. s možnou technickou chybou, selháním lidského faktoru nebo úmyslným poškozením, komplikuje minimalizaci následků v případě prolomení slabin celého systému. Nástup nových technologií generuje nové příležitosti pro rozvoj společnosti, ale také přináší nové zranitelnosti a tím i nová zadání pro zajištění bezpečnosti ICT i celé společnosti.

Události posledních let naznačují, že je nezbytné adaptovat se na mnohem četnější výskyt krizových situací způsobených nejen extrémními vlivy, ale bohužel i akcemi mezinárodního terorismu. Zajištění ochrany kritické infrastruktury se stává reálnou potřebou pro zvládání krizových situací, ochranu života a zdraví osob a majetku, zajištění minimálního chodu ekonomiky a základních funkcí státu. Pod ochranou kritické infrastruktury se pak zařazují všechny činnosti zaměřené na zajištění její funkčnosti, nepřetržitosti a celistvosti s cílem snížit úroveň rizika hrozeb a zranitelnosti.

Zavádění bezpečnostních norem a standardů v informačních systémech, jejichž bezpečný provoz je pro chod státu nezbytně důležitý, je jedním z předpokladů pro posílení kybernetické bezpečnosti těchto systémů. Efektivní kybernetická bezpečnost vyžaduje povinnou implementaci a důsledné dodržování těchto bezpečnostních norem a standardů s důslednou a periodickou kontrolou jejich dodržování v orgánech veřejné správy. Průběžně budou zpracovávány metodické materiály pro dosažení požadované minimální úrovně kybernetické bezpečnosti (směrnice a doporučené postupy).

Investování do kybernetické bezpečnosti znamená investice do naší budoucnosti a ekonomického růstu. Úroveň kybernetické bezpečnosti je souhrnem všech opatření, jak národních tak mezinárodních, přijatých k ochraně dostupnosti informací komunikačních technologií a integrity, autenticity a důvěrnosti dat v kybernetickém prostoru. Kybernetická bezpečnost musí být založena na komplexním přístupu, což vyžaduje intenzivní sdílení informací a koordinaci aktivit. Při budování kybernetické bezpečnosti je třeba prosazovat spolupráci mezi civilními a ozbrojenými složkami, veřejným a privátním sektorem a mezi národními a mezinárodními institucemi. Pouze takovým způsobem lze zajistit spolehlivý provoz

informačních a komunikačních infrastruktur v kritických sektorech, rychlé a efektivní reakce na kybernetické útoky a odpovídající legislativní ochranu v digitálním světě. Problematiku kybernetické bezpečnosti nelze vnímat jako izolovaný problém ČR nebo izolovaný problém jedné nebo několika částí naší společnosti. Je to problém nejenom mezinárodní, meziresortní, veřejné nebo privátní sféry, ale problém celé společnosti. Proto si zajištění kybernetické bezpečnosti zaslouží vysokou prioritu.

Je zájmem státu, aby stanovil pravidla pro bezpečnost ICT tak, aby všichni uživatelé kybernetického prostoru (státní instituce, subjekty kritické infrastruktury, veřejné instituce, komerční podniky i občané) a poskytovatelé služeb přijali ve svých informačních a komunikačních systémech přiměřená opatření k tomu, aby systém byl odolný proti vnějším i vnitřním útokům a aby nebyl potenciálním rizikem pro ostatní systémy.

9 OCHRANA KRITICKÉ INFORMAČNÍ INFRASTRUKTURY – ZKUŠENOSTI A MOŽNOSTI

Úspěšná ochrana kritické informační infrastruktury rozhodující měrou závisí na připravenosti. Proti některým útokům se lze ovšem bránit jen velmi obtížně, pokud vůbec. Jedná se o útoky označované jako „zero–day–attack“, tj. útoky využívající dosud neznámých zranitelností, případně zranitelností, vůči nimž dosud neexistuje ochrana (známé zranitelnosti by měly být nejen u významných systémů bez prodlení eliminovány). Takové útoky jsou prakticky vždy unikátní a předem nelze stanovit jejich charakteristiky. Základem ochrany je jejich co nejrychlejší odhalení, například prostřednictvím vyhledávání anomálií provozu autonomními sondami. Problémem ovšem může být nízká intenzita provozu, který je nese.

Jako příklad byly zvoleny útoky, které souvisí s provozem velkých sítí a které tedy mohou negativně ovlivnit značné množství uživatelů, jak lokálních poskytovatelů připojení, tak i v samozřejmě důsledku uživatelů koncových.

Přestože přesné okolnosti potenciálního útoku samozřejmě předem nelze znát, je nanejvýš vhodné seznámit se vybranými příklady těch útoků, které se již odehrály.

Uvedené útoky jsou obvykle realizovány formou masivního provozu vedeného vůči oběti. Takový provoz zpravidla nelze generovat z jediného zdroje. První bariéru totiž představují vlastnosti fyzické vrstvy připojení zdroje útoku k Internetu. Rychlost tohoto připojení bude na rozdíl od minulosti v naprosté většině případů výrazně nižší, nežli je rychlost internetových páteřních spojů. Dalším omezením úspěšnosti takového útoku je snadná lokalizace jeho zdroje a tudíž možnost jednoduché filtrace, která může být v některých případech nastavena i automaticky [40].

V současnosti takové útoky probíhají jinak. Zdroje útoku jsou distribuovány a jejich počet je značně vysoký, obvykle nejméně tisíce. Prakticky vždy se jedná o tzv. botnet, což je skupina počítačů infikovaných programem, umožňujícím jistou míru dálkového ovládání z řídicího centra. Toto řídicí například může všem členům botnetu specifikovat oběť, formu útoku a dobu jeho zahájení. Odvrátit takový útok je dosti komplikované a někdy i nemožné, leda za cenu kompromisů.

9.1 Směrování ve velkých sítích

Směrování ve velkých sítích je odvozeno od jiných postupů, nežli je tomu v sítích středních či malých. Základním a prakticky jediným používaným protokolem je zde protokol BGP (Border Gateway Protocol). Jeho první verze vznikla již v roce 1989, zatím dosud poslední verze, číslo 4, byla vydána v roce 2006 a to jako standard RFC 4271, A Border Gateway Protocol 4 (BGP-4). Následně pak byly publikovány desítky jeho doplňků, dále analýzy, bezpečnostní úvahy a vylepšení, implementační specifikace atd.

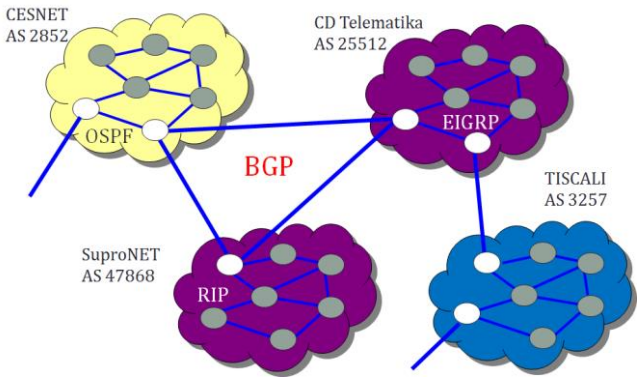
Tento protokol má pro běh velkých sítí naprosto fundamentální význam a ohrožení jeho správné funkce zpravidla znamená dalekosáhlé důsledky. Naopak jej lze využít jako obranný mechanismus, neboť umožňuje distribuovat údaje, pomocí kterých lze některým útokům účinně čelit.

Protokol BGP je dosti složitý, zmíněný standard jakožto základ má rozsah přes 100 stran textu. Dále uvedené hlavní charakteristiky by měly napomoci v pochopení jeho významu i možností. Jedná se o pokus o názorný popis, byť na úkor přesnosti.

Protokol BGP náleží mezi externí směrovací protokoly, slouží pro směrování mezi tzv. autonomními systémy, viz další odstavec. Protikladem jsou protokoly RIP, OSPF či EIGRP, které patří mezi interní směrovací protokoly – řeší směrování uvnitř autonomního systému (protokol BGP lze ovšem provozovat i uvnitř jednoho autonomního systému, pak se hovoří o interním BGP). Na rozdíl od interních směrovacích protokolů., které rozhodují o nejlepší cestě podle dané, obvykle velmi jednoduché metriky (odvozené např. od šířky pásma), se protokol BGP řídí tzv. politikou. V úvahu může brát množství atributů, kterými lze ovlivnit proces směrování i pro individuální pakety výrazně ovlivnit.

Klasická definice autonomního systému říká, že se jedná o množinu směrovačů náležejících pod jednotnou správu, používajících jednotný interní protokol, společnou metriku atd. V současnosti je autonomní systém charakterizován obecněji a to tak, že se jedná o skupinu sítí, a že jiným autonomním systémů skýtá jeden koherentní interní směrovací plán a konzistentní obraz cílů, které jsou skrze něj dostupné. Je vhodné upozornit, že pojem autonomní systém se vyskytuje i mimo prostředí protokolu BGP. Pak má odlišný význam, což může neznalé mást.

Každý autonomní systém má unikátní číslo, původně 16bitové, nyní 32bitové. Toto číslo je přidělováno centrálně, resp. globálně institucí IANA (Internet Assigned Numbers Authority) obdobně jako je tomu u IP adres sítí; tj. nikoliv přímo, ale přes příslušné internetové registrátory, konkrétně regionální – Regional Internet Registry (pro Evropu je jím RIPE NCC – Réseaux IP Européens Network Coordination Centre). Například sdružení CESNET, jehož členy jsou české vzdělávací a vědecké instituce, má přiděleno číslo autonomního systému 2852. Velké sítě, typicky Internet, lze chápat jako množinu autonomních systémů, které jsou vzájemně různě popropojovány (jedná o tzv. peering).



Obr. 15. Protokol BGP – varianta propojení autonomních systémů (naznačené interní směrovací protokoly neodpovídají realitě) *(zdroj vlastní)*

Cesta od odesílatele k cílové síti tudíž může vést přes několik autonomních systémů. Vztahy sousedství mezi sítěmi (přesněji mezi sousedícími směrovači) se u protokolu BGP definují vždy manuálně. Komunikaci se uskutečňuje pomocí protokolu TCP (!), portu 179.

Jak již bylo uvedeno, při volbě cesty k cílové síti protokol BGP zohledňuje řadu kritérií (tzv. atributů), nejzřejmějším je počet (resp. seznam) mezilehlých (tranzitních) autonomních systémů. Příslušný algoritmus se označuje jako Path Vector. Jedná o obdobu algoritmu distančního vektoru, známého ze směrovacích protokolů RIP nebo EIGRP. Optimální cesta je tedy ta, která vede přes nejmenší počet mezilehlých autonomních systémů, pokud se ovšem neuplatní jiné atributy, filtrační pravidla aj. Protokol BGP je totiž velmi flexibilní a umožňuje administrátorům zásahy, kterými mohou proces

směrování významným způsobem ovlivnit, tj. nastavit směrovací politiku podle daných potřeb.

Toto je zjevné v situaci, kdy je pro zvýšení spolehlivosti daná síti připojena k Internetu více spoji, ev. i k více poskytovatelům připojení (přesněji kdy je daný autonomní systém připojen několika spoji k jinému nebo k jiným autonomním systémům; pokud by připojení bylo realizováno pouze jediným spojem, nemělo by použití BGP smysl).

Účelem tohoto textu však je pouhé seznámení s protokolem BGP, nikoliv podrobný popis jeho funkcí či implementace. Za podrobnější zmínku stojí tzv. „prepend“, jedná se o postup, pomocí kterého může administrátor záměrně znevýhodnit zvolenou cestu (jedná se o manipulaci s atributem zvaným AS_PATH). Toho docílí velmi jednoduše, danou cestu formálně prodlouží opakovaným vložením číslo vybraného mezilehlého autonomního systému (např. místo 111–222–333 zapíše 111–222–222–222–333).

Pozornost si dále zasluhuje volitelný atribut zvaný Community. Umožňuje filtraci příchozích či odchozích cest, BGP směrovače totiž mohou značkovat zvolené cesty pomocí identifikátoru (tagu; je jím číslo) a další směrovače pak mohou rozhodovat o směrování konkrétních paketů podle této značky.

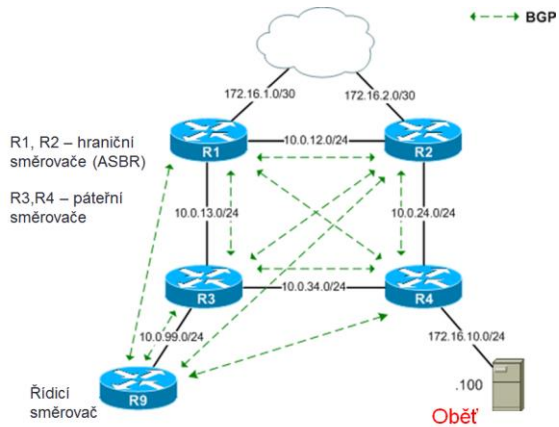
9.2 Obrana proti útoku záplavou paketů jejich odvedením do černé díry

Jedná se o obranný mechanismus vhodný pro situace, kdy je proti dané konkrétní oběti (např. serveru, přesněji IP adrese) veden natolik masivní útok, že dochází k zahlcení síťové infrastruktury instituce, kde oběť sídlí. Zdroj útoku je přitom natolik distribuovaný, typicky se může jednat o botnet, že nelze aplikovat prostá filtrační pravidla a blokovat provoz podle adresy odesilatele. Potenciální oběť budoucího možného útoku, ale provozuje vlastní autonomní systém, používá protokol BGP (a to i interně) a je k Internetu připojena prostřednictvím několika spojů, vedoucích k odlišným poskytovatelům připojení.

Jedno z možných řešení obrany nabízí dokument RFC5635 „Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)“. Řešení, jehož první část je zde popsána, využívá možností protokolu BGP.

Není nijak komplikované, avšak vtipné; skládá se ze dvou úkonů:

- příprava obrany,
    - volba řídicího směrovače,
    - konfigurace hraničních směrovačů autonomního systému (ASBR – Autonomous System Border Router),
        - prostřednictvím protokolu BGP lze distribuovat statické cesty včetně atributu `tag`,
- aktivace obrany v případě útoku,
    - identifikace oběti, tj. IP adresy (adres) cíle útoku,
    - vytvoření statického směrovacího záznamu v řídicím směrovači,
        - odvedení provozu, směřujícího k oběti, tj. nesoucího útok, do černé díry,
    - okamžitá distribuce tohoto statického směrovacího záznamu (injekce) všem hraničním směrovačům.



Obr. 16. Příklad uspořádání obrany proti útoku záplavou paketů jejich odvedením do černé díry [58]

[58] Detaily viz http://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing [25].

9.2.1 Příprava obrany

Příprava obrany spočívá jednak ve volbě řídícího směrovače, z něhož bude po zjištění útoku a jeho analýze obrana aktivována. Dále pak je třeba ve všech hraničních směrovačích připravit černé díry. To spočívá v definici statického směrovacího záznamu v každém z hraničních směrovačů (je třeba provést manuálně), například takto:

```
R1(config)# ip route 192.0.2.1 255.255.255.255 Null0
```

Z tohoto záznamu plyne, že data zasílaná na adresu `192.0.2.1/32` budou předávána do zařízení `Null0`, tedy ihned zahazována. Samotná adresa (zde `192.0.2.1/32`) kupodivu není důležitá, což je vysvětleno dále; stejně dobře by posloužila jakákoliv jiná, ovšem nikoliv se reálně vyskytující v používaných sítích. Toto je zde splněno, neboť adresa `192.0.2.1/32` náleží do rozsahu adres určeného pro testovací účely („TEST-NET“, viz RFC 3330).

Dále je třeba v řídicím směrovači R9 vytvořit mapu cest (route-map) pro budoucí redistribuci označkované statické cesty s modifikovanou hodnotou adresy dalšího skoku.

Mapa může mít následující podobu:

```
R9(config)# route-map RTBH
R9(config-route-map)# match tag 666
R9(config-route-map)# set ip next-hop 192.0.2.1
R9(config-route-map)# set origin igp
R9(config-route-map)# set community no-export
```

Jedná se o podstatu celého řešení. První řádek definuje vlastní mapu, jmenuje RTBH. Další řádek je zcela zásadní – pokud bude napříště ve směrovacích informacích šířených protokolem BGP nalezena cesta označená tagem 666 (`match`), budou aplikovány zbývající řádky, začínající klíčovým slovem `set`. První (třetí od počátku) říká, že pro pakety odpovídající uvedené cestě se jako další skok nastaví adresa `192.0.2.1`. Zbývající dva mají věcný význam, zabraňují proniknutí údajů mimo vlastní autonomní systém.

Stručně vyjádřeno každá cesta propagovaná do hraničních směrovačů s adresou dalšího skoku `192.0.2.1` bude již dříve vytvořenou statickou

cestou rekurzívně přesměrována do zařízení `Null0` a odpovídající provoz bude tudíž zahozen.

Následně je v řídicím směrovači R9 nutno povolit redistribuci statické cesty s využitím dané mapy cest:

```
R9(config)# router bgp 65100
R9(config-router)# redistribute static route-map
RTBH
```

9.2.2 Aktivace obrany v případě útoku

Pokud je potvrzen útok spočívající ve vedení masivního provozu z velkého počtu různých zdrojů směrem k oběti, je možno aktivovat připravenou obranu. Toho se docílí velmi jednoduše zavedením příslušné statické cesty v řídicím směrovači takto:

```
R9(config)# ip route 172.16.10.100 255.255.255.255
            Null0 tag 666
```

Tuto cestu nelze kvůli síťově nekorektní adrese dalšího skoku `Null0` přímo propagovat do hraničních směrovačů. Proto byla přidána značka (tag) `666`, aby se zajistilo, že mapa cesty bude tuto cestu redistribuovat s modifikovanou adresou dalšího skoku.

Parametr `no-export` v mapě cest zamezí neplánovanému prosáknutí této cesty mimo vlastní autonomní systém.

Pro úplnost - ověření správné funkce, tj. toho, že hraniční směrovače zahazují provoz směřující k oběti, lze dosíci takto:

```
R1# show ip route 172.16.10.100
Routing entry for 172.16.10.100/32
  Known via "bgp 65100", distance 200, metric 0,
type internal
  Last update from 192.0.2.1 00:06:14 ago
  Routing Descriptor Blocks:
  * 192.0.2.1, from 10.0.99.9, 00:06:14 ago
  Route metric is 0, traffic share count is 1
  AS Hops 0
R1# show ip route 192.0.2.1
```

```
Routing entry for 192.0.2.1/32
  Known via "static", distance 1, metric 0
(connected)
  Routing Descriptor Blocks:
  * directly connected, via Null0
  Route metric is 0, traffic share count is 1
```

První příkaz, `show ip route 172.16.10.100`, ukáže, že dalším skokem pro pakety s touto cílovou adresou je `192.0.2.1`. Druhý příkaz, `show ip route 192.0.2.1`, dále upřesňuje, že cesta k adrese `192.0.2.1` vede skrz místní zařízení `Null0` (`directly connected, via Null0`).

9.2.3 Dílčí závěr

Infrastruktura dané instituce je nyní chráněna proti zahlcení nadměrným provozem vedoucím k předmětné oběti. Není to ovšem zadarmo, neboť dané opatření zahazuje veškerý provoz k ní včetně zcela korektního; je to ovšem cena, se kterou bylo předem počítáno. Toto zahazování se však realizuje na hranicích autonomního systému a netýká se tedy provozu, majícího původ uvnitř vlastního autonomního systému. U velkých poskytovatelů připojení s množstvím uživatelů proto může být negativní dopad daného opatření neznatelný, neboť významná část provozu se odehrává v něm.

Mírného vylepšení funkce lze dosáhnou ve spolupráci se jmenným systémem (DNS). Lze předpokládat, že údaj o oběti byl jednotlivým distribuovaným útočníkům v rámci botnetu předán formou její IP adresy. Naopak běžný uživatel přistupuje k cíli (serveru) prostřednictvím jeho doménového jména, které jmenný systém převede na IP adresu. Nabízí se možnost přidělit doménovému jménu oběti jinou IP adresu a upravit příslušný záznam v DNS. Přináší to dvě nevýhody, doba platnosti DNS záznamu by musela být krátká, aby se stroje uživatelů nespokojily s jednou získanými daty. Krátká doba platnosti DNS záznamů by se týkala všech žadatelů, takže by vzrostl trvale počet DNS dotazů. No a kromě toho útočník může změnu odhalit a předat botnetu novou IP adresu.

9.3 Narušení chodu Internetu v únoru 2009 českým[59] přičiněním

Ochrana kritické informační infrastruktury je někdy zúženě prezentována jako obrana před cíleným útokem jedince, neformální skupiny nebo nepříznivě nakloněného státu (pokud by se jednalo o spojence, pak by se bylo namístě neklasifikovat takovou aktivitu jako útok), případně jako soubor opatření mající za cíl zajistit fyzickou ochranu zařízení, nepřerušitelnost napájení, řádné zabezpečení vzdáleného přístupu apod.

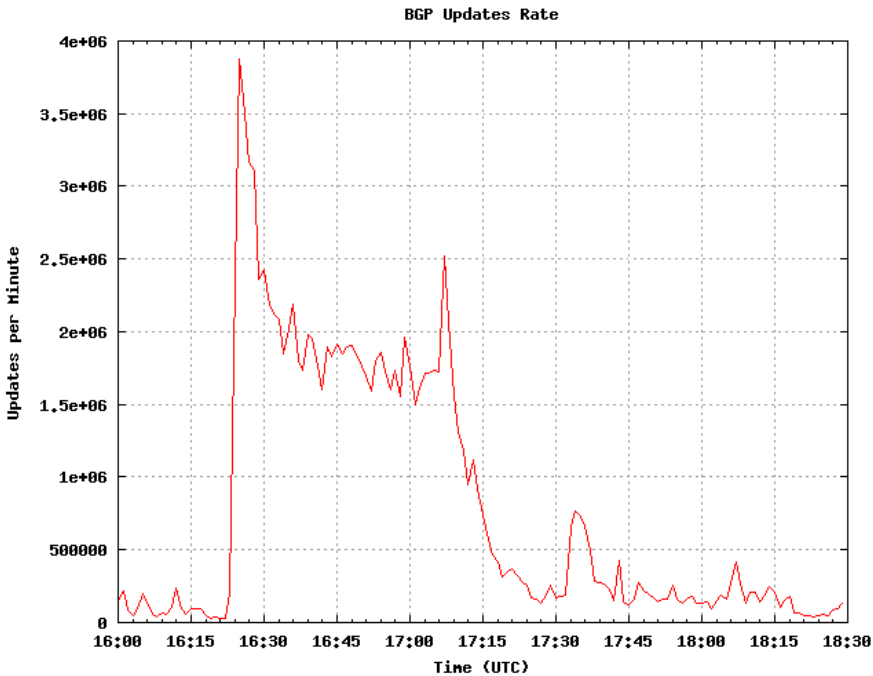
Dne 16. února 2009 však došlo k události, která již poněkolikáté demonstrovala, že významné narušení činnosti rozsáhlých sítí (v daném případě Internetu) může vyvolat naprosto nepravděpodobná kombinace softwarových opomenutí byť velmi významných výrobců, přičemž na počátku může stát školácká chyba administrátora malého místního poskytovatele připojení.

Je namístě připomenout základní fakta o protokolu BGP – slouží pro výměnu směrovacích informací mezi autonomními systémy, vztah sousedství spolupracujících směrovačů se nastavuje manuálně, komunikace mezi nimi probíhá protokolem TCP. Výhodnost té či oné cesty k cílové síti (obvykle k celému bloku adres sítí, zvaných též prefixů) se posuzuje podle počtu mezilehlých autonomních systémů, menší počet značí lepší cestu (není-li politikou, tj. pomocí potenciálně značného množství atributů stanoveno jinak). Chce-li administrátor některou cestu znevýhodnit, použije tzv. prepend, opakovaně uvede (bezprostředně po sobě) číslo některého mezilehlého autonomního systému, čímž se daná cesta o příslušný počet opakování prodlouží.

Co se tedy onoho dne, bylo to pondělí, odehrálo? Přibližně v 16:20 (UTC) zaznamenaly senzory firmy Renesys[60], které sledovaly stav směrovacího protokolu BGP po světě, abnormální aktivitu [27]. Tempo aktualizací šířených protokolem BGP skokově vzrostlo oproti obvyklým hodnotám až na přibližně

[59] Přesněji moravským, resp. ještě přesněji slováckým přičiněním.
[60] Od 3. 10. 2014 Dyn Research, viz http://research.dyn.com, odkud je čerpána většina popisovaných údajů včetně obrázků a tabulek.

stonásobek a následně začalo docházet k různým výpadkům dostupnosti celých regionů.



Obr. 17. Celosvětový nárůst počtu aktualizací protokolu BGP dne 16. února 2009

9.3.1 Průběh zmíněného jevu

Společnost SUPRO[61] (AS 47868) obvykle oznamuje jeden prefix, 94.125.216.0/21 a to jednomu poskytovateli, CD–Telematika (AS 25512). Dne 16. února v 16:23:30 UTC, začal tento prefix přicházet přes jiného poskytovatele, Sloane Park Property Trust (AS 29113), ale s délkou cesty

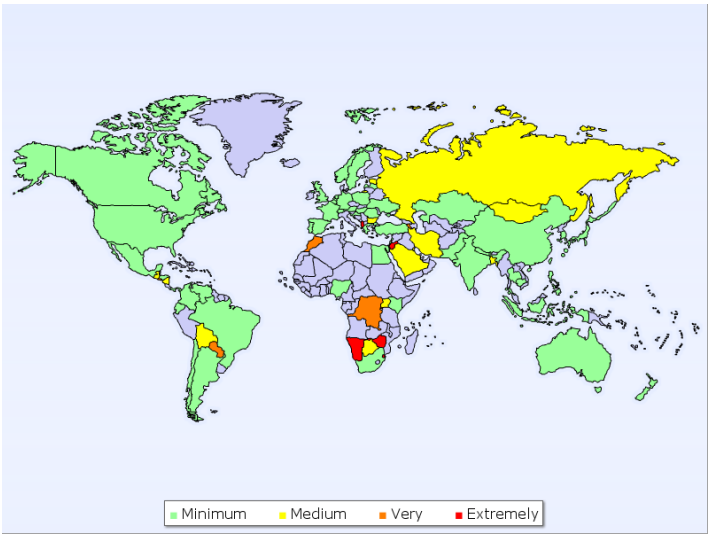
[61] SUPRO, spol. s r.o., mj. poskytuje telekomunikační služby a používá označení SUPRONET

přesahující 255 tranzitních autonomních systémů. Ony zprávy pokračovaly téměř přesně jednu hodinu, konkrétněji do 17:23:00 UTC. Šíření této cest do světa bylo pozorováno i dalšími poskytovateli, například Level 3 (AS 3356), Tiscali (AS 3257) a TeliaSonera (AS 1299), finálně uvedené problematické oznámení odesílalo celkem 230 unikátních autonomních systémů.

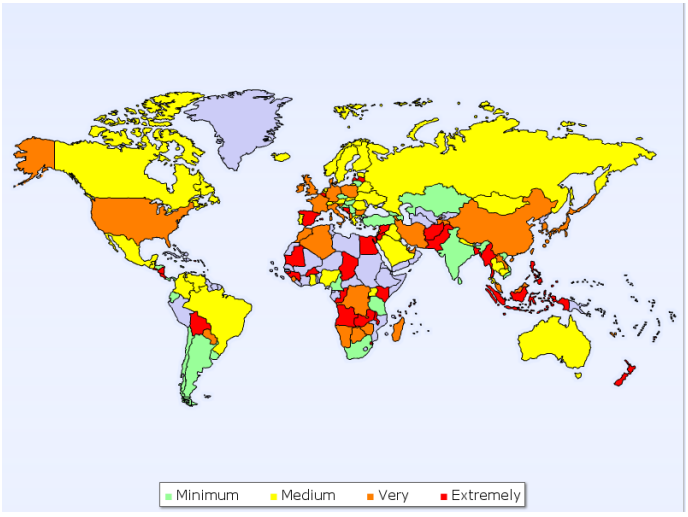
Malý český poskytovatel dokázal díky částečně nekorektním (viz dále) oznamováním jednoho prefixu způsobit obrovský nárůst globální rychlosti aktualizací (v důsledku pak přepočtů směrovacích údajů protokolem BGP), ve špičce až 107 780 aktualizací za sekundu. Tento vrchol nastal v 16:30:54 UTC, méně než 8 minut po prvním oznámení.

Pro porovnání – běžnou hodinu před touto událostí došlo celkem k 1215 změnám globálních prefixů z celkového počtu 271 175 (průvodním jevem je zpravidla dočasná nedostupnost příslušné sítě, neboť probíhá přepočet směrovacích tabulek; hovoří se o nestabilitě směrování). Během předmětného dění vzrostl tento počet na 12 920 neboli 4,8 % všech prefixů na zeměkouli. Jediné oznamování od jediného poskytovatele způsobilo desetinásobný nárůst nestability směrování v celosvětového měřítku, a to na celou hodinu. Nejvíce byla postižena Severní Amerika (nárůst se zvýšil z 0,35 % na 4,76 %), zatímco Jižní Amerika utrpěla nejméně (z 0,52 % na 1,75 %).

Nárůst nestability směrování je graficky znázorněn na dvou následujících obrázcích.



Obr. 18. Nestabilita globálního směrování dne 16. února 2009 v 15:00 (před událostí; podle států, odvozeno od procenta všech v něm přidělených prefixů)



Obr. 19. Nestabilita globálního směrování dne 16. února 2009 během události počínaje 16:00 (podle států, odvozeno od procenta všech v něm přidělených prefixů)

Celé dění bylo, jak je zřejmé, ukončeno po hodině, kdy byl aktivován filtrační mechanismus blokující nekorektní údaje, pocházející od firmy SUPRO. Co se ale vlastně stalo?

9.3.2 Co se vlastně stalo?

Podrobný průběh událostí spojených s dotyčnou událostí byl sestaven na základě různých informací později a přinesl jej například zdroj „Lupa: internetový server o českém Internetu“[62],[63] odkud jsou částečně převzaty následující pasáže [28, 29]. Je třeba mít na mysli, že se zčásti jedná o dohady, byť kvalifikované - s tím, jak přesně bylo popisované dění spuštěno, se firma SUPRO nepochlubila.

Na počátku stála chyba konfigurace protokolu BGP. Firma SUPRO (AS 47868) měla připojení ke dvěma poskytovatelům, přičemž administrátor chtěl pravděpodobně jedno z nich pomocí prependu (opakovaného uvedení čísla mezilehlého autonomního systému) znevýhodnit, tedy uměle prodloužit příslušnou cestu. Přitom se dopustil banálního omylu.

Prepend je běžná záležitost, avšak na problém bylo zaděláno tím, že počet opakování (tj. délka cesty) není neomezený – za limit se všeobecně považuje 255 položek. Toto omezení není pro reálný život nijak zásadní, neboť protože jen velmi málo cest v současném Internetu obsahuje více než šest položek (je delších než šest mezilehlých autonomních systémů), a cesta obsahující více než 15 položek je zcela výjimečná.

Co se tedy stalo konkrétněji? Dotyčný administrátor danou cestu skutečně znevýhodnil, ovšem zcela jinak, nežli zamýšlel. Není zcela jasné, jakým konkrétním způsobem toho dosáhl, avšak použitou platformou, na které k uvedenému problému došlo, byl pravděpodobně MikroTik RouterBoard, tedy zařízení primárně určené pro poněkud jiné nasazení než je ASBR

[62] http://www.lupa.cz/clanky/maly-cesky-isp-zpusobil-svetovy-kolaps/
[63] http://www.lupa.cz/clanky/proc-a-zda-supronet-shodil-internet/

(Autonomous System Border Router). Platforma Mikrotik používá vlastní operační systém MikroTik RouterOS, vycházející z Linuxu.

Zde je vhodné upozornit, že firma Cisco Systems, jejíž výrobky nemůže žádný síťový administrátor ignorovat, má ve svém operačním systému Cisco IOS při znevýhodňování cesty zavedenu syntaxi v podobě „`set as-path prepend last-as N`“. Číslo `N` říká, kolikrát se naposledy uvedené číslo AS v cestě má zopakovat a toto `N` může nabývat hodnoty 1 – 10, což se kontroluje.

Podle dokumentace k platformě MikroTik by počet opakování měl být v rozsahu 1 – 16, avšak skutečně vložená hodnota nebyla systémem kontrolována (!). Administrátor totiž pravděpodobně zadal místo násobku číslo svého autonomního systému 47868, což nebylo hlášeno jako chyba. To však nebylo vše, ono číslo nebylo použito přímo, nýbrž z něj bylo vzato dolních 8 bitů, tedy fakticky bylo provedeno dělení modulo 256. Zbytek po dělení 256 z čísla autonomního systému 47868 činí 252, což je přesně hodnota, která byla použita jako onen vzpomenutý násobič. Na absolutní hodnotě čísla autonomního systému tedy nezáleželo, pokud by bylo jen o čtyři větší, nestalo by se pravděpodobně vůbec nic, protože zbytek po dělení by byl roven 0. K hodnotě 252 vzešlé z uvedeného opakování je nutno ještě přičíst další, zadané manuálně. Výsledek pak přesáhl hodnotu 255.

Příběh však stále nekončí, MikroTik totiž i přes svou chybu nemohl vygenerovat údaj, který by byl v rozporu s RFC 4271. Ve specifikaci BGP je délka atributů omezena pouze maximální velikostí zprávy, ve které jsou tyto předávány (BGP UPDATE), a ta činí 4 kB. Bohužel se v praxi se stává, že pokud nejsou pevně stanoveny limity, výsledné implementace používají svoje, které jsou různé, případně dokonce žádné. Na směrovačích Cisco je od verze IOS 12.4 implicitní limit na maximální počet čísel mezilehlých autonomních systémů nastaven na 255 (předtím jen 75). Pokud byla tato hodnota vyšší, byla taková cesta zahozena.

Teprve tady se projevil skutečný problém. Jakmile směrovač Cisco přijal zprávu s počtem autonomních systémů větším nežli 255, vygeneroval další nevalidní BGP UPDATE zprávu, její příjemce (příjemci) tudíž ohlásil chybu, a následně korektně (dle RFC) spojení ukončil. Směrovače se následně snažily

spojení obnovit, následkem čehož docházelo k opakovaným restartům a generování onoho množství BGP zpráv.

Podstata cyklického rozpadávání BGP spojení a jejich opětovného navazování tedy spočívala nikoli ve směrovačích, který zprávu BGP UPDATE přijímaly, ale na směrovačích, které tuto zprávu generovaly. Hlavní příčina nestability BGP spočívala v nově objevené chybě v operačním systému IOS směrovačů Cisco. Tato chyba byla oficiálně publikována pod označením CSCsx73770.

9.3.3 Shrnutí

Původní článek firmy Renesysu poukazoval na okolnost, že takto velký kolaps z takto zanedbatelné příčiny napovídá, že musela nastat řada zanedbání na různých úrovních. Obecně se dá říci, že na všech stranách došlo k porušení tzv. Postelova zákona, které říká: Buď konzervativní v tom, co děláš, a buď liberální v tom, co přijímáš od ostatních.

Reálné příčiny onoho „světového kolapsu“ jsou čtyři, jejich pořadí podle závažnosti vypadá takto:

1. Nově objevená chyba v operačním systému IOS směrovačů Cisco
2. Chyba v operačním systém RouterOS směrovačů MikroTik
3. Nedostatečné nebo žádné filtry u tranzitních operátorů
4. Překlep administrátora firmy SUPRO v konfiguraci směrovače MikroTik

9.4 Dílčí závěr

Tato kapitola si klade za cíl seznámit čtenáře v minimální míře s některými specializovanými tématy technického charakteru. Současný svět se opírá o počítačové sítě; ba dokonce je na nich závislý. Je fascinující, jak rychle k tomu došlo – celé to netrvalo déle nežli 10 – 20 let.

Průvodním jevem, bohužel ne zcela doceňovaným, je bezpečnost. Představuje totiž dodatečné náklady, které jsou z pohledu některých manažerů zbytečné, neboť nepřináší měřitelný zisk. Takové názory jsou dnes již sice verbálně v menšině, ale v praxi, tj. v ochotě vynakládat prostředky na řešení, která možná nebudou nikdy využita, je situace dosti často mlhavá. V České

republice platí od 1. 1. 2015 předpis č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zkráceně „zákon o kybernetické bezpečnosti“). Ten definuje klíčové pojmy, stanovuje zodpovědnosti a vytváří instituce.

Kapitola nahlíží do světa správy počítačových sítí a to prostřednictvím dvou vybraných témat. Oběma se prolíná externí směrovací protokol BGP, který je ve velkých sítích používán.

První téma je zasvěceno popisu jedné z možností obrany před útokem označovaným jako distribuované odepření služeb (DDoS - Distributed Denial of Services). Konkrétně se jedná o obranu před nadměrným provozem pocházejícím z velkého množství zdrojů a cíleného na určitou oběť, známou jako RTBH – Remotely-Triggered Black Hole.

Druhé téma pak ukazuje případ narušení funkce významné části světového Internetu, zapříčiněné malým tuzemským poskytovatele internetového připojení.

10 PSYCHOLOGICKÝ PROFIL ÚTOČNÍKA

Úspěšnost a výsledek práce subjektů (firem, organizací, institucí) je závislý na ochraně informačních systémů, které představují svým obsahem kapitál, který má nezaměnitelnou specifickou hodnotu a význam. Může však současně představovat oblast zájmu a terč útoku jednotlivce nebo zájmové skupiny, jejichž cílem je získat informace či údaje se záměrem danou organizaci poškodit. Z poznatků a rozboru mnoha událostí vyplývá poznání, že je potřebné a účelné věnovat pozornost osobnostním dispozicím a schopnostem pracovníků, kteří se na provozu a organizaci systémů bezprostředně podílejí. Při své práci využívají svých znalostí, zkušeností i osobní invence k dosahování kvalitních výsledků práce a současně prokazují zdravou loajalitu vůči svému zaměstnavateli. V opačném případě se však může stát jejich jednání problémem.

Informační a komunikační technologie jsou v současnosti využívány ve všech oblastech společenského i soukromého života. Staly se nedílnou součástí ekonomických činností, veřejné správy, armády, průmyslu, zdravotnictví, vzdělávání atd. Informace, se kterými se v těchto oblastech pracuje, jsou implementovány do informačních systémů a ty jako celek představují vysoce ceněnou hodnotou. Jde často o citlivé údaje, které se týkají organizace a struktury jejich činností, výrobních procesů, obchodních informací, personálních údajů apod. Vzhledem k rozvoji potřeb a možnostem neustále se zdokonalující techniky jsou v převážné míře údaje digitalizovány. Dochází tím k výrazným úsporám lidské práce, snížení nároků na čas i na prostor. Vzniká však problém s bezpečností zpracovávaných a uložených dat, které se postupně staly předmětem obchodu, většinou velmi výnosného. Informace, zvláště aktuální s vysokou vnitřní hodnotou, jako jsou výsledky různých výzkumů nebo obchodních transakcí, jsou v daném oboru využitelné jako výrazná úspora vlastních nákladů například při vývoji nových postupů a metod.

Jsou však svým obsahem velmi lehce zneužitelné k poškození záměrů původního majitele, zvláště v konkurenčním prostředí daného oboru. Záměrné zneužití digitalizovaných informací představuje velmi nebezpečnou zbraň. Dosažené výsledky dlouholetého vývoje informačních technologií tak kromě

pozitivního vlivu na celkový rozvoj společnosti poskytují jako druhotný produkt prostor k možnosti vzniku kriminálního či závadového jednání.

Rozvoj moderních technologií a informačních systémů s sebou nese výrazné změny, které ovlivňují myšlení a chování lidí, kteří se těmito technickými prostředky zabývají a to buď profesně, anebo v rámci svého osobního zájmu. Postupně se zvyšuje a zdokonaluje počítačová gramotnost uživatelů, přístup k internetu má díky cenovým relacím téměř každý. Rozšiřuje se sortiment výrobků, které jsou dosažitelné širokému spektru zájemců a stávají se součástí denní potřeby nejen profesionálů. S tím roste příležitost k provádění pokusů s ověřováním a využíváním svých schopností a vědomosti nabytých studiem, anebo vytvářením vlastních produktů, které v dané oblasti dosud realizovány nebyly. V případě úspěchu může také vzniknout podnět k realizaci útoku na zvolený objekt, kdy základním cílem a záměrem je získání osobního prospěchu, případně získané údaje jsou předmětem záměru se širšími souvislostmi.

Reálná možnost zneužití informačních technologií v celosvětovém měřítku je hrozbou, která nesmí být v žádném ohledu zpochybňována. Týká se to zejména rozvojových zemí, které mají stávající minimální technologickou úroveň, ale která se v některých případech postupně mění a může se stát výhodnou základnou nebo přestupní stanicí kybernetických útoků. Podle poznatků různých zdrojů je zneužívána nízká, popř. nulová úroveň legislativy, která je pro útočníky neodolatelným lákadlem. Často slouží jako cílová stanice, do které jsou informace nebo získané prostředky přeposílány.

Elektronická informační kriminalita se stala součástí činnosti a výrazného zájmu některých jednotlivců. Ukradená data, získaná více či méně sofistikovaným způsobem, jsou dále využívána k podvodným transakcím (e-commerce, e-banking), internetovému obtěžování atd. A nejde jen o útoky na bankovní účty či na vybranou osobnost, jde také například o oblast ochrany autorských práv, která jsou v prostředí internetu masivně porušována, případně k ovlivňování svobody soukromých osob.

V našem prostředí se nejčastěji setkáváme s termínem počítačová kriminalita, kterou můžeme chápat jako páchání trestné činnosti, v níž figuruje počítač jako souhrn technického a programového vybavení včetně dat, či pouze některá z komponent počítače, případně více počítačů propojených

do počítačové sítě. Výpočetní technika se stala předmětem významným nejen pro komunikaci, ale současně i nástrojem trestné činnosti.

Člověk se však na vzniku informačních technologii svojí myšlenkovou produkcí podílel a veškeré technika i technologie jsou výsledkem této činnosti. Je proto evidentní, že bez lidského myšlenkového potenciálu, kreativity a dovedností by stávající prostředky nespatřily světlo světa a nebylo by možné je využívat. A současně i zneužívat.

Lidský faktor v těchto souvislostech vystupuje jako „spouštěč" a technika se stala prostředkem k dosažení vytýčeného osobního záměru. Není podstatné, zda jde o snahu někoho poškodit, sebe obohatit, anebo jen poukázat na problém, který nikdo jiný dosud nepoznal či neodhalil. Poznání, že je schopen dosud neřešený či nepoznaný problém nebo postup sám vyřešit a stát se prvním kdo to dokázal, je významným motivem k činnosti, která ovlivňuje myšlení člověka a orientuje jeho další rozhodování. Ověření svého poznání v praxi pak představuje například vytvoření metody vstupu do chráněného systému, třeba s konkrétním cílem získat určitá data, finanční prospěch nebo informace.

Zdrojem promyšlené činnosti je vlastní rozhodnutí člověka, zda s využitím kognitivního postupu a kreativitou vytvoří návod, který pomocí techniky realizuje. V procesu děje klasické kriminality se měří doba spáchání trestného činu na minuty, hodiny, dny, kdežto trestný čin v kyberprostoru kriminality může být spáchán v několika tisících sekundy a pachatel ani nemusí být přímo na místě činu. Další významnou charakteristikou je vlastní hodnota ztrát, které vznikají jako důsledky kybernetické kriminality. Ať již mají podobu finančních částek, nebo mají podobu zneužití získaných informací.

V mnoha případech hodnota získaných údajů není pro pachatele prioritní záležitostí. Jde mu v podstatě o potvrzení vlastních představ o sobě samém, vyrovnávání se s pocity vnitřní nedostatečnosti, která je důsledkem prožitých událostí v minulém ontogenetickém vývoji. Zdrojem uvedeného jednání může být problém s vlastní identitou, případně je modifikovanou formou protestu vůči minulosti, se kterou se někteří jedinci vyrovnávají po celý život. Odhalení důvodu jejich jednání je v řadě případů složité, protože si jsou do jisté míry vědomi svých vnitřních pocitů a dovedou je v daných situacích vědomě regulovat.

Jde-li o promyšlenou a plánovitou činnost s cílem získat osobní profit a současně prokázat svoji schopnost a „nedostižnost“, je možné uvažovat o jednání, kdy podstatou je osobní pomsta nebo záměr někoho výrazným způsobem poškodit, případně způsobit problémy. Tento způsob jednání je charakteristický určitou diskrétností trestné činnosti. Vzhledem k časovým dimenzím je problematické rychle vytvořit konkrétní psychologický profil pachatele. Většinou chybí viditelný a čitelný motiv jeho činnosti. Zdrojem jeho jednání jsou podobné pohnutky jako v předchozích případech, záměr je však převážně jasný. Psychologickou podstatu jednání je možné s převahou jistoty potvrdit vybranými znaky profilu osobnosti.

10.1 Osobnost pachatele

Pachatele můžeme charakterizovat z několika úhlů pohledu na jejich osobnost, strukturu a hlavně motivaci jejich činnosti. Obvykle jsou označováni jako hackeři, kteří se dopustili jednání s následkem a dopadem v některé z oblastí kybernetické činnosti. Označení hacker však prodělal v průběhu cca 50. let vývoj, který odráží jeho vnitřní význam v současném (byť nepřesném) pojetí. Zatímco dříve bylo synonymem pro člověka, ke kterému se vzhlíží s úctou, dnes jej většina lidí považuje za označení počítačového kriminálníka.

V obecném pojetí můžeme říci, že hacker je člověk nadšený programováním, kterého baví zkoumat detaily a způsoby využití systémů; překonávání překážek tvořivým způsobem je pro něj výzvou a k realizaci svého záměru či ověření své schopnosti je ochoten obětovat cokoliv.

Je třeba zdůraznit, že činnost pravého hackera spočívá v pronikání do ochraňovaných systém s cílem prokázat své schopnosti a kvality bez zájmu získat informace či narušit systém. Podstatné je překonávání ochranných bariér, což je považováno za zábavu, dobrodružství a potvrzení svých schopností [30].

Pro opravdové hackery je typické jejich sociální chování, používaný jazyk, uznávání morálních hodnot a samozřejmě provádění vlastní aktivity. Pojem hacking označuje činnosti, které pravý hacker provádí a kterými získává uznání a respekt. Výsledkem jeho činností jsou např. získání a zpřístupnění zdrojového kódu programů, odhalení slabin informačního systému

a zpřístupnění příslušných informací, doporučení k případně nápravě nedokonalostí systému apod. Publikuje užitečné informace na internetu, poskytuje rady a pomoc při administrativě a provozu diskusních skupin, seznamů, archivů atd. Hacking, který není prováděn tak, aby způsobil někomu jinému škodu či jinou újmu nebo sobě či jinému neoprávněný prospěch, není kvalifikován jako trestný čin, a tudíž není postižitelný.

Pojem hactivismus představuje politicky motivované napadání internetových stránek. V důsledku různých medializovaných kauz průniků do sítí se výraz „hacker“ vžil jako nálepka pro vandalství, poškozování informačních a komunikačních systémů.

Označení cracker se objevilo v souvislosti s pojmem *crack, který představuje narušení zabezpečení ochrany a integrity programu nebo systému*. Podle jednoho pohledu jde o osoby schopné prolomit kód určitého SW a umožnit tak jeho *nelegální kopírování, z jiného hlediska jde o osoby, které pronikají do počítačového systému s úmyslem jejich poškození.* Cracking je činnost, kdy dojde k narušení informačního systému zvenčí (prolomení ochrany). Cracker zpravidla nepracuje sám, ale ve skupinách. Členové skupiny bývají hierarchicky rozděleni, každý má na starosti konkrétní činnost. Skupiny bývají tematicky specializované na herní oblasti, weby a aplikace.

Mezi skupinami panuje poměrně vysoká soutěživost, své úspěchy pečlivě dokumentují a zpravidla i zpřístupňují na internetu. Crackeři se sami často považují za hackery, avšak jejich znalosti informačních systémů, internetových protokolů a programování *nejsou na tak vysoké úrovni jako u hackerů.* Crackeři používají k průniku do informačních systémů především zveřejněné slabiny, na které ještě administrátoři nezareagovali.

Zásadní rozdíl, odlišující tyto patogenní osobnosti od hackerů, spočívá v pronikání do systémů s cílem data získat a následně zneužít ve vlastní prospěch. K těmto charakteristikám můžeme ještě přiřadit potěšení z destrukce systému. Z přehledu vývoje označení subjektů v oblasti kybernetické bezpečnosti vyplývá, že v základním dělení lze rozdělit osoby na:

- Amatéry, kam je možné zařadit hackery, crackery, neúspěšné kritiky a mstitele. Jde o osoby pronikající náhodně nebo cílevědomě do informačních systémů tak, že najdou či vyhledávají zranitelná

místa. Jejich cíle nebo motivace jsou různé. Častým prohlášením je snaha upozornit na nějaký nedostatek v systému, anebo vyjádření osobního nesouhlasu s prohlášením nebo dějem, který je prezentován.
- Profesionály, kam lze zařadit pracovníky speciálních tajných služeb, detektivovy, žurnalisty, podnikatele, specialisty- informatiky,
- Softwarové piráty či teroristy tvořící zvláštní skupinu organizovaného zločinu, jejichž základním cílem je poškodit systém, organizaci nebo jednotlivce.

Někteří pachatelé provádějí trestnou činnost samostatně, ale ve většině případů jde o sdružování a spolupráci více osob, které se formují do určitých skupin, jejichž podstatou je společný záměr. Členové se většinou ani osobně neznají, neboť veškerá komunikace probíhá elektronicky. Vzájemné vztahy mezi skupinami, zabývající se trestnou činností, jsou poměrně spletité.

Kybernetika zkoumá obecné zákonitosti procesů řízení, přenosu a zpracování informací. Je to nauka o řízení pomocí informací. Požadavky na pracovní schopnosti je možné stanovit jako kritérium psychických dispozic jedince, např. v oblasti myšlení:

Způsoby myšlení lze členit takto:

- Konvergentní myšlení – použití již známého způsobu řešení.
- Divergentní myšlení – vynalezení nového způsobu řešení, tj. tvořivé myšlení.

Základní teorém na rozmezí kybernetiky a psychologie:

- Konvergentní myšlení lze simulovat (uměle napodobovat) počítačem).
- Divergentní myšlení, tvořivé, tvůrčí, nelze simulovat počítačem.

Programování je vlastně simulace konvergentního myšlení počítačem.

Umělá inteligence se člení takto:

- Slabá umělá inteligence představuje simulaci konvergentního myšlení strojem (to se již podařilo, viz počítače).
- Silná umělá inteligence představuje simulaci divergentního myšlení strojem (to se stále nedaří).

Zda se někdy vůbec podaří simulovat divergentní myšlení strojem je stále otevřeným problémem. Podíl lidského činitele je natolik významný, že jej v současnosti nelze nahradit. Divergentní myšlení (divergent thinking) je podle J.P. Guiforda myšlení málo ohraničené cílem a je určeno mnoha faktory tvořivosti, např. flexibilitou, originalitou, jedinečností, tj. určitými vlastnostmi osobnosti daného jedince.

Myšlení konvergentní (corvengent thinking) *myšlení zužující prostor je* charakteristické hledání správné odpovědi na určitý úkol; na myšlení konvergentním jsou založeny např. testy inteligence.

V kybernetickém prostoru neexistuje efektivní zastrašování, neboť již jen identifikace útočníka je extrémně těžká, a dodržování mezinárodních práv je patrně téměř vyloučeno. Za těchto okolností je jakákoliv forma represálií velmi problematická.

10.2 Význam lidského faktoru

Z uvedených souvislostí vyplývá nutnost zaměřit pozornost na lidský faktor, který v oblasti kybernetické bezpečnosti sehrává nosnou a nezastupitelnou roli. Bez přítomnosti divergentního způsobu myšlení není reálné uskutečnit jakýkoliv kybernetický útok. Schopnost myšlení a řešení úkolů bez lidského potenciálu není možné a proto musí být pozornost jakékoliv formy obrany zaměřena na subjekty vlastnící tento potenciál.

Struktura osobnosti odborníka pracujícího v oblasti výpočetní techniky je poznamenána projevem osobního zájmu a ambicí ovládnout techniku a být sám sobě regulátorem dosahování cílů, který představuje určitou výjimečnost svým významem a posláním i možnostmi. Je nutno klást otázku, do jaké míry se daná osobnost bude realizovat pouze v oblasti vědy a její aplikace do praxe, případně kdy tato pomyslná mez bude překonána.

Jednou z možností projevů je osobní snaha (motivace) dosahovat obecného uznání v odhalování možností dalších kvalitativních změn v oboru, které dosud nebyly objeveny a jejich prezentace přinese vnitřní uspokojení a uznání schopnosti (*altruistic aggression – agrese zaměřená na ochranu jiných*). To může představovat přínos pro vytvoření nových bezpečnostních prvků do kybernetické bezpečnosti organizací a celkového procesu systému.

Druhá reálná možnost je vytvoření osobního záměru k využití dosud nepoznaného postupu překonání bariéry v programu a místi upozornění a vytvoření obrany bude tato znalost a dispozice využita v opačném záměru. Buď jako anonymní upozornění na chybu systému (vnitřní uspokojení z vlastní schopnosti a bez škodlivých následků), anebo jako činnost překračující hranici obecné normy s cílem poškodit klienta (organizaci, firmu, státní zájem etc.). V tomto případě jde o projev agrese zlobné (*angry aggression*), směřující k poškození či ničení cílového objektu.

Poznat projevy osobnosti v jednotlivých fázích činnosti je složitým úkolem, který je nutno řešit postupně s ohledem na hierarchii vlastní činnosti. Musí být respektována výchozí dovednost a znalosti pracovníka a jejich prožívání v normálních podmínkách práce a rovněž v kritických a extrémních situacích.

10.3 Osobnost a její charakteristika

Osobnost je v literatuře definována a posuzována z mnoha stránek jejich projevů. Nejčastěji je definice osobnosti charakterizována jako soubor vyhraněných vlastností, jejichž nositel se jimi charakterizuje v prostředí své činnosti.

Případně je pojmem osobnost označován nějaký jedinec, nacházející se ve význačném postavení (např. politik, vědec etc.) Toto hodnocení je svým pojetím charakteristikou sociologickou.

Univerzální znaky osobnosti podle V. Smékala [34] tvoří soubor znaků, které při hodnocení musíme mít na zřeteli, protože jsou „spíše dimenzemi než výlučnými kvalitami typu „vše nebo nic“. Z toho důvodu je nutno každou osobnost posuzovat z hledisek:

- celistvosti
- potenciálů
- struktury a funkce
- individuálnosti a specifičnosti
- proaktivnosti a reaktivnosti
- organizace
- integrovanosti
- subjektovosti

- vědomí
- poznání
- svobody a determinismu

Z uvedeného přehledu je pojem osobnost možno chápat jako individualizovaný systém psychických procesů, stavů a vlastností, které vznikají působením výchovy a předmětné činnosti jedince. Celkový obsah znaků osobnosti pak doplňují jeho sociální styky v konkrétní činnosti, která rovněž působí na přizpůsobování se daným podmínkám. Poznáním svých možností a vlastní regulací individuální podmínek a směru vývoje je člověk autorem své činnosti. Přitom zůstává ve svém vnitřním světě stálou bytostí, ale současně otevřenou změnám, tj. působení vnějších vlivů. Má ve svých rukách vlastní rozhodování a jednání, které v určitých situacích může být z osobního pohledu chápáno jako pozitivní vůči determinaci prostředí, ale v obecném pohledu může být kontraproduktivní činností. Záleží tedy na něm samotném, k jakému jednání se rozhodne, anebo jaké pohnutky v jeho myšlení budou převažovat nad základním stylem jeho prožívání a jednání.

10.4 Definice osobnosti

Osobnost je něco, co skutečně existuje a co má skutečné účinky. Behavioristé osobnost chápou jako odvozeninu chování, je samo jediným a pozorovatelným a měřitelným jevem, Teorie představuje rámec, který si může vytvořit každý na základě dokázaných skutečností k vysvětlení větších či menších problémů.

Interakci dynamických sil působících v životě každého člověka vysvětluje v teorii osobnosti kombinace vlastností. Mnoho lidí se vnitřně vymezuje v pojmech schopností a kontroly. Hrdost že jsem schopen ovládat nějaké médium, nějakou činnost, je pozitivní věc. Vědomí své schopnosti a přesvědčení o své jedinečnosti posiluje vědomí člověka a vytváří prostor pro další, navazující snahy se dále rozvíjet. Ale když se člověk definuje prostřednictvím toho, co dokáže na expertní úrovni a přestane se ve svém konání kontrolovat, (anebo sníží svoji schopnost sebekontroly), pak je svět bezpečných věci silně limitován. Protože věci mají tendenci být věcmi, ne lidmi. Profesionální mistrovství může začít stagnovat a tak ovlivňovat

osobní vývoj a působit kontraproduktivně. Stává se způsobem zastírání strachu ze sebe a složitosti okolního světa.

Počítače podporují růst a osobní rozvoj člověka, vývoj jeho schopnosti a znalostí. Zároveň však i možnost uvíznutí v pasti svých představ o jisté osobní výjimečnosti. Počítač na rozdíl od jiných věcí má své specifické kvality, které ho pro uživatele činí zvláště přitažlivým. Jeho odlišností od jiných forem zábavy je možnost individuálního využití funkcí a technických parametrů kdykoliv a k čemukoliv. Zvládání výpočetní techniky obecně je podporována již školou, dále rodinou a nakonec individuálním i profesionálním využitím.

K mistrovství v ovládání se lze dopracovat i samostatnou usilovnou činností. Tato skutečnost dělá z počítačů tak přitažlivou záležitost, že počítač postupně umožňuje plně rozvinout posedlost „perfektního zvládnutí“. Je možné realizovat i skryté osobní představy a tužby, které v extrémním případě se mohou stát nástrojem „ odplaty“ těm, kteří „ mi nevěřili, případně mi něco nedobrého udělali“.

Existují případy lidí-studentů informatiky, kteří předčasně ukončili studium jen proto, aby se mohli plněji věnovat práci s počítačem jako svému základnímu povolání. Je otázkou, zda nabyté zkušenosti zdokonalené osobní invencí budou jen prostředkem budování kariéry, anebo se stanou základem negativního (kriminálního) jednání. Lze předpokládat, že v některých případech může u jedinců vzniknout pocit vlastní výjimečnosti z dosažení úrovně znalostí nabytých vlastním přičiněním, které paralelně v prožívání vyvolají pocit neoprávněné moci. Záleží tedy na osobnosti daného jedince, jak s tímto prožíváním naloží, zda své schopnosti bude směrovat k dalšímu rozvoji, anebo ve směru opačném.

Podle zkušeností a názorů autorů řady publikací z oblasti psychologie práce Štikara, Rymeše, Riegla a Hoskovce [26] je nutné pro přesné identifikování osobnostních schopností a dispozic mít k dispozici představu o požadavcích práce – profesiogram. Stanovení jednotlivých požadavků se odvíjí od stanovení požadavků zadavatele, tj. organizace. Podle zkušeností z diagnostické práce však ne vždy je tento požadavek specifikován s určením požadovaných limitů.

V některých případech jsou naopak požadavky na zjištění osobnostních kvalit stanoveny jako kritérium běžným postupem psychodiagnostické práce nezjistitelné (např. požadavek na míru jistoty u nového pracovníka pro práci s finančními prostředky, zda je schopen se nedopustit krádeže). Takový požadavek nelze zjistit, je však možné identifikovat v profilu osobnosti tendence, které jsou na okraji přijatelného rozsahu daného jevu a z kombinace několika výsledků měření s určitou mírou pravděpodobnosti stanovit předpoklad jednání daného jedince v situaci, které představuje určitou míru rizika. Stanovit hranici, která by vytyčovala pravděpodobnou hodnotu osobního prožívání možného zvratu v jednání, je docela složité a lze vyvodit jen oblast či znaky, které by na možnost přechodu k agresivnímu jednání mohly vést.

Podle teorie Adolfa ADLERA (in Drapela, [23]) člověk usiluje o překonání pocitů méněcennosti zakotvených v dětství a o dosažení nadřazenosti. Úsilí o nadřazenost prospívá jedinci pouze tehdy, když je sociálně zaměřeno. Sebestředné, antisociální jednání o nadřazenost je regresivní, Adler je považoval za zdroj deviací chování a charakterových selhání. Zdravé projevy směřování k nadřazenosti se vyznačují činy, které prospívají všem lidem.

Důležité prvky tvoří volby cílů a cílesměrné chování. Pocity méněcennosti jsou psychologickým jevem, jejich základ je ve fyziologické stavbě lidského (dětského) těla. „Maskulinní protest“ je formou a zdrojem změn na vůli k moci, který později vede k manifestaci a usilování o nadřazenost. Situace nedostatku se změní na situaci dostatku prostřednictvím usilování o nadřazenost [30].

Pokusy bojovat o moc nebo antisociální usilování o nadřazenost vedou k poruchám, k přecitlivělosti a konečně k touze „postavit se sám proti celému světu“. Toto úsilí může v konečné podobě být zdrojem a počátkem či spouštěčem nečekaných projevů, které vedou ke snaze se v praktickém životě prosadit způsobem přinášejícím danému jedinci vnitřní uspokojení a pocit moci.

C.G.JUNG ve svém bádání vyslovuje názor, že každý je schopen vyjádřit svoji individualitu a jedinečnost. EGO člověka posuzuje jako spíše aktivní než reaktivní.

Upřesňuje pojmy „introverze – extraverze“, které vyjadřují zaměření jedince na svůj intrapsychický svět, nebo na své okolí. Ve své teorii využívá pojmů „ čtyř mohutností“, jejichž funkce je možno najít v procesech:

- Myšlení – zkoumá, co vnímaný předmět je.
- Cítění – oceňuje hodnotu předmětu.
- Smyslové vnímání- zahrnuje veškerou smyslovou činnost.
- Intuice – poznává skrytý význam předmětu.

Pojem přesunutá energie je dle názorů autora využita k hodnotným účelům. Podle jeho názorů lze vysuzovat, že procesy odehrávající se v myšlení člověka a charakterizující jeho EGO představují potenciál, jehož využití má pro daného jedince význam v pozitivním slova smyslu. Je předpokladem pro vytváření podmínek k získávání poznání a specializaci v oboru, kterému se jedinec věnuje jako svému povolání.

Raymond CATTELL považuje „osobnost je to, co umožňuje předpovědět, co daná osoba učiní v dané situaci“ [30]. Názor těsně souvisí s psychometrickým přístupem ke zkoumání osobnosti. Podle názoru Cattella poskytuje přesné měření základ pro vědecký pokrok a závěry je možno aplikovat přenosem do systému práce s lidmi.

Podrobnějším rozvedením rysové a faktorové soustavy lze zkoumat povahu osobnosti, provádět interpretaci jeho chování a individuálního zaměření. Poznané hodnoty představují podle této teorie základní faktory a limity, s nimiž může daný jedinec disponovat a které tvoří jeho energetický potenciál. Jedinečné a společné rysy jsou podle názoru autora vyvozovány ze způsobů chování, které se projevují či vyskytují s určitou mírou pravidelnosti a soudržnosti. Nejsou to jen abstraktní rysy, ale ty, které se projevují u většího množství lidí (jako společné rysy). Povrchové a pramenné rysy – povrchové – jsou zjevné v chování osoby, pramenné jsou zdrojem a příčinami tohoto chování. Konstituční rysy jsou prostředím utvářené a rovněž vlivy prostředí se podílí na jejich utváření. Schopnostní a temperamentové rysy ukazují, nakolik je schopen člověk schopen dosahovat určitých zvolených cílů. Zahrnují například inteligenci a fyzickou zručnost. Dynamické rysy jsou motivační síly, které jedince pohání a vybízí k určité činnosti. Výsledné poznatky jsou sumou informací, které napomáhají poznat skutečnou

profilovou stránku osobnosti a s určitou mírou pravděpodobnosti určit její skutečné dispozice a předpoklad chování.

Způsoby sběru dat jsou podle Cattella rozděleny na:

L – data (Life data) - odhalují chování jedince ve společenství a data jsou převážně získána zprostředkováním.

Q – data (Questionnaire) – získávají se zpracováním dotazníku, který je dané osobě předložen. Výsledek po zpracování je možné porovnat s L-daty a posoudit shodnost údajů.

T – data (objektivní testy) jsou výsledky zkoušek, které zkoumané osoby absolvují, aniž by měly odezvu k testovým proměnným, které se hodnotí.

Z vyšetření mají přednostní význam např. údaje z testu 16-PF, který prokazuje úroveň inteligence, sílu ega, dominance – submise, emocionálnost-realismus, úroveň tenze-uvolněnost apod.

Dynamika osobnosti spočívá v hodnocení dynamických pojmů a procesů, z nichž nejvýznamnější je (sentiment of self) - jáský sentiment. Tento faktor zahrnuje sebeuvědomění, sebehodnocení, touhu po sebevládě, uchování vlastní reputace, splnění mravních povinností apod.

Intrapersonální procesy je nutno hodnotit v souladu a vzájemné interakci všech dostupných faktorů. Závěrečným posouzením a vyhodnocením je možné stanovit profil osobnosti a případně posoudit hodnotu a předpoklady jejího chování.

Na základě výzkumů Abraham MASLOW dospěl k názoru, že sebeaktualizující proces u člověka je jeho neustávajícím úsilím. Stanovil 15 znaků, které se u osob vyskytují a jsou ve svých projevech shodné.

Odstup a potřeba soukromí. Osoby dokáží být sami, aniž by cítily osamění. Mnozí se velmi cení samoty a soukromí.

Nezávislost na kultuře a okolí – autonomie a asertivita. Vlastní soudy jsou jim přednější, než kulturní normy a sami razí svůj životní styl v souladu se svými potřebami. Vyznačují se sebekázní, rozhodností a odpovědností. Jsou poměrně stabilní při vystavení nějakým tlakům okolí, protože nejsou závislí na souhlasu druhých.

Humor bez nepřátelství – žertování je zacíleno na nesrovnalosti v situacích, nikoli na slabosti druhých.

Originalita a tvořivost – Jedinci mají bohatou představivost a využívají fantazii při zvládání různých problémů.

Sebetranscendence – sebepřesažení je pokládáno za dominantu příznačnou pro tento typ jedinců.

Problémem je paradox – při pokusu popsat složitý postoj k vlastnímu „já“ u růstově zaměřené, sebeaktualizující osobnosti. Osoby se silou ega zapomínají na své ego, dokáže se nejvíce zaměřit na problém, zapomíná na sebe, je spontánnější. To představuje základ pro vytvoření jisté zaměřenosti až zarputilosti při řešení nějakého problému, který se vyznačuje obtížností či náročností. Jde o možnost vytvoření osobnostního zaměření se na prokázání svých schopností bez ohledu na vnitřní omezení, spočívající v interiorizovaných hodnotách, daných výchovou nebo naučených činností. Obecné hodnoty přestávají být překážkou a jsou nahrazeny spontaneitou vedoucí k získání převahy nad sebou samým.

10.5 Poznávací procesy

Kritériem myšlenkových operací a logických kritérií je tvořivé myšlení spojené s jinými procesy syntetického charakteru a v souvislosti s určitými prvky reality [31].

V těchto souvislostech má velký význam novost poznání, efektivnost, užitečnost, které jsou součástí každého nového objevu. Přestože se na první pohled mohou jevit jako nesmyslná, platí zde jiná pravidla než jen logika (formální disciplína, podobně jako matematika, využívá pouze některé části).

Při každém objevu a pravděpodobně u každé objevené operace je vždy poznání určitých příčinných, účelových a instrumentálních vztahů a souvislostí reality, které lze využít [31]. Na vzniku a využívání operací se podílí:

- učení, nápodoba a výcvik
- smyslové, intelektuální a jiné dispozice biologického základu
- kognitivní a jiné aktivity vyplývající z činnosti a řízení člověka směrované k určité činnosti.

Podle vyjádření řady badatelů (např. Piaget, Cattell, Chalupa et all.) má hlavní úlohu v poznávání nových způsobů činnosti v různých oborech lidský subjekt. Přestože jsou k využití v různých oborech činnosti stroje, nástroje a pomůcky, vždy je součástí těchto aplikovaných metod myšlenkové procesy člověka jako základní zdroj řešení problémů.

Východiskem je psychický obraz reality, který vychází z poznání skutečného stavu, jeho vyhodnocení v rámci dosažených (dosažitelných) informací osobností, jejím vědomím a mírou aktivity. V případě nesouladu s předpokládaným, nebo požadovaným a nutným stavem může nastat problémová situace a její řešení vyžaduje zvolení určitého postupu.

Podle Chalupy [31] je možné zvolit základní bloky:

Popis funkcí systému

1. předmět poznání a praktického působení
2. strukturu činnosti
3. systém psychické regulace činnosti
4. kognitivní a operativní modely
5. výsledky a produkty činnosti

Systém psychické regulace

1. psychické procesy
2. psychické obsahy
3. procedury
4. psychické stavy a vlastnosti

Kognitivní modely

1. konkrétně názornou formu
2. abstraktně názornou formu
3. pojmově sémantickou formu
4. relačně sémantickou formu

Použití některé z těchto variant je nutné přizpůsobit dané potřebě, v případě hledání a nalézání nových přístupů k řešení zvolené činnosti v systému práce s programem a manipulací v něm.

10.6 Řešení problémů a kreativita

Práce v oblasti výpočetní techniky je spojena s požadavkem připravenosti a schopnosti řešit samostatně řadu problémů, které s výkonem činnosti jsou spojené. V nemalé míře je to však i odpovědnost či spoluodpovědnost při zpracování informací, mnohdy důvěrného charakteru. Specifika práce vyžaduje postupy a činnosti, které se vyznačují osobnostními charakteristikami jednotlivých projevů, tj. systematičností, racionalitou myšlení, schopností řešit nečekané nebo složité problémy v relativně krátkých časových úsecích. V neposlední řadě jde o dispozici být přístupný málo používaným způsobům řešení, případně být schopen řešit úkoly nové, neznámé či nepoznané. Rozčlenit je na dílčí postupy a tyto jednotlivě poznávat, spojovat a tvořit tak smysluplný výsledek.

Podle Belze a Siegrista [33] jsou zásady kreativity a schopnost řešit problémy tyto:

- Nic není problém.
- Nejsou-li otázky, nejsou odpovědi.
- S cílem před očima se dá zvládnout i ta nejtěžší cesta.
- Řešení problémů a kreativita se nedá vynutit.
- Do Říma vede vždy více cest.
- Nemáme k něčemu odvahu nikoliv proto, že je to obtížné, ale protože k tomu nemáme odvahu, je to obtížné.
- Kam bychom došli, kdyby všichni říkali „Kam bychom došli?“ a nikdo by se nešel podívat, kam bychom došli, kdybychom šli.

Schopnost dobře strukturovat problém je základním východiskem, které by měl schopný pracovník v oblasti informačních technologií zvládnout.

10.7 Agrese a agresivita

Agrese patří do repertoáru chování lidí a z pohledu psychologie představuje složitou problematiku pro svoji širokou škálu projevů. Člověk je schopen agresivně myslet, komunikovat, snít, ale také se agresivně chovat [32].

Agrese označuje vlastní pozorovatelné chování a v jistém smyslu představuje vnitřní pohotovost organismu se agresivně chovat. Jde o vnitřní dispozici, nebo osobnostní vlastnost, které je většinou chápána jako relativně stálá

s problematickou regulací svého chování. Ve svých projevech se může agresivita projevit i v pozitivním projevu, např. při pomoci někomu v kritické situaci jako ochrana osoby a bez úmyslu poškodit druhé.

Přesto je nutné brát v úvahu možnosti projevu v životě člověka, který svoji agresivitu dovede skrýt a využít jen pro vlastní prospěch, bez vystavování na odiv druhým lidem. Znaky tohoto druhu jsou destruktivní a cíl je někoho poškodit, nějakým způsobem mu ublížit, třebaže zde nejde o projev viditelný. Citové projevy agresora mohou být různé, od uspokojení z akce, až po škodolibou radost, že poškozený v podstatě nemá možnost přímé obrany.

Výrazná destruktivní agresivita je v psychologii posuzována jako porucha osobnosti a signalizuje narušení vztahu dané osoby s realitou.

Psychologické pojetí zdrojů kriminálního jednání podle Čírtkové [32]:

- Jako důsledek impulzivního životního stylu.
- Jako instrumentální chování.
- Jako důsledek přizpůsobení se skupině.
- Jako důsledek neadekvátních strategií při zvládání stresu.

Impulzivní osobnost se podle autorky zpravidla utváří jako souhrn dispozic a daného prostředí. Prostředí, které jedince formuje od útlého mládí (zpravidla v rodině) má rozhodující význam pro pozdější osobnostní projevy daného jedince. Jeho vnitřní prožívání i názory nejsou konformní s obecným pojetím správného jednání a mohou se svými důsledky projevit jako svérázný projev etiky jednání, spravedlnosti apod. Tato stránka osobnosti může způsobit v konkrétním pracovním zařazení problémy v dodržování jak společenského úzu, tak i v plnění pracovních povinností,

10.8 Výběr pracovníků

V psychologii práce byla pro výběr pracovníků vydána řada metodologických materiálů a pomůcek, které jsou mezi psychology uznávány pro svoji kvalitu a odpovídající možnosti využití v diagnostické činnosti.

Pro stanovení požadavků na výběr pracovníka má významnou funkci analýza pracovního místa s popisem činnosti, kterou má pracovník vykonávat. Obsah analýzy je nedílnou součástí vlastní přípravy celého diagnostického procesu a současně slouží jako podklad k výběru metod pro proces posouzení

způsobilosti konkrétního pracovníka. Výsledek a hodnota ověřených osobnostních dispozic a profilu osobnosti slouží pro zařazení pracovníka na určitou funkci a pracovní místo.

Po získání základních informací o pracovníkovi je nutné využít osobnostní dotazník, ve kterém je mapována jeho životní historie. Získané údaje jsou významným prvkem pro vytvoření uceleného komplexu potřebných dat a jsou součástí dokladů pro zpracování celkového závěru s příslušným doporučením.

Součástí vytvoření celkového osobnostního profilu pracovníka je i objektivní hodnocení předchozího pracoviště (v případě čerstvého absolventa studia hodnocení školy). Možná struktura je následující:

1. Pracovní výsledky
    - odborná způsobilost
    - dosahování stanovených cílů, úkolů
    - dodržování časových limitů při plnění úkolů
2. Pracovní chování
    - poměr a vztah k novým úkolům a pracovním situacím
    - dispoziční schopnosti
    - pracovní odpovědnost a spolehlivost
    - styl práce a rozhodování v náročných situacích
3. Sociální chování
    - spolupráce s dalšími kolegy a pracovníky
    - ochota a spolehlivost při řešení nečekaných úkolů
    - projevy sounáležitosti k dané organizaci

Vyhodnocení je nejčastěji prováděno hodnotící stupnicí a podle zvolené škály, buď jako školní hodnocení 1 – 5, nebo 1 až 10, případně slovní formulací, například výrazy:

- 1 – vynikající
- 2 – poměrně dobrý
- 3 – přijatelný
- 4 – poměrně špatný

- 5 – špatný

Případné další formy mohou být:

- má hluboké znalosti v oboru, je schopen tvořit originální postupy řešení,
- má dobrý přehled o oboru, je schopen pracovat pod vedením,
- ovládá běžné rutinní úkoly, pracuje samostatně,
- v některých situacích potřebuje vedení a kontrolu nad výsledky své činnosti
- jeho znalost oboru je slabá, může pracovat pouze pod dozorem, je nesamostatný.

Metodu hodnotících stupnic lze prezentovat jako grafickou škálu, která vyjadřuje v číselné hodnotě dosažený výsledek práce a současně může být doplněna stručným komentářem.

Pro kategorii pracovníků v profesích programátor, analytik, operátor počítačů nebo technický zaměstnanec jsou využitelné a vhodné standardizované psychologické metody například:

- Testy všeobecných schopností.
- Testy schopností pro nové technologie NIT.
- Cattellův 16 faktorový dotazník 16PF.
- Gordonův inventář profilu osobnosti GPP-I.
- Pětifaktorový indikátor osobnosti NEOPS.
- Indikátor stresu v zaměstnání OSI.
- Projektivní metody.
- Názorové řady.

Případně další standardizované testové materiály, které se k výzkumu osobnosti pracovníka průběžně doplňují.

11 OSOBNOST PRACOVNÍKA V OBLASTI IT

Zkoumání vzorku pracovníků - profesionálů v oblasti IT

Cílem zkoumání bylo ověření struktury osobnosti odborníků pracujících v oblasti informačních technologií. Předpokládanými osobnostními projevy byl profesní zájem, míra snahy být sám sobě regulátorem dosahování cílů, které představují jistou výjimečnost svým významem, posláním i možnostmi. Orientace osobnosti v zátěži, míra projevů osobnosti realizovat se pouze na oblast pracovních povinností, rozsah motivace a kognitivních schopností.

Byla sledována osobní snaha dosahovat obecného uznání v odhalování možností dalších kvalitativních změn v oboru, případně snaha prezentovat své úspěchy mezi spolupracovníky. Také schopnost osobní prezentace, přínos vnitřního uspokojení a uznání schopnosti (altruistic aggression – agrese zaměřená na ochranu jiných).

11.1 Důvod stanovení obsahu zkoumání.

Poznání struktury osobnosti pracovníka v oblasti IT a jeho projevová stránka může představovat přínos pro vytvoření nových bezpečnostních prvků do kybernetické bezpečnosti organizací a celkového procesu systému. Poznatky z výzkumu podporují reálné možnosti k vytvoření systému práce s pracovníky, kteří na vybraných místech pracují, případně budou na pracovní místa vybíráni. Poznat projevy osobnosti ve fázích činnosti je aktuálním úkolem, který je nutno řešit od vstupu pracovníka do organizace až po konkrétní vlastní činnost při výkonu práce. Musí být respektována výchozí dovednost a znalosti pracovníka a jejich prožívání v normálních podmínkách práce a rovněž v kritických a extrémních situacích.

11.2 Postup diagnostického šetření.

Realizace vyšetření: psycholog, právník

Účastníci: Byli do zkoumání zařazeni po projednání s realizátory projektu na základě dobrovolnosti. Byla zaručena anonymita probandů (zkoumaných osob) - identifikace kódem.

Prostor pro vyšetření: pracovitě psychologa, klidná místnost vybavena stoly a židlemi, dostatečně osvětlená, tepelné podmínky standardní.

Počet účastníků: **4** Věková struktura dle dat narození- **proband č. 1** - 11 / 1981, **proband č. 2** - 10 / 1987, **proband č. 3** - 2 / 1988 a **proband č. 4** - 4 / 1977. Průměrný věk: 30 let

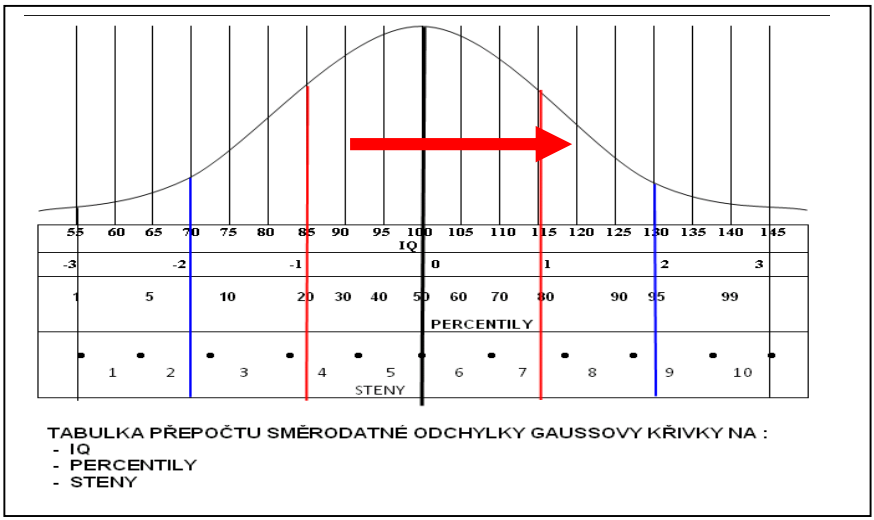
Pomůcky: testové materiály, psací potřeby, stopky, záznamové listy

Diagnostická situace: účastníci seznámeni s průběhem vyšetření, všichni podepsali informovaný souhlas s průběhem vyšetření (v příloze).

Výběr metod (vzory v příloze) a stanovené časy snímání:

1) Osobnostní dotazník (nestandardizovaný - sestavený pro daný účel cca 20 min).
2) T-75 Cattellův 16 PF (cca 45 min.).
3) Big-five – NEOPS – pětifaktorová struktura osobnosti (cca 15 min.).
4) T-78 Bourdonova zkouška (35 min.).
5) T-52 Test koncentrace pozornosti (5 min.).
6) VMT Vídeňský maticový test (25 min.).
7) Baum-t projektivní test (cca 5 min.).

Předpoklad pro dosažení odpovídající hodnoty výsledků jsou v tabulce norm. rozdělení:



Obr. 20. Graf normálního rozdělení s vyznačením předpokládaného (a požadovaného) prostoru výsledků šetření *(zdroj vlastní)*

11.3 Výsledky šetření

Vyhodnocení anamnestického dotazníku

Dotazník byl sestaven s cílem posoudit vybrané události z průběhu dosavadního životního vývoje probandů a jejich vyhodnocením získat informace k doplnění výsledků celkového šetření.

Záměrem tohoto postupu je srovnání teoretických údajů z literárních zdrojů se skutečností, která se týká stávající populace osob, které se zabývají kybernetikou jako profesí.

Období dětství (ot. 1 až 6)

Není zaznamenána žádná významná událost mimo jednoho případu zranění při sportu.

Péče rodičů (ot. 7 až 12)

U žádného z probandů rodiče neuplatňovali tělesné tresty.

V jednom případě proband registruje rozvod rodičů (problém nyní není výrazný). Ostatní hodnotí rodičovský vztah jako harmonický.

Všichni probandi mají jednoho sourozence, se kterým mají dobré vzájemné vztahy.

Školní docházka (ot. 13 – 18)

Školní prospěch hodnotí všichni účastníci jako velmi dobrý jak v průběhu střední školy, tak školy vysoké (jeden v obráceném pořadí).

V průběhu studia měli většinou více kamarádů (jeden uvádí méně).

Problémy s učením neuvádí žádný.

V zaměstnání (ot. 19 – 30)

Žádný z účastníků neuvádí konfliktní vztahy s nadřízenými.

V hodnocení vlastních schopností na odborné úrovni se rovněž shodují, že jsou schopni řešit i náročnější úkoly své práce a rovněž svoji výkonnost hodnotí pozitivně.

Otázku, zda dobrá nápady sděluji dalším lidem, odpovídají negativně, anebo s jistou rezervou.

Osobní život (ot. 31 – 40).

Tři z účastníků se považují za klidného člověka, jeden připouští, že se někdy „rozčílí, nebo pohádá“.

Neschopnost někoho a křivdu hodnotí jako nepřijatelnou a vadí jim (jeden reagoval „nevadí mi“).

Zda jsou schopnější, než druzí hodnotí dva probandi „ano“, dva „ne“.

Mají hodně kamarádů a přátel (mimo jednoho).

Ostatní vyjádření nejsou podstatná a neovlivňují záměr dotazníku.

Závěr: zjištěné výsledky odpovídají názorům teoretických zdrojů. Předpokladem pro vytvoření pozitivního vztahu k práci a odbornosti je výsledkem pozitivní výchovné činnosti v rodině a interiorizace pravidel a obecně lidských zásad chování. Hodnotová orientace je dotvářena v dalším životě vlivy prostředí a druhem činnosti.

Vyhodnocení osobnostního dotazníku 16 PF

Výsledky všech probandů prokazují přibližně stejné výsledky v několika hodnotách, které se týkají vlastností:

- pozitivního vztahu k osobám ve svém okolí
- relativní stabilitě emocionálního prožívání
- kontrolované senzitivitě a vnímavosti
- realitě a praktičnosti s orientací na řešení problémů
- dostatečnému rozsahu vnímavosti ke změnám a schopnosti experimentovat
- sklonem k organizovanosti a sebedisciplině
- z globálních faktorů vystupuje do popředí otevřenost ke změnám a intuici.

Závěr: Zvýrazněné vlastnosti jsou pozitivními prvky osobnosti zkoumaných osob a vzhledem k druhu práce jsou přínosem pro jejich trvalou výkonnost. Ostatní faktory osobnosti jsou v obecně přijatelných normách, u žádného z probandů se neprojevila žádná extrémní hodnota. Zjištěné hodnoty lze přijmout jako obecnou normu pro výběr nových pracovníků.

Vyhodnocení testu BIG.five

Test poskytuje výsledky pěti faktorů projevů osobnosti, např.:

- neuroticismus – vysoký skór značí nestabilitu, snadnou narušitelnost vyrovnanosti,
- extraverze – vysoký skór značí sebejistotu, aktivnost, hovornost, energičnost, optimismus,
- otevřenost – vysoký skór – bohatá fantazie, vnímavost k pozitivním i negativním emocím, nové myšlenka, nekonvenčnost,
- přívětivost – vykazuje interpersonální chování; vysoký skór značí pochopení,
  a porozumění jiných, altruismus, laskavost, vlídnost,
- svědomitost – vysoký skór prokazuje cílevědomost, ctižádost, pracovitost, disciplinovanost.

Závěr: Naměřené hodnoty prokazují (kromě 1 případu nízké hodnoty extraverze), že všichni probandi prokazují pozitivní hodnoty svých výsledků a jsou vhodnými typy pro práci v prostředí kybernetické činnosti. Doporučené věkové normy lze využít v rámci výběrového procesu.

Vyhodnocení testu Bourdonova zkouška

Jde o náročnou zkoušku schopnosti koncentrace pozornosti, jejímž výsledkem je křivka výkonu, spolehlivost a míra chybovosti a prokazuje schopnost snášet zátěž.

Výsledek probandů v průměru prokazuje velmi dobrou schopnost koncentrovat svoji pozornost v časovém stresu (kromě 1 probanda, který se prokázal vyšší míru nepozorností).

Závěr: Celkově chybovost u vzorku zkoumaných osob byla na nízké úrovni, celkový výkon v mírném nadprůměru. Je to znak propojení snahy po dosažení kvalitního výsledku i v podmínkách požadavku koncentrace a současně naznačuje dobrou osobní motivaci. Metodu je možné doporučit jako součást výběrového řízení.

Test koncentrace pozornosti

Test měří (diferenciační) psychomotorické tempo, správnost psychomotorického výkonu, sklon k chybnému výkonu, psychické tempo,

intelektovou úroveň, zprostředkovaně i impulzivnost a další osobnostní rysy (motivaci, ochotu atd.)

Výsledky probandů prokazují ve dvou případech vysokou míru sebekontroly (až přílišnou opatrnost), která ovlivnila kvantitu výkonu, ale zvýraznila kvalitu dosaženého výsledku. Výsledek dalších dvou se pohyboval v průměrných hodnotách s vyšší mírou motivace i výkonu, výsledek je v hlavních rysech podobný předchozímu výsledku.

Závěr: kvalita výkonu u všech dosáhla vysoké hodnoty, přístup k úkolu byl odlišný, motivace byla na úrovni zadání. Je vhodnou metodou pro výběr pracovníků.

Test VMT - Vídeňský maticový test

Test je určen ke zjišťování úrovně neverbální inteligence a patří k jednodimenzionálním testům k měření jedné složky inteligence. Test pracuje se schopnostmi usuzovat, odhalovat vzájemné souvislosti a vyvozovat vztahy, které se považují za základní dimenze obecné inteligence.

Výsledek testu prokazuje u třech probandů vcelku vyrovnané hodnoty, u jednoho se projevil problém spočívající v neschopnosti řešit zadaný úkol v požadované úrovni. V rozhovoru sdělil problém s osobním vnímáním úkolu. Celková hodnota naměřené hodnoty IQ je 106, ev.115 (bez 1 účastníka, jehož hodnota byla 77).

Závěr: Hodnoty naměřené testem VMT dávají předpoklad pro výkon práce a jeden případ vybočující z průměru zřejmě není problémem – v daném případě je pracovník hodnocen vedením organizace pozitivně. Při posouzení dalších znaků z procesu šetření je u jednotlivce zřejmě nutné posuzovat širší souvislosti. Lze využít i další standardizované metody.

Projektivní metoda – Baum-test

U žádného probanda nebyl zjištěn příklon k nějakému projevu psychické poruchy a výsledky byly na úrovni standardních projevů. V navazujícím rozhovoru s probandy byly upřesněny některé otázky, které vyplynuly z procesu šetření a týkaly se jednotlivostí ve výsledcích.

Závěr k diagnostickému šetření a doporučení

Celý proces diagnostického šetření byl zaměřen na zjištění osobnostních předpokladů osob pro práci v oblasti informačních technologií s důrazem na schopnosti, přesahující běžný rámec pracovních povinností (tzv. “hackerů“).

Byla zvolena diagnostická baterie odpovídající využití standardních psychologických metod. Diagnostická situace a postup byl realizován v rámci stanovených zásad a postupů s dodržením etiky práce psychologa.

Výsledky šetření osobnostních projevů a dispozic zkoumaných osob prokazují, že dodržením zásad správného výběru a naplněním požadavků profesiogramů na vybrané funkce je možností jak zabezpečit odpovědný výkon činností v oblasti informačních technologií. Stanovení náročných požadavků na výběr pracovníků a jejich osobnostní kvality je základním krokem k realizaci kybernetické bezpečnosti.

Tab. 4. Anamnestický dotazník

ANAMNESTICKÝ DOTAZNÍK				
Vyplněno dne:		**muž**	**žena**	**Datum narození**:
Vzdělání : **SŠ** – směr: **VŠ** – směr: **Další vzdělání**:				
Povolání:				
Ot. č.	**NE**	**Odpověď označte ve sloupci ANO/NE X**	**ANO**	**Pokud ANO,** upřesněte stručně významné okolnosti:
V dětství:				
1		začal jsem pozdě mluvit, koktal jsem, noční pomočování apod.		
2		byl jsem v náhradní péči		
3		prodělal zánět mozkových blan		
4		měl jsem úraz hlavy s bezvědomím		
5		měl jsem psychické problémy		
6		měl jsem problémy s kázní		
Péče rodičů:				
7		byla velmi srdečná		
8		měl jsem přísnou výchovu		
9		byl jsem často za prohřešky bit		
10		rodiče se rozvedli		
11		měl jsem _____sourozenců		

12		měl jsem konflikty se sourozenci		
Ve škole:				
13		Měl jsem: průměrné výsledky dobré výsledky velmi dobré výsledky		
14		měl jsem konflikty s učiteli		
15		byl jsem spolužáky šikanován		
16		měl jsem mnoho kamarádů		
17		nevyhledával jsem kamarády		
18		byl jsem v psychologické poradně s problémy s učením nebo kázní		
V zaměstnání:				
19		měl jsem (mám) konflikty s vedoucím		
20		měl jsem (mám) konflikty se spolupracovníky		
21		považuji vedoucího za méně schopného		
22		mám za to, že jsem schopen řešit náročné úkoly svého oboru		
23		jsem schopen podat lepší výkon než kolegové		
24		mám více dobrých nápadů, které si nechávám pro sebe		
25		rád odborně radím druhým pracovníkům		
26		jsem vůči nesprávnému jednání na pracovišti kritický		
27		pracovní úkoly řeším raději sám a aktivně		

28		problémy které se mě netýkají, neřeším		
29		myslím, že jsem na pracovišti oblíben a uznáván		
30		v pracovním kolektivu se cítím dobře		
V osobním životě:				
31		považuji se za klidného a racionálně uvažujícího		
32		konflikty řeším klidně a rozvážně		
33		nespravedlnost mě dokáže „vytočit“		
34		neschopnost lidí mě vadí a snažím se ji řešit		
35		jsem schopen křivdu vůči sobě pachateli vrátit		
36		křivdy z mládí si pamatuji dodnes		
37		mám rád svoji rodinu, věnuji jí veškerý volný čas		
38		myslím, že jsem schopnější než spolupracovníci		
39		mám hodně kamarádů a přátel		
40		je málo věcí v životě, které mi vadí		

Prostor pro volné poznámky, doplňky:

VYHODNOCENÍ 16PF-V.verze (protokol)

SROVNÁNÍ VÝSLEDKŮ VŠECH PROBANDŮ

Probandi 1 – 2 – 3 - 4

PRIMÁRNÍ FAKTORY

Tab. 5. Vyhodnocení 16PF-V.verze (protokol)

Faktor	sten	Význam na levé straně (nízký skór)	Standardní skór STEN										Význam na pravé straně (vysoký skór)
						průměr							
			1	2	3	4	5	6	7	8	9	10	
A Vřelost		Rezervovaný, neosobní, odměřený	•	•	•	•	•	•	•	•	•	•	**Vřelý,společenský,pozorný ke druhým**
B Usuzování		**Konkrétní**	•	•	•	•	•	•	•	•	•	•	Abstraktní
C Emocionální stabilita		Reaktivní,emocionálně nestálý	•	•	•	•	•	•	•	•	•	•	**Emocionálně stabilní,přizpůsobivý,zralý**
E Dominance		Submisivní, **kooperativní**,vyhýbá se konfliktům	•	•	•	•	•	•	•	•	•	•	**Dominantní,energický, asertivní**
F Živost		Vážný,**zdrženlivý, opatrný**	•	•	•	•	•	•	•	•	•	•	**Plný života,** živelný,spontánní
G Zásadovost		**Přizpůsobující si pravidla, nekonformní**	•	•	•	•	•	•	•	•	•	•	**Zásadový, se smyslem pro povinnost**
H Sociální smělost		Plachý,senzitivní k hrozbě, nesmělý	•	•	•	•	•	•	•	•	•	•	**Sociálně smělý,dobrodružný**, nezranitelný
I Senzitivita		Utilitární,**objektivní, nesentimentální**	•	•	•	•	•	•	•	•	•	•	Senzitivní,**vnímavý,** Sentimentální
L Ostražitost		Důvěřující,nepodezíravý, akceptující	•	•	•	•	•	•	•	•	•	•	**Ostražitý,podezíravý, skeptický,obezřetný**
M Snivost		**Realistický,praktický, orientovaný na řešení problémů**	•	•	•	•	•	•	•	•	•	•	Snivý,imaginární, orientovaný na nápady
N Uzavřenost		**Přímý, nefalšovaný, přirozený**	•	•	•	•	•	•	•	•	•	•	Uzavřený,**rezervovaný,** nepřístupný
O Ustrašenost		**Sebejistý**,bezstarostný, spokojený sám se sebou	•	•	•	•	•	•	•	•	•	•	Ustrašený,pochybující o sobě,sužující se
Q1 Otevřenost ke změnám		Tradicionalistický, vázaný na rodinu	•	•	•	•	•	•	•	•	•	•	**Otevřený ke změnám, experimentující**
Q2 Soběstačnost		Orientovaný na skupinu, družný	•	•	•	•	•	•	•	•	•	•	**Soběstačný,samotářský, individualistický**
Q3 Perfekcionismus		Tolerující neuspořádanost, neprecizní, **flexibilní**	•	•	•	•	•	•	•	•	•	•	Perfekcionistický, **organizovaný, sebedisciplínovaný**
Q4 Tenze		**Uvolněný, klidný, trpělivý**	•	•	•	•	•	•	•	•	•	•	Napjatý,**energický**,vnitřně neklidný

GLOBÁLNÍ FAKTORY

Faktor		Význam na levé straně				**Průměr**							Význam na pravé straně
			1	2	3	4	5	6	7	8	9	10	
EX Extraverze		Introvertovaný, se sociálními zábranami	•	•	•	•	•	•	•	•	•	•	**Extravertovaný,sociálně participující**
AX Anxieta		**Nízká anxieta, těžce vyveditelný z míry**	•	•	•	•	•	•	•	•	•	•	**Vysoká anxieta, lehce vyveditelný z míry**
TM Strnulost		**Přístupný,otevřený, intuitivní**	•	•	•	•	•	•	•	•	•	•	Tvrdohlavý, Rezolutní, neempatický
IN Nezávislost		**Přizpůsobivý,vstřícný, nesobecký**	•	•	•	•	•	•	•	•	•	•	**Nezávislý,přesvědčivý, svéhlavý**
SC Sebekontrola		**Neovládající se, řídící se pudy**	•	•	•	•	•	•	•	•	•	•	**Ovládající se, tlumící své pudy**

Vysvětlivka: - - - - - - - - - - - - - = předpoklad optimálního profilu pro výkon funkce

_____ = skutečný výsledek - profil probanda

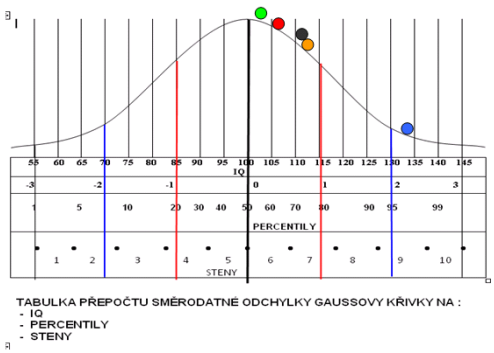
Faktor: EX **rozsah** 4 – 7-8
AX 1 – 6 max.
TM 5 – 6 – 7
IN 5 – 6 – 7
SC 5 - 10

SROVNÁNÍ VÝSLEDKŮ TESTU BIG-FIVE

PROBANDI 1-2-3-4

Výsledek hodnot testu BIG-five
v křivce normál.rozdělení
Proband č. 1

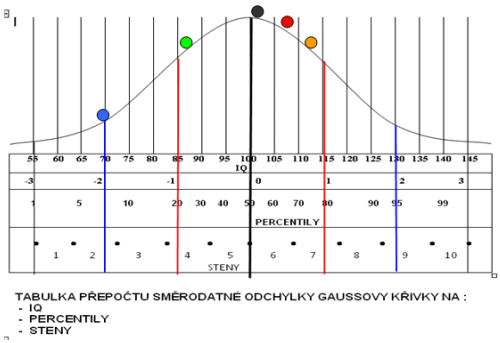
Proband	Věk	N	E	O	P	S
1	27	63	97	58	75	73



Obr. 21. Výsledek hodnot testu BIG-five u probanda č. 1 *(zdroj vlastní)*

Výsledek hodnot testu BIG-five
v křivce normál.rozdělení
Proband č. 2

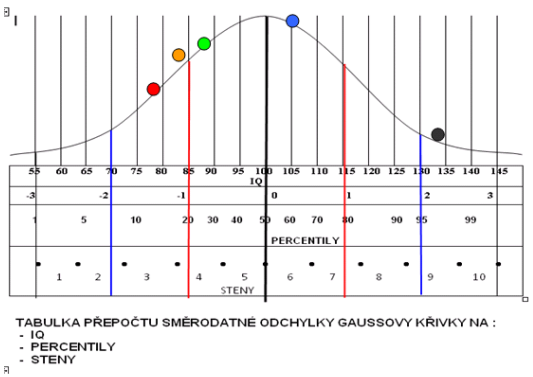
Proband	Věk	N	E	O	P	S
2	27	63	7	24	75	51



Obr. 22. Výsledek hodnot testu BIG-five u probanda č. 2 *(zdroj vlastní)*

Výsledek hodnot testu BIG-five
v křivce normál.rozdělení
Proband č. 3

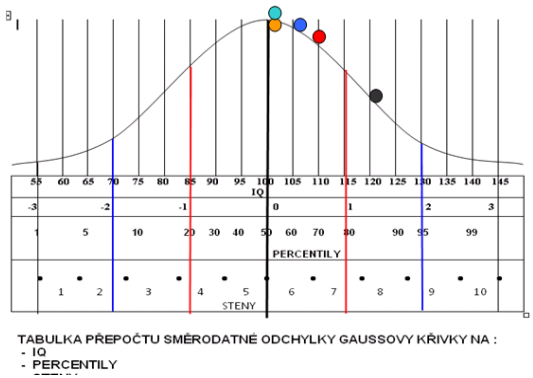
Proband	Věk	N	E	O	P	S
3	26	14	60	26	19	97



Obr. 23. Výsledek hodnot testu BIG-five u probanda č. 3 *(zdroj vlastní)*

Výsledek hodnot testu BIG-five
v křivce normál.rozdělení
Proband č. 4

Proband	Věk	N	E	O	P	S
4	37	70	63	53	53	85

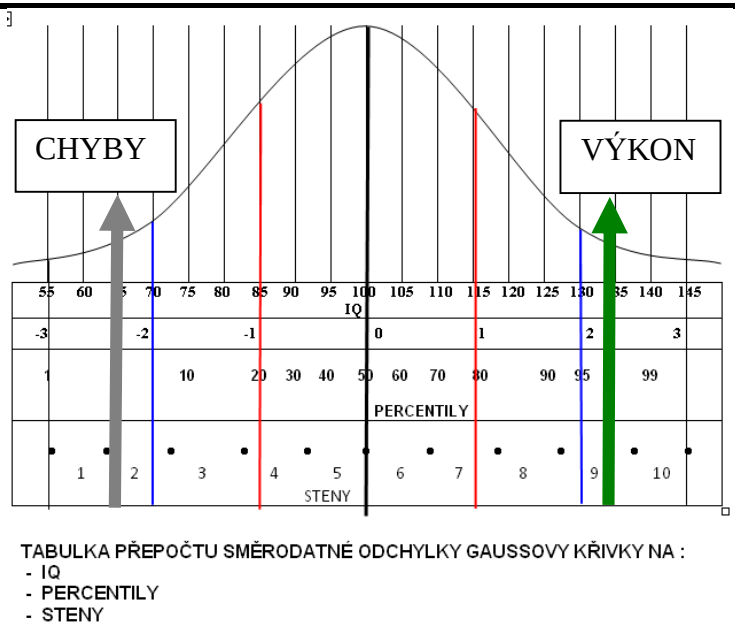


Obr. 24. Výsledek hodnot testu BIG-five u probanda č. 4 *(zdroj vlastní)*

VYHODNOCENÍ TESTU BOURDONOVA ZKOUŠKA

Tab. 6. Vyhodnocení testu Bourdonova zkouška

PROBAND Č. 1	PROBAND Č. 2	PROBAND Č. 3	PROBAND Č. 4
Výkon: 2402	Výkon: 2494	Výkon: 2111	Výkon: 2045
Počet chyb: 229	Počet chyb:45	Počet chyb:112	Počet chyb:61
Chyb na řádek:7,63	Chyb na řádek:1,5	Chyb na řádek:3,7	Chyb na řádek:2,0
HONOCENÍ V PERCENTILECH A STENECH			
VÝKON: 100	VÝKON: 100	VÝKON: 90	VÝKON: 90
STENY: 10	STENY: 10	STENY: 8	STENY: 9
% CHYB: 9,2	% CHYB: 1,8	% CHYB: 5,3	% CHYB: 2,98
PRŮMER ZA SKUPINU			
VÝKON : 2263 = 95 PERCENTILŮ = 9 STEN (z 10 st. škály)			
Počet chyb: 112 = 2 sten			



Obr. 25. Grafické znázornění výsledku testu Bourdonova zkouška *(zdroj vlastní)*

TEST KONCENTRACE POZORNOSTI A VÝKON V ČASE

Použitá forma testu: A

Proband č, 1 : 1,00

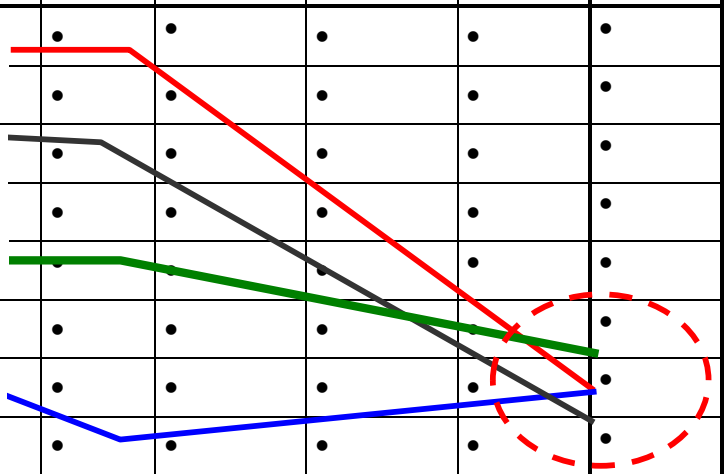
Proband č. 2: 0,990

Proband č. 3: 0,988

Proband č. 4: 1,00

Tab. 7. Test koncentrace pozornosti a výkon v čase

Znaky	Řešeno	Správně	Vynecháno	Špatně škrt.	Chyby celkem	SPR./ ŘEŠ.
č.1	47	47	0	0	0	1,00
č.2	108	107	1	0	1	0,990
č.3	85	84	1	0	1	0,988
č.4	71	71	0	0	0	1,00
STENY č.1 č.2 č.3 č.4						9 7 7 9
1.	•	•	•	•	•	•
2.	•	•	•	•	•	•
3.	•	•	•	•	•	•
4.	•	•	•	•	•	•
5.	•	•	•	•	•	•
6.	•	•	•	•	•	•
7.	•	•	•	•	•	•
8.	•	•	•	•	•	•
9.	•	•	•	•	•	•
10.	•	•	•	•	•	•

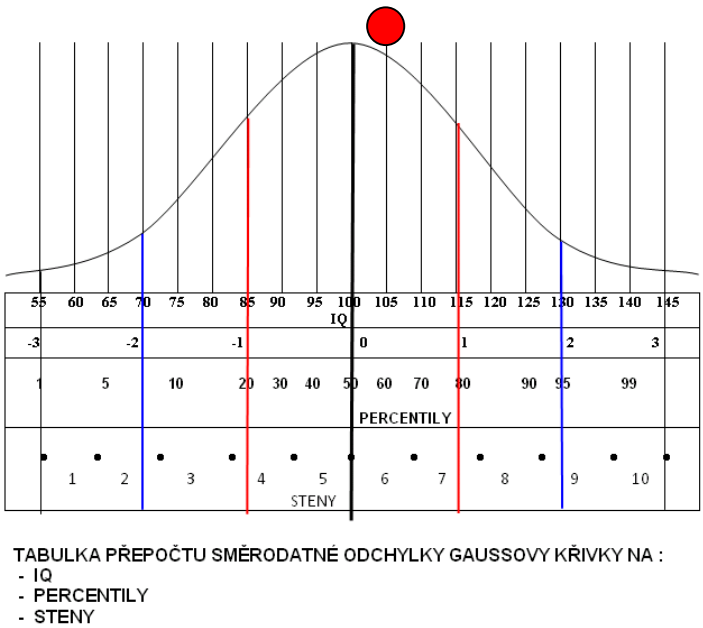


VYHODNOCENÍ TESTU VMT

Probandi 1-2-3-4

Tab. 8. Vyhodnocení testu VMT

Proband č.	výkon			
	řešeno	nesprávně	výkon celkem	přepočet na IQ
1	24	15	9	77
2	24	2	22	120
3	24	3	21	116
4	24	6	18	110
průměr za skupinu				
Σ	24	6,5	17,5	106



Obr. 26. Grafické znázornění výsledku testu VMT *(zdroj vlastní)*

11.4 Dílčí závěr

V kapitole jsou popsány výsledky zkoumání osobnostního profilu vybraných probandů – profesionálů v oblasti IT technologií. Cílem výzkumu bylo potvrzení předpokladu vycházejícího z teoretických zdrojů pro posuzování osobnostního profilu pracovníků vybraných profesí. Výsledky standardizovaného psychologického šetření prokazují, že péče věnovaná výběru pracovníků je nutností, která by měla být systémovou součástí procesu výběru a přijímání nových pracovníků na exponovaná pracovní místa v oblasti informačních technologií. Cílem je vytvoření podmínek pro eliminaci negativních vlivů osobnostních faktorů pracovníků, kteří nejsou schopni se v plné míře vyrovnat s některými svými osobnostními prožitky a v konečné formě je mohou řešit ve své činnosti. Důsledný a promyšlený výběr a vstupní ověřování osobnostních dispozic jsou východiskem k vytvoření bezpečnostní bariéry, která spolu s průběžnou kontrolou činností může vytvářet odpovídající podmínky pracovního procesu.

12 PRACOVIŠTĚ KYBERNETICKÉ BEZPEČNOSTI

Pohled na kybernetickou bezpečnost se i v naší společnosti rapidně změnil. Dřívější vnímání bezpečnostních opatření, ať vyvolaných jako okamžitá reakce na vzniklé bezpečnostní incidenty a kriminální činy, nebo jako domnělá prevence před v čase neurčitými a nejasnými činy fiktivního útočníka a opatření, která řešila pouze instalace samostatných bezpečnostních technologií ve správě provozovatelů IT, je již minulostí. Dnes kybernetickou bezpečnost vnímáme jinak. Útoky na aktiva organizací, na jejich řídící, komunikační a informační infrastrukturu jsou na denním pořádku. Útočníci jsou sice stále ještě převážně anonymní, ale velmi reální a následky jejich činů jsou hmatatelné a mnohdy nevyčíslitelné. Dnešní pohled na kybernetickou bezpečnost je pohledem vnímajícím ji jako komplex cílených a systémových opatření, která jsou především nutností a tedy ne jen dobrovolným počinem bez zcela jasného přínosu. Zahrnují jak organizační, tak technická i personální opatření, která postupně bezpečnost aktiv a systémů nejen zavádí, ale kontinuálně vylepšují. Takovou činností se na straně jedné staví účinná hráz proti kriminálním činům útočníků, na straně druhé však nabývá na objemu množství informací a dat, které bezpečnostní technologie produkují a které je nutné zpracovávat. Existují sice automatizované nástroje, se schopností zpracovat obrovská množství událostí, ale i ty vyžadují nejen obsluhu, ale i specialisty s analytickými schopnostmi pro jejich konfigurace a správné využití. Úměrně s velikostí organizace rostou i nároky na počty takových osob, které se bezpečnosti věnují jako své hlavní pracovní činnosti. Přichází a rostou požadavky nejen na technické a analytické specialisty, ale také na specialisty se schopností koordinace řešení kybernetických bezpečnostních hrozeb, událostí a incidentů, ale také na manažery řídící celé bezpečnostní týmy a právě takovým týmům se věnuje tato kapitola.

Z původních amatérských bezpečnostních týmů, které se sdružovaly v různých komunitách, se postupně zformovala profesionální pracoviště, obvykle i se stálým finančním rozpočtem. Prvním týmem s vlastní definovanou strukturou byl tým, který vznikl již v roce 1988 na americké univerzitě Carnegy Mellon, jehož značka CERT (Computer Emergency Response Center) se postupem doby stala certifikátem a etalonem pro nově vznikající profesionální kybernetické bezpečnostní týmy a pracoviště.

Computer Emergency Response Center (CERT) – vyšší typ bezpečnostního pracoviště. Jedná se o skupinu specialistů, kteří identifikují a řeší kybernetické bezpečnostní incidenty (KBI) organizace.

Security Operations Center (SOC) – základní typ bezpečnostního pracoviště. Vyvinul se z původních provozně-bezpečnostních dohledů a je tak pracovištěm na provozní úrovni. Jeho specialisté se věnují dohledu nad provozem bezpečnostních technologií a vyhodnocování zachycených kybernetických bezpečnostních událostí (KBU).

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) – bezpečnostní tým z prostředí kritické infrastruktury, chránící řídicí systémy a snižující rizika jejich ohrožení.

Computer Security Incident Response Center (CSIRT) – alternativní název k CERT, s prioritním zaměřením na řešení kybernetických bezpečnostních událostí **(KBU**), kybernetických bezpečnostních incidentů (**KBI**) a sdílení informací.

Governmental Computer Emergency Response Center (GovCERT) – vládní tým CERT, s prioritním zaměřením na řešení KBU, KBI a sdílení informací ve státní správě a v mezinárodním měřítku.

Computer Incident Response Capability (CIRC) – bezpečnostní tým z armádního prostředí, chránící důležité segmenty stacionárních i polních informačních systémů AČR.

12.1 Typy bezpečnostních pracovišť

Pracoviště na provozní úrovni - SOC

Charakteristika pracoviště:

- Základní komunikační a dohledové pracoviště.
- Dohled nad provozem bezpečnostních technologií.
- Základní vyhodnocování KBU z logů a ze senzorů.
- Obsluha nástroje SIEM.
- Příjem informací o KBU/KBI.
- Řešení KBU/KBI na základní úrovni.
- Sdílení informací.

- Směna 24/7.

Role:

- Operátoři SIEM.
- Analytici KBU/KBI.
- Bezpečnostní manažer / koordinátor.

Pracoviště na vyšší, tzv. taktické úrovni - CERT, CSIRT, CIRT

Charakteristika pracoviště:

- Komunikační a dohledové pracoviště.
- Analytické pracoviště.
- Příjem informací o KBU/KBI.
- Příjem a výměna informací o KB zranitelnostech a hrozbách, o malware.
- Zpracování pokročilých analýz.
- Klasifikace KBU/KBI.
- Koordinace řešení KBU/KBI.
- Schopnost sestavit mobilní tým rychlé reakce (RRT).
- Směna 24/7.

Role:

- Operátoři SIEM.
- Analytici KBU.
- Analytici malware.
- Koordinátoři.
- Bezpečnostní manažer.

Pracoviště na nejvyšší, tzv. strategické úrovni - Centrum KB

Charakteristika pracoviště:

- Komunikační a dohledové pracoviště (SOC).
- Analytická pracoviště se samostatnými týmy analytiků pro každý proces KB.
- Pracoviště provozu a rozvoje bezpečnostních technologií.

- Pracoviště informační a PR podpory.
- Pracoviště koordinace řešení KBU/KBI.
- Stálé jádro týmu rychlé reakce (RRT).
- Příjem a výměna informací o KBU/KBI.
- Příjem, získávání a výměna informací o KB zranitelnostech a hrozbách, o malware.
- Zpracování pokročilých analýz.
- Klasifikace a řešení KBU/KBI.
- Řešení KB hrozeb a zranitelností.
- Odhalování a testování malware.
- Penetrační testování.
- Aktivní investigativní činnost.
- Šíření bezpečnostního povědomí.
- Tréning a vzdělávání, organizace kybernetických cvičení.
- Metodická pomoc provozovatelům IS.
- Posuzování SW a HW z hlediska KB.

12.2 Procesy a role bezpečnostního pracoviště

Při výběru typu a velikosti bezpečnostního pracoviště, včetně rozsahu jeho služeb je nutné vycházet z předchozí analýzy bezpečnostních rizik. Ta odhalí, jakým bezpečnostním hrozbám je organizace vystavena. Odhalí zranitelnosti a slabá místa, definuje, jaká jsou aktiva a kde jsou soustředěna a jaký dopad by měla jejich ztráta. Tvorba bezpečnostního týmu pak spadá mezi přijatá opatření, která snižují rizika a chrání aktiva organizace před danými hrozbami. V okamžiku, kdy máme všechny potřebné vstupní informace, můžeme přistoupit k definování procesů, rolí a tvorbě projektu implementace pracoviště.

Obvyklé procesy:

- Zvládání bezpečnostních incidentů.
- Zvládání bezpečnostních zranitelností.
- Detekce a analýza malware.
- Provoz a rozvoj bezpečnostních technologií.
- Šíření informací.

- Zpracování doporučení, rad.
- Šíření bezpečnostního povědomí.
- Vzdělávání.

Při výběru vhodných procesů a šíře jejich implementace musíme zvážit i personální a finanční možnosti organizace. Nedostatečně obsazený tým bez patřičné finanční podpory není schopen naplnit všechna očekávání a naopak naddimenzované požadavky budou obtížně naplněny. Kritický je nedostatek dostatečně vyškoleného personálu a bezpečnostní technologie jsou velmi drahé. Nejen při pořízení, ale především při nutné pravidelné podpoře jejich provozu. V prvopočátku nasazení bezpečnostního týmu proto nejdříve volíme zavedení základních procesů a po jejich zvládnutí jejich prohloubení a rozšíření o další procesy.

Základní role:

- Operátor.
- Správce.
- Analytik.
- Koordinátor.
- Manažer.

Definování jednotlivých rolí vychází ze zaváděných procesů a z personálních a finančních možností. Každý bezpečnostní tým bude řešit KBU/KBI, proto musí obsadit role operátorů SIEM a bezpečnostních analytiků. Pokud tým bude ve větší míře komunikovat s partnery a provozní správou při řešení KBU/KBI, bude k tomu potřebovat další specialisty. Tým bude mít ve správě vlastní bezpečnostní nástroje a jiné technologie, a to bude vyžadovat vyškolené specialisty - správce. Procesy KB bude nutné řídit a koordinovat a k tomu bude zapotřebí odborníků nejen technicky zdatných pro zvládání KBU/KBI, ale i se znalostmi bezpečnostních politik, norem a legislativy. Informace o KBU/KBI bude nutné vhodně prezentovat a informace předávat partnerům, vedení organizace, publikovat na informačním portálu organizace, a to bude také vyžadovat další specialisty. Podle možností organizace lze dočasně některé role slučovat.

12.3 Bezpečnostní nástroje

Většina organizací má implementovány základní ochranné nástroje a řešení, jako jsou firewally, demilitarizované zóny (DMZ), překladače adres (NAT), proxy servery, antivirové a antimalware nástroje, systémy řízení přístupu apod. Vlastní také i některé z bezpečnostních prvků, jako jsou senzory Intrusion Detection System (IDS), Intrusion Prevention System (IPS), NetFlow senzory. Mohou mít nasazeny i nejrůznější skenery a nástroje kontroly zabezpečení a integrity. Možné úniky cenných a citlivých dat mohou sledovat pomocí nástroje Data Loss Prevention (DLP). Ke korelacím informací o bezpečnostních událostech a jejich analýze mohou používat i Security Information & Event Management (SIEM). V drtivé většině případů však tyto bezpečnostní nástroje nebyly pořízeny na základě naplňování bezpečnostní strategie, ale byly pořízeny při řešení konkrétního problému konkrétního místa datové sítě nebo informačního systému. Často je proto nelze vzájemně integrovat a tyto technologie tak nejsou schopny poskytovat smysluplné informace, které mohou být použity pro komplexní odhalování bezpečnostních hrozeb a incidentů a pro řízení procesů kybernetické bezpečnosti. Pořízení nákladných bezpečnostních řešení a nástrojů musí vycházet z důkladné analýzy rizik, z hodnocení aktiv, z bezpečnostní strategie organizace a přijatých bezpečnostních politik.

Základní bezpečnostní technologie:

- Senzor
- Firewall
- Kolektor
- Logger
- SIEM
- Analyzátor
- Tester
- Honeypot
- Sandbox

Senzory jsou základními zdroji informací, ne však jedinými. Pořízení a provoz bezpečnostních senzorů není levnou záležitostí a finanční náklady se s růstem jejich počtů násobí. Senzory IDS/IPS pro detekci nových hrozeb

vyžadují také nová pravidla - signatury. Tato pravidla může vytvářet i znalý specialista, obvykle však je k tomu zapotřebí celého výzkumného týmu, což není v silách běžné organizace a pravidla se tedy musí pravidelně nakupovat u výrobce senzoru. Jiným typem senzoru je NetFlow senzor. Jeho činnost není založena na detekci událostí, které splňují určité pravidlo, ale na detekci anomálií v datovém toku. Senzor je schopen poskytnout informace a statistiky o datové komunikaci. Nevyžaduje aktualizace pravidel. U tohoto typu senzoru se provádí aktualizace firmware a softwarových modulů. Často nevyužívanými zdroji informací, které nevyžadují žádné dodatečné finanční náklady, jsou logy událostí, které se ukládají na aktivních prvcích systémů a datových sítí. V nich leží nevyužito značné množství užitečných informací. Většinou přitom postačuje pouhé spuštění služby, která informace z logů vyčítá a odesílá je na určené místo ke zpracování.

Firewally patří k nejrozšířenějším bezpečnostním prvkům. Jsou použity k oddělení segmentů sítí s různou důvěryhodností nebo jako ochrana vstupní brány z veřejného prostředí do datových sítí organizace. Firewall obsahuje pravidla, podle kterých řídí vzájemnou komunikaci mezi sítěmi, které odděluje. Firewally mohou být paketové, aplikační brány, ale také stavové paketové filtry. V poslední době se objevují firewally tzv. nové generace, které v sobě sdružují více funkcí a obsahují i moduly senzorů, filtrů spamu, malware, ochrany citlivých informací před únikem (DLP), webové komunikace apod. Tyto rozšiřující moduly jsou převážně založeny na signaturách a většinou tedy vyžadují kontinuální provozní podporu od výrobce nebo vývojového týmu.

K předzpracování událostí ze senzorů NetFlow slouží **kolektory.** Kolektory umožňují ukládání velkého množství statistických dat a síťových charakteristik, sloužících k dalším analýzám. To vše z důvodu odlehčení zátěže hlavního analyzátoru, který by velké množství dat nebyl schopen korektně zpracovat. Podle velikosti sítě a objemu zpracovávaných dat lze kolektory škálovat pro zajištění požadovaného výkonu nebo zálohovat pro zajištění dostupnosti statistických dat v případě havárie některého z nich. Některé kolektory obsahují i pokročilejší analytické funkce a u méně náročných nasazení mohou nahradit SIEM.

Podobnou funkci jako kolektory mají zařízení pro ukládání, agregaci a správu logů ze zařízení, čili záznamníky logů neboli **loggery**. Jsou schopny přijmout i objemné logy, mohou pracovat s různými formáty logů, provádět indexaci záznamů, agregace, korelace, základní analýzy a výstupy vizualizovat nebo zasílat do analyzátorů SIEM.

Technologie **SIEM** jsou nástroji, bez kterých se neobejde žádné profesionální bezpečnostní pracoviště. Existují v různých provedeních a jsou také licencovány různým způsobem. Najdeme open source řešení, kterým však chybí provozní náplně - pravidla, bez nichž SIEM vykonává jen ty nejobecnější funkce. Uživatel si je musí doplnit sám, případně je musí dokoupit od výrobce. Většinou však jsou používány profesionální komerční nástroje, s výrobcem garantovanou podporou. SIEM se od sebe odlišují nejen schopnostmi korelace a analýzy dat, ale i množstvím informací, které jsou schopny uložit a v reálném čase zpracovat. Od toho se také odvíjí výsledná cena licence. Dalším hlediskem při výběru správného SIEM je portfolio zdrojů, ze kterých mohou přijímat data, rychlost jejich zpracování, možnost vytváření vlastních pravidel a alertů, škála vizualizací a reportů, které lze v nástroji vytvořit.

Jednoúčelové **analyzátory a testery** slouží bezpečnostním specialistům k vyhledávání zranitelností, bezpečnostních děr, k testování, rozšířeným a hloubkovým analýzám zákeřného malware, čili škodlivých kódů, virů, trojanů, spyware, adware a podobně. Lze pomocí nich provádět forenzní bádání a forenzní analýzy, ať počítačových nebo mobilních zařízení. Lze jimi testovat webové portály na zranitelnosti a hrozby. Slouží k namátkovým nebo pravidelným kontrolám a analýzám. Jsou dostupné buď jako samostatný software pro nainstalování na určitý operační systém nebo jako kompletní nástroj s příslušným hardwarem. Vhodné je volit nástroje, ke kterým je také dostupná lokální podpora a periodická školení.

K speciálním bezpečnostním nástrojům patří **honeypoty**. Jsou to klamavé prvky, vhodně umístěné v datové síti, které slouží jako návnada pro případného útočníka nebo malware. Konfigurovány jsou tak, aby byly snadným soustem, a proto i prvním cílem útoku. Pokud jsou pod stálým dohledem bezpečnostního týmu, mohou být zdrojem důležitých informací, díky nimž se lze na hrozící kybernetický útok připravit a zamezit jeho

spuštění. Výsledky analýzy pak lze použít k trvalým proaktivním opatřením. Kybernetický útok proti honeypotu nenapáchá žádné škody na aktivech organizace.

Sandboxem rozumíme autonomní prostředí, ve kterém se provádí testování podezřelých souborů, které by jinak mohly poškodit hostitelský systém a data, případně by se při testování mohly rozšířit i na okolní počítače. Sandbox může být instalován na speciálně k tomu vyhrazeném serveru nebo i na běžném PC. Rozdíl však bude ve výkonu a tím v době, která bude potřebná k jednotlivým analýzám. V sandboxu je testovanému souboru omezen přístup k pevnému disku, paměti, k síti, k operačnímu systému apod. Přístup ke všem zdrojům je nejen omezen, ale i přísně kontrolován. V případě použití virtuálního testovacího prostředí je nutné počítat se skutečností, že škodlivý kód se nemusí vůbec spustit, protože vnitřní kontrolní mechanizmy ho chrání před rozkrytím jeho škodlivých funkcí. Při testování malware je proto vhodné vlastnit a použít fyzickou část testovacího prostředí, aby testovaný malware nepoznal, že je analyzován. Testovací prostředí patří mezi základní vybavení profesionálního bezpečnostního pracoviště a je nutností pro úspěšnou analýzu KB zranitelností a hrozeb a řešení KBU/KBI.

12.4 Možnosti využití

Kybernetická bezpečnost přináší do života organizace nové procesy. S vytvořením bezpečnostního týmu se také zároveň zavádí systém nepřetržitého monitoringu vybraných segmentů datových sítí a důležitých prvků informačních, komunikačních a řídicích systémů. S monitoringem pak také přicházejí nové procesy nakládání s bezpečnostními incidenty. Zdroje monitoringu neustále dodávají velké množství bezpečnostních událostí. Tyto události nelze zpracovávat jinak, než ve vhodných nástrojích velkého výkonu. Specialisté týmu vytváří a upravují pravidla pro filtraci falešných poplachů přímo na senzorech a v analyzátoru. Událostí relevantních pro bezpečnost aktiv bývá zpravidla několik týdně. Ty jsou týmem důkladně analyzovány, klasifikovány patřičným stupněm, který vychází z bezpečnostních politik, interních předpisů, norem, zákonů a vyhlášek. Taková události jsou pak řešeny jako bezpečnostní incidenty. Informace se předávají bezpečnostnímu manažerovi a správě provozu dotčených systémů, se kterou tým dále úzce spolupracuje na řešení bezpečnostních incidentů. Tým je nápomocen jak

radou, tak svými nástroji, až do okamžiku úplného vyřešení. Veškeré důležité informace se dokumentují a uchovávají ve znalostních databázích. V budoucnu je lze využít při řešení opakujících se nebo obdobných případů. Mimo proces vlastního řešení bezpečnostních incidentů tým také vydává informační zprávy, reporty a bulletiny pro bezpečnostního manažera a vedení organizace. Tyto informace jsou důležité pro rozhodovací procesy vedení organizace.

CERT/CSIRT tým provádí namátkové i periodické kontroly na výskyt již definovaných zranitelností nebo špatných konfigurací aktivních prvků, které ohrožují bezpečnost. Tým provádí kontroly stavu instalací výrobcem doporučených aktualizací organizací používaných operačních systémů i aplikací. Provádí bezpečnostní testování webových portálů a jejich zranitelností, které mohou být zneužity jako způsob cesty k aktivům organizace. Výstupem těchto kontrol je report, který tým předává bezpečnostnímu manažerovi organizace k dalšímu řešení.

CERT/CSIRT tým má významnou roli při posuzování bezpečnosti nově zaváděných systémů, jejich prvků, software a aplikací. Tým zpracovává odborné bezpečnostní posudky k novým projektům. Při jejich zpracování využívá informace o známých KB zranitelnostech a jiných bezpečnostních hrozbách.

CERT/CSIRT tým také může být řešitelem záležitostí spojených nejen s detekcí, ale i analýzou škodlivého malware. Odborně zdatní specialisté mohou provádět testování chování zachyceného malware ve speciálním testovacím prostředí. Výsledky analýz napomáhají k odhalení způsobu kybernetického útoku, jeho rozsahu, k identifikaci napadených aktiv a podobně. Slouží také při tvorbě proaktivních opatření. Specialisté mohou provádět forenzní analýzy napadených zařízení nebo zařízení, která sloužila jako nástroj činu kybernetické kriminality. Pomocí speciálních nástrojů tak mohou získat potřebné informace, bez ohledu na to, zda se jedná o „stolní“ nebo mobilní zařízení.

CERT/CSIRT tým u organizace provádí kontroly legálně používaného software, dodržování zákonů na ochranu autorských práv, duševního vlastnictví a ochranu osobních údajů.

CERT/CSIRT tým přijímá a šíří informací z oblasti kybernetické bezpečnosti, využívá k tomu jak externí, tak interní zdroje. Tyto informace také zpracovává a uchovává pro další využití ve svých znalostních databázích. Mezi takové patří detailní informace o KB hrozbách a zranitelnostech nebo o úspěšných kybernetických útocích a způsobu jejich provedení, dále nejrůznější seznamy nedůvěryhodného hardware, IP adres botnetů, serverů šířících malware, a podobně. Informace z externích zdrojů mohou být volně šiřitelné v rámci nejrůznějších bezpečnostních komunit, mohou to však být i zpoplatněné nebo důvěrné informace, bez možnosti jejich předávání třetím stranám. Tým je používá pro bezpečné konfigurace ochranných prvků datových sítí nebo pro tvorbu vlastních pravidel pro bezpečnostní senzory. Také ne všechny interní informace jsou veřejné. O způsobu šíření interních informací rozhoduje bezpečnostní manažer organizace.

CERT / CSIRT tým nemá jen reaktivní roli po identifikovaném kybernetickém kriminálním činu, ale má i roli v preventivní ochraně. Jedná se o činnost takového charakteru, kdy jsou provedeny preventivní kroky k předcházení možným kybernetickým útokům, hrozbám a zranitelnostem, které by mohly být k činu zneužity. Tyto kroky mohou být učiněny právě na základě získaných informací z interních i externích zdrojů. Těmito opatřeními se zvyšuje jak odolnost systémů, tak zároveň se zvyšuje i bezpečnost aktiv.

CERT/CSIRT tým se kontinuálně vzdělává a podílí se i na vzdělávání v oblasti kybernetické bezpečnosti u správy a uživatelů informačních, komunikačních a řídicích systémů organizace. Tento proces se označuje jako šíření bezpečnostního povědomí. Tým k tomu využívá informační portál. Nejvhodnějším způsobem vzdělávání je e-learning a elektronicky zpracované školící materiály a testy. Mnoho kybernetických bezpečnostních incidentů pochází z nevědomosti zaměstnanců organizace. Nejen připravený informační, komunikační nebo řídící sytém, ale především znalý personál je základem bezpečnosti aktiv organizace a napomáhá k eliminaci bezpečnostních rizik.

12.5 Dílčí závěr

Kybernetický bezpečnostní tým má pro organizaci klíčový význam. Veškerá aktiva, která jsou uložena v informačních a komunikačních systémech, nebo jsou spravována pomocí řídicích systémů, jsou nepřetržitě ohrožována

převážně neviditelnými kybernetickými útoky. Kompromitace nebo ztráta aktiv může mít pro organizaci fatální následky. Jak již bylo zmíněno, při plánování zavedení procesů kybernetické bezpečnosti a vytvoření příslušných rolí, je nutné vycházet z hodnocení aktiv a analýzy rizik. Výstupem pak právě může být nutnost vytvoření týmu kybernetické bezpečnosti. Čím je hodnota aktiv a rizika jejich ztráty nebo zneužití vyšší, tím je nutné vytvoření silnějšího týmu s větším rozsahem poskytovaných služeb. Organizace se pravděpodobně při řešení této situace bude rozhodovat mezi dohledovým bezpečnostním pracovištěm typu SOC se základním portfoliem služeb a plnohodnotným CERT nebo CSIRT týmem. Z hlediska prudkého vývoje v kybernetické kriminalitě a vzhledem k obrovskému množství kybernetických bezpečnostních hrozeb a zranitelností a s tím související nárůst pracovních povinností kybernetického bezpečnostního týmu je volba týmu typu CERT/CSIRT zároveň i investicí do budoucnosti. Tým SOC se samozřejmě může stát jádrem budoucího týmu vyšší úrovně, ale jeho schopnosti, nástroje a také prostory, ve kterých působí, nemusí vždy dostačovat a ne vždy lze jít jen cestou dalšího rozšíření. Například hlavní analytický nástroj SIEM lze sice pomocí rozšiřujících licencí povýšit na dostačující úroveň, tu však už nemusí zvládat jeho hardware. Nákup nového a výkonnějšího nástroje pak muže být další investicí v řádu až desítek milionů korun, přičemž pro stávající nástroj nebude využití. Toto je jeden z mnoha možných příkladů, které by měly ovlivnit vedení organizace při řešení své vlastní kybernetické bezpečnosti.

Mimo řešení interní bezpečnosti by měl být samozřejmostí i příspěvek každé organizace do společné snahy o zajištění bezpečnosti kybernetického prostoru České republiky. Mnohé povinnosti vyplývají ze zákona č. 181/2014 Sb. a s ním souvisejících vyhlášek, kde jsou přímo definovány povinnosti, které se týkají osob uvedených v §3 a definovaného okruhu významných informačních a komunikačních systémů a prvků kritické informační infrastruktury. Mimo záležitosti administrativního charakteru, jako je hlášení kontaktních údajů a zpracování povinných dokumentů, jsou zde již uzákoněna i technická opatření, jako detekovat a po zpracování hlásit závažné kybernetické bezpečnostní události a incidenty a provádět opatření k zajištění kybernetické bezpečnosti. Tyto technické aspekty již nelze naplnit organizačními opatřeními, ale bude nutné je řešit systémově. Konkrétně

vytvořením systemizovaných míst, utvořením bezpečnostních týmů a pořízením potřebných bezpečnostních technologií. Teprve pak bude možné dostát povinnostem vyplývajícím ze zákona, detekovat a sdílet relevantní informace a posilovat nejen vlastní kybernetickou bezpečnost. Jedině tímto způsobem náš stát získá prostřednictvím Národního centra kybernetické bezpečnosti ucelený obraz o stavu kybernetické bezpečnosti České republiky a bude moci účinně reagovat na vzniklé hrozby a masivní kybernetické útoky.

13 POPULARIZACE KYBERNETICKÉ BEZPEČNOSTI

Pokud si uvědomíme význam pojmů medializace a popularizace a vztahy mezi nimi, můžeme stavět další svou činnost směřující k prezentaci výsledků práce. Medializace výsledků znamená aktivní, záměrnou prezentaci vědy v médiích pro laickou i odbornou veřejnost. Cílem medializace je sdělovat informace o dosažených výsledcích. Popularizace výsledků musí zahrnovat proces sdělování informací s cílem propagovat kybernetickou bezpečnost v očích veřejnosti, vzbudit o ní zájem a motivovat k aktivnímu zapojení.

13.1 Medializace a popularizace kybernetické bezpečnosti

Popularizaci kybernetické bezpečnosti je věnována v ČR stále větší pozornost, a to zejména na úrovni státu. Nyní je dalším krokem, aby kybernetická bezpečnost byla chápána jako priorita všemi zainteresovanými stranami do odpovědných osob včetně.

Klíčovou skupinou, která bude do značné míry ovlivňovat směřování dalších popularizačních aktivit, je sama odborná komunita. Nesmíme ovšem zapomenout na popularizaci výsledků adekvátní formou pro zvolené cílové skupiny. Pro prezentování výsledků projektu je zapotřebí zabývat se marketingem a to zejména z toho důvodu, aby byla prezentace výsledků zaměřena na konkrétní cílovou skupinu.

Medializace a popularizace musí obsahovat mix dosažených výsledků s nástroji marketingu jako je komunikace, reklama, publicita, komunikační strategie, komunikační sdělení, styl. Veškeré aktivity spojené s výsledky jsou také pevně svázané s rozpočtem.

U koho s popularizací začít?

Počet uživatelů internetu v České republice stále narůstá. Hlavními lídry nových komunikačních forem a uživatelů technologií jsou **jednoznačně děti a teenageři**. Zatímco v celé populaci je podle studie přibližně 60 % uživatelů internetu, mezi dětmi ve věku od 9 do 16 let mají uživatelé internetu zastoupení v 90 %. Právě tito uživatelé ochotně a bez výhrad akceptují většinu nových trendů. Na internet a do mobilních telefonů přesouvají významnou část svého sociálního života. Rodiče ale i pedagogové ztrácejí přehled o tom,

jak děti a dospívající mládež tráví čas na internetu nebo s mobilem a jaká rizika jim při používání nových médií hrozí.

Dospělí a ani pedagogové nevědí, jak tuto oblast nových médií zapracovat do výchovných a pedagogických témat. Největším problémem pedagogů a dospělých je, že nevědí, jak děti a dospívající upozorňovat na závažná hrozící nebezpečí.

Děti a dospívající používají nová média v první řadě pro komunikaci a k zviditelnění se na sociálních sítích. Právě sociální sítě jim dávají možnost být ve spojení s mnoha lidmi najednou a především se před nimi aktivně prezentovat s využitím fotografií, videí, odkazů a komentářů. Sdílení multimediálního obsahu patří k důležitým formám zábavy teenagerů. Internet je pro teenagery také důležitým a často jediným zdrojem informací, které využívají pro svůj osobní život i školní výuku.

Dospívající na internetu vyhledávají příležitosti ke komunikaci, vytvářejí si nové vztahy, experimentují se sebeobrazem a ochotně jej vysílají do světa. Na rozdíl od dnešních dospělých nerozlišují komunikaci a vztahy na virtuální a skutečné. Komunikace a vztahy uskutečňované online jsou pro ně stejně reálné a důležité jako ty tváří v tvář. Zjednodušeně se dá říci, že internet a jeho aplikace pomáhají naplňovat přirozené potřeby mladých uživatelů. Pozornost věnují situaci tady a teď, budoucí dopady svého jednání příliš neřeší. Ke komunikaci přistupují nenuceně a neohroženě, ale hlavně s důvěrou. Ochotně poskytují osobní údaje, soukromé informace, fotografie. Experimentují se sexualitou, ve zdánlivě anonymním prostředí internetu snadněji než v kontaktu osobním. Jsou kritičtí, neváhají zveřejňovat nekonformní názory, mají tendenci k radikálnímu hodnocení a řešení. To vše v prostředí internetu.

13.2 Propagace a osvěta kybernetické bezpečnosti v ČR

V současnosti neexistuje kvalitativní hodnocení propagace a osvěty kybernetické bezpečnosti v ČR a jen v některých případech je vykazováno hodnocení kvantitativní. Z hlediska kvantitativního bývá nejčastěji uváděn počet návštěvníků či účastníků nebo počet reakcí (například v hlasování, anketách, soutěžích apod.). Z hlediska hodnocení účinnosti a kvality je to ovšem kritérium jen dílčí. Vypovídající jsou také čísla o sledovanosti

televizního pořadu, kde jsou výsledky poskytovány nezávislými firmami a navíc obsahují i strukturované údaje o publiku. Zde je potřeba vyzdvihnout podle nás velice úspěšný osvětový projekt „Jak na Internet“ od sdružení CZ.NIC, který je vysílaný ve veřejnoprávní televizi [49].

Pro kvalitativní hodnocení zpětné vazby neexistují kritéria ani vhodná metodika; krátkodobost akcí navíc vylučuje správné hodnocení, které má často střednědobý či dlouhodobý horizont. Spolupráce soukromého a veřejného sektoru nejen v oblasti kybernetické bezpečnosti je v dnešní době prioritou nejen v praxi, ale je i prioritou na politické úrovni. Z výše zmíněného vyplývají pro stav propagace kybernetické bezpečnosti v ČR tato hlavní obecná pozitiva:

- rostoucí zájem médií o témata kybernetické bezpečnosti;
- dobrá vzdělanost pracovníků pro medializaci a popularizaci kybernetické bezpečnosti;
- stoupající povědomí veřejnosti o významu kybernetické bezpečnosti pro ekonomickou budoucnost ČR i pro jednotlivce.

Za hlavní negativa lze naopak považovat:

- neexistující koncepce medializace a popularizace kybernetické bezpečnosti na národní úrovni [50];
- nedostačující množství aktivit v této oblasti;
- rostoucí „zneužívání“ kybernetické bezpečnosti v některých médiích a ohrožování její důvěryhodnosti.

V ČR se zlepšuje situace ohledně propagace kybernetické bezpečnosti, ale stále je co zlepšovat, a to zejména ve vytvoření koncepce, priorit, cílů a identifikaci odpovědných aktérů za jejich naplňování. ČR již má akce, na které je možné navázat. O některých akcích či spíše projektech, které mohou posloužit k propagaci a popularizace kybernetické bezpečnosti, pojednává následující kapitola [51].

Ale ještě bych se zmínil o jedné velice významné instituci v ČR, která se o oblast kybernetické bezpečnosti nejvíce zajímá. Jedná se o **Národní centrum kybernetické bezpečnosti** (**NCKB**), jako součást Národního bezpečnostního úřadu, se sídlem v Brně.

Úlohou NCKB je koordinovat spolupráci na národní i mezinárodní úrovni při předcházení kybernetickým útokům i při návrhu a přijímání opatření při řešení incidentů i proti probíhajícím útokům [53].

Hlavní oblasti činnosti centra jsou:

- provozovat Vládní CERT České republiky (GovCERT.CZ),
- spolupráce s ostatními národními CERT® týmy a CSIRT týmy,
- spolupráce s mezinárodními CERT® týmy a CSIRT týmy,
- příprava bezpečnostních standardů pro jednotlivé kategorie organizací v ČR,
- osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti,
- výzkum a vývoj v oblasti kybernetické bezpečnosti [47].

Na webových stránkách NCKB je možné najít následující informace:

- Úvod – informace o vzniku a hlavní činnosti NCKB.
- Vládní CERT – informace o vládním CERTu (GovCERT.CZ).
- RKB – informace o Radě pro kybernetickou bezpečnost a o jejích hlavních úlohách, dokumentech a informace o zasedání Rady pro kybernetickou bezpečnost.
- Informační servis – informace o zranitelnostech, akcích a událostech, seznam bezpečnostních incidentů po jednotlivých měsících, pracovní příležitosti, RSS, informace CSIRT.CZ – aktuality z bezpečnosti a výkladový slovník.
- Legislativa – informace o legislativě v oblasti KB, další dokumenty, smlouvy a memoranda týkající se NCKB.
- KII / VIS – informace o kritické informační infrastruktuře a významných informačních systémech, formuláře pro hlášení kontaktních údajů a kybernetických bezpečnostních incidentů.
- Odkazy – seznam národních a mezinárodních odkazů k problematice KB.
- Kontakty – kontakty na NCKB, PGP klíče a RFC 2350 standard.

13.3 Kybernetická bezpečnost a vzdělávání dětí

Děti si neuvědomují nebezpečí, které na ně v prostředí Internetu číhá. Uveřejňují své osobní informace či fotky a dávají tak možnost tyto informace

zneužít. Dalším smutným faktem je, že ani o tuto problematiku nejeví zájem. Problémem je neznalost možného nebezpečí. Rodiče děti o nebezpečí neinformují. Zde proto musí významnou roli sehrávat školy. Informace, které získávají na základní či střední škole, nejsou plně dostačující.[48]

Základní škola je hlavní zdroj informací, a mělo by se tak přistupovat i v případě bezpečnosti na Internetu. Žáci se zde většinou poprvé setkávají s počítačem, Internetem a učí se základy práce na počítači. Předmět informatika se začíná povinně vyučovat v 5. a 6. třídách základní školy. Avšak děti začínají i mnohdy pracovat s počítačem již v nižším věku. Do školy vstupují již se základními dovednostmi, avšak jim chybí základní návyky v oblasti bezpečnosti. V hodinách informatiky se dozvídají základní informace o sestavě počítače, historii a učí se práci s programy Word, Excel, PowerPoint. Problematice bezpečnosti učitelé věnují pouze část hodiny na začátku školního roku a tím celý blok bezpečnosti končí [48].

Pro podporu výuky bezpečnosti existuje i celá řada podpůrných materiálů. Jedná se povětšinou o internetové zdroje, kde se žáci mohou dozvědět základní informace o sociálně-patologických jevech, jsou zde i kontaktní místa, kam se mohou děti obrátit v případě, že se potýkají sami nebo jejich kamarádi s touto problematikou. Nachází se zde i cvičné testy, kterými mohou učitelé ověřovat, zda žáci dané problematice rozumí. Stránky nejsou určeny nejen dětem, ale také rodičům, kteří se mohou touto cestou dále vzdělávat [48]

Další možností je spolupráce učitelů s žáky na tvorbě profilů na sociálních sítích. Žákům nelze zakázat tyto sociální sítě používat, a proto by se měl změnit také přístup. Mělo by se žákům vycházet vstříc, pochopit jejich potřeby vlastnit profil na sociální sítí a snažit se jim poradit, jak mít správně zabezpečený profil. Existuje celá řada literatury, která tyto správné postupy sumarizuje, avšak pokud se sám žák o tuto problematiku nezajímá, nemá možnost se k ní dostat [48].

Výuka ve středních školách by měla navazovat na znalosti získané na základních školách. Studenti si zde své základní informace prohlubují a získávají další informace. Střední školy se problematice bezpečnosti na Internetu věnují více a podrobněji. Avšak na všeobecných školách jako jsou např. gymnázia a střední odborné školy hlavně netechnického charakteru opět problematika bezpečnosti na Internetu ustupuje do pozadí. Je jí věnována

většinou pouze úvodní hodina na začátku školního roku. V dalších předmětech, jako je rodinná výchova, ustupuje také do pozadí. Výjimku tvoří učitelé, kteří se o tuto problematiku více zaujímají a studenty vtahují do této problematiky pomocí úkolů, jako je tvorba prezentací na dané téma. Studenti si touto cestou cvičí tvorbu prezentací či textových dokumentů, ale zároveň se dozvídají podrobnější informace a ty pak sdělují svým spolužákům. Opět mají možnost využívání podpůrných materiálů, jako jsou internetové stránky e-bezpečí.cz, saferinternet.cz a tak dále [48].

Ve výuce například Rodinné výchovy či občanské výchovy by měli být podněcovány diskuze se studenty na danou problematiku. Například co si studenti myslí, že je vhodné umístit na internet nebo také jejich osobní zkušenosti, zda se již s některým ze sociálně-patologických jevů setkali oni sami či jejich kamarádi. Je důležité, aby si studenti uvědomili, že svěřit se vyučujícímu nebo svým kamarádům není ostuda. A také zvládání stresových situací například kyberšikany je důležité provádět za pomoci buď rodičů, nebo nejlépe vyškolených odborníků [48].

Na státní úrovni jsou zpracovávány rámcové vzdělávací programy (RVP) pro jednotlivé obory vzdělání. Tyto programové dokumenty konkretizují obecné cíle vzdělávání, specifikují klíčové kompetence důležité pro rozvoj osobnosti žáků, vymezují věcné oblasti vzdělávání a jejich obsahy, charakterizují očekávané výsledky vzdělávání a stanovují rámce a pravidla pro tvorbu školních vzdělávacích programů, včetně učebních plánů. Učitelé už tak nejsou vázáni na tradiční „osnovy“, kterých se musí držet, protože učitel v plánech nepopisuje, „co má probrat“, ale popisuje, jaké dovednosti mají jeho žáci/studenti mít. Lze tedy velmi snadno některé méně podstatné pasáže látky vynechat či zredukovat, za účelem splnění základních cílů výuky nebo naopak některý přínosný obsah výuky prodloužit [48].

Je velmi důležité jít s dobou a reagovat na nové technologie. A právě základní a střední školy jsou primárním a také hlavním zdrojem pro získávání informací. Zde by měli žáci/studenti získat správné návyky, které si odnesou i do své dospělosti. Dalším možným krokem je rozvíjení znalostí u rodičů žáků/studentů. Velmi často se stává, že děti mají větší dovednosti v oblasti informačních technologií než jejich rodiče. Právě rodiče jsou nejbližší osoby

pro děti a měli by znát nebezpečí, která na ně číhají a v případě potřeby dokázat dětem pomoci nebo vědět, kam se o pomoc obrátit [48].

13.4 Kybernetická bezpečnost a vzdělávání seniorů

Otázka vzdělávání seniorů se řeší v České republice již několik desítek let. S postupující globalizací světa, kdy jsou rušeny časové a prostorové bariéry je zapotřebí reagovat odpovídajícím způsobem. Vzdělávání by mělo být chápáno jako aktivní, cílevědomý a informovaný přístup seniora ke svému životu, tak aby dokázal využít možností dostupných technologií. Stárnutí populace a masivní nasazování ICT sebou přináší mnoho nesnází. Ochrana seniorů před hrozbami při používání ICT se stává celospolečenským problémem. Vyvstává zde reálná potřeba ochránit tuto skupinu před reálnými hrozbami při používání ICT.

Je nutné zaměřit se na to, zda existují nabídky vzdělávacích příležitostí pro populaci osob v postproduktivním věku. Čím dál tím více seniorů pociťuje ekonomické aspekty svých špatných nebo ukvapených rozhodnutí. Proto je nutné si uvědomit, že celoživotní vzdělávání je chápáno jako ucelený koncept, jež obsahuje formální, neformální a informální učení během celého života jedince. V dnešní dynamické společnosti je zřejmé, že i vzdělávání musí být dynamické, kontinuální a dlouhodobé. Už neplatí, že jednou nabyté znalosti nám vystačí na celý život. Nejvíce zranitelné jsou převážně osoby v seniorském věku, je zapotřebí seniory adekvátně chránit. Jedním z prostředků jak je připravit, je nabídnout jim možnost vzdělávacích aktivit. Ty jim mohou napomoci k bezpečnému používání ICT k jejich prospěchu (komunikace a služby). Senioři budou senioři patřičné vzděláni jak chránit sebe a svá aktiva.

Celoživotní vzdělávání má tři základní etapy. První etapou je předškolní výchova, druhou je pak vzdělávání školní. Třetí etapa, se týká vzdělávání dospělých, kde je řízena zpravidla potřebami v zaměstnání. Nesmíme ale opomenout vzdělávání dospělých v post produktivním věku, oni jsou ta nejohroženější skupina.

13.4.1 Jak vzdělávat seniory?

Nejprve si musíme určit místo, které chceme řešit, a proto si provedeme rozdělení vzdělávání dospělých, kde pozornost zaměříme na další vzdělávání:

- Vzdělávání dospělých.
    - Další vzdělávání.
        - Občanské vzdělávání.
        - Zájmové vzdělávání.
        - Další profesní vzdělávání.
- Kvalifikační vzdělávání.
- Rekvalifikační vzdělávání.
- Normativní školení a kurzy.
- Vzdělávání ve školách.

V oblasti dalšího vzdělávání, je žádoucí aby se edukační aktivity soustředily do dalšího vzdělávání a tam do občasného a zájmového, protože je oblast, která bude seniory nejvíce využita.
Koncept celoživotního učení, vyžádal rozlišování různých forem vzdělávání a učení. Formální vzdělávání se realizuje ve vzdělávacích institucích a formální učení je definováno jako učení vedoucí k získání diplomů a kvalifikaci v rámci vzdělávacího systému. Neformální vzdělávání je organizované a systematické vzdělávání, které se realizuje mimo formální vzdělávací systém a jedná se rozšíření určité schopnosti např. jazykový kurz, rekvalifikační kurz apod. Přirozenou součástí každodenního života je vzdělávání informální. V informálním vzdělávání se nemusí jednat o záměrné sebevzdělávání. Vyplývá z každodenních činností, jako je např. čtení novin, literatury, sledování televize apod., kde dochází k získávání nových informací. Nejedná se tedy o záměrné sebevzdělávání, přestože dochází k osobnímu rozvoji jedince. Ve stáří převažuje informální učení. V současné době je patrné dle zájmu seniorů, že využívají nabídek neformálního učení, které je záměrné a institucializované.

Cílem vzdělávání seniorů je rozvoj schopností, znalostí a rozvoj osobnosti. Obsah vzdělávání by měl odpovídat jejich zájmům a respektovat jejich potřeby. Cílem vzdělávání seniorů by měly být aktivity směřující ke zvládání nových či obtížných situací jako je např. zvládání technologií, se kterými senior přijde do kontaktu.

Proces učení je v každém věku ovlivňován různými faktory neboli podmínkami k učení. Tyto podmínky se dělí na subjektivní a objektivní. Do subjektivních podmínek řadíme:

- intelektové schopnosti,
- motivace, postoje nebo potřeby a zájmy,
- fyzické,
- sociální a sociokulturní podmínky.

Mezi objektivní podmínky řadíme:

- učivo – obsah, rozsah,
- vzdělavatelé a organizátoři,
- realizační prostředí – dostupnost.

Velkou bariérou pro seniory může být jejich nízké sebevědomí, které může pocházet z dosaženého nižšího stupně vzdělání nebo z negativního pohledu společnosti na seniory. Bariérou může být i nízká informovanost seniorů o možnostech vzdělávání se nebo přístup společnosti ke vzdělávání seniorů. Bariér ve vzdělávání může být spousta a bariérou se může stát téměř cokoli. Nedostupnost vzdělávání se postupně daří eliminovat s narůstajícím počtem institucí věnujících se vzdělávání seniorů. Mezi efektivní nástroje na snižování bariér lze zahrnout také média, jakou jsou rozhlas, televize, noviny, časopisy jak odborné, tak i zájmové apod.

13.4.2 Jakým způsobem vzdělávat seniory?

Příprava seniorů v oblasti kybernetické bezpečnosti může být realizována následovně:

- Přímá výuka, tato forma výuky umožňuje osobní kontakt lektora s účastníkem, označuje se to jako prezenční vzdělávání.
- Kombinovaná výuka – vznikla ze snahy zvýšit podíl individuálního studia na celkovém objemu vzdělávání – vstupní seminář, individuálně řízené studium, výcvikové semináře, závěrečný seminář. V oblasti kybernetické bezpečnosti se jeví jako nejefektivnější.
- Korespondenční, distanční vzdělávání, e-vzdělávání.

Každá forma má své výhody nevýhody. Na jedné straně můžeme najít přímý osobní kontakt lektora s účastníkem. Na straně druhé můžeme najít nepřímý

kontakt lektora s účastníkem (prostřednictvím počítače, využití Learning Management Systém (LMS), využití Knowledge management Systém, distančního vzdělávání, e-learning). Pokud vzdělávací instituce je schopna využít obě výše uvedené formy, pak můžeme hovořit o kombinované formě výuky [54].

Pro vzdělávání seniorů je důležité brát na zřetel odlišnosti seniorů jako účastníků vzdělávací aktivity. Právě spousta odlišností jednotlivců tvořících vzdělávanou predikuje, že neexistuje jediná správná nebo univerzální metoda. Pokud během přednášky lektor dává okamžitý prostor k diskuzi a vybudí pravděpodobně větší zájem o přednášenou problematiku. Je velmi vhodné dávat v průběhu přednášky krátký prostor k diskuzi. Pokud budeme chápat přednášku jako výkladovou metodu, je nutné výuku následně doplnit cvičením zpravidla v menších skupinách, kde bude prakticky docházet k řešení problému a kde lze ověřit pochopení problému ze strany seniorů.

Pro přípravu seniorů musíme vzít do úvahy postupy, které:

- podněcují motivaci účastníků z řad seniorů,
- zajišťují jejich aktivní účast,
- respektují jejich individualitu a specifický styl učení,
- zabezpečují zpětnou vazbu,
- umožňují využití získaných poznatků v praxi.

Vzdělávání seniorů patří do systému vzdělávání dospělých v rámci celoživotního vzdělávání. Tímto směrem se vzdělávání seniorů začalo rozvíjet nejprve na humanitně zaměřených univerzitách. Rozkvět nastal v 90. letech a roku 1995 byla založená Asociace Univerzit Třetího Věku (AU3V). V současné době je v asociaci registrováno 21 vysokých škol. Školné neboli poplatky za studium nejsou pro budoucí studující seniory vysoké, činí obvykle několik set korun, přičemž jim přednáší akademičtí pracovníci jednotlivých univerzit. Je také patrné, že oblast nabídky je a bude šířeji doprovázena nabídkou středních škol, dle svého zaměření.

13.4.3 Jak realizovat vzdělávání seniorů

Asi nejefektivnější počáteční aktivitou se jeví uspořádat úvodní popularizační přednášku, následně uspořádat seminář či workshop: nejprve musí senioři překonat ostych a získat sebedůvěru a navázat přímý kontakt s přednášejícím

či cvičícím. Je vhodné zorganizovat tyto akce samostatně anebo také jako součást již existujících popularizačních akcí.

- Spolupráce s organizacemi, které pracují s cílovými skupinami (kluby důchodců, oslovení radnic ve městech s možností nabídky akce…);
- Dny otevřených dveří vzdělávacích institucí či firem;
- Vytvořit mnemotechnické pomůcky pro jednotlivá bezpečnostní pravidla/hru.

Jako další formu jak uvědomit seniory na problematiku bezpečnosti je medializace problémů v médiích a zejména v těch, které jsou zaměřeny na tuto cílovou skupinu. Na vhodných příkladech rozebrat k čemu došlo, kde byla příčina, jaké jsou následky a především zdůraznit jak z toho plyne poučení. Pokud se nám podaří zapojit cílovou skupinu do studia problematiky bezpečnosti během přímého kontaktu s nimi, tak se jeví jako efektivní, nabídnout jim a velmi podrobně názorně předvést, že se mohou vzdělávat sami v době, která jim vyhovuje například pomocí e-learningových kurzů.

13.4.4 Jak začít s popularizací kybernetické bezpečnosti u seniorů?

Počet uživatelů ICT mezi seniory má stoupající tendenci. Mnohdy umožňuje seniorům, kteří jsou méně pohybliví anebo odloučení, kontakt se svými blízkými. Pořizovací náklady nejsou vysoké a šance být v kontaktu a nebýt sám, směřuje seniory k používání moderních technologií. Problémem zůstává, že jsou většinou bez odborného zázemí a jsou vystaveny mnoha hrozbám. Pak je jen na nich jak se rozhodnou a jaké to bude mít důsledky. Jejich mnohdy nadměrná důvěra v neprověřené záležitosti jim následně způsobuje obrovské problémy. Senioři nepatří mezi lídry v bezpečném používání komunikačních forem. Senioři mnohdy akceptují nebezpečné jednání druhých osob jednání bez jakéhokoliv podezření, že by je to mohlo ohrozit. Protože nad nimi není dohled jako u dětí, mohou se nesprávně rozhodnout. Po překonání prvních bariér z používání stolních PC se seznamují s dalšími prostředky komunikace a tím jsou dneska převážně chytré telefony. Pokud nejsou senioři ve spojení s rodinou nebo přáteli, které mohou požádat o radu jak bezpečně používat ICT, dostávají se pod tlak a aby nemuseli něco řešit, ochotně souhlasí s nebezpečnými praktikami např. s podvodnými maily, falešnými a podvodnými SMS [58].

13.4.5 Zvýšení bezpečnostního povědomí pro seniory.

Senioři jako nejohroženější skupina osob se denně setkává s mnoha hrozbami, která působí na jejich aktiva. Televizní zpravodajství je denně informuje o tom, že jsou v neustálém nebezpečí ze všech stran. Z jedné strany útočí podomní prodejci z druhé strany podvodné emaily a SMS apod. V případě, že nemá senior normální kontakt s okolním světem, lehce může podlehnout dojmu, že je celý svět proti němu. Pak je velmi složité se k němu dostat a získat jej na svou stranu. U mnoha seniorů je zřetelná obava z jednání s ostatními lidmi. Lze také konstatovat, že to čím společnost v České republice prošla v uplynulých 25 letech, nedává seniorům příliš velkou důvěru, že se dovolají svých práv a že v případě jejich újmy, jim bude škoda nahrazena. Potencionální útočníci neustále zdokonalují své metody jak nalézt nový způsob jak potencionální oběť připravit o co největší majetek. Útočníci zkouší osobní kontakty za účelem nabízení zboží či služeb. Zasílají nevyžádané podvodné maily, falešné exekuční příkazy apod. Po rozsáhlé kampani v České republice, je možno sledovat větší zájem společnosti na ochranu této skupiny, formou zpřísnění podmínek ohledně toho způsobu podnikání [59].

Stále ale zůstává problém, že senior používá sofistikované technologie IT a není na to připraven z bezpečnostního hlediska. V dobré víře ostatním vyhovět, se senioři mohou dopouštět vážných pochybení, které mohou mít vážné následky. Zkusíme si nyní vymezit základní okruhy, jaké aktivity zpravidla senior realizuje s různými prostředky:

1. **Senior má doma v bytě stolní počítač**, který užívá sám např. k následujícím účelům:
    - Surfování na internetu.
    - Stahování softwaru.
    - Sledování filmů.
    - Internetbanking.
    - Komunikace s přáteli:
        - Online komunikátor (SKYPE, ICQ atd.).
        - Email.

2. **Senior vlastní notebook**, který používá jak doma tak mimo domov k následujícím účelům:
   - Surfování na internetu.
   - Stahování softwaru.
   - Sledování filmů.
   - Internetbanking.
   - Komunikace s přáteli:
     - Online komunikátor (SKYPE, ICQ atd.).
     - Email.
3. **Senior vlastní tablet**, který používá jak doma tak mimo domov k následujícím účelům:
   - Surfování na internetu.
   - Stahování softwaru.
   - Sledování filmů.
   - Internetbanking.
   - Komunikace s přáteli:
     - Online komunikátor (SKYPE, ICQ atd.);
     - Email.
   - Navigace;
   - Fotografování.
4. **Senior vlastní chytrý telefon:**
   - Surfování na internetu.
   - Stahování softwaru.
   - Sledování filmů.
   - Internetbanking.
   - Komunikace s přáteli:
     - Online komunikátor (SKYPE, ICQ atd.).
     - Email.
   - Navigace.
   - Fotografování.
5. **Senior vlastní platební kartu** (debetní nebo kreditní) a používá ji k následujícím účelům:
   - Platba na internetu.

Výše uvedené prostředky a aktivity může provádět senior, aniž by potřeboval nějaká školení. Pokud má hotovost, může si zakoupit počítač či jiné zařízení a může elektronicky komunikovat. Pak nastává kritická chvíle, která může způsobit velmi vážné problémy. Nepřipravený senior nemusí mít ani potuchy jaké nástrahy jej mohou potkat při používání internetu. Rozhodne jen jeho obezřetnost. Toto kritické místo je mnohdy vyplněno rodinou, která může seniorovi poskytnout základní bezpečnostní instrukce jak se chovat na internetu. Nedává nám ale záruku k tomu, že rady a doporučení budou správné a že jim senior bude rozumět.

V tomto smyslu slova je zapotřebí podporovat a rozvíjet veškeré aktivity, které podporují seniory v bezpečném používání internetu či jiných elektronických prostředků, kterými si mohou sami pomoci a mohou si jimi usnadnit život.

Je zapotřebí mít na mysli vzdělávání seniorů spíše jako zájmovou činnost, při minimálních vstupních poplatcích. Budeme-li se zabývat přípravou vzdělávacích aktivit, klíčovou otázkou bude, kdo bude školitelem. Protože tento člověk rozhodne o úspěchu celé přípravy. Musí to být osoba, která je připravena jak po stránce odborné v oblasti IT, tak po stránce vzdělávání dospělých zejména seniorů. Pokud to bude vynikající IT odborník hovořící příliš erudovaným jazykem, tak tato aktivita nemá smysl, senioři ve velké většině tomu asi nebudou rozumět.

Další klíčovou otázkou je místo odborného školení a jeho vybavenost. Ve velkých městech kde sídlí univerzity, jsou často tyto vzdělávací aktivity součástí nabídky univerzity třetího věku. V případě, že tomu tak není, je potřeba se zamyslet nad tím, co je pro českou společnost charakteristické. Jsou to veřejné knihovny, kde je volný přístup k internetu. Pokud to prostorově vyhovuje, je to ideální místo. Knihovna je neutrální místo a přináší všem spíše příjemné vzpomínky a zřizovatelem ve většině případů bude obec. V případě, že knihovna nevyhovuje, tak většina obcí zřizuje základní školu. Při plánování výuky se zcela jistě najde místo pro seniory aby zasedli do školních lavic v odpoledních hodinách.

Pokud budeme mít vyřešeno, kdo provede školení a kde. Musíme si také říci, jaká by měla být délka výuky a forma výuky. Zcela určitě se mine účinkem aktivita, která začne testováním a pokračuje obsáhlou přednáškou

doprovázenou promítáním snímků. Výuka seniorů musí být kontaktní, modelovaná na příkladech a senioři nesmí mít pocit, že jsou ti hloupí a ještě k tomu musí projít zkouškami. Je zapotřebí je osobně získat pro aktivní účast a prokládat problematiku příklady z praxe, vyhodnocovat co se objevuje v médiích. Přednášky by měly na sebe navazovat. Je vhodné seniory vybavit po každé hodině názornými kartami, na kterých je vyobrazeno ve zkratce a výstižně téma dané přednášky. Po získání sebevědomí seniorů a dosažení minimálně úrovně znalostí, je možno po pečlivém zvážení nabídnout možnost přípravy e-learningu. V první fázi s přihlašovacími údaji, které přímo neidentifikují danou osobu. Pak se to dá změnit a blíže vysvětlit, že je lepší zaměřit pozornost na konkrétní osobu s cílem mu detailně pomoci, samozřejmě diskrétně. Jako optimální se může jevit dotace ve výši 30 min přednášek a 30 min k diskuzi.

Jak velká by měly být pracovní skupina? Mělo by jít o skupinu cca 15-20 osob, která je přibližně na stejné vědomostní úrovni. Při tomto počtu může být výuka stále kontaktní a osobní.

13.5 Nejznámější projekty propagace a osvěty v ČR

Kromě uvedených aktivit veřejné správy existuje řada programů, zaměřujících se na osvětovou činnost a pomoc uživatelům internetu při bezpečném pohybu na síti. Z těchto iniciativ je možné zmínit zejména stránky www.bezpecnyinternet.cz a www.saferinternet.cz, které poskytují především mladistvým a dětským uživatelům internetu (a jejich rodičům) cenné rady a poukazují na rizika spojená s používáním internetu (např. pohybem na sociálních sítích). Zároveň je na stránkách www.horka-linka.cz provozováno kontaktní centrum, které přijímá hlášení týkající se nezákonného obsahu na internetu (zejména zneužívání dětí), zatímco na portálu www.pomoconline.cz lze nalézt krizové centrum, pomáhající dětským obětem internetové kriminality. (www.psp.cz/sqw/text/orig2.sqw?idd=176205)

Nesmíme zapomenout na velice úspěšný osvětový projekt „**Jak na Internet**“ od sdružení CZ.NIC (www.nic.cz, www.jaknainternet.cz). Cílem tohoto projektu je přiblížit Internet a jeho možnosti co nejširší skupině občanů České republiky. Osvěta je prováděna pomocích zábavných dvouminutových videí, kde se diváci dozvědí o obecné problematice Internetu. Tato videa moderuje Roman Zach. Ke každému videu je na internetových stránkách navíc

doprovodný text, který se dané problematice věnuje více do hloubky. Pro učitele jsou navíc u každého dílu připravené vzdělávací balíčky ke stažení, pomocí kterých mohou obohatit výuku informatiky i dalších obdobných předmětů ve škole. Podle tohoto projektu lze rozdělit i výuku pro žáky základních škol a některá témata i pro studenty středních škol [49].

13.5.1 Projekty pro koncové uživatele

Doménový prohlížeč

Doménový prohlížeč je aplikace, která slouží k zobrazování údajů z doménového registru a je přímo propojena s účtem mojeID. Pokud máte svůj účet mojeID vedený u domény v roli držitele či administrativního kontaktu, můžete si zkontrolovat v prohlížeči její stav, ověřit datum, do kterého je doména zaplacena (a u kterého registrátora lze prodloužit její platnost) nebo zda je chráněna technologií DNSSEC [56].

MojeID

MojeID je bezplatná služba, díky níž mají uživatelé českého Internetu možnost používat pro přihlašování na různé internetové stránky a k různým webovým službám, které tuto službu podporují, jednotné identifikační údaje (uživatelské jméno a heslo) [56].

Dobrá doména CZ

Stránky vysvětlující jednoduchou formou koncovým uživatelům, proč a k čemu je dobré mít vlastní doménu. Součástí webu je krátký tutoriál, který zájemce o doménu provede třemi základními kroky směřujícími k vlastní doméně: výběrem nejvhodnějšího doménového jména, ověřením jeho dostupnosti a nakonec jeho registrací [56].

Jak na Internet

Osvětový projekt, televizní miniseriál, jehož cílem je přiblížit Internet a jeho možnosti široké veřejnosti. Diváci se mohou seznámit s tématy, jako jsou například internetové seznamky, 3D tisk nebo třeba jak funguje Internet. Všechny epizody, včetně rozšiřujících textů, jsou k dispozici na webu [55].

CAPTCHA Help

Především pro nevidomé nebo dyslektiky zápasící s písmenky vznikla služba CAPTCHA Help. CAPTCHA, je obrázek s kódem, který ověřuje, že uživatel není robot. Tento obrázek s kódem je v dnešní době na mnoha webech a někteří si s ním nedokáží sami poradit [55].

Akademie CZ.NIC

Akademie CZ.NIC nabízí zájemcům možnost odborného vzdělávání v oblasti Internetu a internetových technologií. Součástí výukového centra je také laboratoř vybavená hardwarem a softwarem potřebným k testování a experimentování v rámci výuky [55].

Katalog routerů

Katalog routerů nabízí recenze routerů pro domácí použití. Hlavním cílem katalogu je otestovat podporu nových technologií v koncových zařízeních (IPv6, DNSSEC) a nabídnout uživatelům nezávislé informace [55].

Turris

Turris je výzkumný, neziskový projekt zaměřený na oblast síťové bezpečnosti. V rámci projektu je vyvíjen bezpečný router, který obsahuje sondu pro analýzu anomálií v síťovém provozu a další bezpečnostní prvky [55].

Tablexia

Aplikace pro tablety určená dětem a mladým lidem s dyslexií. Cílem aplikace je formou her a cvičení trénovat schopnosti, které jsou dyslexií nejvíce oslabené. Tablexia je moderní vzdělávací pomůcka pro děti na druhém stupni základní školy. Aplikace je ke stažení zdarma [55].

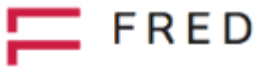
Edice CZ.NIC

Vydávání odborných a naučných knih je jednou z dalších aktivit sdružení. Cílem je, podobně jako v řadě dalších případů, osvěta v oblasti domén, Internetu a internetových technologií. Kromě tištěných verzí vychází v edici i elektronická podoba knih [55].

Bezpečné domény CZ

Bezpečnost domén je základním předpokladem bezpečného používání Internetu. Bez zabezpečení domény pomocí technologie DNSSEC není používání žádné internetové služby zcela bezpečné! A to bez ohledu na to, jaké další formy zabezpečení služba používá. Uživatelé služeb, které běží na nezabezpečených doménách a mohou být například poměrně jednoduše přesměrováni na podvodné stránky [55].

13.5.2 Projekty pro odbornou veřejnost



FRED

Software určený ke správě internetové domény libovolné úrovně. Je vyvíjen sdružením CZ.NIC a je šířen jako open source. Aktuálně ho používá celá řada doménových registrů v čele s doménami. CZ, .EE, .MK, .AL, .CR, .TZ, .FO a .AO [56].

BIRD

Směrovací démon pro dynamické směrování IP protokolu je určený pro Linux a BSD. Projekt vznikl na půdě Matematicko-fyzikální fakulty Univerzity Karlovy a Laboratoře CZ.NIC se podílejí na jeho dalším vývoji [56].

Knot DNS

Knot DNS je autoritativní DNS server vyvíjený Laboratořemi CZ.NIC. V roce 2012 se podařilo dosáhnout největšího výkonu (qps) mezi dostupnými open source řešeními (BIND, NSD), a to bez kompromisu na straně funkčnosti a podpory standardu. Knot DNS je v současné době využíván také jako autoritativní DNS server pro českou doménu [56].

CSIRT.CZ

CSIRT.CZ je národní bezpečnostní tým České republiky, který koordinuje řešení bezpečnostních incidentů v počítačových sítích. Cílem CSIRT.CZ je pomáhat provozovatelům internetových sítí v České republice zřizovat jejich vlastní bezpečnostní týmy a infrastrukturu, řešit incidenty a tím zlepšovat bezpečnost jejich sítí i globálního Internetu [56].

Laboratoře CZ.NIC

Laboratoře CZ.NIC jsou organizačně odděleným vývojovým a výzkumným pracovištěm sdružení, které se zabývá výzkumem v oblasti Internetu, internetových protokolů, analýzy síťových provozů, pasivním i aktivním monitoringem a návrhem prototypů pro další vývoj v rámci sdružení [56].

Turris

Turris je výzkumný, neziskový projekt zaměřený na oblast síťové bezpečnosti. V rámci projektu je vyvíjen bezpečný router, který obsahuje sondu pro analýzu anomálií v síťovém provozu a další bezpečnostní prvky [56].

Skener webu

Celá řada webových aplikací obsahuje závažné zranitelnosti. Provozovatel webu o tom většinou ani netuší. Zdarma nabízí provozovatelům webů zjištění možných zranitelností oskenováním a rychlým ručním testem. Zaměřují se především na zjištění slabin ze spektra desíti nejzávažnějších zranitelností webových aplikací [56].

Podpora zavádění IPv6

Přechod na internetový protokol verze 6 – IPv6 – je jedním z nejaktuálnějších celosvětových technologických témat. Protokolu IPv6 se sdružení CZ.NIC věnuje v rámci svých osvětových aktivit soustavně již několik let [56].

Podpora technologie DNSSEC

DNSSEC je rozšíření systému doménových jmen (DNS), které zvyšuje jeho bezpečnost. DNSSEC poskytuje uživatelům jistotu, že informace, které z DNS získali, byly poskytnuty správným zdrojem, jsou úplné a jejich integrita nebyla při přenosu narušena. [56].

13.6 Dílčí závěr

Vznik kybernetického prostředí přinesl spoustu příležitostí, ale i nové možnosti pro páchání trestných činů. Čím více se budou informační technologie rozvíjet, útočníci budou rozvíjet i své znalosti a nové technologie, jak zaútočit. Nesmíme zapomenout, že útočníci jsou vždy o krok napřed.

Děti a dospívající na internetu vyhledávají příležitosti ke komunikaci, vytvářejí si nové vztahy, experimentují se sebeobrazem a ochotně jej vysílají do světa. Na rozdíl od dnešních dospělých nerozlišují komunikaci a vztahy na virtuální a skutečné. Nejvíce opomíjenými uživateli jsou **děti a dospívající mládež.** Ti jsou o kybernetických hrozbách a způsobech ochrany před nimi málo informováni. Rodiče většinou nemají své znalosti na takové úrovni, aby svým dětem mohli vysvětlit nebezpečí, které jim může neopatrné chování na internetu způsobit potíže. Dalšími, kteří by se měli do osvěty kybernetické bezpečnosti zapojit, jsou pedagogové na základních a středních školách. V současnosti jsou na tom studenti po odborné stránce v používání nových technologií výrazně lépe, než jejich pedagogové.

S bezpečností v prostředí Internetu jsou žáci ve školách nejčastěji seznamováni v rámci hodin výuky informatiky a výpočetní techniky. Problematikou se ovšem zabývají žáci také v předmětech Občanské výchovy, Rodinné výchovy, Výchovy ke zdraví, Člověk a svět práce. Žáci zde získávají základní informace o bezpečnosti. V některých školách je řešení problematiky vyvěšeno i na vývěsných tabulích, či jsou na to zpracovávány eseje do hodin Českého jazyka. Provázanost této problematiky se dá najít ve všech společensko-vědních předmětech.

Dospělí a ani pedagogové většinou vůbec nevědí, jak tuto oblast zapracovat do výchovných a pedagogických témat. Největším problémem pedagogů a dospělých je, že nevědí, jak děti a dospívající upozorňovat na závažná hrozící nebezpečí.

Školy také v hojném počtu využívají pomoci strážníků Městské Policie či Policie ČR, kteří v rámci svého působení navštěvují školní zařízení a zajímavou formou se snaží děti o této problematice informovat.

Medializaci a popularizaci kybernetické bezpečnosti je v posledních letech v ČR věnována stále větší pozornost. I přesto, že výstupy jednotlivých mediálních a popularizačních aktivit jsou jen velmi těžko měřitelné, je i tak možné konstatovat, že na cílové skupiny zatím nedopadají v takovém rozsahu, v jakém by si autoři a organizátoři akcí sami přáli [60].

Proto je důležité spojit nejen znalosti odborníků z kybernetické bezpečnosti, ale zapojit i pracovníky z ostatních sfér lidského života – neméně důležitý je i management a marketingová propagace (sami to vidíme i v běžném životě: člověk může vědět spoustu věcí, ale pokud neví, jak své vědomosti prodat, v dnešní rychlé době přijdou nazmar). K osvětě v oblasti kybernetické bezpečnosti by nemalou měrou přispěla i propagační činnost realizovaná jednak formou tematických skládaček a letáků, jednak formou výstav. Právě výstavy jsou vítanou příležitostí nejen zviditelnit otázku kybernetické bezpečnosti, ale upozornit i na výsledky výzkumu v této oblasti.

Senioři nepatří mezi lídry v bezpečném používání komunikačních forem. Senioři mnohdy akceptují nebezpečné jednání druhých osob jednání bez jakéhokoliv podezření, že by je to mohlo ohrozit. Protože nad nimi není dohled jako u dětí, mohou se nesprávně rozhodnout. Počet uživatelů ICT mezi seniory má stoupající tendenci. Mnohdy umožňuje seniorům, kteří jsou méně pohybliví anebo odloučení, kontakt se svými blízkými. Pořizovací náklady nejsou vysoké a šance být v kontaktu a nebýt sám, směřuje seniory k používání moderních technologií. Problémem zůstává, že jsou většinou bez odborného zázemí a jsou vystaveny mnoha hrozbám. Pak je jen na nich, jak se rozhodnou a jaké to bude mít důsledky. Jejich mnohdy nadměrná důvěra v neprověřené záležitosti jim následně způsobuje obrovské problémy [62].

Závěrem lze říci, že bohužel není v ničích silách vymýcení kybernetické kriminality a sociálně-patologických jevů v prostředí internetu. Avšak existuje možnost, jak proti nim bojovat a snižovat jejich dopady.

ZÁVĚR

Tato odborná publikace shrnuje výsledky řešení projektu výzkumu, vývoje a inovací s názvem „Aktuální kybernetické hrozby v České republice a jejich eliminace“. Zaměřuje se na analýzu a dopady vyplývající z nově přijatého Zákona o kybernetické bezpečnosti a jeho prováděcích předpisů. 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.

Dále je v publikaci provedena deskripce současné situace v oblasti kritické informační infrastruktury v ČR. Jsou zmíněny i způsoby odhalování kybernetické kriminality a nástroje k tomu používané.

Dalším přínosem publikace je šetření psychologického profilu útočníka, kterého je možné charakterizovat z několika úhlů pohledu na jeho osobnost, strukturu a hlavně motivaci jeho činnosti. Naopak bylo také zkoumáno ověření struktury osobnosti odborníků pracujících v oblasti informačních technologií. Celý proces diagnostického šetření byl zaměřen na zjištění osobnostních předpokladů osob pro práci v oblasti informačních technologií. Výsledkem je návrh souboru testů.

Na závěr publikace se autoři zaměřili na popularizaci kybernetické bezpečnosti, která by se měla ubírat směrem k dětem, dospívající mládeži a v neposlední řadě také k seniorům. Počet uživatelů informačních a komunikačních technologií mezi seniory má stoupající tendenci. A právě senioři mnohdy akceptují nebezpečné jednání druhých osob bez jakéhokoliv podezření, že by je to mohlo ohrozit.

CONCLUSION

This publication summarizes the results of the project of the research, development and innovation entitled "Current cyber threats in the Czech Republic and their elimination." The book is focused on the analysis and implications which ensues from newly adopted cyber security law and its implementing regulations. On the base of executed analysis and comparison of the national, European and international law there has been created a set of suggestions and recommendations for possible amendments of legal standards for further development in the field of cyber security in the Czech Republic.

Furthermore, the publication consists of a description of the current situation in the field of critical information infrastructure in the Czech Republic. There were mentioned ways of detecting of cybercrime and the tools to use.

Another benefit of the publication is investigation of the psychological profile of the attacker, which can be characterized from several points of view of his personality, structure, and especially by the motivation of his/ her activities. Conversely, it was also examined the personality structure of experts working from information technology area. The entire process of diagnostic investigation was focused on finding personal abilities of people for work in information technology area. The result of the investigation is a proposal of set of tests.

Authors focused in the final part of the publication on the popularization of cyber security, which should proceed towards to children, adolescents and the primary line also to seniors. The number of users of information and communication technologies among seniors has been increasing. And older people often accept the dangerous behavior of other people without any suspicion that it might endanger to them.

RESUME

Attentive readers, who had read up to this page, surely noticed that what we predicted at the beginning of the publication was gradually met within previous chapters. We can state that all goals were fulfilled not only in general, but also concretely with aim to expand view about the area of cyber security.

Scope, exploitation and continuously expansion of information and communication systems within society increases dependence of the society on the proper function of these systems. The success of individual entities (companies, organizations, institutions) is dependent on the protection of these systems, which in its content and meaning can be targeted by various interest groups or individuals whose goal is to gather information, data, or the intention is damage of the organization.

Information and communication technologies are currently used in all spheres of public and private life - the economy, public administration, the military, industry, health sector, education, etc. Information, which is worked in the area, are implemented in information systems and they are highly prized value for individual entities. There is often a very sensitive data about the structure and activities of the organization, production processes, business information, and personal data. Data are largely digitized due to the development of technology and development opportunities. This results in a significant savings in labour, reduced space requirements, as well as time demands of work. But there is a problem with security constraints and increased access to this information.

Information in the digital form is universally applicable, duplicated and transformable, and therefore can be easily exploitable. Digitized data are on the one hand significant benefits to human society, but on the other hand they can be in the case of misuse very dangerous weapon. Technological progress gives space and the possibility of criminal behavior.

Development of all kinds' of technologies, including computer equipment is strong and aggressive. Together with this is growing ingenuity of perpetrators of crime electronic information. The computer literacy has been gradually increasing and access to the internet has nearly everyone because the price is very low. The number of range products is increasing, that are easily affordable to a wide range of users - professionals and other

interested parties due to the acceptable price. Together with this we can track the growing opportunity for creation of the targeted attack on organizations or consumers with the intent of data exploitation for their own enrichment.

POUŽITÁ LITERATURA A INFORMAČNÍ ZDROJE

1. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů ČR, 2014, ročník 2014, částka 75, číslo 181.
2. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitosti podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). In: Sbírka zákonů ČR, 2014, ročník 2014, částka 127, číslo 316.
3. Vyhláška o významných informačních systémech a jejich určujících kritériích. In: Sbírka zákonů ČR, 2014, ročník 2014, částka 127, číslo 317.
4. ČSN ISO/IEC 27001. Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky. Praha: Český normalizační institut, 2006.
5. Příloha II směrnice Rady 2008/114/ES, ze dne 8. prosince 2008, o určování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.
6. Zákon o elektronických komunikacích, ve znění pozdějších předpisů (zákon o elektronických komunikacích). In: Sbírka zákonů ČR, 2005, ročník 2005, částka 43, číslo 127.
7. HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti. *Revue pro právo a technologie*. 2013, roč. 4, č. 8. ISSN 1804-5383
8. VOLEVECKÝ, Petr. Kybernetické hrozby a jejich trestněprávní kvalifikace. *Trestní právo*. 2011, roč. 15, č. 1.
9. Zákon o krizovém řízení, ve znění pozdějších předpisů (krizový zákon). In: Sbírka zákonů ČR, 2000, ročník 2000, částka 73, číslo 240.
10. PROCHÁZKOVÁ Dana. *Metodiky hodnocení rizik*, časopis 112, č. 3 (2004)
11. Kolektiv autorů. *Ochrana kritické infrastruktury*. Praha: 2011, 1. vydání, 189 s. ISBN 978-80-260-1215-3.
12. UČEŇ, Pavel a kolektiv: Metriky v informatice. Grada Publishing, 2001, 140 stran, ISBN 80-247-0080-8.

13. DOUCEK, Petr; NEDOMOVÁ, Lea; NOVÁK, Luděk; SVATÁ, Vlasta. Řízení bezpečnosti informací. Druhé přepracované vydání, Praha: Professional Publishing, 2011, ISBN 978-80-7431-050-8.
14. MLÝNEK, Jaroslav. Zabezpečení obchodních informací. 1. BIZBOOK, 2007-02-05. ISBN 9788025115114.
15. POŽÁR, Josef. Systém řízení informační bezpečnosti. In Kný, Milan; Požár, Josef. Aktuální pojetí a tendence bezpečnostního managementu a informační bezpečnosti. Brno: Tribun EU, 2010, s. 93 - 110. ISBN 978-807399-067-1.
16. DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.
17. ČERMÁK, Miroslav. Řízení informačních rizik v praxi. V Tribunu EU Vyd. 1. Brno: Tribun EU, 2009, 134 s. ISBN 978-80-7399-731-1.
18. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. In: Sbírka zákonů ČR, 2010, ročník 2010, částka 149, číslo 432.
19. Nařízení vlády, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury In: Sbírka zákonů ČR, 2014, ročník 2014, částka 127, číslo 315.
20. Přednášky a studijní materiály k předmětu Management bezpečnostního inženýrství, Ing. Martin Hromada.
21. Risk Analysis Consultants: Překlad a interpretace normy BS ISO/IEC 27001:2005 pro české prostředí 2005.
22. BEJDA, Radek. *Návrh a stanovení nových povinností provozovatelů a poskytovatelů služeb elektronických komunikačních sítí*. Zlín, 2015. Diplomová. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Vedoucí práce Ing. Martin Hromada, Ph.D.
23. PIKNER, Ivo; ZŮNA, Pavel; SPIŠÁK, Ján; GALATÍK, Vlastimil; KUBEŠA, Milan; KRČMÁŘ, Miroslav; DUBEC, Radek; ČEP, David; FRANK, Libor. Operační koncepce: Přístupy a postupy. Praha: Powerprint s. r. o., Praha, 2012, 96 s. ISBN 978-80-87415-68-9.
24. KUMARI, Warren – MCPHERSON, Danny. *Remote Triggered Black Hole Filtering with Unicast Reverse Path*

Forwarding (uRPF) [online]. 2009 [cit. 2015-10-10]. Dostupné z: https://tools.ietf.org/html/rfc5635

25. STRETCH, Jeremy. *Remote Triggered Black Hole Routing* [online]. 2009 [cit. 2015-10-10]. Dostupné z URL: http://packet-life.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/
26. ZMIJEWSKI, Earl. *Longer is not always better* [online]. 2009 [cit. 2015-10-10]. Dostupné z: http://research.dyn.com/2009/02/longer-is-not-better/
27. POSPÍCHAL, Zbyněk. *Malý český ISP způsobil světový kolaps* [online]. 2009 [cit. 2015-10-10]. Dostupné z URL: http://www.lupa.cz/clanky/maly-cesky-isp-zpusobil-svetovy-kolaps/
28. SURÝ, Ondřej. *Proč a zda Supronet shodil Internet* [online]. 2009 [cit. 2015-10-10]. Dostupné z URL: http://www.lupa.cz/clanky/proc-a-zda-supronet-shodil-internet/
29. Hacker. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2014 [cit. 2014-12-10]. Dostupné z: https://cs.wikipedia.org/wiki/Hacker
30. DRAPELA. Viktor, J. *Přehled teorií osobnosti*. Praha: Portál, 1997. 175s. ISBN 80-7178-766-3
31. CHALUPA, Bohumír. *Studie z kognitivní psychologie*. Brno: Littera, 2011. 199s. ISBN 978-80-85763-65
32. ČÍRTKOVÁ, Ludmila. *Policejní psychologie*. Praha: SUPPORT,1996. 2.vyd, 304 s.ISBN 80-902164-0-4
33. BELZ, Horst, SIEGRIST, Marco. *Klíčové kompetence a jejich rozvíjení*. Praha. Portál, 2001. 1.vyd. 376s. ISBN 80-7178-479-6
34. SMÉKAL, Vladimír. *Pozvání do psychologie osobnosti*. Brno: BARRISTER PRINCIPAL, 2002, I.vyd. ISBN 80-85947-80-3
35. ŠTIKAR, Jiří, RYMEŠ Milan, RIEGEL, Karel, HOSKOVEC, Jiří. *Psychologie ve světě práce*. Praha: UK-Karolinum, 2003. ISBN 80-246-0448-5
36. ČR, Deloitte, Legislativní a organizační rámec kybernetické bezpečnosti v ČR, [cit. 2015-09-24].

37. WEBSTER, F. *Theories of the information society*. 2nd ed. London: Routledge, 2002, 304 s. International library of sociology. ISBN 04-152-8201-2.
38. Úmluva Rady Evropy č. 185 ze dne 23. 11. 2001 o kybernetické (počítačové) kriminalitě. In: *Council of Europe* [online]. Strasbourg: Council of Europe, 2015 [cit. 2015-08-22]. Dostupné z: http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm
39. SMEJKAL, V., SOKOL, T., VLČEK, M. *Počítačové právo*. Praha: C. H. Beck, 1995, s. 220
40. Wall, D. S. *Cybercrime: The Transformation of Crime in the Information Age.* Policy press, 2007.
41. POLČÁK, R. GŘIVNA. T. *Kyberkriminalita a právo*. Vyd. 1. Praha: Auditorium, 2008, 220 s. ISBN 978-80-903786-7-4.
42. VOLOVECKÝ, P. *Konference Pokroky v kriminalistice: sborník příspěvků z mezinárodní konference konané 24.-25. září 2008*. Vyd. 1. Praha: Policejní akademie České republiky, 2008, 1 CD-ROM. ISBN 978-80-7251-290-4.
43. JIROVSKÝ, V. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství.* 1. vyd. Praha: Grada, 2007, 284 s. ISBN 978-80-247-1561-2.
44. ECKERTOVÁ, Lenka a Daniel DOČEKAL. *Bezpečnost dětí na Internetu: rádce zodpovědného rodiče*. 1. vyd. Brno: Computer Press, 2013, 224 s. ISBN 978-802-5138-045.
45. PAVLÍČEK, Antonín. *Nová média a sociální sítě*. Vyd. 1. V Praze: Oeconomica, 2010, 181 s. ISBN 978-802-4517-421.
46. KOPECKÝ, Kamil a Veronika KREJČÍ. *Rizika virtuální komunikace*. Olomouc: NET UNIVERSITY, 2010. ISBN 978-80-254-7866-0.
47. Národní centrum kybernetické bezpečnosti. In: *govcert.cz* [online]. 2014 [cit. 2014-12-30]. Dostupné z: http://www.govcert.cz/cs/
48. NÁPLAVOVÁ, Magdalena. *Pojetí bezpečnosti v kyberprostoru na základních a středních školách.* Diplomová práce. Brno: Univerzita obrany, 2014. 64 s.
49. Sociální sítě. *JAK NA INTERNET* [online]. 2013 [cit. 2014-02-06]. Dostupné z: http://www.jaknainternet.cz/page/1751/socialni-site/

50. PIKNER, Ivo; GALATÍK, Vlastimil. Information management as a part of future operational environment in operational concepts. Zagreb, Croatia : University of Zagreb. The Faculty of Teacher Education, 2010, 4 p. ISBN 978-953-7210-30-4.

51. Jaké jsou internetové děti 2: Návyky nejmladších uživatelů internetu. In: *Seznam.cz Výzkumník* [online]. 2014 [cit. 2014-12-14]. Dostupné z: http://vyzkumnik.seznam.cz/news_items/48?from=index

52. Zabezpečení počítače. In: *Bezpečný internet.cz* [online]. 2014 [cit. 2014-12-16]. Dostupné z: http://www.bezpecnyinternet.cz/zacatecnik/zabezpeceni-pocitace/default.aspx

53. Jaké jsou internetové děti 1:Co si odnesou z hodin informatiky?. In: *Seznam.cz Výzkumník* [online]. 2014 [cit. 2014-12-08]. Dostupné z: http://vyzkumnik.seznam.cz/news_items/46?from=index

54. Tipy pro výuku. In: *Bezpečný internet.cz* [online]. 2014 [cit. 2014-12-06]. Dostupné z: http://www.bezpecnyinternet.cz/skoly/tipy-pro-vyuku/tipy-pro-vyuku.aspx

55. Projekty pro koncové uživatele. In: *nic.cz* [online]. 2014 [cit. 2014-12-09]. Dostupné z: http://www.nic.cz/page/2086/projekty-pro-koncove-uzivatele/

56. Projekty pro odbornou veřejnost. In: *nic.cz* [online]. 2014 [cit. 2014-12-09]. Dostupné z: http://www.nic.cz/page/2049/projekty-pro-odbornou-verejnost/

57. PRAHA - bezpečně online. Národní centrum bezpečnějšího internetu. In: *Saferinternet.cz.* [online]. 2014 [cit. 2014-12-10]. Dostupné z: http://www.saferinternet.cz/finish/4-metodiky/22-praha-bezpecne-online-brozura-uvod-do-tematu-pocitacove-bezpecnosti

58. Jak na Internet. In: *nic.cz* [online]. 2014 [cit. 2014-12-10]. Dostupné z: http://www.jaknainternet.cz/

59. Senioři v hledáčku nových projektů Nadace Vodafone a Seznam.cz. In: *ebezpeci.cz* [online]. 2014 [cit. 2014-12-30]. Dostupné z: http://www.e-bezpeci.cz/index.php/home/4-vzdlavani/948-senioi-v-hledaku-novych-projekt-nadace-vodafone-a-seznamcz

60. HRŮZA, Petr. *Kybernetická bezpečnost*. Vyd. 1. Brno: Univerzita obrany, 2012, 90 s. ISBN 978-80-7231-914-5.

61. TANEČEK, David. Na Facebooku je 4,2 milionu Čechů. Jejich počet za rok stoupl o desetinu. In: *Deník.cz* [online]. 2014 [cit. 2014-02-04]. Dostupné z: http://www.denik.cz/z_domova/na-facebooku-je-4-2-milionu-cechu-jejich-pocet-za-rok-stoupl-o-desetinu-20140203.html

62. HRŮZA, Petr; PITAŠ, Jaromír; ŠANDA, Jaroslav; BRECHTA, Bohumil. *Kybernetická bezpečnost II.* Brno: Univerzita obrany, Brno, 2013, 100 s. ISBN 978-80-7231-931-2.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AS	Autonomous System
APT	Advanced persistent threat
BCMS	Business Continuity Management System
BOZP	Bezpečnost a ochrana zdraví při práci
BPI	Bezpečnostní politika informací
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
ČR	Česká republika
DoS	Denial of Service
DDoS	Distributed Denial of Services
EIGRP	Enhanced Interior Gateway Routing Protoco
ENISA	Evropská agentura pro informační a síťovou bezpečnost
ETA	Event Tree Analysis
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard Operation Process
HRA	Human Reliabitity Analysis
ICQ	Aplikace pro on-line komunikaci přes internet
ICT	Information and Comunication Technologies
IDS	Intrusion Detection System – systém pro odhalení průniku do sítě
IP	Internet Protocol
IPS	Intrusion Prevention System – systém pro detekci a prevenci průniku do sítě
S	Informační systém

ISMS	Information Security Management System
ISVS	Informační systémy veřejné správy
IT	Informační technologie
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
LAN	Local Area Network
MPO	Ministerstvo průmyslu a obchodu
MV	Ministerstvo vnitra
NAC	Network Access Control – kontrola přístupu k síti
NBÚ	Národní bezpečnostní úřad
OSPF	Open Shortest Path First
OSWAP	Open Web Aplication Security Project
PHA	Preliminary Hazard Analysis
PHM	pohonné hmoty a maziva
PO	Požární ochrana
PSA	Probabilistic Safety Assesment
QRA	Quantitative Risk Aalysis
RIP	Routing Information Protocol
RTBH	Remotely Triggered Black Hole
RR	Relative Ranking
VIS	Významné informační technologie
VoIP	Voiceover Internet Protokol
WAN	Wide Area Network
ZEK	Zákon o elektronických komunikacích

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

AUTOŘI PUBLIKACE

Ing. Martin Hromada, Ph.D.

Martin Hromada v roce 2008 absolvoval vysokoškolské vzdělání na UTB ve Zlíně v odb. Bezpečnostní technologie, systémy a management. Dizertační práci "Technologické aspekty ochrany kritické infrastruktury ČR" obhájil v roce 2011. V současnosti pracuje jako odborný asistent na Ústavu bezpečnostního inženýrství, Fakulty aplikované informatiky, Univerzity Tomáše Bati ve Zlíně a jako konzultant společnosti Deloitte Advisory, s.r.o. V rámci vědecko-výzkumných aktivit se aktivně věnuje problematice ochrany a odolnosti kritické (informační) infrastruktury a problematice hodnocení funkčnosti systémů fyzické ochrany. Publikuje a přednáší na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Petr HRŮZA, Ph.D.

Petr Hrůza je absolventem Vojenské akademie v Brně v roce 1995. Pracuje až doposud v různých výzkumných a pedagogických funkcích na Vojenské akademii v Brně a následně na Univerzitě obrany. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematikou managementu, bezpečností informačních systémů, kybernetickou bezpečností, ochranou kritické infrastruktury, geografickými informačními systémy, informační podporou velení a řízení. Publikuje a přednáší na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Josef KADERKA, Ph.D.

Josef Kaderka absolvoval Vojenskou akademie v Brně v roce 1987, obor Automatizace velení – elektronické počítače. Zastával různé vědeckopedagogické funkce na Vojenské akademii v Brně a následně na Univerzitě obrany, působí i na jiných institucích. Ve své odborné, publikační a pedagogické činnosti se zabývá problematikou počítačových sítí a jejich bezpečnosti. Významně se podílel na praktické implementaci počítačových sítí i informačních systémů na škole. Je aktivní jako instruktor výukového programu Cisco Networking Academy. Publikuje a přednáší na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Oldřich LUŇÁČEK, Ph.D.

Oldřich Luňáček vysokoškolské vzdělání dosáhl v roce 1989 na Vysoké vojenské technické škole v Liptovském Mikuláši. Za dobu působení u útvarů a zařízení Armády České republiky zastával velitelské a štábní funkce zejména v oblasti komunikačních a informačních systémů, posléze působil v oblasti KIS ve velitelských strukturách NATO (1989-2001). Disertační práci obhájil v roce 2010. V současné době pracuje na Univerzitě obrany, Fakultě vojenských technologií, Katedře komunikačních a informačních systémů jako odborný asistent. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematickou ochrany informací, fyzickou bezpečností a znalostním managementem. Publikuje a přednáší na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Miroslav NEČAS, Ph.D.

Miroslav Nečas je absolventem České zemědělské univerzity v Praze v roce 2003. Od roku 2006 pracuje ve společnosti TOVEK jako projektový manažer. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematikou managementu znalostí, kybernetickou bezpečností a oblastí bezpečnosti obecně, geografickými informačními systémy, informační a znalostní podporou rozhodování. Přednáší na vysokých školách v ČR a publikuje na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

PhDr. Mgr. et Mgr. Bohumil PTÁČEK

Je absolventem Masarykovy univerzity v Brně, obory psychologie, pedagogika. Pracuje jako psycholog a učitel na Vysoké škole pozemního vojska ve Vyškově, po vzniku Univerzity obrany v Brně jako akademický pracovník. Zabývá se výukou obecné a aplikované psychologie v základní i kombinované formě studia a odborných kurzech organizovaných v rámci UO Brno i na dalších vysokých školách. Provádí psychodiagnostické služby v rámci poradenské činnosti. Je akreditovaným lektorem vzdělávání dospělých v oblasti prevence sociálně nežádoucích jevů. Podílí se na řešení úkolů projektů zaměřených na osobnost v pracovním procesu. Publikuje hlavně učební texty a odborné články na tematických konferencích.

Mgr. Ing. Leopold SKORUŠA, Ph.D.

Leopold Skoruša je absolventem Vysoké vojenské školy pozemního vojska (1982), Vojenské akademie (1998) a Právnické fakulty Masarykové univerzity (2009). V roce 2012 získal doktorát v oboru Ochrana obyvatelstva na Univerzitě obrany. Do roku 2000 byl ve služebním poměru vojáka z povolání a působil na velitelských a štábních funkcích u průzkumných jednotek a u Vojenské policie. Od roku 2004 působí jako akademický pracovník - odborný asistent na Univerzitě obrany. Ve své vědecko-výzkumné, publikační a pedagogické činnosti se zabývá problematikou aplikace práva v oblasti bezpečnosti a obrany státu, včetně kybernetické bezpečnosti a boje proti terorismu. Do těchto oblasti je zaměřena i jeho tuzemská i zahraniční publikační činnost. Přednáší na vědeckých konferencích jak v tuzemsku, tak i v zahraničí.

Ing. Richard SLOŽIL

Richard Složil vystudoval radiotechniku na Vojenské akademii v Brně (1986). Po škole pracoval u armádních útvarů se specializací na rádiovou techniku. Od roku 1994 se na technických a manažerských pozicích začal věnovat armádním datovým sítím a posléze i jejich bezpečnosti. Vykonával funkci Spojovacího náčelníka posádky Brno a podílel se na digitalizaci brněnské vojenské posádky. V lednu 2007 byl ustanoven velitelem nově založeného střediska kybernetické bezpečnosti a byl u zrodu armádních schopností reakce na počítačové incidenty CIRC. Se střediskem CIRC dosáhl výrazných úspěchů především v zahraničí, v rámci odborných technických cvičení amerického ministerstva obrany a NATO. Na funkci setrval až do odchodu do zálohy v roce 2015. Zapojil se i do vědecké práce v oboru kybernetické bezpečnosti u brněnské Masarykovy univerzity a Univerzity obrany.