MINISTERSTVO PRŮMYSLU A OBCHODU

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OPPI

Projekt:
Energetická a kybernetická bezpečnost

etapa II.

Praha 2014

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

Tento projekt je financován z ERDF prostřednictvím OPPI a ze státního rozpočtu ČR.

– OBSAH –

STRUČNÉ SHRNUTÍ II. ETAPY

1. Shrnutí II. etapy

Ve II. etapě projektu jsme rozpracovali celou řadu témat týkajících se kybernetické bezpečnosti v energetickém sektoru ve světle různých perspektiv. Prvně bylo cílem identifikovat konkrétní dosavadní standardy a procesy jejich tvorby (od identifikace problému, přes vývoj technologie jej řešící, po konkrétní standard) v našich oborech, primárně komunikačních systémech. Kybernetická bezpečnost v energetickém sektoru se v této etapě soustředila na legislativní uchopení standardů a jejich roli v českém právním prostředí, konkrétně pak roli naší platformy tak, abychom pracovali v co nejproduktivnějším souladu s iniciativami veřejného sektoru, konkrétně Národním bezpečnostním úřadem, Úřadem pro normalizaci a meteorologii a další. Mezi studie či kapitoly rozebírající spíše blízkou budoucnost se řadí jistě témata jako aktivní kybernetická obrana energetické infrastruktury nebo role bezpilotních prostředků při kontrole energetické infrastruktury.

První zmiňované je v naprostém počátku a bude předmětem hutné analýzy v etapě následující už proto, že je nyní silným tématem na světové úrovni. V příštích měsících se očekávají výsledky práce NATO CCD COE v Estonsku zaměřené právě na aktivní kybernetickou obranu. Nicméně druhé zmiňované téma je zde uvedeno primárně v kontextu významné inspirace v oboru – letectví, kde bezpečnost bezpochyby patří mezi ty nejvíce akcentované předpoklady stabilního fungování. Mezi doplňující práce lze zařadit komparaci kybernetických incidentů, kterou jsme zařadili z toho důvodu, aby abstraktní debaty o standardech technologiií dostaly jistou kontextuální hodnotu, se kterou celé úsilí dostává jasnější podobu.

Jako velmi zajímavou studii bychom rádi akcentovali práci kolegy doc. Polčáka, který zpracoval velmi podnětnou studii zabývající se právní perspektivou v oboru s přesahem možných budoucích rolí platformy TPEB v českém legislativním procesu.

2. Výhled do III. etapy

Na základě nashromážděných znalostí bude III. etapa primárně zaměřená na přípravu konkrétních výzkumných projektů v rámci finančního nástroje Horizon 2020. Konec III. etapy je plánován na 31.7.2014, přičemž deadline pro podání projektů je 28.8.2014. Během této etapy vznikne řada studií zaměřených na konkrétní problematiku

připravovanou pro evropské projekty Horizon 2020. Smyslem studií bude odborná příprava znalostního pozadí interdisciplinárního charakteru využitelná jako odborné pozadí pro text projektových přihlášek. Interdisciplinaritou zde chápeme překlenutí mezi strategickými cíli (např. aktivní kybernetické obrany), technickým řešením, jeho legislativními dopady a v neposlední řadě standardizačními a legislativními procedurami. Výsledek třetí etapy přinese konkrétní návrhy technického řešení vhodného pro standardizační procedury včetně aktualizace SVA.

CESTOVNÍ MAPA

Technologické oblasti / Strategické cíle	I. etapa	II. etapa	III. etapa
	Identifikace problémů; definice priorit; aktualizace SVA v návaznosti na zájem a potřeby veřejného i soukromého sektoru;	Rozpracování výzkumných priorit; analýza jejich implementačních možností; propojení s iniciativami v rámci EU;	Návrh (implementace) legislativních, standardizačních/certifikačních opatření; Návrh (implementace) technologických řešení;
Komunikační technologie	Zálohování a zabezpečení činnosti komunikačních systémů; Optimální autonomní napájení komunikačních systémů;	Analýza rizik spojených s použitím vybraných komunikačních systémů a možnosti doplňkového zabezpečení těchto komunikačních systémů	Návrh technologických řešení/standardů v oblasti zabezpečení a ochrany zkoumaných komunikačních systémů a jejich napájení.
Kybernetická bezpečnost	Analýza kybernetických hrozeb a rizik ve vybraných segmentech; Standardizace praxe ve veřejném sektoru; Proces utváření standardů v návaznosti na EU procesy;	Analýza hrozeb a rizik spojených s energetickým sektorem, smart gridy, cloudy. Návrh řešení v návaznosti na iniciativy EU. Možnosti aktivní obrany ve veřejném i soukromém sektoru;	Návrh „best practises“ týkajících se praxe ve veřejném sektoru. Návrh technologických řešení/standardů spojených s prioritními sektory. Koncepce strategie aktivní obrany na národní úrovni s přesahem do soukromého sektoru;
Fyzická bezpečnost	Potenciál vytváření jednotné platformy pro monitoring a částečné ovládání integrací; Identifikace legislativních potřeb v této oblasti	Návrh jednotné platformy (komunikačního protokolu) umožňujícího propojit integrační platformy v oblasti fyzické bezpečnosti KI.	Návrh legislativních opatření a konkrétního technologického řešení kontroly integračních platforem;
Technologie sledování prvků KI		Letecká cesta jako součást kritické infrastruktury a zkušenosti vyplývající z její ochrany za pomocí standardizace	

SHRNUTÍ VÝSLEDKŮ II. ETAPY

Tento materiál reprezentuje výsledek práce expertů jednotlivých výzkumných oblastí projektu energetické a kybernetické bezpečnosti ve II. etapě projektu, jenž je výsledkem iniciativy definované v SVA TPEB. Tato aktivita se primárně odvíjí ve čtyřech technologických oblastech – komunikační technologie, kybernetická bezpečnost, technologie sledování prvků kritické infrastruktury a fyzická bezpečnost.

Ve všech těchto oblastech došlo v rámci první fáze naplňování SVA k identifikaci klíčových priorit, které budou výzkumně nadále rozvíjeny v dalších fázích. V souladu s implementačním plánem byla v první fázi provedena analýza stávajícího stavu v daných oblastech s ohledem na technologickou, legislativní, ale i personální (ve smyslu znalostí a kapacit) situaci. S přihlédnutím k expertním i technickým kapacitám v rámci TPEB byla poté identifikována klíčová témata, která budou dále rozpracována.

Dosažené cíle II. etapy:

- proběhlo shrnutí celé řady standardizovaných technologií a konkrétních standardů s cílem identifikovat možné výzkumné oblasti
- 30.1.2014 jsme zorganizovali ve spolupráci s centrem SIX Vysokého učení technického v Brně konferenci s mezinárodní účastí
- výstupem z konference je rozpracovaný projekt výzkumu komunikačních systémů ve spolupráci s britskou univerzitou v Sheffieldu s financováním z rámcového programu Horizon 2020
- identifikovali jsme řadu podnětných oblastí, ve kterých budeme v následující etapě připravovat další projektové žádosti a vytvářet výzkumná konsorcia, ve kterých propojíme akademickou a soukromou sféru především z řad členů platformy

1. Shrnutí kapitol etapy II.

1.1. Kapitola: Bezpečnost komunikačních systémů a standardy

V kapitole věnované komunikačním systémům jsme se pokusili odpovídajícím způsobem přiblížit problematiku standardů ve světě v komparaci s českým úřadem pro normalizaci a meteorologii. Zhodnotili jsme různé standardizační autority a jejich postupy při uznávání technologie a její charakteristiky jako standardu. Zhodnocení

postupu, nebo lépe řečeno procesů, u různých standardizačních autorit je inspirativním vhledem do problematiky z mezinárodní perspektivy, jejímž výstupem je kritické zhodnocení možnosti uplatnění vlastních výzkumných výstupů pro standardizační ambice v III. etapě projektu. Zaměřili jsme se na ty standardy, které mají významnější působnost v energetice.

1.2. Kapitola: Kybernetická rizika a pojišťovny

V této kapitole se podrobně zabýváme problematikou pojištění a kybernetických útoků. Kromě několika zajímvých textů, které se touto problematikou již zabývaly, se autor rozepisuje podrobnou analýzou kybernetického rizika a pojišťovnictví, stejně jako problematikou pojišťovnictví jako takovým. Problém kybernetických hrozeb je zde dán do souvislosti s finanční újmou způsobenou kybernetickým útokem, kterou pojištovny nevnímají jako hrozbu. Proto je následující argumentace dána do souvislosti s principy pojišťovnictví a uzavíra, jakým způsobem by bylo vhodné s pojišťovnami postupovat, aby kybernetické hrozby začaly vnímat realisticky. Mezi nejcitlivější oblasti kybernetických hrozeb patří jistě energetická síť ČR, jejíž provozovatelé patří mezi první subjekty, které by měly s pojišťovnami začít spolupracovat, aby nastavily jisté standardy v nově vznikající oblasti rizik. Konkrétním příkladem je produkt CyberEdge pojišťovny AIG, která jako první začala pojištění proti škodě způsobené kybernetickým útokem poskytovat.

1.3. Kapitola: Analýza rizik fyzické bezpečnosti v energetické oblasti

Nedílnou součástí celého dokumentu je tato kapitola zabývající se analýzou hrozeb ve smart gridech používaných v energetickém sektoru. Studie přibližuje metodiku analýzy fyzické bezpečnosti dle specifických standardů, důraz je kladen na metodu PLSM, která identifikuje typické hrozby pro tyto inteligentní sítě, na jejichž základě následně definuje několik desítek opatření rozdělených do řady domén.

Kapitola fyzické bezpečnosti se dále zabývá problematikou tvroby jednotného komunikačního protokolu pro sběr dat z různých technologických řešení používaných v tomto bezpečnostním oboru. V současné době sice existují technologická řešení, nicméně autor zde dochází k jejich nedostatkům a na ty se snaží odpovědět návrhem řešení. Dvouvrstvé řešení sběru informací zajistí větší spolehlivost, především u kriticky důležitých instalací, jako jsou např. elektrárny v energetice. Jednotný sběr všech dat na jednom integrovaném pracovišti pak zajistí lepší reakci a vyhodnocení situace personálem, který má kontrolu fyzické bezpečnosti v daném objektu na starosti.

1.4. Ochrana kritické infrastruktury v EU

Tato kapitola se zabývá zdánlivě netradiční součástí kritické infrastruktury a to leteckou cestou. Velmi podrobně popisuje celý systém letecké dopravy z perspektivy, která je inspirativní pro standardizaci technologií v oblastech, na který se tento projekt primárně soustřeďuje. Nedílnou součástí této kapitoly je zmínka o bezpilotních prostředcích, které jsou realitou blízké budoucnosti nejen ve vojenství, ale i komerčním sektoru. Např. nově vstupující společnost na český trh, Amazon, se netají svou vizí doručovat balíky vlastním dopravním systémem nezávislým na všech ostatních dopravcích bezpilotními prostředky. Podobné představy vznikají v případě potřeby vizuální kontroly prvků energetické soustavy, které jsou rozmístěné často i na špatně dostupných místech. Stadardizace nejen použitých technologií komunikačních systémů, ale i jistá spojitost se současnou legislativou je jistě na místě a pro české úřady bude v blízké budoucnosti velkou výzvou.

Zkušenosti ze standardizačních a certifikačních projektů v oblasti řízení letového provozu, ať už civilního nebo nově vznikajícího prostředí bezpilotních prostředků jsou jednoznačně velmi inspirativní, neboť důraz na funkčnost a bezpečnost je v tomto oboru jedinečný. V závěru této kapitoly naleznete konkrétní podobu návrhu výzkumného projektu, který budeme v příští etapě připravovat pro podání do programu Horizon 2020.

1.5. Příloha č. 1 – Principy a perspektivy kybernetické bezpečnosti ČR z právního hlediska

V této příloze doc. Polčák, renomovaný právník, autor věcného záměru Zákona o kybernetické bezpečnosti, rozebírá velmi do detailu a velmi podnětně celý legislativní proces reflexe kybernetické bezpečnosti v ČR. V závěru své práce pak klade důraz na roli standardizačních projektů, jako je tento a technologických platforem je orgazujících. V konečném důsledku je tato studie nesmírně cenným příspěvekm do II. etapy projektu, neboť nastiňuje velmi realisticky možnosti standardizace technologií a jejich oporu pro dodržování Zákona o kybernetické bezpečnosti a jeho související požadavky kladené na soukromé společnosti s přesahem do energetického sektoru.

1.6. Příloha č. 2 – Aktivní kybernetická obrana

Ve studie zabávající se aktivní kybernetickou obranou (či ochranou) rozvíjíme téma, které se na mezinárodním poli hodně v současné době skloňuje. V principu se jedná o aktivní přístup, namísto pasivní ochrany, který je z celé řady důvodů sporný, způsobuje tendenci militarizovat kybernetický prostor a balancuje na hraně zákona. Je

nutné vzít v úvahu, že ne všechny aktivity jsou natolik diskutabilní. Přes všechny tyto problémy však řada podob aktivní ochrany existuje v podobě konkrétních produktů, např. detekční systémy anomálií v síti nebo klamné systémy vábící hackery s cílem následného studia jejich znalostí a dovedností. Nicméně v neposlední řadě se jedná o konkrétní techniky zpětného napadnutí útočícího systému s cílem jeho terminace. Tuto problematiku do jisté míry otevírá i studie předešlá.

Energetický sektor je primárním odvětvím, ve kterém získání času před případným naplněním probíhajícího útoku může hrát kritickou roli, aby dodávka energií nebyla přerušena. K tomu slouží právě klamná / decepční řešení, tzv. honeypoty nebo honeynety, které pro útočníka vytváří zrcadlené prostředí bez faktických dopadů na řízené systémy.

1.7. Příloha č. 3 – Komparace významných kybernetických incidentů

Tato vesměs spíše deskriptivní studie rozebírá výběr nejznámějších incidentů v nedávně době, aby čtenáři na konkrétních případech přiblížila realitu kybernetických incidentů, útoků, komplexních operací s jejich potenciálními dopady. Cílem této studie je především přinést konkrétní podobu kybernetických incidentů. Ačkoliv se řada z nich může jevit velmi specificky a v tomto světle jako nemožné replikace, pak je zde vhodné podotknout, že např. kód Zeus doznal řádově desítky tisíc unikátních kompilací. Z toho plyne, že jeho původní kód byl pro útoky na internetové bankovnictví použit možná i tisícovkami lidí.

1.8. Příloha č. 4 a 5 – SCADA systémy a Smart Gridy

Tyto závěrečné studie rozebírají problematiku standardizace u SCADA systémů užitých v průmyslových podnicích, resp. u inteligentních rozvodných energetických sítí Smart Grid.

NÁVRHY NA VÝZKUMNÉ PROJEKTY III. ETAPY

Zájemci ze soukromého sektoru v České republice jsou vítáni v případě zájmu participace na níže uvedených projektech.

Projekt z II. etapy:

Projekt:	**CySmart? Cybersecurity & Trust in (Wireless?) Communications Systems**
Deadline:	Duben, 2014, **podáno**
Zdroj:	Horizon 2020
Zúčastnění:	TPEB The University of Scheffield Brno University of Technology University of Surrey a přibližně 10 dalších ze soukromého sektoru napříč Evropou

Témata pro projekty připravené ve III. etapě:

Projekt:	**Vývoj a realizace bezpilotního prostředku (UAV) střední velikosti s hybridním pohonem**
Deadline:	Srpen, 2014
Zdroj:	Horizon 2020
Zúčastnění:	TPEB, ???
Projekt:	**Rozvoj kryptografických algorytmů (privacy-enhancing technologies, digital identity protection, data collection systems)**
Deadline:	Srpen, 2014
Zdroj:	Horizon 2020
Zúčastnění:	TPEB, VUT Brno, ???
Projekt:	**Zabezpečení inteligentních sítí kritické infrastruktury**
Deadline:	Srpen, 2014
Zdroj:	Horizon 2020
Zúčastnění:	TPEB, VUT Brno, ???
Projekt:	**Rozvoj forenzních systémů proto kyberkriminalitě**
Deadline:	Srpen, 2014
Zdroj:	Horizon 2020
Zúčastnění:	TPEB, VUT Brno, ???
Projekt:	**Prostředky aktivní kybernetické ochrany**
Deadline:	Srpen, 2014
Zdroj:	Horizon 2020
Zúčastnění:	TPEB, VUT Brno, ???

Další témata k výzkumu:
Implementace behaviorální analýzy do školicího programu pracovníka bezpečnosti kontroly
Rozšíření působnosti ATSKC na oblast certifikovaných školení AVSEC Training Centre for Aviation Security
Evropský portál sdílení znalostí a informací mezi subjekty zapojenými v řetězci ochrany před protiprávními činy v civilním letectví
Vytvoření nového studijního oboru „Bezpečnostní studia zaměřený na Aviation Security Management“
Improving Aviation Security Level by Using European Information and Knowledge Exchange Centre for Stakeholders in Aviation Security Chain

BEZPEČNOST KOMUNIKAČNÍCH SYSTÉMŮ NORMY A STANDARDY

1. Úvod

Bezpečnost komunikací (COMSEC, *communications security*) je samostatná disciplína, která se zabývá prevencí neautorizovaných přístupů k přenášeným datům. Tato prevence zahrnuje kryptografické zabezpečení, zabezpečení přenosu a zabezpečení fyzické infrastruktury.

Výše uvedeným zabezpečením se věnujeme v následujících kapitolách.

Mezi nástroje využívané k zajištění bezpečného provozu komunikačního zařízení patří doporučení, normy a standardy. Mezi celosvětově uznávané instituce, které se vydávání doporučení, norem a standardů věnují, patří:

- National Institute of Standards and Technology (NIST)
- International Organization for Standardization (ISO)
- Institution of Electrical and Electronics Engineers – Standards Association (IEEE-SA)
- European Committee for Standardization (CEN)

Implementaci mezinárodních standardů v českém prostředí a harmonizaci českých standardů se standardy mezinárodními má na starosti:

- Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (UNMZ)

V následujících kapitolách popisujeme aktivity dílčích organizací na poli standardů pro zabezpečení komunikačních systémů.

2. National Institute of Standards and Technology

NIST byl založen v roce 1901. V současnosti je NIST součástí U.S. Department of Commerce. Součástí NIST je Computer Security Division (CSD).

Computer Security Division (CSD) byla zřízena zákonem 107-347 *E-Government Act*, který definoval povinnosti a zodpovědnosti CSD. Zákon 107-347 *E-Government Act* byl schválen kongresem USA a podepsaný prezidentem USA v prosinci 2002 jako výraz

uznání důležitosti informační bezpečnosti pro oblast ekonomických a národních zájmů Spojených států amerických.

CSD vydává speciální publikace řady 800. Tyto publikace představují dokumenty, které se věnují bezpečnosti počítačových systémů a zabezpečení jejich vzájemné komunikace. Speciální publikace řady 800 začaly být vydávány v roce 1990.

Publikace řady 800 mají charakter doporučení. Vydaná doporučení jsou průběžně aktualizována. Výběr vybraných doporučení je uveden v příloze č. 1.

Postup, jakým NIST připravuje návrhy doporučení a standardů, lze ilustrovat na zveřejnitelném šifrovacím algoritmu:

1. V roce 1997 NIST oznámila, že chce nahradit stávající standard DES (*Data Encryption Standard*) standardem novým AES (*Advanced Encryption Standard*).
2. Byla vyhlášena veřejná soutěž. V průběhu soutěže bylo specifikováno, že se má jednat o blokovou šifru s velikostí bloku 128 bitů a velikostmi klíčů 128, 192 a 256 bitů.
3. Do soutěže bylo přihlášeno 15 různých návrhů z několika zemí. Návrhy byly posouzeny z hlediska bezpečnosti, možnosti implementace na různých platformách a možnosti využití v různých aplikacích.
4. V prvním kole bylo vybráno pět nejlepších návrhů (kompromis bezpečnosti, možnosti implementace a šíře aplikací), v druhém kole byl vybrán vítěz.
5. Na základě vítězného návrhu byla v roce 2001 vytvořena odpovídající norma.

3. International Organization for Standardization

ISO je celosvětově největším vydavatelem dobrovolných mezinárodních standardů. ISO byla založena v roce 1947 a během doby svého trvání vydala téměř 20 000 mezinárodních standardů. Řada standardů je vztažena právě k problematice bezpečnosti informačních a komunikačních systémů. Standardy z této oblasti spravuje technický výbor ISO/IEC JTC 1/SC 27 – IT Security techniques.

Dílčí podmnožinou výše uvedených standardů je rodina standardů ISO 27000. Tyto standardy pomáhají organizacím zajistit bezpečnost informačních aktivit.

Organizace využívají tyto standardy zejména k ochraně finančních informací, k ochraně duševního vlastnictví, a ochraně údajů o zaměstnancích.

ISO/IEC 27001 je nejznámějším standardem z rodiny 27000. Tento standard definuje požadavky na systém managementu informační bezpečnosti (ISMS, *information security management system*). ISMS aplikuje na lidi, procesy a informační systémy management rizik.

Stejně jako v případě ostatních ISO standardů týkajících se systému managementu existuje nepovinná ISO/IEC 27001 certifikace.

Výběr standardů je uveden v příloze č. 2 této kapitoly.

Proces přijetí standardu je rozdělen do následujících kroků:

1. **Předběžná etapa** je věnována přípravě práce na standardu. Výsledkem předběžné etapy je dokument, který je předán odpovídajícímu technickému výboru.
2. **Etapa návrhu**. Technický výbor posoudí dokument z předběžné etapy. Je-li výsledek posouzení kladný, jmenuje technický výbor pracovní skupinu, která zahájí práce na návrhu standardu.
3. **Přípravná etapa**. Pracovní skupina vypracuje draft standardu. Získá-li návrh standardu většinu hlasů v hlasování, je tento draft předán komisi.
4. **Etapa komise**. Komise návrh standardu posoudí a hlasuje o něm. Návrh musí získat většinu hlasů.
5. **Dotazovací etapa**. Úspěšný návrh je rozeslán národním členům organizace ISO k vyjádření a hlasování. Standard musí získat tři čtvrtiny kladných hlasů.
6. **Etapa schvalování**. Standard je rozeslán národním orgánům ke konečnému schválení (zde již nejsou přípustné žádné technické změny). Standard je přijat, získá-li alespoň dvě třetiny hlasů.
7. **Etapa zveřejnění**. Finální verze standardu je zveřejněna jako mezinárodní standard.

4. Institution of Electrical and Electronics Engineers – Standards Association

Institution of Electrical and Electronics Engineers (IEEE) je celosvětovou profesní organizací elektrotechnických inženýrů. Součástí IEEE je asociace pro standardy (SA, Standards Association).

IEEE-SA je organizací, která vypracovává globální standardy ze všech oblastí elektrotechniky a informatiky. Každým rokem IEEE-SA posuzuje na 200 návrhů standardů z hlediska jejich spolehlivosti a důkladnosti jejich zpracování.

Posuzování návrhů sestává ze sedmi základních kroků:

1. **Zajištění sponzorství**. Za návrh standardu se musí zaručit jedna z profesních společností IEEE.
2. **Požadavek na zplnomocnění**. Výbor pro standardy prostuduje požadavek profesní společnosti na její zplnomocnění vypracovat standard a doporučí toto zplnomocnění vydat či nikoli.
3. **Vytvoření pracovní skupiny**. Je-li zplnomocnění vydáno, je vytvořena pracovní skupina odborníků, která na standardu pracuje. Schůzky pracovní skupiny jsou z principu veřejné a přístupné všem.
4. **Návrh standardu**. Pracovní skupina vypracuje návrh standardu.
5. **Tajná volba**. Návrh standardu je zaslán všem, kdo projeví zájem o standard. Každý, kdo odpoví kladně na pozvání k hlasování, získává právo o standardu hlasovat. Hlasuje-li pro standard více než 75% hlasujících, postupuje návrh standardu dále. V opačném případě se návrh vrací do kroku 4.
6. **Oponentní komise**. Oponentní komise posoudí, zda je návrh standardů v souladu s předpisy IEEE. V kladném případě komise návrh odsouhlasí.
7. **Konečné hlasování**. Každý člen výboru pro standardy o standardu hlasuje. Je-li většina hlasů kladných, je standard přijat.

Výběr standardů je uveden v příloze č. 3.

5. European Committee for Standardization

CEN byl založen v roce 1961 s cílem vyvinout celoevropské standardy pro evropský vnitřní trh. Dalšími oficiálními evropskými organizacemi pro standardizaci

jsou CENELEC (European Committee for Electrotechnical Standardization) a ETSI (European Telecommunications Standards Institute).

Standardy z oblasti zabezpečení komunikačních systémů vydává ETSI. Výběr standardů týkajících se zabezpečení komunikačních systémů uvádíme v příloze č. 4.

6. Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

Úřad pro technickou normalizaci, metrologii a státní zkušebnictví (ÚNMZ) byl zřízen zákonem České národní rady č. 20/1993 Sb. o zabezpečení výkonu státní správy v oblasti technické normalizace, metrologie a státního zkušebnictví. ÚNMZ je organizační složkou státu v resortu Ministerstva průmyslu a obchodu ČR. Hlavním posláním ÚNMZ je zabezpečovat úkoly vyplývající ze zákonů České republiky upravujících technickou normalizaci, metrologii a státní zkušebnictví a úkoly v oblasti technických předpisů a norem uplatňovaných v rámci členství ČR v Evropské unii. Od roku 2009 zajišťuje také tvorbu a vydávání českých technických norem.

Odbor technické normalizace odpovídá zejména za zabezpečování tvorby, vydávání a řádné distribuce českých technických norem, normalizačních dokumentů a publikací; zabezpečování odborných činností souvisejících s vydáváním a řádnou distribucí českých technických norem v rozsahu a za podmínek stanovených zákonem č. 22/1997 Sb., o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů; spolupráci s evropskými a mezinárodními normalizačními organizacemi v rámci působnosti odboru.

Odbor mezinárodních vztahů zodpovídá zejména za zabezpečování výkonu působnosti MPO v oblasti sbližování technických předpisů ČR se souborem právních předpisů ES s technickým obsahem (dále jen technické předpisy ES), za zabezpečování meziresortní organizace a koordinace notifikací návrhů technických předpisů v rámci Dohody *World Trade Organization* o technických překážkách obchodu (TBT) a směrnice 98/34/ES, za zabezpečování činnosti sektorové skupiny Technické harmonizace v rámci Ministerstva průmyslu a obchodu, a za zabezpečování mezinárodní spolupráce a obecných vztahů s EU v oblastech působnosti Úřadu. Zajišťuje implementaci směrnice 98/34/ES, ve znění pozdějších předpisů.

7. Závěr

Cílem předložené studie bylo vytvořit stručný přehled institucí a organizací, které se zabývají vytvářením standardů na poli zabezpečení informačních a komunikačních

systémů. U vybraných institucí jsme popsali způsob vytváření standardů jako příklad *best practices* v daném oboru.

Ze studie vyplývá doporučený postup při vytváření vlastních standardů v oblasti zabezpečení informačních a komunikačních systémů:

1. Podrobná rešerše stávajících mezinárodních standardů. Jelikož se Česká republika zavázala k harmonizaci svých standardů se standardy evropskými, je třeba respektovat standardy vydávané ETSI. Pokud na evropské úrovni standard neexistuje, ale je dostupný v rámci ISO, IEEE či NIST, je optimální iniciovat převzetí existujícího standardu. To může být námětem národního projektu (např. TAČR).
2. Pokud standard pro danou oblast vůbec neexistuje, je vhodné vytvořit předběžný návrh standardu, který by byl široce diskutován v rámci celé Evropy (zde mohou svými kontakty pomoci univerzity).
3. Získá-li návrh standardu dostatečnou podporu, je zapotřebí obrátit se na UNMZ s žádostí o zahájení procesu vytváření normy. I když bude norma vytvářena na národní úrovni, bylo by dobré proces vytváření co nejvíce otevřít i pro odborníky z ostatních evropských zemí.
4. Nepokryté oblasti diskutovat s členskými firmami TPEB. U prioritních oblastí připravit osnovy vlastních standardů a snažit se pro ně získat podporu v rámci EU. To může být námětem evropského projektu.
5. Vyústí-li celý proces v přijetí české státní normy, bylo by dobré iniciovat přijetí této normy na evropské úrovni.

8. Příloha č. 1 – Vybraná doporučení vydaná CSD, NIST

CSD vydává speciální publikace řady 800. Tyto publikace představují dokumenty, které se věnují bezpečnosti počítačových systémů a zabezpečení jejich vzájemné komunikace. Speciální publikace řady 800 začaly být vydávány v roce 1990.

Speciální publikace řady 800 jsou dostupné na webové adrese: http://csrc.nist.gov/publications/PubsSPs.html

Níže uvádíme výběr z uvedené řady dokumentů:

- SP 800-164 10/2012, Guidelines on Hardware-Rooted Security in Mobile Devices, draft

- SP 800-161 08/2013, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, draft
- SP 800-153 02/2012, Guidelines for Securing Wireless Local Area Networks (WLANs)
- SP 800-152 01/2014, A Profile for U. S. Federal Cryptographic Key Management Systems (CKMS), draft
- SP 800-147 04/2011, Basic Input / Output System (BIOS) Protection Guidelines
- SP 800-146 05/2012, Cloud Computing Synopsis and Recommendations
- SP 800-144 12/2011, Guidelines on Security and Privacy in Public Cloud Computing
- SP 800-137 08/2011, Information Security Continuous Monitoring for Federal Information Systems and Organizations
- SP 800-135 12/2011, Recommendation for Existing Application-Specific Key Derivation Functions
- SP 800-133 12/2012, Recommendation for Cryptographic Key Generation
- SP 800-132 12/2010, Recommendation for Password-Based Key Derivation Part 1: Storage Applications
- SP 800-131 A 01/2011, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- SP 800-130 08/2013, A Framework for Designing Cryptographic Key Management Systems
- SP 800-128 08/2011, Guide for Security-Focused Configuration Management of Information Systems
- SP 800-127 09/2010, Guide to Securing WiMAX Wireless Communications
- SP 800-126 11/2009, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.0
- SP 800-124 01/2013, Guidelines for Managing the Security of Mobile Devices in the Enterprise

- SP 800-123 07/2008, Guide to General Server Security
- SP 800-122 08/2010, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
- SP 800-121 01/2012, Guide to Bluetooth Security
- SP 800-119 12/2010, Guidelines for the Secure Deployment of IPv6
- SP 800-117 08/2010, Guide to Adopting and Using the Security Content Automation Protocol (SCAP) Version 1.0
- SP 800-116 11/2008, A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
- SP 800-115 08/2008, Technical Guide to Information Security Testing and Assessment
- SP 800-114 11/2007, User's Guide to Securing External Devices for Telework and Remote Access
- SP 800-111 11/2007, Guide to Storage Encryption Technologies for End User Devices
- SP 800-108 10/2009, Recommendation for Key Derivation Using Pseudorandom Functions
- SP 800-100 10/2006, Information Security Handbook: A Guide for Managers
- SP 800-98 08/2007, Guidelines for Securing Radio Frequency Identification (RFID) Systems
- SP 800-97 02/2007, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i
- SP 800-95 08/2007, Guide to Secure Web Services

9. Příloha č. 2 – Mezinárodní standardy vydané ISO

Standardy z oblasti zabezpečení informačních a komunikačních systémů spravuje technický výbor ISO/IEC JTC 1/SC 27 – IT Security techniques. Přehled všech souvisejících standardů je dostupný na adrese http://www.iso.org/iso/home/store/catalogue_tc/catalogue_tc_browse.htm?commid=45306&published=on&includesc=true

Ke standardům této kategorie například patří:

- ISO/IEC 18014-1:2008 Information technology – Security techniques – Time-stamping services – Part 1: Framework
- ISO/IEC 18014-2:2009 Information technology – Security techniques – Time-stamping services – Part 2: Mechanisms producing independent tokens
- ISO/IEC 18014-3:2009 Information technology – Security techniques – Time-stamping services – Part 3: Mechanisms producing linked tokens
- ISO/IEC 18028-4:2005 Information technology – Security techniques – IT network security – Part 4: Securing remote access
- ISO/IEC 18031:2011 Information technology – Security techniques – Random bit generation
- ISO/IEC 18033-1:2005 Information technology – Security techniques – Encryption algorithms – Part 1: General
- ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers
- ISO/IEC 18033-3:2010 Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers
- ISO/IEC 18033-4:2011 Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers

Zvláštní pozornost si zaslouží standardy řady ISO/IEC 27001. Tyto standardy ošetřují management informační bezpečnosti. Standardy řady ISO/IEC 27001 jsou dostupné na webové adrese: http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

Mezi standardy této řady patří:

- ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements
- ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security controls
- ISO/IEC 27003:2010 Information technology – Security techniques – Information security management system implementation guidance

- ISO/IEC 27004:2009 Information technology – Security techniques – Information security management – Measurement

10. Příloha č. 3 – Mezinárodní standardy vydané IEEE-SA

Standardy z oblasti zabezpečení informačních a komunikačních systémů spravuje technický výbor ISO/IEC JTC 1/SC 27 – IT Security techniques. Přehled všech souvisejících standardů je dostupný na adrese http://odysseus.ieee.org/query.html?charset=iso-8859-1&style=standard&qt=communication+security&st=26

Ke standardům této kategorie například patří:

- 802.1AR-2009 Secure Device Identity
- 802.10a-1999IEEE Standard for Interoperable LAN/MAN Security (SILS)
- 802.10g-1995IEEE Local and Metropolitan Area Networks: 802.10 Supplement: IEEE Standard Secure Data Exchange (SDE) – Security Label (Annexes 2I, 2J, and 2K)
- 802.1X-2010 IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control
- 8802-1X-2013 IEEE/ISO/IEC Information technology – Telecommunications and information exchange between systems – Local and metropolitan area networks
- 1609.2-2006 IEEE Trial-Use Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages
- 1711-2010 IEEE Trial-Use Standard for a Cryptographic Protocol for Cyber Security of Substation Serial Links
- 1901-2010 IEEE Standard for Broadband over Power Line Networks: Medium Access Control and Physical Layer Specifications
- 2030-2011 IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads

11. Příloha č. 4 – Mezinárodní standardy vydané ETSI

Standardy z oblasti zabezpečení informačních a komunikačních systémů spravuje technický výbor ISO/IEC JTC 1/SC 27 – IT Security techniques. Přehled všech souvisejících standardů je dostupný na adrese http://pda.etsi.org/pda

Ke standardům této kategorie například patří:

- ETSI ETR 336 Telecommunications Management Network (TMN); Introduction to standardizing security for TMN
- ETSI ETR 340 Telecommunications security; Guidelines for security management techniques
- ETSI ETR 367 Telecommunications security; Guidelines on the relevance of security evaluation to ETSI standards
- ETSI EG 200 234 Telecommunications security; A guide to specifying requirements for cryptographic algorithms
- ETSI EG 201 057 Telecommunications security; Trusted Third Parties (TTP); Requirements for TTP services
- ETSI EG 201 620 Intelligent Network (IN); Security studies for Cordless Terminal Mobility (CTM)
- ETSI EG 202 238 Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON); Evaluation criteria for cryptographic algorithms
- ETSI EG 202 387 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables
- ETSI EG 202 549 Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Design Guide; Application of security countermeasures to service capabilities
- ETSI EN 300 920 Digital cellular telecommunications system (Phase 2+) (GSM); Security aspects (GSM 02.09 version 7.1.1 Release 1998)
- ETSI EN 302 109 Terrestrial Trunked Radio (TETRA); Security; Synchronization mechanism for end-to-end encryption
- ETSI EN 301 261 Telecommunications Management Network (TMN); Security; Part 3: Security services; Authentication of users and entities in a TMN environment

KYBERNETICKÁ RIZIKA A POJIŠŤOVNY

1. Úvod

Svět obchází nové strašidlo – strašidlo kybernetického útoku. Podvody v on-line bankovnictví, krádeže identity v databázích, DDoS útoky na firemních webových stránkách, kybernetická špionáž, útoky na kritické infrastruktury, kybernetický terorismus - World Wide Web nabízí zločincům nespočet možností k útoku.

Chci se v této práci zaměřit na možnost pojištění kybernetického rizika ze strany komerčních pojišťoven, objasnit důvody, které vedou pojišťovny v České republice k výlukám těchto rizik z pojištění, jaké jsou možnosti řešení a pokusit se navrhnout kroky ke změně tohoto stavu.

2. Analýza současného stavu

V rámci přípravy jsem oslovil významné pojišťovny na českém trhu (Česká pojišťovna, Allianz, Kooperativa, ČSOB Pojišťovna, Generali a Pojišťovna ČS) s jednoduchým dotazem: "Mám zájem o pojištění kybernetického rizika naší firmy z hlediska ztráty zisku, dat, důvěry a v neposlední řadě i poškození dobrého jména. Můžete mi, prosím, poskytnout základní informace co obsahuje pojistné krytí, jak určit pojistnou částku, jaká je její maximální výše, jaké jsou výluky ap. V neposlední řadě mne také zajímá cena, spoluúčast ap." Ze všech pojišťoven mi přišla v zásadě stejná zamítavá odpověď: "Děkujeme Vám za poptávku pojištění u naší společnosti. Pojištění tohoto typu však naše pojišťovna neposkytuje. "

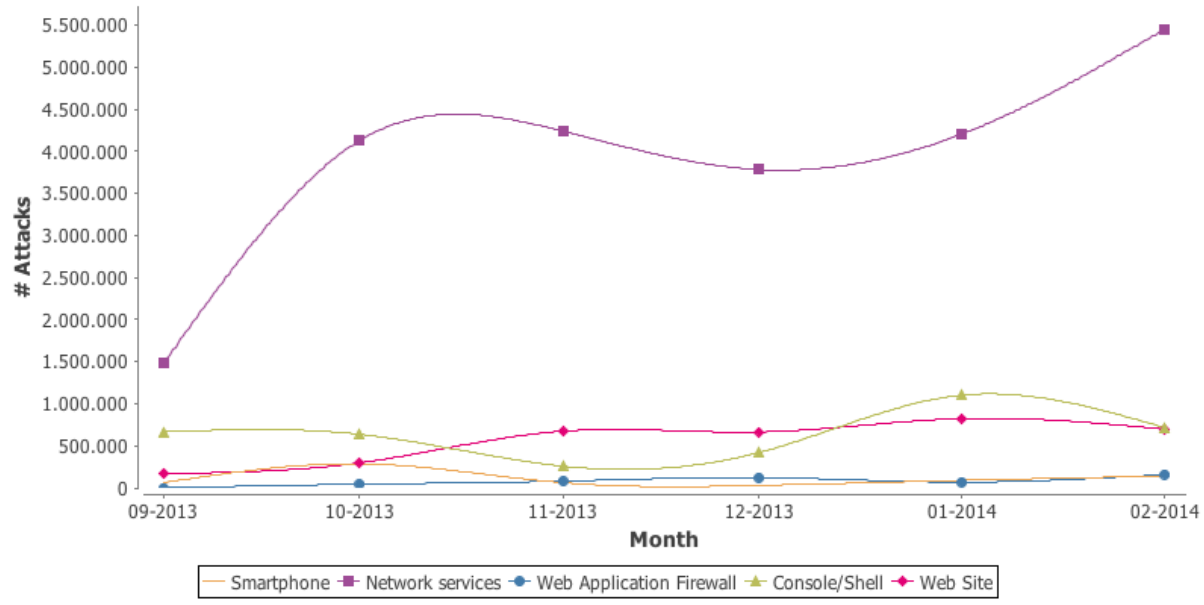
V roce 2011 bylo celosvětově zaznamenáno více než 855 případů narušení bezpečnosti, během kterých bylo zasaženo 174 milionů dat. Jaké jsou údaje o nejčastějších kybernetických útocích? 71% ze všech případů, kdy došlo k narušení bezpečnosti a ztrátě dat se týkalo malých a středních společnosti s 1 – 100 zaměstnanci; 96% všech útoků bylo provedeno velmi jednoduchým způsobem; v 97% všech případů se dalo předejít ztrátě dat dodržováním základních bezpečnostních pravidel a aktualizací bezpečnostních systémů; každou minutu je globálně zasaženo malwarem 232 počítačů. (Antič & Hanzal, 2013)

Za pomocí velice primitivních programů lze ohrozit firemní data, zjistit hesla, údaje o zákaznících atd. Důsledky jsou rozmanité - ztráta některých údajů může omezit poskytování služeb, může mít za následek porušení práv duševního vlastnictví,

soukromí nebo osobnostních práv. Postižené firmy by měly očekávat, pokuty a penále. Kyberšikana nebo hackerské útoky přinášejí závažné důsledky.

Současně společnostem vznikají dodatečné náklady: IT systémy mohou selhat kvůli útokům software. Také interní firemní síť může být poškozena, čímž se zpomalí její provoz. Kybernetické útoky jsou schopné zasáhnout společnosti i jednotlivce. Zejména smartphony a další mobilní zařízení jsou velice citlivá na útoky přes www a musí být po útoku opraveny nebo jsou dále nepoužitelné, totéž platí pro poškozené hardware a rozhraní. Kupodivu společnosti považují tato rizika za velmi nízká.

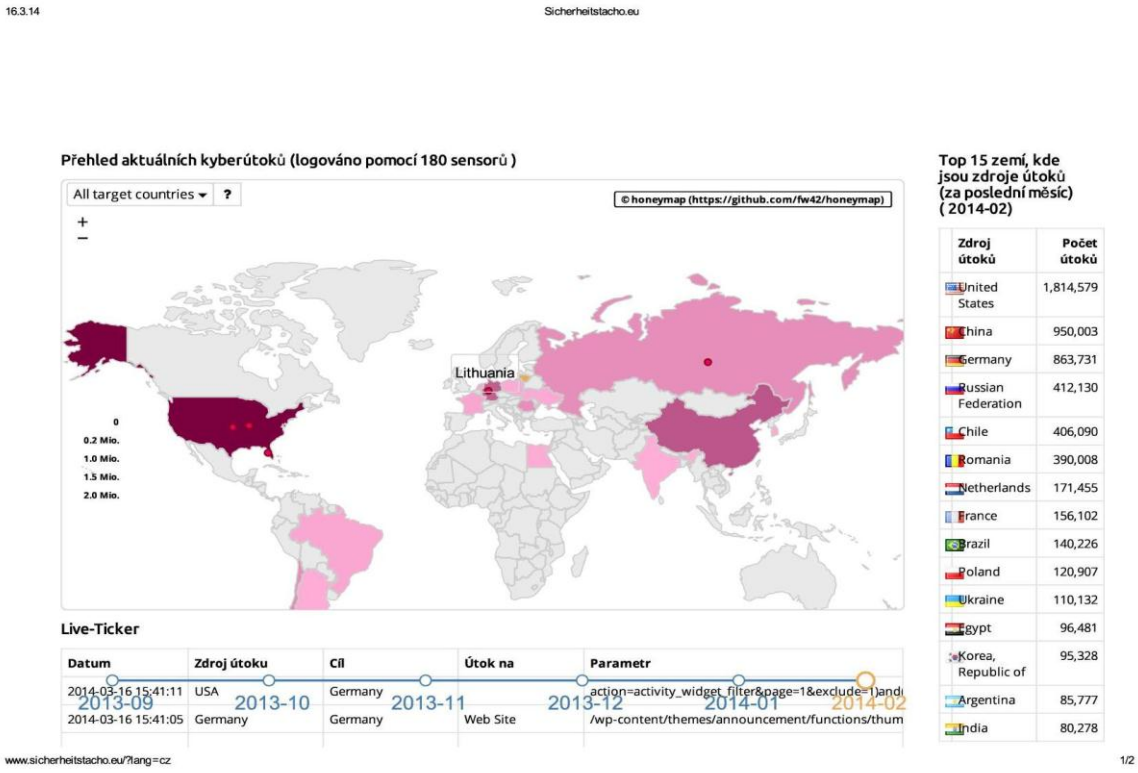
Kybernetické úroky jsou závažným problémem. S rostoucí mírou závislosti mnoha institucí a firem na výpočetní technice spolu se stále širším využitím internetu tak útok na počítačové sítě vypadá z pohledu zvenčí čím dál lákavěji. Světový terorizmus je stále problémem číslo jedna. Neexistuje již oblast lidské činnosti, která by se nějakým způsobem neodrážela na globální síti. A stále více společností v USA se zajímá o to, jak se co nejlépe chránit před kybernetickými útoky, jejichž výskyt v poslední době jednoznačně narůstá. S tím souvisí i fakt, že podle posledních údajů stoupl počet společností, které si zakoupily produkty kyberpojištění, ve srovnání s rokem 2012 o 33 %. U některých oblastí, jako je například vzdělávání, odborné poradenství, účetnictví, obchod, právní služby je pak tento nárůst obzvláště markantní. (Antič & Hanzal, 2013)



Obr. 1 – Celosvětový počet útoků po měsících za období 09/2013 až 02/2014

Statistika trestné činnosti ve Spolkové republice Německo uvádí dle podkladů Spolkového kriminálního úřadu (BKA) za rok 2012 celkem 64.000 případů počítačové

kriminality a 230.000 případů útoků přes internet. Uvedená čísla ovšem tvoří jen špičku ledovce a mnoho kybernetických zločinů se do statistik vůbec nedostane. Podle aktuální studie e-Crime poradenské společnosti KPMG čtvrtina z 500 společností v Německu byla postižena v posledních dvou letech kyberzločinem a Bavorská obchodní asociace odhaduje, že škody způsobené kybernetickou trestnou činností připraví německou ekonomiku o 50 miliard EUR ročně.



Obr. 2 – Přehled aktuálních kyberútoků dle Deutsche Telecom AG pro den 16. 03. 2014 (Deutsche Telecom AG)

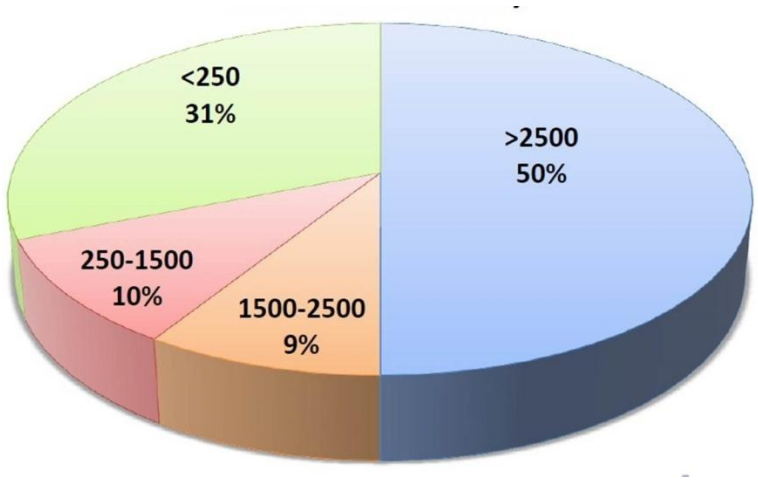
Podle dotazovaných odborníků se meziročně téměř zdvojnásobil počet firem, které si připouštějí ohrožení kybernetickými riziky. Ten stoupl z loňských (rok 2013) osmi procent na letošních 15 procent, u ztráty dobré pověsti pak z 6 procent na 10 procent. (Finanční noviny)

"V roce 2012 došlo meziročně k 42% nárůstu cílených útoků, přičemž jejich cílem byly často krádeže duševního vlastnictví. Stále častěji jsou terčem firmy z výrobního sektoru a malé organizace - druhé jmenované nyní až v 31 % případů." Tvrdí to alespoň společnost Symantec ve své zprávě Internet Security Threat Report (ISTR). Malé podniky jsou podle zástupců firmy atraktivními cíli samy o sobě, ale zároveň

mohou být prostředkem pro ohrožení větších firem prostřednictvím útoků typu „watering hole“.

„ISTR 2013 ukazuje, že kyberzločinci nezpomalují své tempo a pokračují v hledání nových způsobů, jak krást data z organizací všech velikostí,“ říká Stephen Trilling, chief technology officer Symantecu. „Propracovanost útoků ve spojení s dnešním složitým IT světem, zejména díky virtualizaci, mobilitě a cloudu, vyžaduje od firem i nadále proaktivní přístup a používání komplexních bezpečnostních řešení, pokud chtějí zůstat v bezpečí,“ dodává.

Symantec podle zprávy zaznamenal největší nárůst cílených útoků mezi podniky s méně než 250 zaměstnanci. Malé podniky jsou nyní terčem ve 31 % všech těchto útoků, což je významný nárůst oproti roku 2011. Zatímco malé podniky mohou mít pocit, že jsou imunní vůči cíleným útokům, zločince zjevně lákají jejich informace o bankovních účtech, údaje o zákaznících i duševní vlastnictví. Útočníci se zaměřili na malé podniky, které často nedodržují adekvátní bezpečnostní postupy a nemají odpovídajícím způsobem zabezpečenou infrastrukturu. (SymanTec)



Obr. 3 – Podíl počítačových útoků dle počtu zaměstnanců firmy

3. Základní pojmy z pojišťovnictví

Pojišťovna je finanční instituce, která pojišťuje, tj. na základě smlouvy o pojištění (pojistné smlouvy) s pojišťujícím subjektem (pojistníkem) a placení pojistného finančně kryje pojištěná rizika pojištěného subjektu (pojištěnce), tj. proplácí v případě škodní (pojistné) události pojištěnému subjektu (pojištěnci) náhradu škody nebo její určenou část.

Pojištění některých rizik může být povinné ze zákona. V České republice je povinné ze zákona například zdravotní pojištění osob a některá pojištění odpovědnosti, zejména pojištění odpovědnosti z provozu vozidla (povinné ručení) nebo pojištění podnikatelů pro případ pracovních úrazů jejich zaměstnanců.

Ostatní pojištění jsou dobrovolná na základě smlouvy uzavřené s pojišťovnou. Její zákonnou součástí bývají všeobecné pojistné podmínky, které v České republice schvaluje Ministerstvo financí a pojišťovny je musí dodržovat.

Jednotlivé pojišťovny mohou krýt rizika plynoucí ze smluv s klienty z podnikatelské sféry z vlastních prostředků jen z určité části. Zbývající část rizik, zejména pro velké či méně běžné případy pojištění podniků, se běžně sjednávají u jiné pojišťovny buď formou společného pojištění (tzv. soupojištění) anebo je mohou smluvně přenést na specializovanou instituci - zajišťovnu.

Pojištění lze definovat jako pomoc v nouzi. Z hlediska ekonomického to znamená vytvářet z příspěvků zájemců o pojištění (pojistníků) rezervy, které slouží k náhradám škod nebo k úhradě potřeb, které vzniknou pojištěným z nahodilých událostí. Jde o právní vztah mezi pojistitelem a pojistníkem. Základním účelem pojištění je zmírnit či odstranit nepříznivé důsledky způsobené nahodilými událostmi a dále efektivní způsob tvorby a rozdělování peněžních rezerv k úhradě potřeb, které vznikají z pojistných událostí. Ta je definována jako nahodilá skutečnosti, blíže označená v pojistné smlouvě nebo ve zvláštním právním předpisu, na který se pojistná smlouva odvolává a se kterou je spojen vznik povinnosti pojistitele poskytnout pojistné plnění.

4. Definice a činnost risk managementu pojišťovny

Fyzické i právnické osoby jsou denně vystaveny velkému množství nejrůznějších rizik. Podniky přitom riziko chápou jako něco, co může ohrozit jejich existenci, hospodářské výsledky, postavení na trhu, pověst apod. Snaží se proto přijmout taková opatření, která realizaci rizika zabrání nebo alespoň zmírní jeho následky. Snaha lidí o zvládnutí rizika pomocí určitých vědeckých přístupů vedla v minulosti ke vzniku speciálního oboru s názvem risk management, řízení rizik. Vznik vědní disciplíny risk management se datuje zhruba do poloviny sedmdesátých let minulého století.

Nejinak je tomu v pojišťovnictví. Zvýšená hrozba katastrof, teroristických či kybernetických útoků, podvodného jednání a také přísná státní regulace a silná konkurence v oboru – to jsou faktory, které pojistitele nutí klást stále větší důraz na kvalitní systémy řízení rizik a znalost realistické úrovně potřebného kapitálu.

Risk management pojištění je ve své podstatě řízení rizik, která pojišťovna přebírá od svých klientů. Smyslem jeho činnosti je ochránit pojišťovnu před možnými a zbytečnými ztrátami v případě předvídatelných škodních událostí a systematicky zkvalitňovat klientské portfolio pojišťovny. Zaměřuje se přitom na oblast neživotního pojištění – řízení rizik se stalo nedílnou součástí pojištění majetku a odpovědnosti za škodu v rámci pojištění velkých průmyslových podniků a postupně se začíná orientovat i na menší podnikatelské subjekty. Hlavní pozornost je stále upřena na velké průmyslové podniky a bezpečnostní standardy jejich fungování.

Do rámce risk managementu patří především odhad a identifikace rizika, analýza škod, nebezpečí a rizikových faktorů, stanovení pravděpodobnosti možné škody, stanovení maximální možné a pravděpodobné škody pro jednotlivá pojišťovaná nebezpečí, a to jak pro přímé, tak pro následné škody.

Součástí aktivit risk managementu pojištění je dále stanovení podmínek pojištění závažných průmyslových havárií a snaha postupně zvyšovat provozní bezpečnost pojištěných podniků.

5. Pojištění velkých průmyslových podniků

Pojištění velkých průmyslových podniků se označuje jako průmyslové či korporátní pojištění, případně pojištění velkých rizik. Mezi nejvýznamnější pojistná nebezpečí tohoto segmentu patří živelní rizika (požáry, povodně a exploze) a speciálně pak riziko ztráty v důsledku přerušení provozu.

Průmyslové pojištění tvoří obvykle malou část klientského portfolia, pojišťovny mu ale právě proto věnují při řízení rizik mimořádnou pozornost. Jedná se totiž o pojištění klíčových průmyslových odvětví, kde díky malému počtu případů selhává statistická analýza a při pojišťování korporátních klientů ve většině případů nelze vycházet z „tabulkových“ postupů, ale je potřeba vypracovat individuální strategii. Navíc škody vzniklé z titulu výše uvedených rizik bývají díky velikosti pojištěných podniků zpravidla velmi vysoké. Je tedy lepší případným ztrátám včas zabránit.

5.1. Analýza rizik a riziková zpráva

Základem risk managementu pojištění je důsledné analyzování rizik vstupujících do pojištění a jejich ohodnocení podle profilu rizik (výšky předpokládané škody, její frekvence a úrovně preventivních opatření). Při pojišťování velkých průmyslových podniků musí vykonat příslušný risk manager prohlídku provozů a areálů přímo na

místě. Cílem této činnosti je odhalit všechny možné škody, které zde v budoucnu mohou vzniknout.

Kromě klasického postupu hodnocení rizika, zejména v oblasti požární bezpečnosti, se risk management pojištění orientuje také na další druhy potenciálních nebezpečí, jako jsou rizikové procesy v oblasti chemie nebo nakládání s nebezpečnými látkami a postupně se zaměřuje také na oblast environmentální pojištění (životního prostředí).

Při pojišťování majetku se běžně využívají výstupy z geografického informačního systému. Ten zahrnuje informace o nebezpečí povodní a záplav a postupně do něj přibývají informace o dalších možných nebezpečích (např. vichřice, krupobití a zemětřesení). Informace užitečné pro hodnocení a ovlivňování rizik v této oblasti přináší prohlubování vzájemných vazeb s likvidací pojistných událostí, stejně jako spolupráce se zajistiteli ve všech oblastech pojistného rizika. Konečným výsledkem analýzy rizik je riziková zpráva. Ta obsahuje informace, na jejichž základě se upisovatel rozhoduje, zda daného klienta a za jakou výši pojistného přijme do portfolia. Zpráva dále vyjmenovává opatření, které klient musí provést při přijetí do pojištění, a doporučení, která přijmout může, ale nemusí. I na základě přístupu k těmto doporučením je pojištěný následně posuzován. Neživotní pojištění se upisují na jeden rok a před výročím smlouvy lze přístup ke klientovi modifikovat (upravit pojistné či naopak neobnovit smlouvu).

5.2. Úspěšnost a cíl risk managementu pojištění

Úspěch řízení rizik je charakterizován tzv. škodovostí (dříve škodním průběhem), což je procentuální poměr mezi vyplaceným pojistným plněním a předepsaným pojistným. Platí přitom, že čím je tento ukazatel nižší, tím je risk management pojištění úspěšnější. Pokles škodovosti předpokládá správné odhadování a oceňování rizik, jakož i účinnou zábranu škod.

Na základě škodovosti lze hodnotit působení risk managementu pojištění. Stále však existuje riziko, že jediná velká škoda může příznivý vývoj tohoto ukazatele zvrátit. Jen v míře velmi omezené lze přitom ovlivnit působení přírodních nebezpečí (povodeň, vichřice ap.). Cílem risk managementu je proto zvyšovat bezpečnostní standard fungování podniků. Hlavní pozornost je upřena na zlepšování technického a organizačního zabezpečení v procesu průmyslové výroby. Tímto způsobem lze chránit finanční stabilitu pojišťovny a zároveň zvyšovat provozní jistotu klienta. Naplnění tohoto cíle předpokládá soustavnou a systematickou práci s každým klientem.

5.3. Pojistně technické riziko a jeho řízení

Pojistně technické riziko úzce souvisí s nejistotou ohledně budoucích výplat pojistných plnění. V praxi musí být pojistitel neustále připraven na to, že riziko, které přebírá do pojištění, bude mít jiný průběh než jaký byl odhadnut na základě ocenitelných vnějších znaků rizika. Škodní průběh, tedy výše vyplacených pojistných plnění, se proto může lišit od očekávaného scénáře. K tomu, aby byly očekávané škody správně vyčísleny, používají pojišťovny výpočtové modely co nejvíce simulující vývoj rizika. Při svých kalkulacích vycházejí z minulého průběhu škod, z něhož odvozují průběh škod v budoucnosti. Ten mimo jiné závisí na současném a hlavně budoucím chování pojištěných. Problém tkví v tom, že toto chování může být neočekávané a podstatně jiné než doposud.

5.4. Postačitelnost pojistně technických rezerv

Hlavními prvky pojistně technického rizika jsou rizika plynoucí z pojistného a z výše pojistně technických rezerv a týkají se jejich dostatečné výše s ohledem na kapitálovou přiměřenost a závazky plynoucí z uzavřených pojistných smluv.

5.5. Koncentrace pojistně technického rizika

Při posuzování pojistně technického rizika je důležité vzít v úvahu jeho koncentraci. Ta udává, do jaké míry může pojistná událost nebo řada takových událostí ovlivnit závazky pojišťovny. Může vzniknout z jedné pojistné smlouvy nebo z více souvisejících smluv, a může být dále způsobena kumulací rizik z různých druhů pojištění. Ke koncentraci přitom nejčastěji dochází v důsledku událostí s nízkou četností a významným dopadem (živelní pohromy), při nečekaných změnách trendů (změny ve vývoji např. úmrtnosti či v chování pojistníků) a taktéž v případě závažných soudních sporů nebo legislativních rizik, které mohou způsobit jednorázovou velkou ztrátu.

5.6. Řízení pojistně technického rizika

Řízení pojistně technického rizika je velice složitý proces, v jehož rámci se uplatňují nejrůznější metody vyloučení rizika, zejména jeho diverzifikace, transfer a tvorba výkyvových rezerv. Díky nahodilosti pojistné události ovšem neexistuje spolehlivý způsob, který by pojistně technické riziko zcela odstranil. Pokud má být pojistně technické riziko úspěšně redukováno, je třeba uplatnit komplexní strategii jeho řízení. Je nutno je zakomponovat do vývoje nových produktů a stanovení výše pojistně technických rezerv. Pojišťovna musí mít dále vypracována kritéria pro stanovení ceny pojistného, strategii zajištění i pravidla pro přijetí do pojištění. Musejí se pravidelné sledovat rizikové profily, rizika plynoucích z pojištění a řízení aktiv a pasiv.

5.7. Strategie v oblasti uzavírání pojistných smluv

Strategie v oblasti uzavírání pojistných smluv vychází z ročního obchodního plánu. Ten určuje, jaké pojistné produkty budou v daném období poskytovány, a specifikuje taktéž cílové skupiny klientů. Jakmile je zvolená strategie schválena představenstvem, je dále rozpracována, tj. stanoví se limity pro jednotlivé upisovatele - výše, druh pojištění, území a sektor. Dochází tak k diverzifikaci rizika, jehož cílem je dosažení odpovídajícího rozložení rizik v rámci pojistného kmene. Součástí strategie je i opatření týkající se pojistných smluv v rámci neživotního pojištění – ty jsou každoročně přezkoumávány oprávněnými pracovníky, kteří mohou změnit podmínky smlouvy nebo zamítnout její obnovení.

5.8. Strategie v oblasti zajištění

Mezi výrazné možnosti zvládání pojistně technického rizika patří přenesení části rizika na zajišťovnu. Zajištěním rozumíme vertikální dělení rizika, kdy prvopojistitel postoupí část u něj pojištěných velkých rizik na specializovanou pojišťovnu – zajišťovnu. Zajištění nezmenšuje rozsah škod, činí jejich ekonomické dopady pro pojistitele únosnější. Zajištění představuje vztah mezi pojistitelem a zajistitelem, klient do něj nevstupuje. Obvykle se uplatňuje několikanásobné zajištění v zájmu dělení rizika. Zajistným označujeme odměnu zajistiteli za převzetí rizika, zajišťovací provize je ta část zajistného, kterou vrací zajistitel pojistiteli na pokrytí správních nákladů.

6. Definice kybernetického rizika

Kybernetická rizika jsou součástí našeho života ve světě plném informací a informačních technologií. Jakákoliv společnost, která přichází do styku s elektronickými daty, ať již v mobilních zařízeních, počítačích, serverech nebo online, je vystavena takovým rizikům.

Nebezpečí jsou různá – od ztráty informací z jednoho notebooku či počítače, až po hrozby cloud computingu. V podnikání mohou dále nastat i problémy s přístupem k systémům, neoprávněnými zásahy či přerušením webových služeb. Rizika a nebezpečí se vyvíjejí a stávají se stále komplexnějšími. Zatímco v minulosti společnosti investovaly do zabezpečení a ochrany hmotného majetku, nyní nastává čas zvážit bezpečnost a ochranu informací a informačních systémů.

Z pohledu pojistné události z důvodu kyberzločinu lze škody rozdělit do několika skupin.

Věcná škoda je v tomto případě nejjednodušší riziko – pojišťovna poskytne pojistné plnění za náklady práce (tzv. člověkodny). Daleko důležitější roli zde hraje zábrana škod, které spočívá např. v pravidelné zálohování dat a jejich ukládání na bezpečném místě. Tato činnost musí být kodifikována interní směrnicí konkrétní firmy a její dodržování důsledně vymáháno.

Ztráta dobrého jména - nelze objektivně určit výši škody, stanovení výše je ryze subjektivní, může být nadhodnoceno i podpojištěno. Limit pojistného plnění si nicméně vždy určuje klient.

Nelze určit četnost rizika – u korporátního pojištění se v mnoha případech uplatňuje tzv. pojištění na první riziko. Jedná se o pojištění vědomě sjednávané pouze na část známé pojistné hodnoty věci. Limit stanovuje (na svou odpovědnost) pojistník a je horní hranicí plnění pojistitele ze všech pojistných událostí vzniklých za určenou dobu.

7. Možnosti pojištění kybernetického rizika v ČR

Na tuzemském pojistném trhu se donedávna kyberpojištění nenabízelo. Jako nejbližší produkt bylo využíváno pojištění pro případ přerušení nebo omezení provozu podniku – ve všeobecných pojistných podmínkách najdeme však většinou pasáž, která škody podobné těm způsobeným kybernetickými útoky z pojištění vylučuje. (Antič & Hanzal, 2013)

V ČR působí na základě §5, odst. 1 zákona číslo 363/1999 Sb. o pojišťovnictví vedle domácích pojišťoven také organizační složky zahraničních pojišťoven. Z nich pouze dvě nabízejí pojištění kybernetického rizika.

ACE European Group Ltd., Organizační složka pro Českou republiku. Mateřská ACE European Group sídlí v Londýně a poskytuje pojistné služby ve 27 zemích Evropy, Středního východu a Afriky. Mezi její klienty se řadí společnosti, které působí v různých zemích, podnikají v různých průmyslových odvětvích. Jedná se především o mezinárodní korporace i lokální firmy, které jsou klienty z pohledu pojištění majetkových nebo odpovědnostních rizik. Působí také jako zajišťovna. Kyberpojištění bude nabízet od dubna 2014, zatím neposkytla žádné informace ani externím makléřským sítím.

AIG Europe Limited, Organizační složka pro Českou republiku, která je součástí American International Group, Inc. (AIG) Ta patří k největším světovým poskytovatelům neživotního pojištění a pečuje o své klienty ve více než 130 zemích. Klienti z řad jednotlivců, středních i velkých mezinárodních společností mají k dispozici

jednu z nejrozsáhlejších sítí poboček s vysokou kvalitou poskytovaných služeb. Akcie společnosti AIG jsou obchodovány na burze cenných papírů v New Yorku i Tokiu.

Společnost AIG začala pod označením **CyberEdge** nabízet jako první pojišťovna českým firmám speciální produkt v podobě pojištění kybernetických rizik. Vznik tohoto nového druhu pojištění vychází v reakci na stále přibývající případy kybernetických útoků.

Po USA, kde již tato možnost funguje, a Evropě, kde ji AIG začala nabízet na konci roku 2012, si tak mohou nyní pojistit svůj virtuální majetek i české firmy. CyberEdge je unikátním spojením tradiční pojistné ochrany za účelem náhrady škody způsobené samotným útokem, odcizením, či ztrátou dat a současně zahrnuje i krytí nákladů, které daná společnost musí vynaložit v důsledku vzniklé škody – např. náklady na právní služby, IT odborníky či PR specialisty. Produkt je koncipován tak, aby jej mohly využít různé typy společností, které na českém trhu působí. Ceny a konkrétní podmínky jsou nastavovány individuálně na základě určených parametrů a mohou se pohybovat v závislosti na rozsahu pojistného krytí, typu a velikosti firmy v řádech desetitisíců, resp. statisíců až milionů Kč ročně. Zajišťují však úhradu vysokých škod, které mohou kybernetické hrozby způsobit.

Produkt v sobě zahrnuje několik oblastí pojistného krytí. V základním nastavení je obsaženo finanční zajištění v důsledku neoprávněného nakládání s údaji, krytí nákladů spojených s udělením sankcí a pokut dozorovými orgány a v neposlední řadě i úhrada výdajů vynaložených na odborné služby. Volitelná rozšiřující pojištění pokrývají výpadek serveru či únos a vydírání klienta ve spojení s kyberkriminalitou. Pojištění se vztahuje na zjevné i skryté následky kybernetických rizik, což umožňuje společnostem pokračovat v jejich podnikání bez obav z „domino“ efektu a případného celkového kolapsu. Dále spojuje AIG znalosti o pojištění a rizicích z podnikání, a zároveň dává možnost využít služeb renomovaných odborníků na informační rizika, PR a právní problematiku.CyberEdge je navržený tak, aby poskytoval ochranu před škálou rizik, která nejsou kryta běžným odpovědnostním pojištěním.

CyberEdge pomáhá zmírnit nejen finanční dopady úniku, zneužití nebo ztráty dat, ale také dopady na IT systémy či dobré jméno společnosti tím, že poskytuje kombinaci tradiční pojistné ochrany a služeb profesionálních konzultantů. Produkt je určený pro jakékoliv společnosti.

Základní krytí je zaměřeno na neoprávněné nakládání s údaji, na povinnosti pojištěného vůči dozorovým orgánům a na náklady na odborné služby. Neoprávněným nakládáním s údaji jsou myšleny osobní údaje, důvěrné informace společnosti, data související se subdodavatelskými společnostmi v obchodním řetězci, ale také důsledky nekvalitního zabezpečení sítě, které může generovat napadení, potažmo zavirování dat třetí osoby, odepření přístupu k datům, neoprávněné získání přístupového kódu, zničení, poškození nebo smazání dat, odcizení hardwaru, ale také zpřístupnění dat samotným zaměstnancem. Každá společnost má co dočinění s dozorovými orgány, které dohlížejí na dodržování pravidel v rámci jejich fungování. V případě neoprávněného nakládání s údaji může dozorový orgán uložit sankce, na které je stejně jako na případné náklady na právní poradenství pamatováno v rámci základního krytí. Pokud dojde k reálnému naplnění některé z výše uvedených hrozeb, postižené společnosti vznikají další náklady na nápravu dobrého jména, ať už společnosti nebo jednotlivce, náklady na oznámení v médiích, IT experty a v neposlední řadě na obnovu dat.

V rámci dalších možností a nastavení, které pojištění nabízí, je dobré zmínit zejména zveřejnění digitálního obsahu, vydírání prostřednictvím sítě nebo výpadky sítě. Zveřejněním digitálního obsahu jsou myšleny například pomluvy a s tím související negativní vliv na dobré jméno, zásahy do práva na soukromí, porušení autorského práva nebo nekalosoutěžní jednání. Mezi další krytí patří i možnost dokoupení takzvaného Výpadku sítě. Produkt zde nabízí možnost krytí finanční ztráty samotné pojištěné společnosti, která může vzniknout přerušením či pozastavením funkce počítačových systémů společnosti.

S rostoucí mírou závislosti mnoha institucí a firem na výpočetní technice společně se stále širším využitím internetu vypadá útok na počítačové sítě z pohledu zvenčí čím dál lákavěji. Tento fakt se v nejbližší budoucnosti bude pravděpodobně jen prohlubovat. Z globálního hlediska půjde o to, aby se z kybernetických sabotáží a kriminality nevyklubal problém kybernetické války. (AIG, 2013)

8. Vyjádření tiskových mluvčí jednotlivých pojišťoven

Oslovil jsem tiskové mluvčí pojišťoven Allianz, Česká pojišťovna, Generali a Kooperativa a položil jim následující otázky:

1/ Poskytuje vaše pojišťovna v Česku firmám pojištění kybernetických rizik (krádež elektronických dat atd.)? Jaký je o produkt mezi tuzemskými firmami zájem? Máte případně nějaká aktuální čísla?

2/ Kryjí dopady kybernetických útoků na firmy v současnosti nějaké alternativní pojišťovací produkty?

3/ Jaké druhy firem mají o pojištění kybernetických rizik zájem?

4/ Kolik tuzemských firem už využilo plnění pojistného?

5/ Jaké problémy může zavádění pojištění kybernetických rizik provázet? Je tato oblast rizika pro potřeby pojištění dostatečně přesně definovaná? Nemůže být problém vyčíslovat v případě kybernetického útoku škody?

8.1. Pojišťovna Allianz, tiskový mluvčí Václav Bálek*:*

1/ Ano, díky podpoře naší skupiny jsme schopni toto specializované pojištění nabídnout, nicméně zatím cítíme velmi nízkou poptávku.

2/ S výjimkou obecných řešení typu alternative risk transfer či individuálních ujednání si nejsem existence produktů dedikovaných pro tento případ vědom.

3/ Nejčastěji IT a telekomunikační firmy.

4/ Vzhledem k tomu, že jde o velmi specifický produkt a klienti těchto individuálních smluv se počítají v jednotkách, k plnění dosud nedošlo. Navíc zájemci o toto pojištění se rekrutují spíše z velkých nadnárodních firem než z tuzemských.

5/ Jde o specializované pojištění, proto je důležitá otevřená oboustranná komunikace, aby bylo řešení adekvátní potřebám klienta. Stejně jako u jiných socializovaných produktů, které jsou na českém trhu využívány výrazně častěji, je obvyklé využívání externích odborných firem, které klientovi v případě škody pomáhají řešit vzniklou situaci a zároveň dávají podklady pro vyčíslení škody pojišťovnou.

Možná na doplnění – každoročně skupina Allianz zveřejňuje žebříček podnikatelských rizik, kterých se firmy napříč celým světem nejvíce obávají. Počítačová rizika jsou stále na druhém konci tabulky, i když postupně se zejména ve vyspělé Evropě posunují směrem vzhůru. Z rizikové studie Allianz z loňského roku vyplývá, že společnosti jsou obecně špatně připraveny na IT poruchy a třeba i výpadky elektrického proudu. Přitom právě IT selhání, ať už vlastním zaviněním, tedy lidskou chybou nebo počítačovou kriminalitou, může znamenat v současném velmi digitalizovaném hospodářství vysoké ekonomické ztráty. Odborníci na pojištění v této souvislosti upozorňují na to, že podnikatelé berou některé rizika opravdu velmi zodpovědně, ale naopak některá zcela podceňují. Pouze 6 % dotázaných risk manažerů Allianz napříč celým světem si myslí, že jejich klienti jsou si výpadků proudu a počítačového selhání dostatečně vědomi.

8.2. Česká pojišťovna, a.s., tisková mluvčí Ivana Buriánková:

Produkt pojištění kybernetických rizik v současné době Česká pojišťovna nenabízí. Na Vaše otázky Vám tedy nemohu poskytnout odpověď. Děkuji za pochopení a přeji hezký den

8.3. Pojišťovna Kooperativa, a.s., VIG, tiskový mluvčí Milan Káňa:

Dobrý den, toto riziko nepojišťujeme. Důvody jsou zřejmé. Jde o poměrně nové riziko, jehož dopady se prozatím poměrně těžko dají předvídat. Nastavení podmínek pojištění v době bouřlivého technologického rozvoje je prakticky nemožné. A také se obávám, že hackeři jsou stále trochu napřed. Zároveň by se i složitě definovala vzniklá škoda - ušlý zisk při přerušení provozu, odčerpané finance nebo ztráta dat.

8.4. Pohled na německý trh

Kybernetické útoky, krádeže identity, internetová sabotáž, ztráta dat - německé malé a střední podniky podceňují rizika počítačové kriminality. Pouze šest procent manažerů bere v úvahu počítačovou trestnou činnost jako možné riziko pro jejich podnikání. Podobně nízké riziko počítačové kriminality se odhaduje na celém světě, v průměru jen čtyři procenta manažerů se obávají počítačové kriminality. To jsou výsledky nedávného průzkumu, který provedla pojišťovna Zurich v rámci výkonných studie u pracovníků a ředitelů středních podniků.

"Náš průzkum jasně ukazuje, že střední třída výrazně podcenila rizika digitálního světa práce, ve kterém se dnes téměř výhradně nacházíme. Počítačová kriminalita nehraje i přes trvalý růst dosud téměř žádnou roli pro živnostníky, zatímco čísla hovoří sama za sebe," zdůrazňuje Ralph Brand, generální ředitel pojišťovny Zurich v Německu. "Firmy žijí v přesvědčení, že stačí pojistit tovární budovy proti požáru a jiným nebezpečím. Nicméně já si myslím, že pojistit jen hmotný majetek už dnes nestačí", vysvětluje Johannes Behrends, který je zodpovědný za pojištění kybernetických rizik v makléřské společnosti Aon. Dokonce i Thomas Blunck, člen představenstva zajišťovny Munich Re, vyzývá k "přiměřenému pojištění proti narušení dat jako standardní součástí komerčního pojištění. Každá firma může v této souvislosti utrpět ztrátu příjmů nebo důvěryhodnosti", řekl Blunck. V současnosti nabízí v Německu pojištění proti kybernetickému riziku zajistitel Munich Re a makléř Aon, z pojišťoven pak nabízí vlastní produkty Allianz a Zurich.

Současná ochrana dat bude posílena novými právními předpisy, novelou Spolkového zákona o ochraně dat z roku 2009, nebo v rámci celé EU plánovaným povinným hlášením hackerského útoku. To klade nové nároky na organizace, které mají v souladu s ochranou dat stále více a více povinností, aby se bránily riziku pokuty nebo vzniku odpovědnosti.

Pojistný trh se musí proměnit. Musí být vnímavý nejen k problémům spotřebitele v oblasti zabezpečení dat, ale také nabízet produkty, které splňují požadavky na rizika. V nadcházejících letech se bude počet připojení k internetu stále výrazně zvyšovat, stále

více a více lidí bude využívat zařízení připojených k internetu. Pojišťovnictví již musí reagovat na tyto problémy. Zatímco předpis pojistného v oblasti kybernetických rizik v USA činí již více než jednu miliardu US $, v Německu se v této oblasti pohybuje jen několik málo pojišťoven. (www.versicherungsbote.de)

9. Závěr

Pro pojišťovny působící v České republice je segment trhu požadující pojištění kybernetického rizika velice malý a v nejbližší budoucnosti nelze předpokládat změnu v přístupu pojišťoven. Otevírá se zde proto prostor komunikovat s organizačními složkami velkých zahraničních pojišťoven, na druhou stranu zde může hrozit cenový či produktový kartel.

Je třeba si také uvědomit, že pojišťovna je komerční soukromý subjekt, jako taková je povinována svým akcionářům tvorbou zisku a nelze ji nutit do ekonomicky nevýhodné činnosti. Pojištění nejen kybernetických rizik lze nabízet při velkém počtu zájemců a jisté pravděpodobnosti rizika, Česká republika je však relativně malé území a české pojišťovny působí pouze na území ČR.

Proto je naprosto odlišná situace u pojišťoven v USA, které působí na obrovském území USA, Kanady či Mexika, a mají zastoupení i v členských zemích Evropské unie. O pojištění kybernetických rizik je v Severní Americe díky atraktivnímu cíli pro kyberteroristy značný zájem. Při porovnání technické vyspělosti států a firem lze kvalifikovaně odhadnout, že do pojištění vstupuje vedle několika málo extrémně ohrožených firem i velké množství firem, kde je reálný útok bagatelní. Tím se vytváří významný finanční obrat na vstupu a je malá frekvence výplat pojistného plnění ve velkých částkách.

Nicméně každého jednou potká problém s kybernetickou bezpečností, je jen otázkou kdy. Vzhledem k současným internetovým hrozbám vzniká nová poptávka na trhu, je vyžadována inovace pojištění. V této nové obchodní oblasti je zapotřebí rozvíjet produktovou škálu pojišťoven, zprostředkovat informace mezi orgány státní moci a pojišťovnami. Propagovat přednášky a diskuse se zaměřením zejména na produkty pojišťoven a zajišťoven, komunikovat vedle pojišťoven současně i s dalšími poskytovateli finančních služeb - pojišťovacími makléři, právníky a konzultanty managementu.

Literatura

AIG. (2013). Produktová brožura - CyberEdge od AIG. Praha.

Antič, M., & Hanzal, M. (2013 йил 24-července). *O pojištění - Informace ze světa pojištění*. (Česká asociace pojišťoven) Retrieved 2014 from Pojistný obzor: http://www.opojisteni.cz/rizika/kyberutoky-nejsou-sci-fi-hackeri-ovladli-i-cesko/

Deutsche Telecom AG. (n.d.). *Sicherheits Tacho*. (Deutsche Telecom AG) Retrieved 20014 йил 16-března from http://www.sicherheitstacho.eu/?lang=cz

Finanční noviny. (n.d.). (Finační noviny) Retrieved 2014 йил 03.-března from http://www.financninoviny.cz/zpravy/pro-firmy-jsou-nejvetsimi-riziky-preruseni-provozu-a-katastrofy/1044770

SymanTec. (n.d.). *Business IT*. Retrieved 2014 йил 16.-března from Business IT: http://www.businessit.cz/cz/utocnici-stale-casteji-ohrozuji-mensi-firmy.php

www.versicherungsbote.de. (n.d.). *http://www.versicherungsbote.de/*. Retrieved 2014 йил 16.-březen from http://www.versicherungsbote.de/

ANALÝZA RIZIK FYZICKÉ BEZPEČNOSTI V ENERGETICKÉ OBLASTI

1. Úvod

Cílem tohoto dokumentu je iniciovat vývoj metodiky analýzy rizik fyzické bezpečnosti, který by vyústil do standardů fyzické bezpečnosti pro lokality energetického systému.

1.1. Zkratky a pojmy

SG - Smart Grid

SGAM - Smart Grids Architecture Model (Model architektury Smart Grid)

PLSM - Proposal for a list of security measures for smart grids

Analýza rizik - analýza rizik zabývající se všemi aspekty bezpečnosti

Analýza rizik fyzické bezpečnosti - analýza rizik zabývající se pouze problematikou fyzické bezpečnosti

Hranice analýzy - hranice oddělující působnost analýzy rizik a analýzy fyzické bezpečnosti. Za podmínky, že jsou uplatněna všechna opatření doporučená analýzou fyzické bezpečnosti, platí předpoklad, že je vysoce pravděpodobné až jisté, že za tuto hranici nezíská přístup neoprávněná osoba.

BIA analýza - Business Impact Analysis (analýza dopadů)

1.2. Odkazy

Smart Grid Reference Architecture - CEN-CENELEC-ETSI Smart Grid Coordination Group - listopad 2012 - (Dále také jen "SGRA")

Proposal for a list of security measures for smart grids - SMART GRID TASK FORCE 4 EG2 DELIVERABLE - prosinec 2013 -(Dále také jen "PLSM")

2. Potřeba analýz fyzické bezpečnosti

SMART GRID TASK FORCE EG2 vydala koncem roku 2013 publikaci "Proposal for a list of security measures for smart grids" (dále také jen PLSM), jenž lze použít jako východisko pro analýzu rizik.

PLSM je prvním krokem směřujícím ke standardizaci v oblasti energetické bezpečnosti, protože popisuje základní elementy pro provedení analýzy rizik a přináší návrh sady bezpečnostních opatření ke zvládání rizik.

To, co doposud řešeno není, je metodika provádění analýzy rizik, která by navazovala na dokument PLSM.

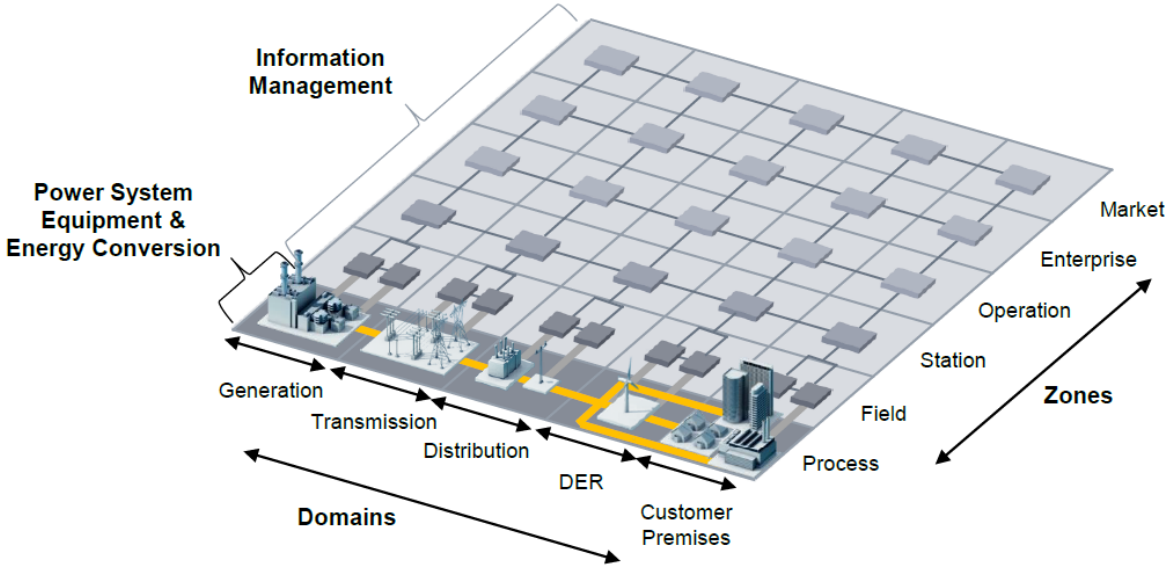
2.1. SGAM model

SGAM model presentuje realitu v třírozměrném zobrazení. Základnu tvoří relace Domén a Zón.

Domény popisují řetězec konverze elektrické energie (infrastrukturu výroby a spotřeby),

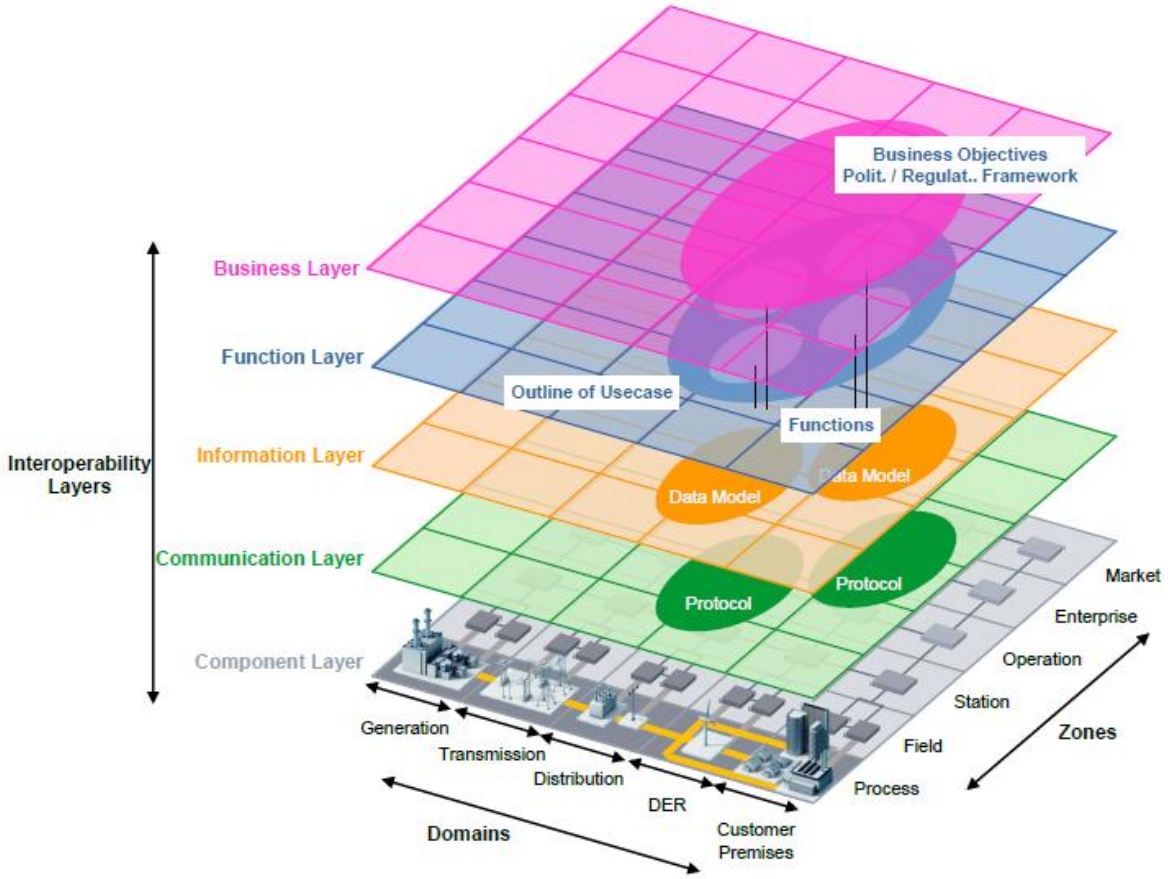
Zóny popisují hierarchické úrovně řízení energetického systému.

Základna modelu je znázorněna na následujícím obrázku, který byl převzat z dokumentu SGRA. Pro potřeby analýzy fyzické bezpečnosti jsou významné zejména zóny Process, Field a Station.



Třetí rozměr modelu tvoří vrstvy interoperability, na kterých se odehrává vzájemná spolupráce řídících energetických systémů, který byl převzat z dokumentu SGRA.

Vrstvy interoperability jsou uvedeny pouze z důvodu úplnosti informací o modelu SGAM. Pro potřeby analýzy fyzické bezpečnosti nemají vrstvy interoperability zásadní význam.



Bližší informace o SGAM modelu jsou uvedeny v publikaci SGRA (Smart Grid Reference Architecture - CEN-CENELEC-ETSI Smart Grid Coordination Group - listopad 2012).

2.2. Proposal for a list of security measures for smart grids (PLSM)

Materiál PLSM ve své části identifikuje typická aktiva Smart Grid, následně identifikuje typické hrozby pro Smart Grids, a závěrem definuje 45 opatření rozdělených do 11 domén.

2.2.1. Aktiva

Aktiva jsou presentována jako typičtí zástupci aktiv vyskytujících se v SG a jsou uspořádána formou, která je výhodná pro identifikaci aktiv v procesu analýzy rizik.

Dokument se ale nezabývá vlastní metodikou analýzy rizika, proto neposkytuje vodítko, jak přistupovat k aktivům, zejména v oblasti stanovování hodnoty aktiva.

2.2.2. Hrozby

Také u seznamu typických hrozeb lze konstatovat, že hrozby jsou pokryty komplexně. Z hlediska fyzické bezpečnosti jsou relevantní dvě skupiny hrozeb. Jedná se o skupinu úmyslný fyzický útok a o skupinu přírodní katastrofy.

2.2.3. Opatření

Opatření jsou v dokumentu rozdělena do 11 domén, v rámci těchto domén je definováno 45 opatření.

Z hlediska fyzické bezpečnosti je důležitá doména č. 8 Fyzická bezpečnost, která ovšem obsahuje pouze 3 opatření.

Tato doména obsahuje následující opatření:

- **31.** Vytvořit a udržovat odpovídající fyzickou bezpečnost zařízení / komponentů / systémů Smart Grid podle kritičnosti, který má být definován vlastníkem majetku.
- **32.** Vytvořit a udržovat funkce pro přihlášení a sledování fyzického přístupu k zařízení / komponentům Smart Grid s přihlédnutím ke kritičnosti zařízení.
- **33.** Zavést zvláštní dodatečné fyzická ochranná opatření na ochranu zařízení umístěné mimo vlastní pozemky, nebo důvody nebo prostory.

Pro srovnání je v následující tabulce uveden seznam opatření fyzické bezpečnosti, které jsou definovány v příloze "A" standardu ISO 27001.

Kód opatření	Popis opatření
A. 9	Fyzická bezpečnost a bezpečnost prostředí
A. 9.1	Zabezpečené oblastí
A. 9.1.1	Fyzický bezpečnostní perimetr
A. 9.1.2	Fyzické kontroly vstupu osob
A. 9.1.3	Zabezpečení kanceláří, místností a zařízení
A. 9.1.4	Ochrana před hrozbami vnějšího prostředí
A. 9.1.5	Práce v zabezpečených oblastech
A. 9.1.6	Veřejný přístup, prostory pro nakládku a vykládku
A. 9.2	Bezpečnost zařízení
A. 9.2.1	Umístění zařízení a jeho ochrana
A. 9.2.2	Podpůrná zařízení
A. 9.2.3	Bezpečnost kabelových rozvodů
A. 9.2.4	Údržba zařízení
A. 9.2.5	Bezpečnost zařízení mimo prostory organizace
A. 9.2.6	Bezpečná likvidace nebo opakované použití zařízení
A. 9.2.7	Přemístění majetku

Porovnáme-li tato opatření s opatřeními fyzické bezpečnosti, které jsou definovány v příloze "A“ standardu ISO 27001, docházíme k závěru, že míra detailu materiálu je stanovena na úrovni požadavku, ale nikoli na úrovni skutečného opatření, kterým by se mělo fyzické bezpečnosti dosahovat.

2.3. Analýza fyzické bezpečnosti

V rámci řešení analýzy rizik je vhodné oddělit analýzu rizik fyzické bezpečnosti od analýzy rizik ostatních aktiv. Analýzy fyzické bezpečnosti by vůči ostatním aktivům měla vytvořit bezpečnostní předpoklady na úrovni místnosti, kde bude garantovat požadovanou míru bezpečnosti.

2.3.1. Rozdíly v analýzách

Pomineme-li případy raketového útoku, je uplatnění každé úmyslné fyzické hrozby podmíněno získáním přístupu útočníka ke chráněnému aktivu.

Oddělení analýzy fyzické bezpečnosti vyplývá ze specifiky této analýzy, kdy rozhodující protiopatření je včasná detekce a následné provedení zásahu, který bude eliminovat působení útočníka.

Hlavní rozdíl spočívá v tom, že analýzy fyzické bezpečnost musí zahrnout také časové intervaly mezi časem detekce útoku a časem provedení zásahu.

2.3.2. Strategie ochrany

Dalším faktorem je zahrnutí strategie ochrany, která ovlivňuje analyzované časové intervaly. Odlišujeme dvě strategie:

ochrana před sabotáží - spočívá v provedení zásahu dříve, než útočník dosáhne chráněného aktiva.

Ochrana před krádeží - vychází z toho, že se nepředpokládá, že útočník chce aktivum zničit, al chce jej pouze odcizit. V tomto případě se doba na provedení zásahu prodlužuje, protože postačuje provést zásah až v době, když útočník opouští s aktivem chráněný prostor.

2.3.3. Bezpečnostní opatření

Zatímco dokument PLSM v opatření **31.** - Vytvořit a udržovat odpovídající fyzickou bezpečnost zařízení / komponentů / systémů Smart Grid podle kritičnosti, který má být definován vlastníkem majetku.

Analýza fyzické bezpečnosti musí řešit opatření na mnohem detailnější úrovni. Opatření doporučená analýzou fyzické bezpečnosti musí být mnohem konkrétnější. Musí stanovit místo, kde detekovat narušení bezpečnosti a zejména stanovit prvky pasivní ochrany (kvalita zdí, kvalita vstupních a průlezových otvorů a jejich zabezpečení), které ovlivňují dobu, než útočník získá přístup k chráněnému aktivu.

3. Metodika analýzy fyzické bezpečnosti

3.1. Hranice analýzy

Analýza fyzické bezpečnosti musí být nedílnou součástí analýzy rizik, a proto musí být jasně stanovený interface (hranice) mezi oběma analýzami.

Hranice analýzy je hranice oddělující působnost analýzy rizik a analýzy fyzické bezpečnosti. Za podmínky, že jsou uplatněna všechna opatření doporučená analýzou fyzické bezpečnosti, platí předpoklad, že je vysoce pravděpodobné až jisté, že za tuto hranici nezíská přístup neoprávněná osoba.

Přesné stanovení hranice by mělo být součástí vývoje metodiky analýzy fyzické bezpečnosti. Jako prozatímní příklad můžeme vzít, že hranice spočívá ve vstupu do místnosti s chráněným aktivem (např. vstup do serverovny).

Tato hranice bude znamenat, že při analýze rizik se bude předpokládat, že byla uplatněna všechna rozumná opatření z oblasti fyzické bezpečnosti, aby do serverovny neměla neoprávněně přístup jakákoli osoba.

Znamená to, že analýza rizik se již nezabývá opatřeními týkajícími se např. bezpečnostního perimetru, nebo přístupu osob do zabezpečené oblasti a předpokládá, že do zabezpečené oblasti mají přístup pouze oprávněné osoby. Z oblasti fyzické bezpečnosti se analýza rizik omezuje jen na omezení přístupu oprávněných osob k určitým zařízením (například uzamykáním racků).

3.2. Hrozby

Celý dokument PLSM je zaměřen zejména na kybernetickou bezpečnost a z této perspektivy přistupuje i k definici hrozeb. Pro analýzu fyzické bezpečnosti bude potřeba skupinu úmyslný fyzický útok doplnit o specifické hrozby týkající se fyzické bezpečnosti, založené na scénářích útoků.

Dalším problémem, který bude muset být řešen, je odhad předpokládané intenzity hrozby. V podmínkách fyzické bezpečnosti (z hlediska odhadu míry zdržení útočníka pasivními prostředky fyzické ochrany) to bude představovat prostředky, které bude mít útočník k dispozici.

3.3. Aktiva

Aktiva jsou presentována jako typičtí zástupci aktiv vyskytujících se v architektuře SGAM nad zónou Process. Vyplývá to ze zaměření PLSM na problematiku

kybernetické bezpečnosti. Vzhledem k faktu, že analýza fyzické bezpečnosti se bude týkat také zóny Process podle SGAM modelu, bude potřeba doplnit typová aktiva zejména z této zóny.

3.3.1. Hodnocení důležitosti aktiv

Vzhledem k tomu, že hodnota aktiva se odvozuje jednak od hodnoty procesu, který je aktivem podporován a také od míry závislosti procesu na daném aktivu, bude nutné provést ohodnocení typových aktiv v zóně "Process".

Metoda stanovení hodnoty aktiva by měla být součástí vývoje metodiky analýzy fyzické bezpečnosti. Pravděpodobně se bude jednat o určitý druh BIA analýzy.

Hodnota aktiva, společně s intenzitou hrozby a zranitelností jsou základními hodnotami, od kterých se odvozuje míra rizika.

3.4. Opatření

Metodika by měla doplnit sadu opatření o specifická opatření z oblasti fyzické bezpečnosti. Opatření by měly pokrývat nejen procesy k zajištění fyzické bezpečnosti, ale také charakteristiky pasivních opatření jako jsou bezpečností charakteristiky budovy (síla a materiál stěn, zajištění vstupních otvorů), která budou prodlužovat interval mezi dobou detekce útočníka a dobou, kdy získá přístup do prostoru s chráněným aktivem. Pasivní opatření by měla být hodnocena podle doby zadržení útočníka (doby, kterou musí útočník vynaložit, než dané opatření překoná). Řazením pasivních opatření do série se prodlužuje doba mezi detekcí útočníka a časem, kdy útočník získá přístup ke chráněnému aktivu.

Dále by mělo být řešeno nasazení detekčních prostředků (EZS, EPS) a identifikačních systémů pro řízení přístupu do prostor (EKV).

4. Výstupy analýzy fyzické bezpečnosti

V podmínkách České republiky vystupují na poli energetických společností velcí hráči s velkými možnostmi investic do bezpečnosti vedle malých výrobců energie, jejichž prostředky jsou výrazně omezené. Zároveň při propojování systémů platí pravidlo, že systém složený z dílčích systémů je natolik bezpečný, jako nejslabší dílčí systém (pravidlo nejslabšího článku).

Z těchto důvodů lze považovat za účelné, aby investice do bezpečnostních analýz fyzické bezpečnosti byla provedena centrálně a analýza byla provedena na dostatečně reprezentativním vzorku, aby závěry této analýzy měly obecnou platnost. To umožní

zobecnit požadavky na bezpečnost do standardů fyzické bezpečnosti, které poskytnou předpis pro hodnocení důležitosti významných aktiv a k těmto aktivům přiřadí požadovanou úroveň bezpečnostních opatření.

4.1. Kategorie fyzické ochrany

Fyzická bezpečnost se týká především zón Process, Field a Station podle SGAM modelu. Podle výsledků analýzy fyzické bezpečnosti bude možné stanovit k typovým aktivům zóny Process požadavky na jejich zabezpečení. Tyto požadavky budou charakterizovány formou definování kategorií fyzické ochrany.

Potom každá energetická společnost (nezávisle na její velikosti) podle aktiv, které v dané lokalitě provozuje, bude moci podle kategorii fyzické ochrany těchto aktiv.

5. Standardy fyzické ochrany

Standardy fyzické ochrany uvedou do relace dobu provedení zásahu, kategorii aktiva a prostředky fyzické ochrany, kterými má být aktivum chráněno.

Tento přístup sjednotí úroveň fyzické bezpečnosti u všech společností působících v energetickém sektoru.

6. Příprava protokolu pro monitoring systémů technické ochrany (STO)

6.1. Definice skupin technických prostředků

PZTS – Poplachový zabezpečovací a tísňový systém (dříve EZS – Elektronický zabezpečovací systém) - soubor zařízení, kterými se signalizuje nebezpečná situace z hlediska neoprávněného vniknutí nepovolaných osob.

Schvalování komponentů PZTS, navrhování, instalace a revize systémů EZS se řídí skupinou harmonizovaných norem ČSN EN 50131-1 ed.2:2007 a ČSN CLC/TS 50131-7:2009. Úroveň zabezpečení se rozlišuje podle čtyř kategorií - rizika velmi vysoká, vysoká, průměrná a nízká. Z hlediska ochrany utajovaných skutečností řeší problematiku zákon č. 412/2005Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění účinném dnem 1.1.2012.

SKV – Systém kontroly vstupu (někdy také EKV – Elektronická kontrola vstupu nebo Access) – Někdy bývá součástí PZTS. Jedná se o systém, který řídí a eviduje průchody osob, zamezuje neoprávněnému vstupu (ve spolupráci s mechanickými zábrannými prostředky – turnikety) do objektu. Nezbytně nutný systém z hlediska

monitoringu pohybu osob po objektu. Někdy využíván i k zamezení tzv. vícenásobného vstupu (antipassback).

Výrobky elektrické kontroly vstupu (EKV) jsou řešeny harmonizovanými evropskými normami ČSN EN řady 50 133, popřípadě i Národním bezpečnostním úřadem dle Zákona č. 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti a vyhlášky NBÚ č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků.

Perimetrická ochrana – většinou součástí PZTS, někdy však instalována jako samostatný systém. Jedná se o detekci narušení perimetru objektu.

CCTV – Closed Circuit Television, uzavřený televizní okruh – slouží k verifikaci událostí z ostatních systémů technické ochrany. V současné době se rozšířila i detekce v obraze a tím se tento systém přiblížil i k PZTS. Z hlediska certifikace však je tento systém neakceptovatelný pro detekci a ta se tedy užívá především jako podpůrný prostředek.

Bezpečnostní kamera je základním prvkem celého systému, podle požadavků na kvalitu obrazu ze snímané scény volíme kamery s příslušným rozlišením, světelnou citlivostí, kompenzací protisvětla nebo rozšířeným dynamickým rozsahem. Vhodnou volbou kamery, tak lze potlačit vliv protisvětla, ovlivnit viditelnost i při velmi nízké hladině osvětlení, nebo potlačit šum v obraze.

Kamerami můžete sledovat barevný obraz ve vnitřních i venkovních prostorách, pro detailní sledování cíle můžete použít otočnou ”dome“ kameru. Kamery mohou být v miniaturním provedení či skryté, pro různá speciální prostředí (výbušná, pod vodu), při nedostatku světla s přepínáním do černobílého režimu, do úplné tmy kamery s infrapřísvitem nebo moderní termocitlivé kamery.

Volba příslušenství výrazně ovlivní využití kamer. Objektiv je okem kamery, jehož volbu ovlivňuje vzdálenost snímaného objektu, světelné podmínky a požadované rozlišení obrazu. U kamerového krytu závisí na typu prostředí, chlazení a stupeň krytí, funguje také jako ochrana proti poškozování kamery. IR reflektor slouží jako okem neviditelný zdroj světla pro noční vidění.

Přenosová trasa videosignálu může být řešena po metalických nebo optických kabelech nebo bezdrátově, přes mikrovlnná a laserová pojítka.

Pro zobrazení živého videa a záznamů používáme rychlé LCD monitory a velkoplošné LCD panely určené pro trvalý provoz a sledování obrazu.

Dnes se používá výhradně digitální záznam obrazu. Výhody jeho použití jsou libovolná kvalita a délka záznamu, rychlé a snadné vyhledávání v záznamu dle různých kritérií, detekce pohybu v obraze, možnost vzdáleného přístupu k obrazovým datům z počítačů místní sítě, přes internet, nebo přes mobilní GSM sítě. Systém také umí posílat automatický email či SMS v případě poplachových událostí.

CCTV, jejich aplikace a přenosové trasy jsou řešeny normami ČSN EN 50132-1 Systémové požadavky CCTV, ČSN EN 50132-5:2002 Požadavky na přenosové trasy CCTV, tato byla rozdělena na tři části a to EN 50132-5-1, EN 50132-5-2, EN 50132-5-3 a nakonec ČSN EN 50132-7:1999 pokyny pro aplikaci CCTV.

EPS – Elektrická požární signalizace – bývá někdy taktéž součástí PZTS – především u menších instalací. V určitých případech (objekty s velkým počtem osob, …) je předepsaná zákonem a někdy i doplněna NZS - Nouzovým zvukovým systémem. EPS slouží především k ochraně zdraví a majetku z hlediska požární bezpečnosti. Podsystémy bývá například detekce plynu, jisker a podobně. Pravidla pro montáž a provoz systému EPS jsou zakotvena ve vyhlášce č. 246/2001 Sb.

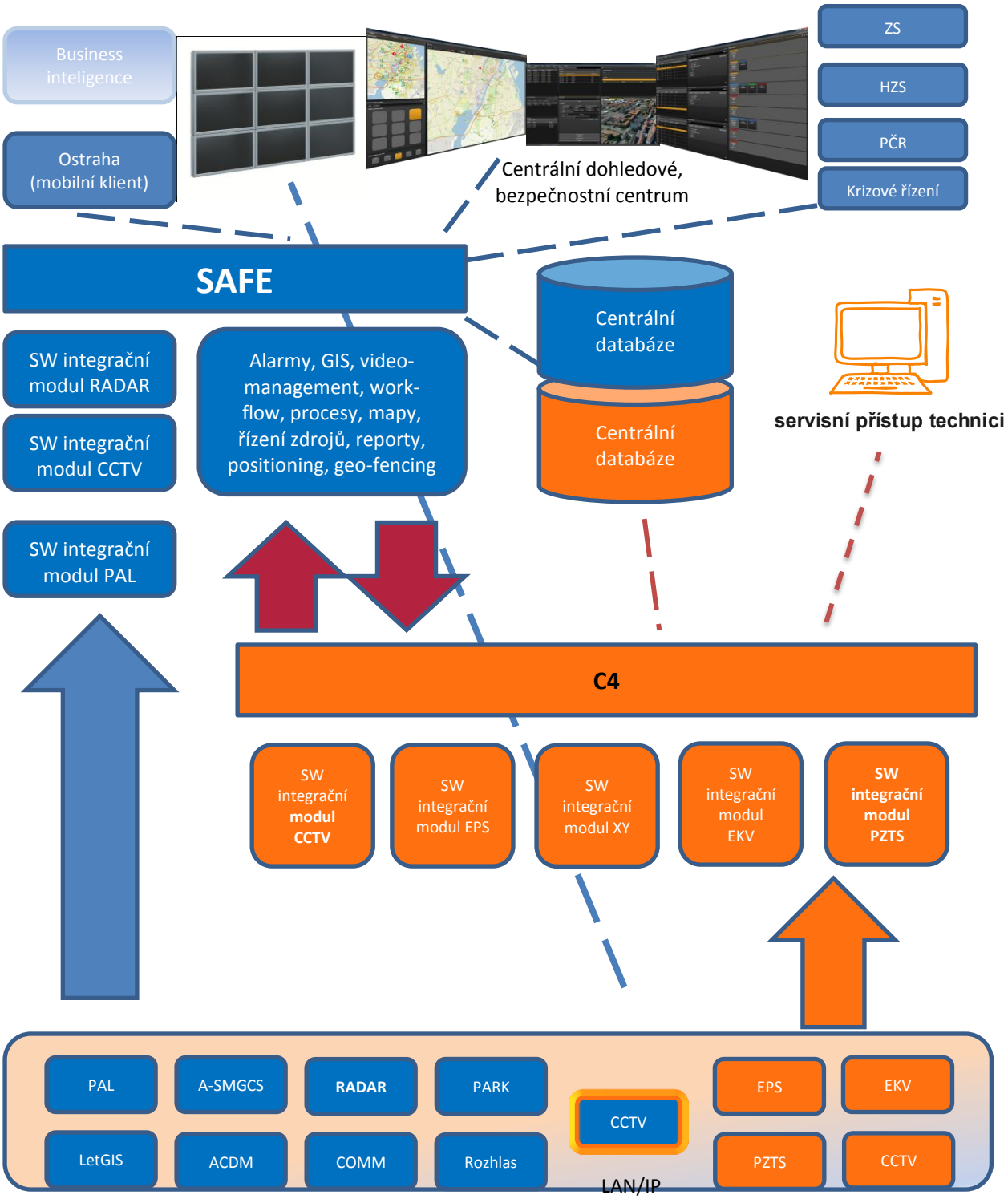
NZS - Nouzový zvukový systém (někdy také ER – Evakuační rozhlas) je systém pro zesílení nebo distribuci zvuku, který se používá pro rychlou a uspořádanou mobilizaci obyvatel při nouzových situacích. Pokud jde o systém používaný k řízení evakuace při požáru, používá se často název Požární rozhlas. NZS může plnit i další funkce jako je přenos hudby a informačních hlášení. Nouzový zvukový systém musí umožňovat vysílání srozumitelné informace o opatřeních, které je třeba uskutečnit k ochraně životů v jedné nebo více stanovených oblastech.

Instalaci a provoz NZS upravují následné normy: Vyhláška 246/2001 Sb. - z této vyhlášky vyplývá povinnost projektovat veškeré systémy sloužící pro technickou ochranu osob podle platných norem. Tím se tedy pro NZS všechny normy, které mají jinak pouze charakter doporučení, stávají závazné. ČSN EN 60849 Nouzové zvukové systémy - nejdůležitější dokument pro NZS, definuje požadavky na návrh systému, způsob zapojení, na technologická zařízení, montáž, zkoušení a provoz NZS, ČSN EN 60268-16 - norma předepisující metodiku měření srozumitelnosti, ČSN 73 0802 - norma specifikující požární bezpečnost staveb, zmiňuje "domácí rozhlas" a ČSN EN 60079 - elektrická zařízení do výbušných prostředí

Integrace systémů – výše zmíněné systémy se v poslední době stále častěji integrují do jednoho celku, v jehož rámci se mezi sebou propojují a nastavují se jednotlivé vazby (například mezi PZTS a CCTV, apod.) Integrace umožňuje jednotné ovládání všech technologií bez ohledu na typ technologie a její model. V případě použití grafiky zjednodušuje orientaci v rámci objektu, ale i správu mezi jednotlivými objekty. Často také usnadňuje správu osob používajících STO.

V současné době lze hledat inspiraci v normách ČSN CLC/TS 50398 - Všeobecné požadavky na kombinované a integrované systémy a ČSN EN ISO 11064 - Ergonomické navrhování řídících center - Uspořádání velínu. Je však bezpodmínečně nutné tuto problematiku vyřešit. Tento materiál však nemá takovéto ambice a směřuje do užšího okruhu monitoringu technických prostředků střežení a EPS v objektech kritické infrastruktury.

6.2. Příklad rozsáhlé dvouvrstvé integrace



6.3. Požadované informace z jednotlivých technologií

Z hlediska monitoringu systémů technické ochrany objektů kritické infrastruktury je nutné informace (stavy) jednotlivých technologií přenášet do lokálního pracoviště pro účely reakce místní obsluhy a určité vybrané stavy by se přenášely na

nadřízené pracovitě (HZS apod.). Z hlediska této studie je nutné specifikovat stavy potřebné k přehledu o technologiích právě na tato pracoviště.

PZTS

- Funkčnost systému
- Informace o výpadku napájení
- Neodborná manipulace – sabotáž
- Eskalovaný poplach způsobený narušením objektu
- Poplach potvrzený, či spuštěný (tísňové tlačítko) obsluhou – cílená informace pro nadřízené pracoviště

SKV

- Funkčnost systému
- Informace o výpadku napájení
- Neodborná manipulace – sabotáž
- Eskalovaný poplach způsobený násilným vstupem
- Pokus o použití neplatné karty či jiného identifikačního média

Perimetrická ochrana

- Funkčnost systému
- Informace o výpadku napájení
- Neodborná manipulace – sabotáž
- Eskalovaný poplach způsobený narušením objektu

CCTV

- Funkčnost systému
- Informace o výpadku napájení
- Neodborná manipulace – sabotáž
- Eskalace ztráty videosignálu
- Možnost jednorázového sledování živého obrazu

EPS

- Funkčnost systému
- Informace o výpadku napájení
- Neodborná manipulace – sabotáž
- Eskalovaný poplach způsobený požárem
- Poplach potvrzený, či spuštěný (tísňové tlačítko) obsluhou – cílená informace pro nadřízené pracoviště
- Případné další informace z podřízených systémů

Společně pro všechny technologie by bylo dobré přenášet informaci o provedených kontrolách (testech) s tím, že tak kde jsou tyto povinné by docházelo v případě jejich neprovedení k přenosu této události na nadřízené pracoviště.

Pro jednodušší přenos informací jak na lokální, tak na nadřízené pracoviště se nabízí jak tzv. převodní můstek či sjednocující člen právě integrační nástroj, dle mého názoru je právě výstup z integrace to správné místo pro aplikování bezpečného protokolu.

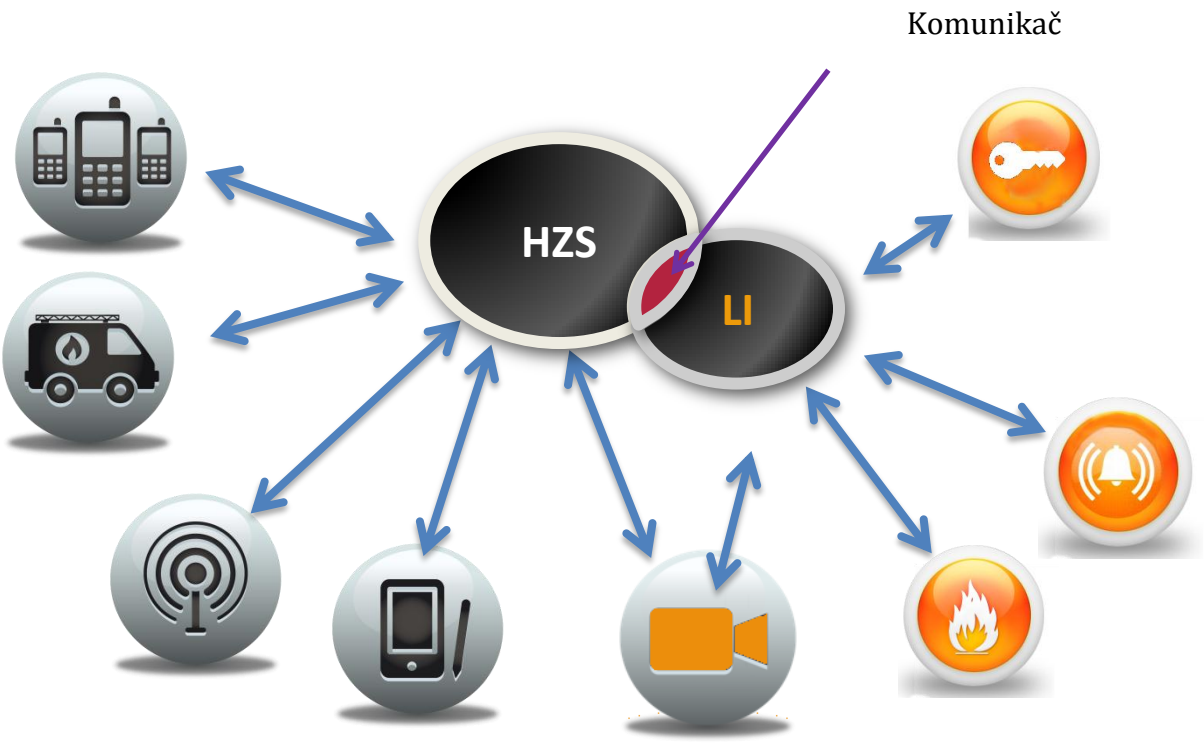
Komunikace mezi technologiemi a integrační platformou dne ve většině případů probíhá po TCP/IP ale jsou i případy, kdy je technologie připojena pomocí sběrnice.

Předpoklad komunikace s nadřízeným pracovištěm je za pomocí datových sítí (TCP/IP), popřípadě radiem. Zde dochází k průniku s ostatními kapitolami a navrhovaný protokol by měl respektovat veškeré doporučení z nich vyplývající.

Komunikace s nadřízeným pracoviště by stačila v jednosměrném provozu, to znamená pouze monitoring.

Dalším logickým krokem by měla být analýza konkrétních technologií a zmapování možností přenosu vytipovaných informací za pomocí komunikačního protokolu zařízení.

Příklad možného přenosu informací:



Legenda:
LI – Lokální Integrace
HZS – Hasičský Záchranný Sbor

Na výše uvedeném obrázku je znázorněna možnost monitoringu bezpečnostních systémů objektů kritické infrastruktury, kde průsečík (červené pole) značí zmiňované unifikované komunikační rozhraní.

Na centrální monitorovací pracoviště mohou být následně připojeny další složky, které se podílí na monitoringu, kontrolách či ochraně objektů kritické infrastruktury.

Veškerá komunikace by měla být zabezpečena proti zneužití dat, či průniku do systémů.

OCHRANA KRITICKÉ INFRASTRUKTURY V EU

1. Letecká dopravní cesta (LDC)

Letecká dopravní cesta je integrální součástí leteckého dopravního systému. Jako jiné systémy je i letecký dopravní systém tvořen jednotlivými základními prvky, které svou provázaností tvoří smysluplný a funkční celek. Na letecký dopravní systém můžeme nahlížet ze dvou pohledů, jedná se o **pojetí systémové a provozní**.

1.1. Systémové pojetí leteckého dopravního systému

V souladu se systémovým pojetím, v němž se odráží analýza chování složitých subjektů, vytvářejí letecký dopravní systém 2 funkčně propojené prvky

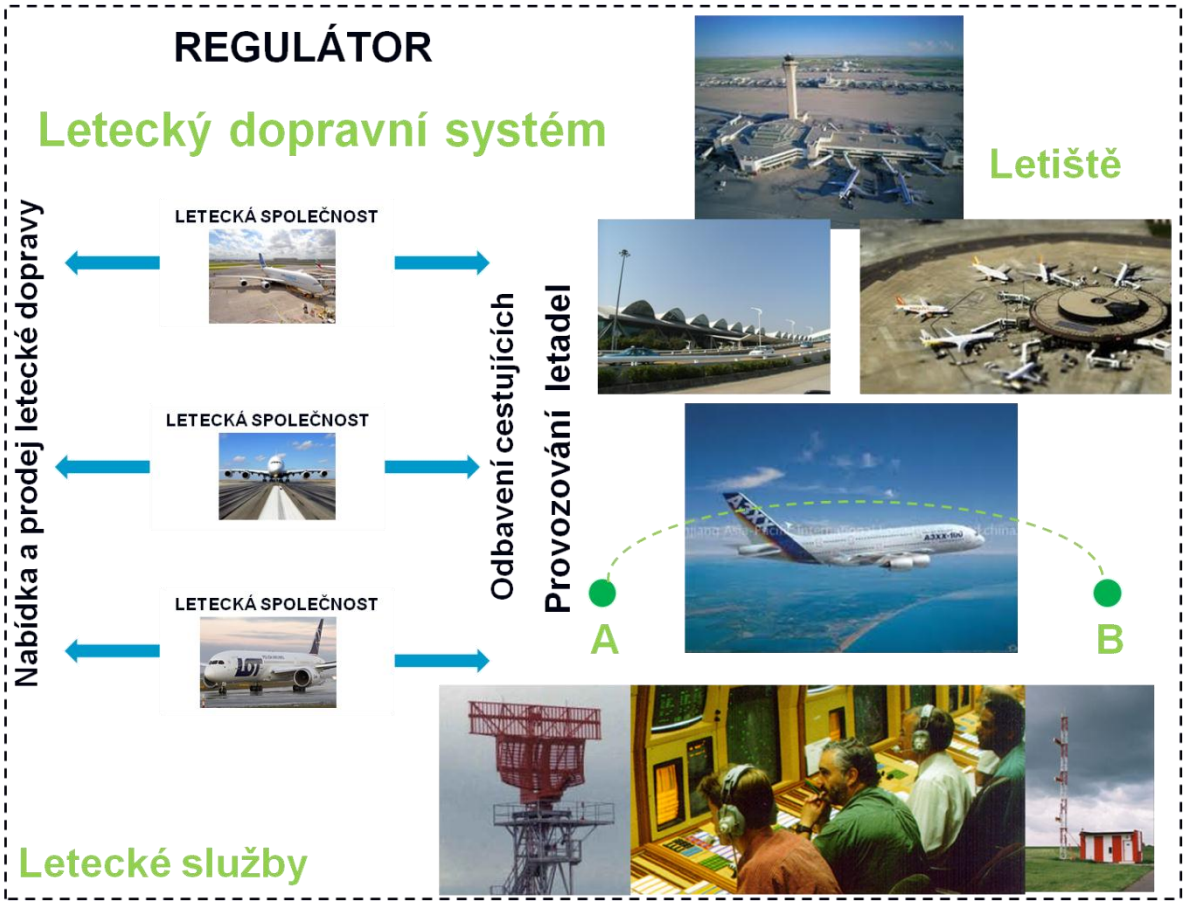
- dopravní prostředek – letadlo
- letecká dopravní cesta – letiště, vzdušný prostor, letové provozní služby

Letecká dopravní cesta musí zajišťovat podmínky pro umožnění plánovaného letu letadla, přičemž letadlo je považováno za složitý dynamický a v čase velmi proměnný systém v důsledku působení nejrůznějších vnějších vlivů a poruch. Problematika je o to složitější, že ve skutečném provozu to není jen jedno letadlo, ale souhrn všech v daném vzdušném prostoru provozovaných letadel, která využívají letištních služeb a prostředků určených pro vedení po trati.

1.2. Provozní pojetí leteckého dopravního systému

Zaměříme-li se na provozní hledisko, které poukazuje na provozní spolehlivost, ekonomickou efektivnost, dodržování ekologických norem a zejména požadavků maximální bezpečnosti, jsou v leteckém dopravním systému patrné 4 prvky:

- Letiště
- Letecké služby
- Letecký dopravce, provozovatel letecké dopravy
- Regulátor



Obrázek 1 Provozní pojetí leteckého dopravního systému

Letištěm se dle definice ICAO (Annex 14) rozumí *„Vymezená plocha na zemi nebo na vodě sloužící ke vzletům a přistáním letadel a pohybům těchto letadel na takto vymezené ploše“.* Definice Zákona č. 49/1997 Sb. o civilním letectví hovoří o letišti jako o *„Územně vymezené a vhodným způsobem upravené ploše včetně staveb a zařízení trvale určené ke vzletům a přistávání letadel a pohybům letadel s tím souvisejícím“.*

Letiště plní v systému letecké dopravy tři základní úlohy:

a) Počáteční a koncový bod přepravního procesu - *umožňuje tedy provozovatelům zajistit nástup a výstup cestujících, naložení a vyložení zavazadel, zboží a pošty*

b) Letiště je místem transferu mezi pozemní a leteckou dopravou - *umožňuje tedy přestup z letecké na městskou, železniční, silniční či vodní dopravu a opačně*

c) Umožňuje mezipřistání linek a přestup cestujících nebo přeložení nákladu mezi leteckými linkami*, tj. transit i transfer*

Leteckými službami rozumíme soubor poskytovaných činností nebo služeb, jejichž úlohou je technická, personální i procedurální podpora sloužící k zajištění bezpečného a spořádaného leteckého provozu a s tím souvisejících operací. Dle § 45 Zákona č. 49/1997 Sb. o civilním letectví jsou leteckými službami:

a) „letové provozní služby včetně letištních,

b) letecká telekomunikační služba,

c) letecká meteorologická služba,

d) letecká služba pátrání a záchrany,

e) letecká informační služba,

f) služby při předletové přípravě a monitorování letu,

g) služby při odbavovacím procesu na letišti".

Letecký dopravce je dle ICAO definován jako podnik, který letadly poskytuje letecké dopravní služby za úplatu nebo nájemné. K tomu, aby letecký dopravce mohl provozovat leteckou dopravu, poskytovat s ní spojené služby a vykonávat mnohé specializované činnosti, musí získat od příslušných státních autorit provozní licenci, která ho opravňuje k výkonu licencí vymezených aktivit, a také Osvědčení leteckého provozovatele (Air Operator Certificate – AOC). Letecká společnost musí pro sféry svých činností povinně vytvořit náležitou organizační strukturu, jasně stanovit řídící pracovníky a určit jejich odpovědnosti za činnosti a hospodaření každé organizační složky podniku.

Spolupráce a úkony v tomto dynamickém systému nesmí být nahodilé a chaotické, proto je třeba, aby byly smysluplně usměrňovány, s cílem zajistit ekonomičnost a bezpečnost provozu, ochranu před protiprávními činy a ochranu životního prostředí. Takový žádoucí dohled má na starosti tzv. „**regulátor**", regulační systém. Působí na vyjmenované prvky tak, aby vzájemná kooperace byla harmonická, bezporuchová a odvíjela se v souznění s národními zákony, mezinárodními ujednáními a

co je nejdůležitější – zachovávala bezpečnost na všech úrovních. Činnost regulátora je vykonávána prostřednictvím státních orgánů.

1.3. Rozdělení vzdušného prostoru

Vzdušné prostory letových provozních služeb (Air Traffic Services Airspaces) jsou definovány jako označené vzdušné prostory stanovených rozměrů, uvnitř kterých mohou být prováděny určité druhy letů a pro které jsou vymezeny letové provozní služby a pravidla provozu. Vzdušný prostor státu je horizontálně vymezen hranicemi státu, vertikálně jde o sloupec vzduchu sahající pod okraj spodní hranice kosmického prostoru (Outer Space). V současnosti neexistuje všeobecně uznávaná právní, technická, nebo politická definice hranice oddělující vzdušný a kosmický prostor, nebo kosmického prostoru jako takového. Legální definice dle ustanovení § 2 odst. 6 zákona č. 49/1997 Sb., ve znění pozdějších předpisů: *„vzdušným prostorem České republiky je prostor nad územím České republiky do výšky, kterou lze využít pro letecký provoz".*

1.3.1. Horizontální rozdělení vzdušného prostoru

Součástí vzdušného prostoru jsou letové tratě i omezené oblasti, tj. části vzdušného prostoru, ve kterých je provoz letadel zakázán nebo omezen v souladu s podmínkami typu a konkrétní oblasti. Každá z omezených oblastí negativně působí na pružné využívání vzdušného prostoru.

a) zakázané prostory

- Prohibited Area (PA) - vzdušný prostor vymezených rozměrů nad pevninou nebo teritoriálními vodami státu, ve kterém jsou lety letadel zakázány

b) omezené prostory

- Restricted Area (RA) - vzdušný prostor vymezených rozměrů nad pevninou nebo teritoriálními vodami státu, ve kterém jsou lety letadel omezeny v souladu se stanovenými podmínkami

c) nebezpečné prostory

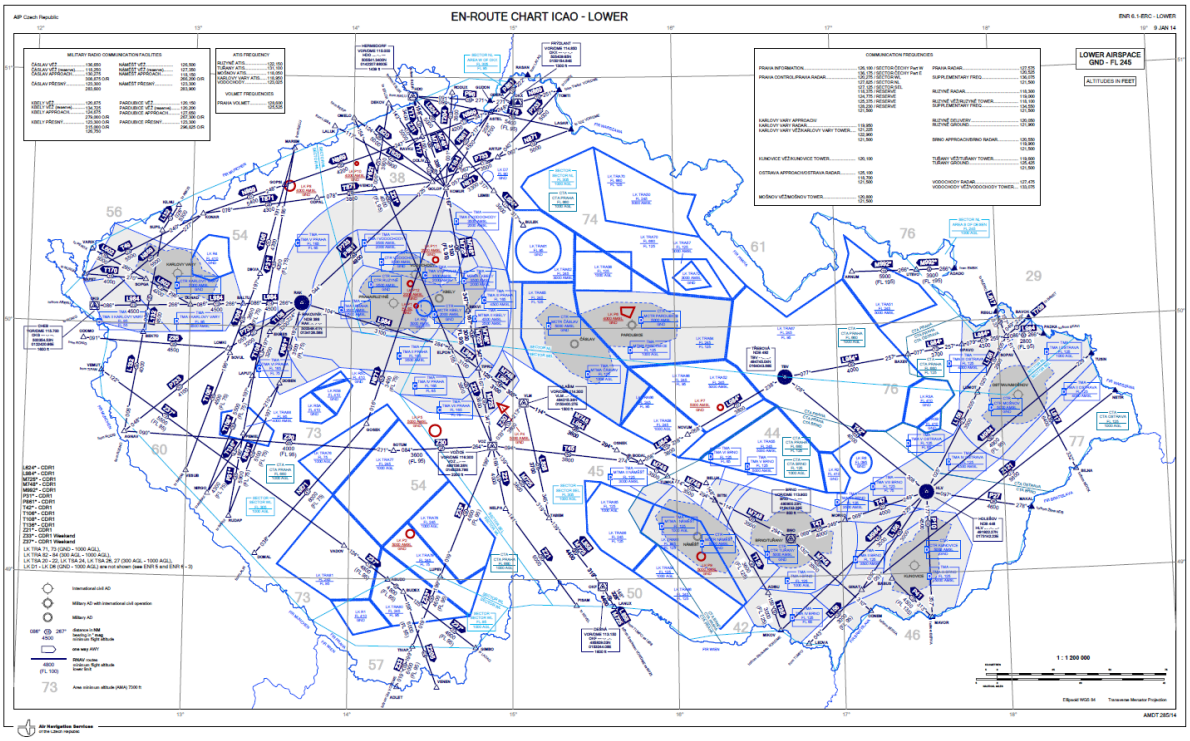
- Danger Area (DA) - vzdušný prostor vymezených rozměrů, ve kterém mohou v určité době probíhat činnosti nebezpečné pro let letadla

d) dočasně rezervované prostory

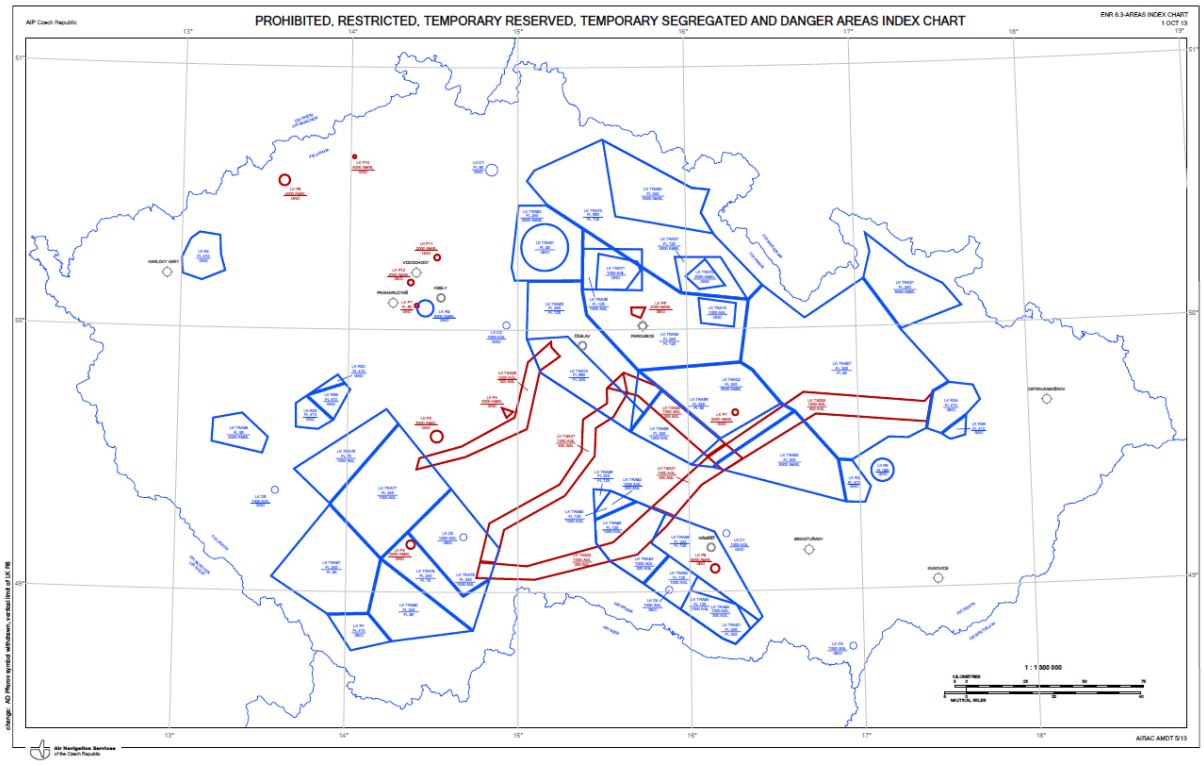
- Temporary Reserved Area (TRA) - definovaná část vzdušného prostoru za normálních okolností v pravomoci jedné složky letectví, která je na základě společné dohody dočasně rezervovaná pro specifické použití jinou složkou letectví a přes kterou může na základě ATC povolení proletět jiný provoz

e) dočasně vyhrazené prostory

- Temporary Segregated Area (TSA) - definovaná část vzdušného prostoru za normálních okolností v pravomoci jedné složky letectví, která je na základě společné dohody dočasně vyhrazená pro specifické použití jinou složkou letectví a přes kterou nebude povolen průlet jinému provozu



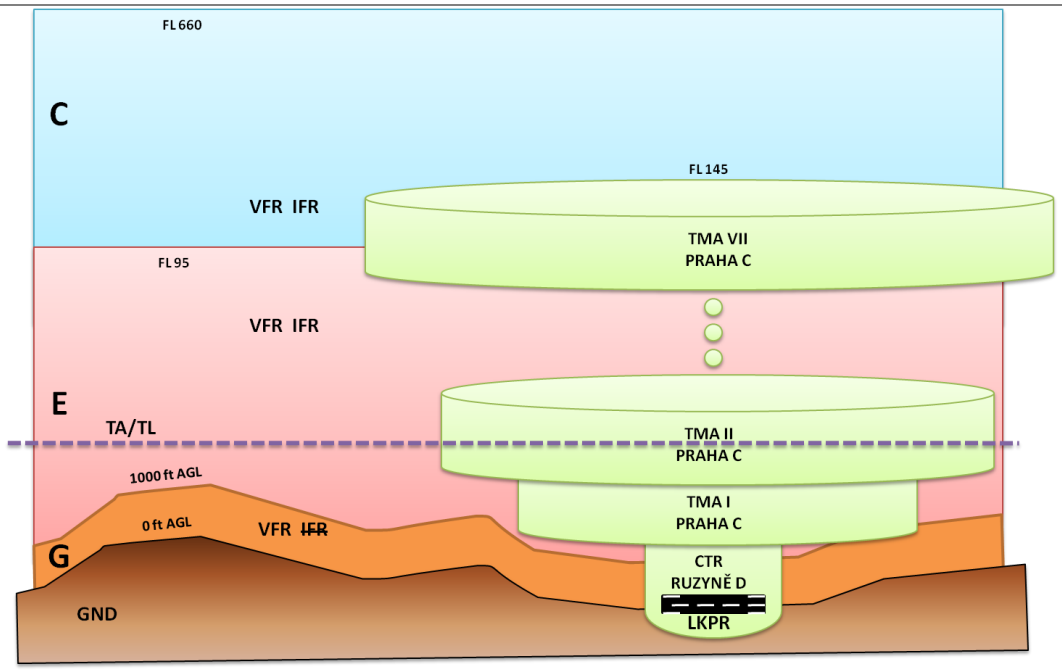
Obrázek 2 Horizontální rozdělení vzdušného prostoru ČR



Obrázek 3 Omezené oblasti vzdušného prostoru ČR

1.3.2. Vertikální rozdělení vzdušného prostoru

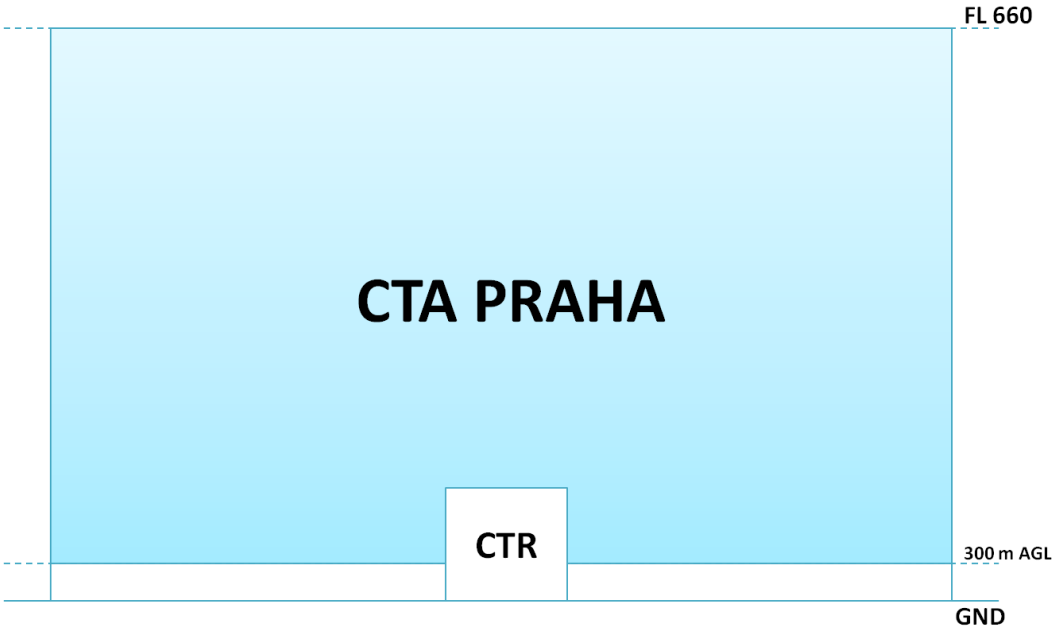
Vertikálně lze vzdušný prostor České republiky rozdělit do tříd označených abecedně písmeny C, D, E, G, lišící se povoleným druhem provozu, rozsahem poskytovaným letových provozních služeb, meteorologickými minimy, rychlostními omezeními, požadavky na radiové spojení a nutností podávat letový plán. Schematické znázornění je uvedeno na obrázku č. 4



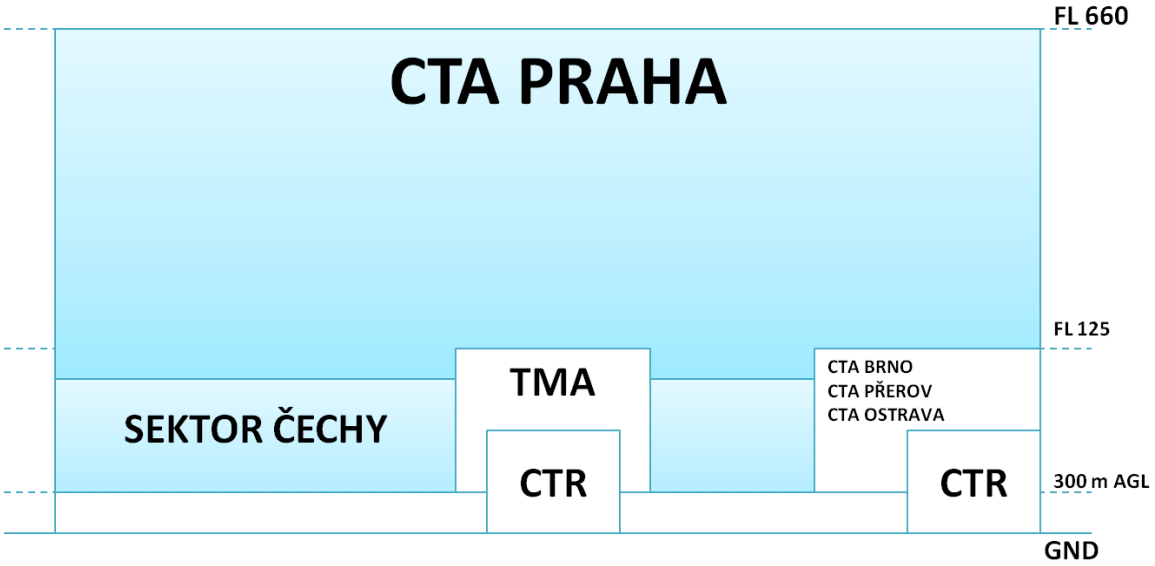
Obrázek 4 Vertikální rozdělení tříd vzdušného prostoru ČR

Základním elementem národního vzdušného prostoru České republiky je Letová informační oblast (FIR) – Flight Information Region. FIR PRAHA vertikálně sahá od země do letové hladiny FL 660.

Součástí Letové informační oblasti ČR je Řízená oblast (CTA) – Control Area, sahající od výšky 300 m AGL do letové hladiny 660.



Uvnitř FIR jsou v blízkosti větších letišť zřizovány Řízené okrsky (CTR) – Control Zone. Je to taková část vzdušného prostoru, kde je poskytována služba řízení letového provozu a její horizontální hranice se nacházejí vně řízených oblastí. Jejich součástí jsou dráhy letů IFR odlétávajících a přilétávajících z letišť, která se používají k letům dle IMC. V místech, kde se tratě letových provozních služeb sbíhají v blízkosti jednoho nebo více letišť, se zřizují Koncové řízené oblasti (TMA) - Terminal Manoeuvring Area.



1.4. Kritická místa infrastruktury LDC

1.4.1. Důvody vymezení kritických míst infrastruktury LDC z pohledu poskytovatele LNS

Kritická infrastruktura (KI) vztahující se na ŘLP ČR, s. p. jako poskytovatele LNS principiálně vychází z požadavku krizového zákona. Požadavky zákona jsou dále rozpracovány v souvisejících prováděcích předpisech.

Krizový zákon definuje KI jako prvek KI nebo systém prvků KI, jehož narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Za prvky KI jsou považovány zejména stavby, zařízení, prostředky nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií. Subjekt KI jako provozovatel prvku KI je z krizového zákona odpovědný za jeho ochranu a je vázán řadou povinností.

1.4.2. Rozsah kritické infrastruktury u poskytovatele LNS

ŘLP ČR, s. p. bylo zařazeno s přesně definovanými prvky KI mezi subjekty KI rozhodnutím vlády České republiky na základě seznamu předloženého Ministerstvem vnitra. Tomuto rozhodnutí předcházelo posouzení průřezových a odvětvových kritérií. U průřezových kritérií byla posouzena závažnost vlivu narušení funkce prvků KI s mezními hodnotami, které zahrnují rozsah ztrát na životě, dopad na zdraví osob, mimořádně závažný ekonomický dopad, dopad na veřejnost v důsledku rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života. U odvětvových kritérií byly posouzeny technické a provozní hodnoty prvku KI v odvětví doprava.

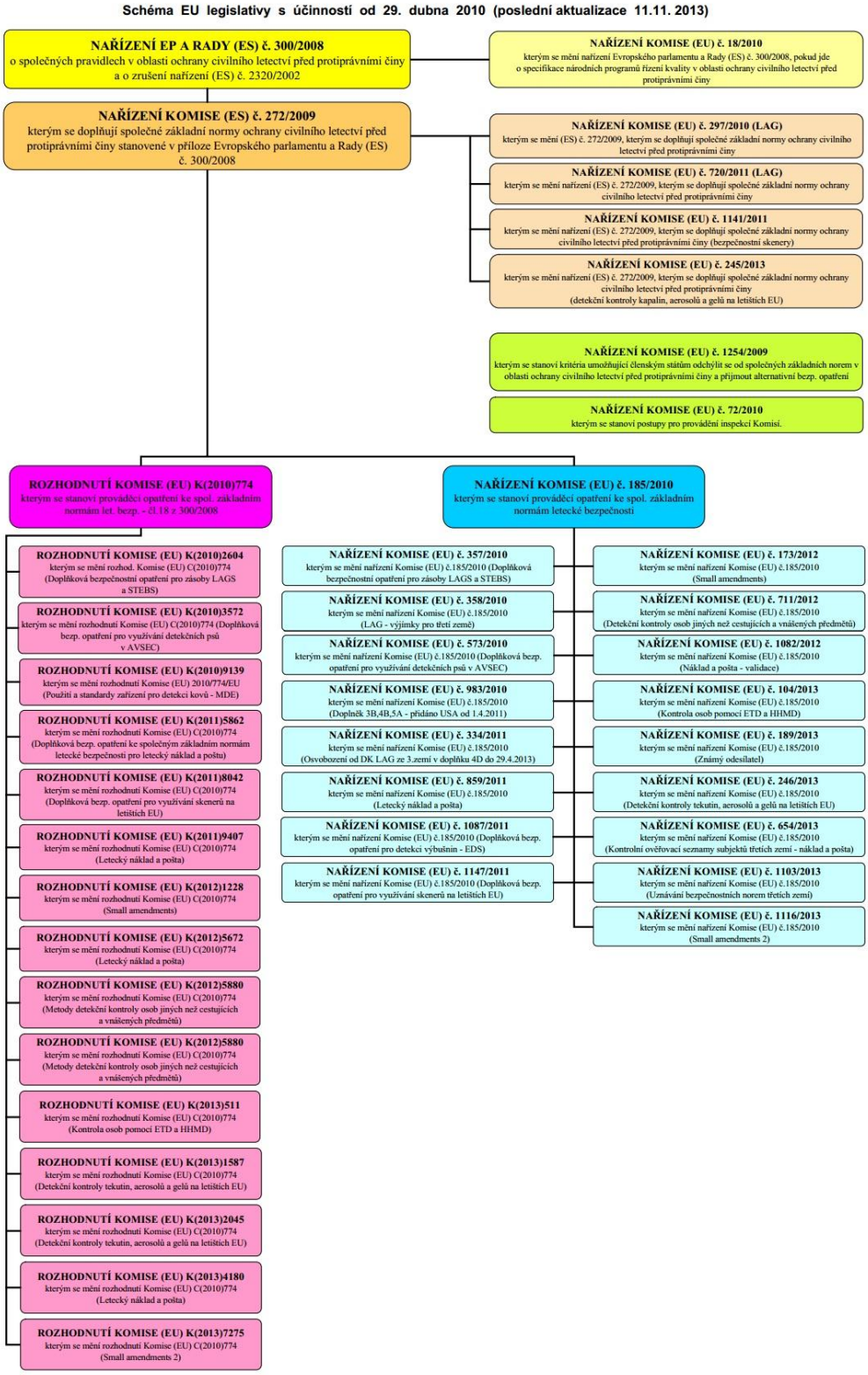
2. Letecká legislativa ve vztahu k ochraně kritické infrastruktury

Předmětná letecká legislativa v oblasti ochrany kritické infrastruktury před protiprávními činy se řídí současně platnými požadavky legislativy Evropské unie a legislativou českého civilního letectví.

2.1. Požadavky současné legislativy EU

Základním dokumentem EU, upravujícím oblast ochrany před protiprávními činy, je Nařízení evropského parlamentu a rady (ES) č. 300/2008 ze dne 11. března 2008 o společných pravidlech v oblasti civilního letectví před protiprávními činy a o zrušení nařízení (ES) č. 2320/2002. Podružným dokumentem je NAŘÍZENÍ KOMISE (ES) č. 272/2009 kterým se doplňují společné základní normy ochrany civilního letectví před protiprávními činy stanovené v příloze Evropského parlamentu a Rady (ES) č.

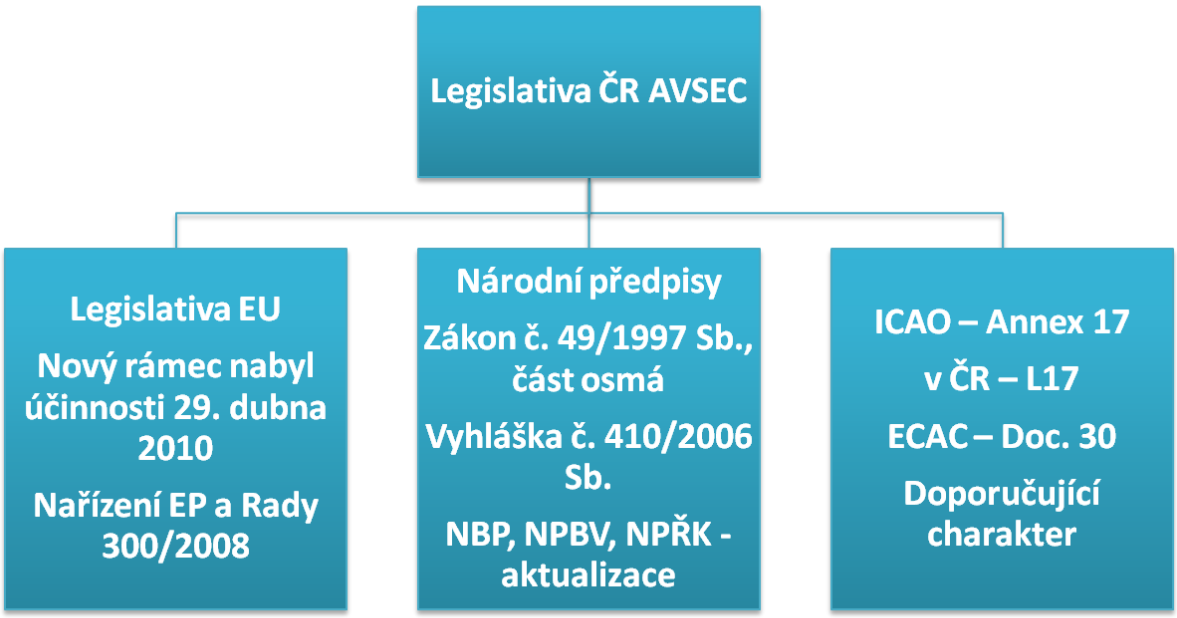
300/2008. Schéma legislativy EU ve vztahu k ochraně civilního letectví před protiprávními činy včetně prováděcích Nařízení a Rozhodnutí Komise je znázorněn na obr. 5.



Obrázek 5 Schéma legislativy EU ve vztahu k ochraně civilního letectví před protiprávními činy

2.2. Řešení legislativy českého civilního letectví

Obrázek 6 představuje schematické znázornění legislativy České republiky ve vztahu k ochraně civilního letectví před protiprávními činy. Jedná se primárně o předpisy, dokumenty volně dostupné veřejnosti, tj. dokumenty Letecké informační služby, EUDOC, veřejné části Národního bezpečnostního programu, Národního programu bezpečnostního výcviku, Národního programu řízení kvality, Nařízení EP a Rady 300/2008 a Nařízení Komise (EU) 185/2010. Některé předpisy a dokumenty jsou poskytovány pouze na principu „potřeby znát", konkrétně jde o utajovanou část Národního bezpečnostního programu a Rozhodnutí Komise K (2010)774.



Obrázek 6 Legislativa ČR ve vztahu k ochraně civilního letectví před protiprávnimi činy

3. Úloha regulátora ve vztahu k potlačení vzniku možných rizik

Regulace obecně znamená řídící či usměrňující činnost, ať už prováděnou člověkem nebo automatickým zařízením (regulátorem). Ve společnosti je regulace ovlivňování nebo ovládání lidského a společenského chování na základě pravidel a omezení.

Státní správu na úseku civilního letectví v České republice vykonávají tyto správní orgány (úřady, veřejné ústavy):

- Ministerstvo dopravy;
- Úřad pro civilní letectví;
- Ústav pro odborné zjišťování příčin leteckých nehod;
- osoba pověřená výkonem státní správy ve věcech sportovních létajících zařízení;
- osoba pověřená vedením „databáze terénu a překážek“

Další významné správní orgány:

- Ministerstvo obrany;
- Ministerstvo vnitra;
- Evropská agentura pro bezpečnost letectví (European Aviation Safety Agency – EASA)

Ministerstvo dopravy ČR:

Obecná působnost dle zákona č. 2/1969 Sb., o zřízení ministerstev a jiných ústředních orgánů státní správy České republiky, ve znění pozdějších předpisů. *„Ministerstvo dopravy je ústředním orgánem státní správy ve věcech dopravy a odpovídá za tvorbu státní politiky v oblasti dopravy a v rozsahu své působnosti za její uskutečňování (viz ustanovení § 17), dále plní v okruhu své působnosti úkoly stanovené v zákonech a v jiných obecně závazných právních předpisech (viz ustanovení § 20). Rovněž se ve veškeré své činnosti řídí ústavními a ostatními zákony a usneseními vlády a zkoumá společenskou problematiku v okruhu své působnosti. Také analyzuje dosahované výsledky a činí opatření k řešení aktuálních otázek (viz ustanovení § 22), pečuje o náležitou právní úpravu věcí patřících do působnosti České republiky a připravuje návrhy zákonů a jiných právních předpisů týkajících se věcí, které patří do jeho působnosti (viz ustanovení § 24). Stejně tak zabezpečuje ve své působnosti úkoly související se sjednáváním mezinárodních smluv, s rozvojem mezinárodních styků a mezinárodní spolupráce (viz ustanovení § 25)“.*

Ve speciální působnosti dle zákona č. 49/1997 Sb., ve znění pozdějších předpisů Ministerstvo dopravy plní funkci odvolacího úřadu ve správním řízení proti

rozhodnutím Úřadu pro civilní letectví vydaným podle tohoto zákona: „*je oprávněno v mimořádných situacích, které bezprostředně a vážně ohrožují civilní letectví, vydat příkazy k provádění letů na dobu nezbytně nutnou“.*

Úřad pro civilní letectví ČR:

Věcnou působnost ÚCL vymezuje tzv. sběrné ustanovení, jímž je ustanovení § 89. Úřad je podřízen Ministerstvu dopravy. V jeho čele stojí generální ředitel, jehož jmenuje a odvolává ministr dopravy. ÚCL dle § 89 zákona 49/1997 „*spolupracuje s Evropskou agenturou pro bezpečnost letectví EASA a uzavírá s ní smlouvu o podmínkách spolupráce a plní úkoly vnitrostátního dozorového orgánu podle přímo použitelného předpisu Evropských společenství. Ve své působnosti rovněž dohlíží na plnění povinností leteckého dopravce týkajících se náhrad a pomoci cestujícím v případě odepření nástupu na palubu, zrušení nebo významného zpoždění letu a vyřizuje stížnosti na porušování těchto povinností“*.

Dle stejného paragrafu ÚCL také „*vede evidenci leteckého personálu, vydává průkaz způsobilosti leteckého personálu a uznává platnost průkazu způsobilosti leteckého personálu vydaného jiným státem, zadržuje nebo odnímá průkaz způsobilosti leteckého personálu, nařizuje a provádí ověřování jeho odborné i letové způsobilosti, ověření odborné způsobilosti nebo přezkoumání zdravotní způsobilosti člena leteckého personálu a omezuje nebo zakazuje činnost, k níž je člen leteckého personálu oprávněn“*.

Dle § 44 zákona 49/1997 pak „*Úřad po dohodě s Ministerstvem obrany rozděluje vzdušný prostor České republiky, omezuje nebo zakazuje užívání vzdušného prostoru, vyhrazuje části vzdušného prostoru k létání a uveřejňuje sdělení o tom, že je užívání vzdušného prostoru České republiky k létání nad určitými oblastmi trvale nebo dočasně nebezpečné v Letecké informační příručce nebo jiným vhodným způsobem“.*

3.1. Organizace a řízení procesu přípravy bezpečnostních pracovníků

Příprava a výcvik bezpečnostních pracovníků probíhají v rámci osnov a požadavků Národního programu bezpečnostního výcviku v civilním letectví České republiky a v souladu s požadavky předpisu L17 Ochrana před protiprávními činy.

Na letišti existují prostory s různým stupněm zabezpečení a s tím spojené kontroly (veřejné prostory, neveřejné prostory, vyhrazené bezpečnostní prostory). Postup přijímání pracovníků, kteří se nepodílejí na zabezpečení a ani nemají přístup do

vyhrazených bezpečnostních prostor (SRA), reguluje samo letiště. Rozdílné přijímací postupy se týkají pracovníků, kteří se sice na zabezpečení přímo nepodílejí, ale mají přístup do těchto zabezpečených prostor. Poslední skupiny, která přímo provádí výkon bezpečnostních opatření, jejich kontrolu nebo za ni nese odpovědnost, se týká nejvyšší prověření a nejvyšší stupeň výcviku.

Do této skupiny patří i bezpečnostní pracovníci a to jak bezpečnostní kontroly, tak i ostrahy letiště. Při náboru nových pracovníků jsou kladeny požadavky na osobní vlastnosti i fyzický stav uchazeče, avšak důležitou složku v přijímacím procesu hraje i minulost uchazeče. Zhodnocení se dosahuje ověřením spolehlivosti, které dokládá beztrestnost a upřesňuje předchozí pracovní pozice u jiných zaměstnavatelů. Podrobnější kritéria pro nábor nových pracovníků jsou následující:

- požadované vzdělání
- pohovor s odpovědným pracovníkem
- lékařské potvrzení o schopnosti vykonávat stanovenou službu nebo činnost
- psychologický test
- jazykové znalosti (podle místa působení pracovníka)
- ověření spolehlivosti

Při posuzování, zda je daný uchazeč vhodný na místo bezpečnostního pracovníka, se přihlíží ke všem vyjmenovaným kritériím. Někteří specializovaní pracovníci mohou projít procesem dodatečného ověření, zda je taková práce pro ně vhodná. Jedná se např. o obsluhu rentgenových zařízení, tzv. screener, kde jedna z prvních zkoušek, kterou uchazeči podstupují, ještě před začátkem samotného výcviku, je tzv. pre-employment testing. Ten se skládá z několika vzorových rentgenových snímků, na kterých je ukryt nebezpečný nebo zakázaný předmět. Úkolem je najít jej v omezeném časovém limitu. Test ověří, zda má daný člověk rozpoznávací schopnosti nezbytné při dalším výcviku.

Celkový výcvik bezpečnostního pracovníka se skládá z několika částí: školení o používání identifikačních karet (IDC), následují 3 dny účasti na pracovišti, kde se daný budoucí pracovník seznamuje s prostředím, používanými výrazy a prostředky. Dalším velkým blokem je 12 denní školení (podle specializace pracovníka), které je zakončeno standardizovanou zkouškou. Po zácviku na pracovišti, kde pracovník provádí výkon své

práce samostatně, ale stále pod dohledem nadřízené osoby, je mu vydáno osvědčení Ministerstva dopravy. Tím se pracovník stává plnohodnotným členem pracovního útvaru a může samostatně vykonávat službu.

4. Realizace požadavků ochrany infrastruktury u poskytovatelů LNS

4.1. Problematika organizace a ochrany vzdušného prostoru

Cílem ochrany civilního letectví před protiprávními činy je bezpečnost cestujících, posádky letadel, pozemního leteckého personálu a ostatní veřejnosti.

Poskytovatel LNS je jedním ze subjektů podílejícím se na ochraně civilního letectví před protiprávními činy. Základní principy ochrany civilního letectví před protiprávními činy jsou primárně definovány v leteckém předpisu L17 Bezpečnost – Ochrana mezinárodního civilního letectví před protiprávními činy, který uveřejňuje Ministerstvo dopravy při aplikaci příslušného textu dokumentu[1] Mezinárodní organizace pro civilní letectví (ICAO). S uvedeným předpisem souvisí vybrané postupy dalších leteckých předpisů, např. L2, L6 nebo L11[2].

Na letecký přepis L17 navazuje evropská a národní legislativa[3].

- ICAO, EU

Kontrolní činnost systému bezpečnostních opatření zajišťujících ochranu civilního letectví před protiprávními činy jsou prováděny inspekčními týmy především ICAO, Evropské komise a ECAC v souladu se standardními postupy a dle metodiky dané mezinárodní organizace.

- Ministerstvo dopravy

Na národní úrovni vytváří Ministerstvo dopravy ve spolupráci s Ministerstvem vnitra systém ochrany civilního letectví, připravuje a implementuje předpisy (např. NBP[4]), postupy a bezpečnostní opatření k ochraně civilního letectví před protiprávními činy. Podmínkou přijímaných bezpečnostních opatření je pak vždy garantovat při

[1] Annex 17 – SECURITY – Safeguarding International Civil Aviation Against Acts of Unlawful Interference

[2] Annex 2 – Rules of the Air (Attachment 3 – Unlawful Interference); Annex 6 – Operation of Aircraft (Chapter 13 – Security); Annex 11 – Air Traffic Services (e.g. Chapter 5. Alerting Services, 5.1.1c)

[3] Legislativa a navazující požadavky hovoří též v souvislosti s poskytovatelem LNS o ochraně ATM systémů *(ATM Security).* ATM systémy = technické zařízení přímo zajišťující poskytování letových navigačních služeb nebo zařízení používané při poskytování letových navigačních služeb. ATM systémy spadají do skupiny letecké pozemní zařízení, které jsou definované v leteckém zákoně. Termínem „ATM systém" jsou dále míněna i technická zařízení určená pro výkon služby SAR *(Search and Rescue)* na RCC *(Rescue Coordination Centre).*

[4] NBP = Národní bezpečnostní program ochrany civilního letectví před protiprávními činy – *National Civil Aviation Security Programme*

zajištění účinnosti těchto bezpečnostních opatření minimální zásah do civilního letecké dopravy, včetně negenerování možných zpoždění.

Ministerstvo dopravy se dále v součinnosti s Ministerstvem vnitra podílí na výměně informací týkající se ochrany civilního letectví s příslušnými orgány jiných členských států. Při vyhodnocování bezpečnostních hrozeb Ministerstvo dopravy úzce spolupracuje s Policií České republiky a jednotlivými členy Meziresortní komise pro bezpečnost civilního letectví.

Ministerstvo dopravy jak u poskytovatele LNS, tak u dalších subjektů podílejících se na ochraně civilního letectví před protiprávními činy vykonává prostřednictvím národních auditorů státní dozor. V případně zjištění závažných pochybení projednává Ministerstvo dopravy související správní delikty v rozsahu své působnosti.

- Meziresortní komise pro bezpečnost civilního letectví

Komise je speciálním orgánem sdružujícím zástupce Ministerstva dopravy, Ministerstva vnitra, Ministerstva obrany, Ministerstva zahraničních věcí a Ministerstva financí pro účely koordinace a plánování bezpečnostních opatření k zajištění ochrany civilního letectví. Mezi hlavní úkoly komise patří zejména zpracovávání doporučení a návrhy opatření k zajištění ochrany civilního letectví před protiprávními činy, projednávání postupů a sledování plnění úmluv ICAO (Tokijská, Haagská, Montrealská apod.), stanovování podmínek pro plnění NBP a poskytování bezpečnostních informací zahraničním provozovatelům letadel a zahraničním leteckým úřadům, projednávání požadavků na poskytování ochrany pro česká letadla v zahraničí či příprava návrhů a stanovisek České republiky k jednání ICAO, ECAC a EU v otázkách ochrany civilního letectví před protiprávními činy.

- ÚCL

Úřad pro civilní letectví vykonává v oblasti ochrany civilního letectví před protiprávními činy u poskytovatele LNS státní dozor zejména na základě evropských požadavků.

- Další subjekty

Další subjekty participující na zajišťování ochrany civilního letectví před protiprávními činy jsou Ministerstvo vnitra, Policie České republiky, Armáda České republiky, celní orgány, provozovatelé letišť, letečtí dopravci, poskytovatelé služeb při odbavovacím procesu na letišti, známý dodavatelé palubních zásob, známý dodavatelé

letištních dodávek, schválení agenti, známý nebo stálí dodavatelé nebo dopravci zásilek, provozovatelé leteckých prací a provozovatelé leteckých veřejných vystoupení a leteckých soutěží, civilní bezpečnostní služby, popř. další fyzické nebo právnické osoby zúčastněné na civilním letectví. Specifickými subjekty spolupodílejícími se na zajišťování ochrany civilního letectví před protiprávními činy jsou pak zpravodajské služby České republiky (BIS, ÚZSI a VZ).

Air policing

Ze strany poskytovatele LNS je též zajišťována součinnostní bezpečnostní podpora při střežení vymezeného vzdušného prostoru. Jde například o nasazení stíhacího letectva Armády České republiky při pomoci s identifikací letounů, včetně jejich bezpečného doprovodu na letiště, popřípadě o omezení vzniklého bezpečnostního rizika.

4.2. Ochrana infrastruktury poskytovatelů LNS

Výchozí koncepce ochrany infrastruktury zahrnující zejména ATM systémy u poskytovatele LNS obsahuje základní komponenty:

- Fyzickou ochranu
- Personální ochranu
- Ochranu informací

Specifickým komponentem v ochraně příslušné infrastruktury je řešení vybraných nestandardních provozních stavů[5], včetně řízení kontinuity činnosti a následné obnovy[6].

4.2.1. Základní přístup k zajišťování ochrany poskytovatele LNS

Nástrojem pro řízení ochrany infrastruktury u poskytovatele LNS je *systém managementu ochrany* (SecMS)[7]. Koncept manažerského systému vychází z principu PDCA a je kompatibilní například s manažerskými systémy kvality (QMS), provozní

[5] Jde o vybrané stavy *emergency, contingency, degradace.* (U některých uvedených stavů je synonymem *krizový* stav dle krizového zákona.)

[6] *Service/Business Continuity and Recovery*

[7] SecMS – Security Management System vychází z technické normy *ISO 28000:2007 Specification for security management system for the supply chain*

bezpečnosti (SMS) nebo životního prostředí (EMS)[8], které jsou v civilní letecké dopravě v různé míře aplikovány.

Ochrana KI u ŘLP ČR, s. p. je pouze jedním ze zákonných a dalších bezpečnostních požadavků v oblasti zajišťování ochrany podnikových aktiv[9], které se v souhrnu počítají na několik desítek. Systémový přístup umožňuje tyto požadavky vhodně sdružovat a využívat tak vzájemné synergie při naplňování všech bezpečnostních požadavků.

Dalšími nespornými výhodami systémového manažerského přístupu v ochraně je:

- zajišťování, udržování a řízení adekvátní ochrany podnikových aktiv v čase[10];
- účinné, funkční a jednotné manažerské řízení ochrany podnikových aktiv;
- prokazatelná bezpečnostní důvěryhodnost pro zainteresované strany (např. dozorové mezinárodní a národní autority[11], jiní poskytovatelé LNS, obchodní partneři);
- podpora efektivního vynakládání finančních prostředků pro zajištění ochrany podnikových aktiv;
- prostředek pro implementaci legislativních a dalších oprávněných bezpečnostních požadavků (koordinační dohody, smlouvy apod.);
- možnost integrace s jinými manažerskými systémy.

5. Ochrana letišť a letů civilních letadel před protiprávními činy

Na základě cílů, definovaných v „Národním bezpečnostním programu“ ministerstva dopravy České republiky, vytvořit podmínky pro dosažení zvýšení efektivity bezpečnostních kontrol na letištích a dalších místech kritické infrastruktury, využitím nově koncipované metodiky přípravy pracovníků bezpečnostních kontrol.

[8] QMS – Quality Management System, SMS – Safety Management System, EMS – Environment Management System

[9] Infrastrukturu lze definovat též jako typ aktiva *(asset)* nebo „chráněný zájem“. Aktivum je širší pojem než infrastruktura a lze ho chápat jako cokoliv, co má pro poskytovatele LNS hodnotu, která může být snížena působením bezpečnostní hrozby. Aktivum může být hmotné (např. personál, objekty, zařízení, finanční hotovost, listinné dokumenty) nebo nehmotné (např. data, know-how, SW, goodwill poskytovatele LNS).

[10] Tj. v souladu s časovou proměnou bezpečnostních hrozeb a dynamikou úrovně souvisejících bezpečnostních rizik nebo bez ohledu na rozvoj a úroveň bezpečnostních technologií.

[11] Kromě již uvedených dozorových autorit typu ICAO, ECAC, Ministerstva dopravy či ÚCL se jedná v případě ŘLP ČR, s. p. dále například NBÚ (Národního bezpečnostního úřad) nebo ÚOOÚ (Úřadu na ochranu osobních údajů).

5.1. Analýza charakteristik lidského činitele ve vztahu k procesům řešení krizových situací v systémech ochrany

Předpokladem pro modernizaci metodiky přípravy bezpečnostních pracovníků bude využití a další rozpracování poznatků ukončeného evropského projektu „Behaviorální modelování pro bezpečnost na letištích“ BEMOSA (Behaviour Modelling for Security in Airports) do konkrétních textů metodiky ověřování behaviorálních charakteristik bezpečnostních pracovníků a formulace postupů pro jejich odbornou přípravu a výcvik.

S využitím poznatků, získaných řešením evropského projektu BEMOSA a ve spolupráci s jeho řešiteli v České republice, tj. Letiště Praha, a.s., Letiště Brno, B & M InterNets s.r.o. Brno a v rámci realizovaných aplikací v práci doktorandů vysokých škol orientovaných na oblast letecké dopravy rozpracovat a ověřit problematiku „Behavior Analyst“ k vytvoření komplexního návrhu výběru a výcviku pracovníků schopných provádět analýzu chování cestujících pro potřeby perspektivních kontrolních bezpečnostních stanovišť (Checkpoint of the Future) na provozní úrovni letišť v Evropě a České republice. Tuto problematiku pak rozpracovat do úrovně použitelné i v jiných oblastech využívajících bezpečnostní kontrolu osob v letectví, stejně tak jako i u jiných módů osobní dopravy. Novost navrhovaného řešení spočívá v očekávané změně přístupu bezpečnostních pracovníků k prováděnému procesu kontroly a tím i k očekávanému zvýšení míry bezpečnosti při provádění bezpečnostních kontrol.

5.2. Zhodnocení procesů odborné přípravy a výcviku lidského činitele ve vztahu k řešení možných krizových situací

K vytvoření komplexního návrhu výběru a výcviku pracovníků schopných provádět analýzu chování cestujících pro potřeby perspektivních kontrolních bezpečnostních stanovišť použít metodu situačního modelování chování bezpečnostních pracovníků podle výsledků projektu BEMOSA a dalších, průzkumem zjištěných charakteristik s aplikací poznatků, umožňujících zvýšení kvality přijímaných řešení. Výsledky modelování ověřit experimenty v praxi. Na základě zjištěných a ověřených výsledků pak zpracovat návrh metodiky pro úpravu teoretické přípravy a výcviku. Po projednání výsledků výzkumu a zpracovaného návrhu metodiky v rámci mezinárodních vědeckých konferencí a u národních regulačních orgánů civilního letectví, pak návrh prezentovat k posouzení na úrovni evropských orgánů civilního letectví.

S využitím zkušeností z vysokoškolské přípravy v provozně technické a ekonomicko-provozní oblasti letecké dopravy a znalostí kvalifikovaných odborníků z

praxe letecké dopravy vypracovat metodiku celoživotního vzdělávání ekonomicko-provozních pracovníků podniků letecké dopravy a zaměstnanců orientovaných na problematiku letecké dopravy ve státní správě s orientací na zkušenosti ze zahraničí. Při přípravě metodiky respektovat možnost nabídky odborné přípravy i pro zahraniční zájemce. Jde o vypracování dosud neexistující koncepce komplexní nabídky odborného celoživotního vzdělávání uvedeného druhu. Vytvořit tak podklady pro zkvalitnění procesu odborné přípravy ekonomicko-provozních pracovníků podniků letecké dopravy a zaměstnanců orientovaných na problematiku letecké dopravy ve státní správě vypracováním akreditovatelné metodiky celoživotního vzdělávání s orientací na zkušenosti ze zahraničí.

Při zpracování metodiky celoživotního vzdělávání ekonomicko-provozních pracovníků podniků letecké dopravy a zaměstnanců orientovaných na problematiku letecké dopravy ve státní správě se aktivně podílet na přípravě Studie koncepce letecké dopravy v České republice, především s orientací na prováděcí části „Proces vzdělávání a sociální aspekty“ a „Ochrana civilního letectví před protiprávními činy“. Současně aktivně studovat a aplikovat zkušenosti ze všech dosavadních forem vzdělávání v civilním letectví, zkušenosti dlouholetých řídicích pracovníků podniků letecké dopravy a respektovat analýzy předpokládaného procesu rozvoje letecké dopravy a s tím spojeného vývoje legislativních, organizačních, technických a provozních požadavků.

5.3. Problematika ochrany perimetrů kritické infrastruktury letišť a obdobných typů národních objektů kritické infrastruktury

Ochranou širšího okolí perimetru se rozumí bezpečnostní opatření přijímána v pásmu přibližně do 7,5 km od prahu vzletové a přistávací dráhy. Ochrana širšího okolí perimetru letiště není povinným bezpečnostním prvkem, který by byl striktně upraven v mezinárodních či národních normách. Přesto je tento způsob ochrany předmětem zájmu bezpečnostních složek, zejména s ohledem na existující riziko teroristického útoku ručními raketovými střelami (MANPADS) proti letadlům. Nedávné případy z evropských zemí (např. informace o událostech ve Francii nebo Nizozemí, kde byli zatčeni extremisté, kteří podobný útok připravovali) svědčí o tom, že tento útok je v dnešní době možný i v evropských zemích (26). Ochrana širšího okolí perimetru musí být realizována zejména státními bezpečnostními složkami, zpravidla místní policií. Patří sem zejména hlídková činnost, dále jsou k monitoringu využívány technické prostředky, jako jsou termovize nebo přístroje pro noční vidění. Riziková místa se vybírají podle těchto kritérií: Místo není přehledné z míst s větším pohybem osob. Místo není pokryto kamerovým systémem. Letadla jsou nad místem v takové výšce, ve které je možno je

zasáhnout. Místo je snadno přístupné a poskytuje dobrý výhled na přilétávající - odlétající letadla. V okolí místa není velký provoz, případnému pachateli tak dává možnost nepozorovaného úniku po odpálení střely.

Ochranu objektu letiště vytváří komplex konkrétních bezpečnostních opatření a postupů, které jednak plní preventivní úlohy, jednak umožňují operativní reakci na případný protiprávní čin. Při koncipování bezpečnostních opatření je však třeba brát v úvahu také požadavek na zachování důležité přednosti letecké dopravy, kterou je rychlost. Platí zde princip, že bezpečnostní opatření nemohou nad míru nezbytně omezovat rychlost a plynulost odbavení cestujících.

Dohled nad bezpečností zajišťují speciálně vyškolení a vycvičení policisté, kteří by měli detailně znát postupy k řešení protiprávních činů, podezření na protiprávní jednání a jednání s podezřelými osobami. Veřejná i neveřejná část letiště by měla být neustále pod dohledem policie nebo bezpečnostního personálu letiště, a to jak uniformovaného, tak i neuniformovaného. Pokud je pro dohled nad prostorami letiště využíván kamerový systém, měla by na jeho použití zřetelně upozorňovat označení.

Bezpečnost je prováděna v následujících prostorech: Sociální zařízení (toalety, sprchy, umývárny) Schodiště Prodejní kanceláře leteckých společností přepážky Check-in Systémy pro transport zavazadel Parkovací plochy v blízkosti terminálu letiště Vyhlídkové prostory pro veřejnost Perimetr letiště Vyhrazené bezpečnostní prostory letiště Vstupní/výstupní prostory Citlivé části letiště (kontrolní věž, rozvodny komunikačních nebo navigačních zařízení, zdroje energie, sklady paliva nacházející se přímo na letišti nebo v jeho okolí).

5.4. Řešení národního informačního zdroje pro oblast Security

Využít veřejně na národní i mezinárodní úrovni prezentovanou koncepci Národního znalostního centra Security, již existujícího spolupracujícího kolektivu odborníků z různých akademických, výrobních nebo provozních oblastí, kapacitních možností vědeckopedagogických pracovníků kateder a odborných pracovišť VŠO a vybraných skupin studentů k postupné realizaci úkolů nutných pro efektivní provoz znalostního centra. Výsledky řešení prezentovat v rámci každoročních, již zavedených a katedrou VŠO organizovaných Mezinárodních vědeckých konferencích „Air Transport Security“. Konečným cílem bude uvedení Národního znalostního centra Security do zkušebního provozu v polovině roku 2017. Novost spočívá v realizaci dosud neexistujícího zařízení tohoto typu, ale aktivně požadovaného provozní praxi.

Pro realizaci koncepce Národního znalostního centra Security využít vedle samotných řešitelů vědeckého úkolu, také závěrečných prací studentů Vysoké školy obchodní v Praze (VŠO) a současně i znalostí a nabídek aktivně zapojených zájemců o spolupráci na národní i mezinárodní úrovni. Tuto činnost budeme orientovat k přípravě odpovídajícího okruhu vstupních znalostních informací, zpracování návrhu nebo i vlastního software pro server VŠO nebo také ke kvalitní přípravě odborných pojednání, rozborů nebo jiných výstupů Národního znalostního centra Security. Všechny dílčí výstupy pak budeme aktivně ověřovat v praxi a pravidelně každoročně prezentovat na mezinárodní vědecké konferenci „Air Transport Security".

6. Bezpilotní systémy jako podpůrné prostředky zabezpečení ochranné infrastruktury

Česká republika je jako členský stát ICAO od roku 1944 vázána Úmluvou o mezinárodním civilním letectví (dále jen „Úmluva") a jejími přílohami, jejichž požadavky jsou zaneseny v zákoně č. 49/1997 Sb., o civilním letectví (dále jen „letecký zákon"), v prováděcí vyhlášce k leteckému zákonu á v leteckých předpisech společně s dalšími národně platnými požadavky.

Článek 8 Úmluvy (transponován do § 52 leteckého zákona) stanovuje podmínku provozu bezpilotních letadel ve formě nutnosti získání povolení k létání. Aby mohl být plně využit společenský přínos bezpilotních letadel při současném udržení stávající vysoké úrovně bezpečnosti letectví, bude zapotřebí vytvořit nemálo speciálních mezinárodních předpisů, dle nichž bude možno bezpilotní letadla navrhovat, vyrábět, plnohodnotně provozovat a stejně jako jejich provozovatele a piloty i certifikovat. Tvorba této kompletní předpisové základny již byla zahájena; dokončení však potrvá ještě řádu let.

Aby byl již nyní umožněn vývoj bezpilotních letadel, získávány provozní zkušenosti á čerpány částečné výhody, které tato letadla skýtají, jsou členské státy ICAO vyzvány k tvorbě prozatímních národních pravidel, umožňujících provoz bezpilotních letadel s omezeními, která dorovnají bezpečnost na přijatelnou úroveň. Týká se to všech bezpilotních letadel provozovaných ve společném vzdušném prostoru s mezinárodním civilním letectvím, tedy i modelů letadel.

V ČR od 30. 5. 2013 začíná platit Doplněk X Předpisu L 2, který rozpracovává výše zmíněný požadavek Úmluvy a Postupy, které stanoví více detailů pro jeho aplikaci. Uvedený předpis definuje provoz letadel bez pilota na palubě, stanovuje podmínky provozu a v návaznosti na vývoj praxe částečně změkčuje použití UAS.

6.1. Definice podpůrných létajících prostředků

Dplněk X Předpisu L2 obsahuje následujíc předmětné definice:

6.1.1. Autonomní letadlo

„Bezpilotní letadlo, které neumožňuje zásah pilota do řízení letu".

6.1.2. Bezpilotní letadlo (UA)

„Letadlo určené k provozu bez pilota na palubě".

Poznámka: V mezinárodním kontextu se jedná o nadřazenou kategorii dálkově řízených letadel, autonomních letadel i modelů letadel; pro účely tohoto doplňku se bezpilotním letadlem rozumí všechna bezpilotní letadla kromě modelů letadel s maximální vzletovou hmotností nepřesahující 20 kg.

6.1.3. Bezpilotní systém (UAS)

„Systém skládající se z bezpilotního letadla, řídicí stánice a jakéhokoliv dalšího prvku nezbytného k umožnění letu, jako například komunikačního spojení a zařízení pro vypuštění a návrat. Bezpilotních letadel, řídicích stánic nebo zařízení pro vypuštění a návrat může být v rámci bezpilotního systému více".

6.1.4. Model letadla

„Letadlo, které není schopné nést člověka na palubě, je používané pro soutěžní, sportovní nebo rekreační účely, není vybaveno žádným zařízením umožňujícím automatický let na zvolené místo, a které, v případě volného modelu, není dálkově řízeno jinak, než za účelem ukončení letu nebo které, v případě dálkově řízeného modelu, je po celou dobu letu pomocí vysílače přímo řízené pilotem v jeho vizuálním dohledu".

6.2. Rozsah působnosti letecké legislativy

Doplněk X dále stanovuje: „*závazné národní požadavky na projektování, výrobu, údržbu, změny a provoz bezpilotních systémů splňujících kritéria přílohy II nařízení Evropského parlamentu a Rady (ES) č. 216/2008 v platném znění a je doporučeným postupem pro provoz modelů letadel s maximální vzletovou hmotností nepřesahující 20 kg".*

6.2.1. Požadavky na projektování a stavbu bezpilotních letadel a bezpilotních systémů

Doplněk stanovuje: „*Projektování, výroba a počáteční letové zkoušky musí být dozorovány ÚCL, případně ÚCL pověřenou osobou, dle stanovených postupů. Bezpilotní*

letadlo musí být vybaveno vestavěným bezpečnostním systémem („failsafe" systém), který při selhání řídícího á kontrolního spoje provede ukončení letu".

6.2.2. Požadavky na provozování bezpilotních letadel a bezpilotních systémů

Tyto požadavky jsou opět sanoveny Doplňke X, který stanovuje: „*Nově je definován provoz (dohled pilota) a je dána rozhodovací pravomoc o provozu ÚCL s odchylkou od definice předpisu. S výjimkou, kdy ÚCL povolí jinak, musí být bezpilotní letadlo provozováno v přímém dohledu pilota, tj. takovým způsobem a do takové vzdálenosti, aby:*

- *pilot během pojíždění a letu mohl udržovat trvalý vizuální kontakt s bezpilotním letadlem i bez vizuálních pomůcek jiných než brýle a kontaktní čočky na lékařský předpis;*
- *pilot, nebo kromě pilota i poučená osoba, mohl sledovat a vyhodnocovat dohlednost, překážky á okolní letový provoz.*

Bezpilotní letadlo nesmí být bez povolení ÚCL provozováno při současném pohybu pilota pomocí technického zařízení".

6.2.3. Certifikace

Certifikace potvrzuje určité charakteristiky objektu, osoby nebo organizace. Toto potvrzení často, nikoliv však vždy, bývá uděleno po určité formě externího přezkoušení, výuce, ohodnocení nebo auditu. Specifickým případem certifikace organizací jsou akreditace.

Typy

- Profesní certifikace – uvnitř dané organizace prokazuje kompetenci dané osoby k výkonu daného povolání nebo úlohy, obvykle na základě složení předepsané zkoušky.
    - buďto s platností na celou dobu výkonu daného povolání,
    - nebo s platností na určitou periodu s definovanými podmínkami recertifikace.
- Licencování – je administrované vládní institucí pro veřejnou ochranu a dává oprávnění vykonávat určitou profesi.

Licencování a certifikace jsou podobné v tom, že vyžadují demonstraci stanovené úrovně znalostí a dovedností. Všeobecně to chápeme jako „způsobilost“ k něčemu.

S certifikací se ale setkáváme i u výrobků – zda výrobek splňuje minimální standardy.

Při certifikaci první stranou jednotlivec nebo organizace poskytující výrobky nebo služby dává garanci splnění určitých požadavků. Při certifikaci druhou stranou je garance poskytovaná sdružením, do kterého jednotlivec nebo organizace patří, nebo smluvním partnerem. Certifikace třetí stranou poskytuje nezávislé ohodnocení výrobku, osoby, procesu nebo organizace procesu.

Typy certifikací:

- Akademický titul
- Profesní certifikát
- Produktový certifikát nebo certifikační známka
- Certifikát informační bezpečnosti
- Digitální podpis
- Profesionální certifikát (počítačové technologie)
- Laboratorní certifikát
- Environmentální certifikát

Certifikace je souhrnný postup, kterým se ověřuje shoda předmětu s požadavky uvedenými v předpisech nebo normách platných pro příslušný předmět.

Certifikát je dokument, kterým se potvrzuje shoda předmětu posuzování s požadavky uvedenými v předpisech nebo normách platných pro příslušný předmět.

Akreditace je proces certifikace kompetence, autority nebo kredibility.

Organizace, které vydávají kredity nebo certifikují třetí strany, jsou samy formálně akreditované akreditačními autoritami. Akreditace by měla ověřit, zda certifikační postupy jsou přijatelné, zejména s ohledem na kompetentní testy a etické ověřování standardů.

Typickým příkladem akreditace je akreditace testovacích laboratoří a certifikace specialistů oprávněných vydávat oficiální certifikáty shody se stanovenými technickými standardy jako jsou fyzické, chemické, kvalitativní nebo bezpečnostní standardy.

Akreditační úřady se v těchto oblastech řídí normou ISO 17011. Akreditované instituce potom jsou posuzované podle souladu se standardy ve stejné normalizační řadě:

- BS EN ISO/IEC 17020: "General criteria for the operation of various types of bodies performing inspection" (2004)
- BS EN ISO/IEC 17021: "Conformity assessment. Requirements for bodies providing audit and certification of management systems" (2011)
- BS EN ISO/IEC 17024: "Conformity Assessment. General requirements for bodies operating certification of persons" (2003)
- BS EN ISO/IEC 17025: "General requirements for the competence of testing and calibration laboratories" (2005)

Akreditační proces je aplikován v mnohých oblastech, namátkou:

- Akreditovaný investor
- Akreditovaný diplomat
- Akreditovaná výuka
- Zdravotnictví
- Akreditovaná zdravotní komise
- Akreditovaná nemocnice
- Profesní certifikace
- Systémové inženýrství
- Akreditovaný tlumočník, překladatel

Příklady mezinárodních institucí, které vyvíjejí a definují specifikace důležité v oboru Dopravy a Dopravních informací:

- European Aviation Safety Agency (EASA)
- International Air Transport Association (IATA)
- International Union of Railways (UIC)
- European Broadcasting Union (EBU) - See TPEG
- World Wide Web Consortium (W3C)
- OpenTravel Alliance (OTA)
- Open Geospatial Consortium (OGC)
- Organization for the Advancement of Structured Information Standards (OASIS)

Výše uvedené principy se v plné míře realizují také v certifikaci techniky, pracovníků a pracovaných postupů v civilním letectví.

Vzhledem na zvláštnosti a celosvětový charakter civilního letectva existují v certifikaci civilního letectva určité zvláštnosti na celosvětové, evropské a národní úrovní.

Evropský parlament a Rada Evropské unie zřídily přijetím nařízení (ES) č. 1592/2002 (dále jen „základní nařízení“) Evropskou agenturu pro bezpečnost letectví (dále jen EASA „agentura“).

V návaznosti na Nařízení č. 216/2008 (1592/2002) Evropského parlamentu a Rady o společných pravidlech v oblasti civilního letectva a o ustanovení EASA kterým se doplňuje a kterým se*: „stanoví prováděcí pravidla pro certifikaci letové způsobilosti letadel a souvisejících výrobků, letadlových částí a zařízení a certifikaci ochrany životního prostředí, jakož i pro certifikaci projekčních a výrobních organizací“.*

Komise Evropského společenství přijala nařízení Komise (ES) č. 1702/2003 na základě nařízení Evropského parlamentu a Rady (ES) č. 1592/2002 (o společných pravidlech v oblasti civilního letectví a o zřízení Evropské agentury pro bezpečnost letectví). Obě nařízení jsou závaznými zákonnými normami členských států EU.

Vzhledem k tomu, že článek 44 základního nařízení mimo jiné požaduje, aby správní rada stanovila průhledné postupy, podle kterých je výkonný ředitel povinen činit jednotlivá rozhodnutí, s ohledem na stanovisko poradního orgánu zúčastněných

osob, přijala toto rozhodnutí: EASA MB 02/04 Rozhodnutí správní rady č. 7-2004 Postupy certifikace výrobků30. března 2004.

Toto nařízení stanovuje obecné zásady postupů, podle kterých má agentura postupovat při provádění certifikace letové způsobilosti leteckých výrobků, letadlových částí a zařízení a certifikace ochrany životního prostředí, včetně činností po typové certifikaci, v souladu s použitelnými prováděcími pravidly základního nařízení.

Nařízení Komise (ES) č. 1702/2003 ze dne 24. září 2003, kterým se: „*stanoví prováděcí pravidla pro certifikaci letové způsobilosti letadel a souvisejících výrobků, letadlových částí a zařízení a certifikaci ochrany životního prostředí, jakož i pro certifikaci projekčních a výrobních organizací".*

Toto nařízení definuje pravidla pro certifikaci letové způsobilosti letadel a certifikaci ochrany životního prostředí. Jeho cílem je vytvořit nový certifikační systém pod správou Evropské agentury pro bezpečnost letectví (EASA). Poskytuje však přechodový systém, aby EASA měla čas přijmout definice a příslušné postupy.

Obsahem tohoto nařízení je 5 základních článků:

1. Oblast působnosti a definice
2. Certifikace výrobků, letadlových částí a zařízení
3. Projekční organizace
4. Výrobní organizace
5. Vstup v platnost

a příloha Část 21 (PART 21)

Příloha obsahuje prováděcí pravidla pro toto nařízení, která jsou obdobou předchozího předpisu JAR-21. Na rozdíl od tohoto předpisu však neobsahuje poradenský materiál a přijatelné způsoby průkazu (dřívější ACJ). Ty jsou obsahem rozhodnutí výkonného ředitele EASA č. 2003/1/RM

V příloze tohoto nařízení „část 21" specifikuje společné technické požadavky a správní postupy pro certifikaci letadel a jejich částí a zařízení a certifikaci ochrany životního prostředí. Nařízení také obsahuje pravidla, která se vztahují na organizace zapojené do projektování a výroby těchto výrobků. Toto nařízení stanovuje podmínky pro:

- vydávání typových osvědčení, typových osvědčení pro zvláštní účely, doplňkových typových osvědčení a změn těchto osvědčení;
- vydávání osvědčení letové způsobilosti, osvědčení letové způsobilosti pro zvláštní účely, povolení k letu a osvědčení o uvolnění oprávněnou osobou;
- vydávání schválení návrhů oprav;
- průkaz vyhovění požadavkům na ochranu životního prostředí;
- vydávání osvědčení hlukové způsobilosti;
- označování výrobků, letadlových částí a zařízení;
- certifikaci projekčních a výrobních organizací;
- vydávání příkazů k zachování letové způsobilosti.

Činnosti po typové certifikaci znamenají jakékoliv činnosti následně po vydání typového osvědčení nebo typového osvědčení pro zvláštní účely. Tyto činnosti zahrnují:

- změny výrobků, letadlových částí nebo zařízení;
- doplňková typová osvědčení;
- opravy výrobků;
- zachování letové způsobilosti výrobku, letadlové části nebo zařízení včetně sběru informací vztahujících se k poruchám, nesprávným činnostem a závadám, rozborů hlášených událostí, provozních informací a vydávání příkazů k zachování letové způsobilosti.

6.3. Určení bezpilotních prostředků

Bezpilotní letadlo může po splnění příslušných požadavků provádět např. letecké práce, letecké činnosti pro vlastní potřebu, rekreační a sportovní létání, atd.

6.3.1. Provádění leteckých prací a jejich příslušné legislativní vymezení dle leteckých předpisů

Leteckými pracemi jsou letecké činnosti, při nichž letecký provozovatel využívá letadlo k pracovní činnosti za úplatu. Leteckými pracemi se dále rozumějí vyhlídkové

lety, využití letadla leteckým provozovatelem při výuce v leteckých školách á činnost leteckých škol.

Leteckou činností pro vlastní potřebu se rozumí lety, kterými zajišťuje právnická nebo fyzická osoba podnikatelskou nebo jinou činnost, k níž je oprávněná podle zvláštních předpisů. Nejedná se tedy o komerční lety za úplatu, ale o lety k zajištění vlastní podnikatelské činnosti.

Rekreačním a sportovním létáním se rozumí užívání letadla pro vlastní potřebu nebo potřebu jiných osob za účelem rekreace, osobní dopravy nebo sportu, které není uskutečňováno za účelem zisku.

Přesné vymezení jednotlivých činností je specifikováno v §73, §76, §77 leteckého zákona.

6.4. Letová bezpečnost – Safety

V současné době je řízení UA závislé na frekvenčním spektru, které není pro UA speciálně vyhrazeno (chráněno) a je tedy pravděpodobné, že může dojít k rušení a následné ztrátě řízení.

6.4.1. Vymezení podmínek letové bezpečnosti pro bezpilotní systémy

Bezpečnostní systém musí zamezit ohrožení osob, majetku a životního prostředí v případě letu mimo kontrolu pilota po ztrátě řídícího spoje a stanovený postup nebo instalovaný bezpečnostní systém musí zamezit ohrožení osob, majetku a životního prostředí při dopadu letadla poté, co systém aktivuje postup ukončení letu.

Nastavení tohoto systému bude závislé na daném typu UA (motorové letouny, vrtulníky, atd.). Zajištění bezpečnosti při dopadu letadla může být řešeno stanovením postupu (bezpečné vzdálenosti od osob a majetku) nebo instalací různých technických řešení, např. padáku nebo airbagu. Ani aktivace těchto systémů však nezbavuje pilota odpovědnosti za bezpečné provedení celého letu.

6.5. Využívání vzdušného prostoru bezpilotními systémy

Doplněk X předpisu L2 tsnovuje, že: „*let bezpilotního letadla a/nebo modelu letadla smí být prováděn jen v prostorech stanovených článkem 7 přílohy pokud ÚCL nepovolí jinak. Obecně tedy:*

- *ve vzdušném prostoru třídy G.*

- *v letištní provozní zóně (ATZ) neřízeného letiště na základě splnění podmínek stanovených provozovatelem letiště a na základě koordinace s letištní letovou informační službou (AFIS) nebo s provozovatelem letiště, není-li služba AFIS poskytována. Nad vzdušným prostorem třídy G lze v ATZ lety provádět jen pokud je poskytována služba AFIS. Let bezpilotního letadla anebo modelu letadla s maximální vzletovou hmotností do 0,91 kg může být prováděn v ATZ i bez koordinace, avšak pouze do výšky 100 metrů nad zemí a mimo ochranná pásma daného letiště.*

- *v řízeném okrsku (CTR á MCTR) letiště do výšky 100 metrů nad zemí, s výjimkou povolení příslušného stanoviště řízení letového provozu a v horizontální vzdálenosti větší než 5 500 m od vztažného bodu řízeného letiště, s výjimkou, kdy tak povolí ÚCL nebo v případě leteckých prací a leteckých veřejných vystoupení na základě koordinace s příslušným stanovištěm řízení letového provozu a provozovatelem letiště. Let bezpilotního letadla a/nebo modelu letadla s maximální vzletovou hmotností do 0,91 kg může být prováděn v řízeném okrsku bez koordinace i v menší vzdálenosti od letiště, avšak pouze do výšky 100 metrů nad zemí a mimo ochranná pásma daného letiště.*

- *při provozu bezpilotního letadla a/nebo modelu letadla v CTR á MCTR ve vzdálenosti větší než 5 500 m od vztažného bodu letiště a současně ve výšce nižší než 100 m nad zemí a při provozu bezpilotního letadla a/nebo modelu letadla s maximální vzletovou hmotností do 0,91 kg ve vzdálenosti menší než 5 500 m od vztažného bodu letiště, do výšky 100 metrů nad zemí a mimo ochranná pásma letiště se neuplatňují požadavky Předpisu L 11 na získání letového povolení a na stálé obousměrné spojení se stanovištěm řízení letového provozu a požadavky stanovené Leteckou informační příručkou ČR (AIP) na vybavení odpovídačem sekundárního radaru. Při provozu bezpilotního letadla a/nebo modelu letadla v CTR a MCTR ve vzdálenosti menší než 5 500 m od vztažného bodu letiště, kromě provozu bezpilotního letadla a/nebo modelu letadla s maximální vzletovou hmotností do 0,91 kg mimo ochranná pásma letiště, nebo ve výšce vyšší než 100 m nad zemí je rozhodnutí o použitelnosti v tomto ustanovení uvedených požadavků ponecháno na uvážení příslušného stanoviště řízení letového provozu.*

Autonomní bezpilotní letadlo nesmí být provozováno ve společném vzdušném prostoru".

6.5.1. Letecká předpisová základna pro využívání letových prostorů bezpilotními letadly

Článek 8 Úmluvy (transponován do § 52 leteckého zákona) stanovuje podmínku provozu bezpilotních letadel ve formě nutnosti získání povolení k létání. Aby mohl být plně využit společenský přínos bezpilotních letadel při současném udržení stávající vysoké úrovně bezpečnosti letectví, bude zapotřebí vytvořit nemálo speciálních mezinárodních předpisů, dle nichž bude možno bezpilotní letadla navrhovat, vyrábět, plnohodnotně provozovat a stejně jako jejich provozovatele a piloty i certifikovat. Tvorba této kompletní předpisové základny již byla zahájena; dokončení však potrvá ještě řádu let.

Aby byl již nyní umožněn vývoj bezpilotních letadel, získávány provozní zkušenosti a čerpány částečné výhody, které tato letadla skýtají, jsou členské státy ICAO vyzvány k tvorbě prozatímních národních pravidel, umožňujících provoz bezpilotních letadel s omezeními, která dorovnají bezpečnost na přijatelnou úroveň. Týká se to všech bezpilotních letadel provozovaných ve společném vzdušném prostoru s mezinárodním civilním letectvím, tedy i modelů letadel.

V ČR od 30. 5. 2013 začíná platit Doplněk X Předpisu L 2, který rozpracovává výše zmíněný požadavek Úmluvy a Postupy, které stanoví více detailů pro jeho aplikaci. Uvedený předpis definuje provoz letadel bez pilota na palubě, stanovuje podmínky provozu a v návaznosti na vývoj praxe částečně změkčuje použití UAS.

Doplněk dále *„stanovuje závazné národní požadavky na projektování, výrobu, údržbu, změny a provoz bezpilotních systémů splňujících kritéria přílohy II nařízení Evropského parlamentu a Rady (ES) č. 216/2008 v platném znění a je doporučeným postupem pro provoz modelů letadel s maximální vzletovou hmotností nepřesahující 20 kg“.*

Nově je definován provoz (dohled pilota) a je dána rozhodovací pravomoc o provozu ÚCL s odchylkou od definice předpisu. *„S výjimkou, kdy ÚCL povolí jinak, musí být bezpilotní letadlo provozováno v přímém dohledu pilota, tj. takovým způsobem á do takové vzdálenosti, aby:*

- *pilot během pojíždění a letu mohl udržovat trvalý vizuální kontakt s bezpilotním letadlem i bez vizuálních pomůcek jiných než brýle a kontaktní čočky na lékařský předpis;*

- *pilot, nebo kromě pilota i poučená osoba, mohl sledovat a vyhodnocovat dohlednost, překážky a okolní letový provoz.*

Bezpilotní letadlo nesmí být bez povolení ÚCL provozováno při současném pohybu pilota pomocí technického zařízení.

Provoz bezpilotního letadla musí být v souladu i s dalšími platnými právními předpisy jako např.: Zákon o nakládání s bezpečnostním materiálem č. 310/2006 Sb., Zákon o ochraně veřejného zdraví č. 258/2000 Sb., Zákon o chemických látkách a chemických přípravcích č. 356/2003 Sb., Zákon o odpadech č. 185/2001 Sb., Zákon o požární ochraně č. 133/1985 Sb., Zákon o vodách č. 245/2001 Sb., Zákon o životním prostředí č. 17/1992 Sb., ve znění pozdějších předpisů a v souladu se stanoviskem Úřadu pro ochranu osobních údajů č. 1/2013". Směrnice CAA/S-SLS-010-1/2012 - Postupy pro vydání povolení k létání letadla bez pilota na palubě.

7. Závěr - návrh dalších postupů

Předpokládaná budoucnost postupů pro řešení kritické infrastruktury EU je zavedení několika projektů řešících jednotlivé dílčí disciplíny této ochrany. Pro správné identifikování těchto projektů a jejich zavedení do praxe je zapotřebí jednak vytvoření správného projektového prostředí a použití náležitého nástroje na vyhledávání nových projektů.

7.1. Projektové prostředí

Projektové prostředí představuje posloupnost určitých fází představující životní cyklus projektu. Jedná se o následující fáze:

- investiční fáze
- provozní fáze
- ukončení projektu

7.1.1. Investiční fáze

Jedná se o první fázi, která zahrnuje činnosti předcházející vlastnímu projektu. Tyto činnosti zahrnují zejména finanční a právní přípravu pro naplnění základních cílů daného projektu. Základním cílem této fáze je analýza finančních možností projektu z hlediska jeho zadavatele a posouzení jeho rizikovosti. Podle druhu projektu pak tato fáze může zahrnovat marketingové studie, zpracování projektových dokumentací, realizace potřebných úkonů před spuštěním projektu apod.

7.1.2. Provozní fáze

Druhá fáze životního cyklu projektu představuje vlastní provoz. Tento provoz by měl být posouzen z krátkodobého a dlouhodobého pohledu. Krátkodobý pohled představuje zejména posouzení s kvalitativním a kvantitativním naplněním daného projektu, tedy např. dostatečná, nebo předimenzovaná kapacita, způsob výroby apod. Dlouhodobý pohled pak představuje posouzení naplnění hlavního cíle projektu z hlediska celkové strategie a ekonomických výsledků.

7.1.3. Ukončení projektu

Poslední z fází životního cyklu projektu představuje činnosti spojené s jeho ukončením. Opět v závislosti na druhu projektu tyto činnosti mohou představovat rozprodej strojů, likvidaci zařízení a budov, úpravu pozemků pro další využití apod. Fáze ukončení projektu může pro zadavatele projektu také představovat určitou formu zisku při prodeji movitého a nemovitého majetku. Ve většině případů však náklady na likvidaci projektu převyšují příjmy z likvidace.

7.2. Marketingové prostředky pro vyhledávání nových projektů

Projekty představují velice důležitou část života firem a vědeckovýzkumných institucí. Z tohoto důvodu je nutné neustále vyhledávat příležitosti pro možnost vytvoření, nebo zapojení do nějakého projektu. Marketingové prostředky pak představují jednotlivé nástroje, které slouží k vyhledávání a následnému posouzení možností pro vznik nového projektu. Tyto nástroje pocházejí zejména z teorie managementu a jsou běžné používány i pro další aktivity v rámci marketingové činnosti firmy. Základním nástrojem pro identifikaci pak může sloužit např. matice TOWS, která představuje posouzení ohrožení (Threats), příležitostí (Opportunities), slabých stránek (Weaknesses) a silných stránek (Strengths). Tato analýza ve většině případů navazuje na analýzu slabých a silných stránek, příležitostí a ohrožení známou jako analýza SWOT.

Výsledkem takovýchto analýz je pak selekce projektů na ty, pro které by měla být věnována další pozornost a posouzení jejich efektivity, a na ty projekty, které jsou z ekonomického hlediska nevýhodné, nebo pro provoz příliš rizikové.

7.3. Jednotlivé projekty a jejich definování

Jednotlivé projekty je nutné zaměřit na vlastní řešení ochrany kritické infrastruktury EU. Z tohoto důvodu se v současné době předpokládá vznik projektů zejména v následujících oblastech:

- **Návrh postupů pro certifikace** – projekt zahrnující úpravu postupů pro certifikaci jednotlivých systémů zabezpečujících ochranu před protiprávními činy.

- **Návrh standardizace procesů** – projekt na vytvoření standardizace procesů pro zajištění ochrany civilního letectví.

- **Návrh protokolů standardizace** – projekt na vytvoření nových a efektivnějších protokolů jako výsledků standardizačních procesů, který umožní jejich lepší archivaci a přehlednost v procesu ochrany. Dílčím cílem projektu je také unifikace podoby těchto formulářů v celém odvětví letecké dopravy.

- **Lidský činitel** – projekt zahrnující vliv lidského činitele na ochranu civilního letectví před protiprávními činy. Výsledkem tohoto projektu bude začlenění problematiky zkoumání lidského činitele do výcvikových programů těch pracovníků, kteří mají přímý vliv na úroveň a efektivitu provádění vlastní ochrany.

- **ATSKC (Air Transport Security Knowledge Centre)** – projekt na vytvoření integrovaného znalostního centra pro oblast Security v letecké dopravě, jako institucionální základna pro efektivnější sdílení úplných a aktuálních informací ve vysoce regulovaném, komplexním a rizikovém odvětví ochrany před protiprávními činy v civilním letectví. Přínosem kooperace se spolupracujícími subjekty bude nejen zefektivnění vynakládaných investic jednotlivých institucí a zabránění duplicitních činností, ale rovněž vytvoření kolektivního hlasu při řešení otázek souvisejícím s předmětnou oblastí.

- **Měření výkonnosti bezpečnostních prostředků využívaných při ochraně KI** – *b*ezpečnostní technické prostředky (systém, zařízení) jsou jednou ze složek bezpečnostního opatření[12]. Pro účinné zajištění výsledného bezpečnostního opatření je proto nezbytné, aby též bezpečnostní prostředky v čase prokazovaly svou dostatečnou výkonnost (efektivnost). Vzhledem k rozmanitosti těchto prostředků, které často mají různé řídící protokoly pro elektronické ovládání a kontrolu, není vždy jednoduché požadované informace účelně shromažďovat pro následnou analýzu. Technologie umožňující (integrované?) měření výkonnosti

[12] Bezpečnostní opatření – soubor postupů a lidských a materiálních (technických) prostředků, které lze ve vzájemné kombinaci použít za účelem ochrany (civilního letectví před protiprávními činy)

odlišných bezpečnostních prostředků může výrazně přispět k systémovější a věcnější zpětné vazbě při zajišťování ochrany (nejen) KI.

- **Jednotný manažerský přístup k ochraně KI** - *p*rojekt na definování jednotného manažerského nástroje v ochraně KI obsahující všechny komponenty (viz kap. 4.2) by bylo možno aplikovat bez ohledu na typ KI[13] a rozsah dalších zákonných nebo jiných bezpečnostních požadavků. Případná normalizace (soubor norem) by umožňovala i následnou certifikaci akreditovanou autoritou. Tento přístup by též zajistil účinnější a ekonomičtější dohled mezinárodních a národních dozorových autorit. V tomto kontextu je vhodné zmínit, že v současné době je připravován soubor norem zabývající se fyzickou ochranou prvku KI[14] (tedy pouze jeden z komponentů; viz kap. 4.2).

8. Závěr

Z obsahu kapitol je zřejmé, že vzdušný prostor ČR je součástí kritické infrastruktury, který může být také objektem, kyberútoků. Oblasti eventuálního napadání kyberútoky lze rozdělit na oblasti fyzické bezpečnosti, komunikační bezpečnosti a ochrany kritické infrastruktury. Z obsahu kapitol je zřejmě, že je legislativně pokryta v rámci evropské legislativy. Implementace bezpečnostních standardů a postupů je rovněž legislativně pokryta v rámci EU, včetně procesu certifikace systémů ochrany civilního letectví před protiprávními činy, např. SeMS a je tedy otázkou, zda je tento komformní systém jedinečný pro civilní letectví, nebo je aplikovatelný v dalších oblastech ochrany kritické infrastruktury proti kyberútokům.

[13] Typy KI – např. energetika, komunikační a informační systémy, vodní hospodářství
[14] ČSN P 73 4450 - Fyzická ochrana prvku kritické infrastruktury (stav k 11/2013)

Příloha: Projekt: Vývoj a realizace bezpilotního prostředku (UAV) střední velikosti s hybridním pohonem

III A. VLASTNÍ PROJEKT[15]	
1.	**Charakteristika řešeného problému**
	a) Stručný popis problému *(uveďte důvody projektového řešení):* Intenzivní rozvoj a používání bezpilotních prostředků všech výkonových a rozměrových kategorií klade vysoké nároky na spolehlivost všech prvků prostředku nevyjímaje pohonný systém. Intenzivní vývoj a důsledné testování všech potřebných komponent pohonu UAV umožňuje postupně zvyšovat jeho výkonové parametry jako je dolet, vytrvalost letu, užitečné zatížení a současně snižovat hlučnost a tepelnou stopu prostředku v zájmovém prostoru. Současně je nezbytné zvyšovat spolehlivost celého kompletu tvořícího UAV a tím zvyšovat jeho užitnou hodnotu.
	b) Předmět řešení *(uveďte co se bude konkrétně řešit):* Předmětem řešení projektu je navrhnout, vyrobit, otestovat a letovými zkouškami ověřit hybridní pohonnou jednotku tvořenou maloobjemovým spalovacím motorem a třífázovým generátorem pro pohon UAV. Pro její ověření je nutné současně navrhnout a vyrobit vlastní nosič, který bude realizovaný modelem UAV (hmotnost 20 kg).
	c) Výchozí stav *(uveďte současný stav, který se má změnit řešením projektu):* V současné době je na UO v Brně na K-204 úspěšně odzkoušený model UAV s elektrickým čtyřmotorovým vrtulovým pohonem, který byl řešený v rámci projektu POV – Záznam II, EA 1821 v letech 2001-2005. Kontinuální pokračování tohoto projektu mělo vyústit ve vývoj hybridní pohonné jednotky pro menší UAV. Personálními změnami na UO v Brně došlo k odložení realizace tohoto záměru vývoje nové hybridní pohonné jednotky pro UAV do dnešní doby. Jedná se o nestandardní konstrukční řešení, které umožňuje dosažení podstatně vyšší spolehlivosti celé PJ při její dostatečně nízké hlučnosti, která zanechává tepelnou

[15] Ve formulářové části III A. Vlastní projekt uveďte **hlavní** charakteristiky návrhu projektu. Projekt **podrobně** popište a rozveďte v následující části III B.

	stopu o nízké intenzitě čímž znesnadňuje sledování UAV nepřátelskými prostředky.	
2.	Současný stav řešení problému ve světě: Navrhovaný systém hybridní pohonné jednotky „spalovací motor – el. generátor" zažívá v současné době dynamický rozvoj především v osobní automobilové technice. **Jeho použití v podobě miniaturizované pohonné jednotky určené k pohonu menších UAV není známo.**	
3.	**Cíl projektu[16]**	
	a)	**Základní cíle projektu je možné shrnout následovně:** **1) Navrhnout, realizovat, v aerodynamickém tunelu ověřit a následně letovými zkouškami odzkoušet model vrtulového UAV (o hmotnosti 20 kg) s nainstalovanou hybridní pohonnou jednotkou.** **2) Navrhnout, vyrobit, na motorové zkušebně odzkoušet, provézt dlouhodobé testy a následně zainstalovat novou hybridní pohonnou jednotku do modelu UAV.** **3) Navrhnout, vyrobit a otestovat elektronické prvky výkonové části a regulace hybridní pohonné jednoty**

[16] V části a) uveďte cíl projektu v českém jazyce, v části b) v anglickém jazyce.

	b)	**1) The aim is to design, to produce, to verify in wind tunnel and to prove the propeller driven UAV model by the flight tests (weighing 20 kg) with an installed hybrid power unit.** **2) The aim is to design, to manufacture, to test and to conduct a long-term test of the new hybrid drive unit and subsequently to install the unit into the UAV model.** **3) The aim is to design, to manufacture and to test electronic components and controls of the hybrid propulsion unit.**
4.	Způsob řešení projektu *(stručně uveďte metody řešení):* 1) Pro úspěšné vyřešení projektu je nutné provézt návrh modelu UAV včetně všech aerodynamických výpočtů. 2) Provézt návrh a v AT změřit aerodynamické charakteristiky předpokládaných vrtulí pro UAV. 3) Navrhnout, konstrukčně modifikovat, odzkoušet a změřit výkonové parametry vhodného dvoutaktního maloobjemového spalovacího motoru. 4) Navrhnout, vyrobit a odzkoušet vhodný generátor pro spalovací motor. 5) Realizovat dodavatelským způsobem výrobu a montáž modelu UAV a celého kompletu hybridní pohonné jednotky. Provézt ověření parametrů celého systému UAV – hybridní PJ letovými zkouškami.	
5.	Časový postup řešení a konkrétní druhy výstupů v jednotlivých letech řešení: 1) 1. rok – Navrhnout model UAV a provézt základní aerodynamické výpočty. Navrhnout konstrukční úpravy spalovacího motoru. Navrhnout vhodný typ generátoru. Navrhnout elektronické prvky systému. 2) 2. rok – Realizovat výrobu modelu UAV, úpravy spalovacího motoru a realizovat výrobu vhodného typu generátoru pro laboratorní zkoušky. 3) 3. rok – dokončit laboratorní zkoušky jednotlivých komponent	

	hybridního pohonu a sestavit je do finální podoby hybridní pohonné jednotky (HPJ). Provézt výkonové zkoušky celého hybridního pohonu (hmot. 4,5 kg , 1,6 - 2,2kW/36-48V) a nainstalovat HPJ do nosiče – modelu UAV. 4) 4. rok – Letovými zkouškami ověřit výkonové parametry modelu UAV s hybridní pohonnou jednotkou.
6.	Očekávané výsledky řešení a jejich přínos pro teorii a praxi obrany státu *(uveďte výsledek a jeho přínos):* 1) Měřením parametrů vrtulových hybridních pohonných jednotek UAV připravit databázi aerodynamických charakteristik a technických podkladů pro jejich návrh a výrobu u externích dodavatelů tak, aby byly aktivně využitelné v projektu budování AČR „Voják 21 –tého století“ 2) Vyvinout a odzkoušet lehkou, mobilní hybridní pohonnou jednotku vhodnou pro pohon UAV. 3) Rozšířit a doplnit experimentální základnu na UO v Brně v oblasti návrhu, zkoušení, měření a realizací menších modelů bezpilotních prostředků (přibl. do 20 kg). 4) Zpřesnění a ověření numerických výpočtů při simulacích enegetických bilancí a letových výkonů v modelech UAV. 5) Výchova nových vědecko pedagogických pracovníků v oboru hybridních pohonů, aplikované průmyslové aerodynamiky, mechaniky letu, měření v letecké a raketové technice. 6) Zvýší se kvalitativní úroveň a kapacita zkušební základny UO v oblasti alternativních mobilních zdrojů elektrické energie a v oblasti průmyslové experimentální aerodynamiky.
7.	Předpokládaný způsob realizace výsledků projektu, popřípadě jejich uživatel*:* 1) Výrobní instituce získají přístup k reálným aerodynamickým

	podkladům pro návrh a výrobu nových UAV s vrtulovými PJ jak s klasickým, tak i hybridním pohonem. 2) Uživatelé získají podklady pro realizaci hybridní pohonné jednotky i v neleteckých aplikacích. 3) Předpokládá se, že výsledky z realizace modelu UAV s hybridní pohonnou jednotkou zvýší (díky kombinované PJ) jejich spolehlivost a tím i zvýší jejich použitelnost.
8.	Rizika řešení problému *(uveďte rizika věcná, finanční, personální, z oblasti řízení, spolupráce a utajení):* 1) Opožděný přístup k přiděleným finančním prostředkům a tím i zpoždění při výrobě a zkoušení jednotlivých komponent celého systému u externích komerčních dodavatelů. 2) Personální změny v řešitelském týmů v důsledků redukce pracovních míst na UO. Zásadní změna v redislokaci školy a jeho pracovišť-zkušební základna je vybudovaná v KČP 29 a KČP 19.

9. VLASTNÍ PROJEKT[17]

a) **charakteristika řešeného problému** (popis problému, předmět řešení, výchozí stav, výchozí podklady a omezující údaje pro řešení)

Popis problému:

Zkoušení, měření a testování vyvíjených zařízení tvoří nedílnou součást vývoje nových prostředků.

V současné době dochází k masivnímu vývoji a postupnému nasazování nejrůznějších typů bezpilotních prostředků. Jejich letové výkony, vnější rozměry,

[17] Část III B. Vlastní projekt uveďte **volnou formou** v doporučeném rozsahu 5 - 15 stran a v pořadí kapitol podle osnovy.

užitečné zatížení a úkoly na ně kladené jsou velmi rozmanité a odpovídají účelu jejich nasazení a použití.

Pro plnění požadovaných úkolů je nutné správně stanovit a navrhnout jejich pohonnou část. **U dnes používaných malých a středních velikostí UAV převládají vrtulové pohonné jednotky se spalovacími motorem**, resp. pohonné jednotky tvořené elektromotorem s vrtulí. V případě pohonu UAV s pístovým vrtulovým pohonem se jedná převážně o jednomotorovou koncepci, neboť vícemotorové jednotky nejsou vzhledem k rozměrům a hmotnostem UAV nutné. **Spolehlivost** tohoto typu pohonu **UAV je limitována spolehlivostí pístového motoru**. V případě jakékoliv poruchy na tomto pohonném agregátu dochází k přerušení plnění požadovaného úkolu a přechod do nouzového režimu, který většinou končí částečným poškozením při přistání**. Pokud se zařízení nachází nad nezabezpečenou oblastí hrozí ztráta celého UAV**. Velkou výhodou hybridního typu pohonu je jeho vyšší spolehlivost, dostatečná vytrvalost letu UAV, která u tohoto typu pohonu dosahuje několika hodin.

Při realizaci pohonné jednotky UAV tvořené elektromotorem s vrtulí lze **zvýšit její provozní spolehlivost vícemotorovou koncepcí** viz. projekt POV 2001-2005 s názvem ZÁZNAM II, poškození cíle EA-1821, která umožňuje **rekonfigurovatelnost** pohonného systému za letu. Vlastní elektrický pohon je funkčně jednoduchý a nenáročný na provoz a při vícemotorovém uspořádání pohonné jednotky UAV je jeho spolehlivost pro plnění úkolu výrazně vyšší než u jednomotorové koncepce.

Výrazným omezením vrtulové pohonné jednotky poháněné elektromotorem je množství energie uložené v pohonných bateriích, které zásadním způsobem omezuje dobu použití elektrického pohonu na max. desítky minut letu UAV. Nespornou výhodou je u tohoto typu pohonu naopak nízká hlučnost, která je nesrovnatelně nižší než u použití spalovacího motoru. Absence jakékoliv tepelné stopy za UAV s elektrickým pohonem je dalším významným pozitivem tohoto typu pohonu.

Logickým řešením, které odstraňuje nevýhody obou výše zmíněných typů pohonu UAV je pohon hybridní, tvořený pístovým motorem a generátorem. UAV s tímto typem pohonu mohou dosahovat několikahodinových dob letu při celkově **vysoké spolehlivosti pohonu**, která je dána vícemotorovým za letu **rekonfigurovatelným** elektrickým vrtulovým pohonem. Významnou výhodou tohoto koncepčního řešení pohonu UAV je téměř „bezhlučný provoz“ v zájmové oblasti, kdy hybridní systém pohonu přechází do tzv. tichého režimu „SILENCE MODE“. V tomto

režimu pracuje spalovací motor ve volnoběžných otáčkách resp.je vypnutý a energie pro pohon prostředku je spotřebovávána pouze z vnitřních baterií. Množství energie akumulované v těchto zdrojích umožňuje zásobovat pohon UAV energií po dobu několika minut. Zvýšení resp. snížení této doby je řešeno modulárním připojováním, odebíráním bateriových modulů, které je závislé na plněném úkolu.

Použití hybridního pohonu UAV – spalovací motor-generátor a vícemotorová elektrovrtulová pohonná jednotka **výrazně zvýšuje spolehlivost celého kompletu** tvořícího pohon UAV a tím i jeho užitnou hodnotu.

Předmět řešení:

Předmětem řešení je návrh, výroba, testování a zprovoznění modelu **UAV střední velikosti** (**rozpětí 4,4 m o hmotnosti 20 kg s vytrvalostí letu >5 hodin**), který bude poháněný nově vyvinutým hybridním pohonným systémem.

Novým typem pohonu UAV je myšlená hybridní pohonná jednotka (HPJ), která je tvořena dvoutaktním spalovacím motorem, třífázovým generátorem, pohonnými elektromotory s vrtulemi, výkonovou a řídící elektronickou částí pohonu, palivovou soustavou a bateriovými zásobníky energie.

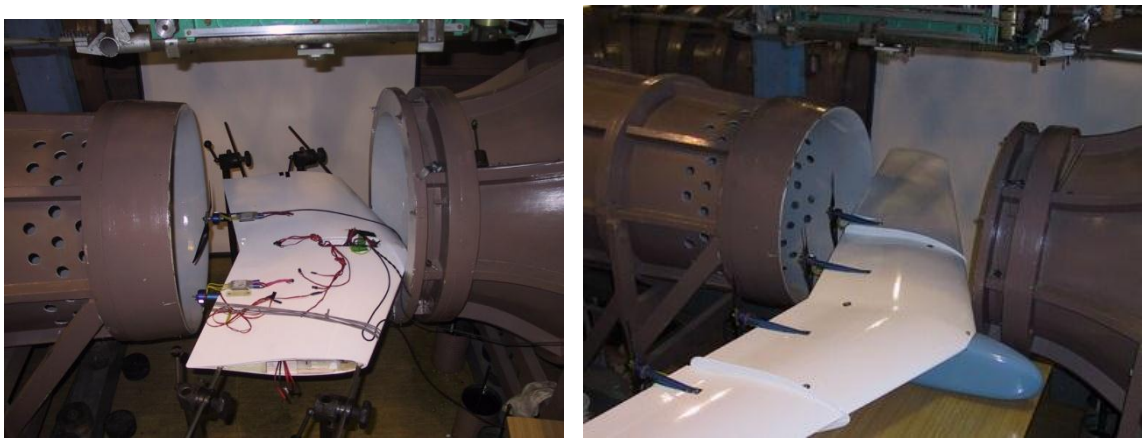
Pro zajištění letových zkoušek, nezbytných pro reálné zkoušení hybridní pohonné jednotky, je nutné modifikovat a vyrobit nosič větší model UAV – FW-44 o celkovém rozpětí přibl. 4,5 m a hmotnosti přibl. 20 kg (v projektu ZÁZNAM II, zasažení cíle, EA-1821, řešený jako POV v letech 2001-2005 byl navržený a letovými zkouškami ověřený menší nosič FW-26 o rozpětí 2,6 m a hmotnost 9 kg s čistě elektrickým čtyřmotorovým vrtulovým pohonem).

Výchozí stav:

V rámci řešení projektu POV v letech 2001-2005 s názvem ZÁZNAM II, poškození cíle., úkol EA-1821 byla odzkoušena verze nosiče – modelu UAV s označením FW-26, která byla po letových zkouškách (bez poškození) vystavována na mezinárodním veletrhu vojenské techniky IDET 2005 a 2007. Na základě úspěšného oponentního řízení projektu ZÁZNAM II v 9/2005 a ohlasů z řad odborné veřejnosti a to jak účastníků, tak i návštěvníků veletrhu bylo na katedře K-204, UO v Brně přijato rozhodnutí o pokračování ve vývoji tohoto typu modelu UAV a jeho nového- hybridního typu pohonu.

Pro úspěšné zvládnutí navrhovaného projektu je na pracovišti UO v Brně, K-204 k dispozici erudovaný tým odborníků, široká, velmi moderní laboratorní základna s nově vybudovanými zkušebními zařízeními na zkoušení a měření aerodynamických charakteristik vrtulí a celých vrtulových pohonných jednotek viz. obr. 1 až 4 a dostatečné zkušenosti pro úspěšné zvládnutí tohoto nově navrhovaného projektu.

Obr. 1 Měření výkonových parametrů vrtulové pohonné jednotky pro bezpilotní prostředky. Vlevo pohonná jednotka tvořená dvoutaktním spalovacím motorem a vrtulí, vpravo pohonná jednotka tvořená elektromotorem a vrtulí.



Obr. 2 Zkoušení a měření výkonových parametrů pohonné jednotky modelu UAV. Ukázka z měření a testování vrtulového pohonu pro FW-26 po její instalaci do nosiče a ověřování jejích skutečných parametrů před letovými zkouškami.

Obr. 3 Úspěšně vyprojektovaný, letovými zkouškami odzkoušený model UAV ozn. FW-26, řešený v rámci projektu ZÁZNAM II, poškození cíle., úkol EA-1821.

Obr.4 Záznam z letových zkoušek modelu FW-26 na letecké základně Přerov.

b) **Úroveň řešení problému** (podrobně se rozvede současný stav řešení problému ve světě)

Navrhovaný typ modelu UAV – vícemotorové samokřídlo, jeho konstrukční řešení, způsob ovládání a zkoušení spadá do oblasti sice méně častých konstrukčních uspořádání, ale nepředstavuje neznámou oblast. Jedná se o koncepci konstrukčního uspořádání, které byly velmi intenzivně testovány v minulosti především **v Německu (Horten I-IX) a USA (B2).** Přes své nesporné výhody v podobě celkové výrazně menší energetické náročnosti pro vlastní let a tím i zvýšení celkového doletu a vytrvalosti letu je toto konstrukční řešení UAV méně časté zejména z důvodu vyšší vzletové a přistávací rychlosti a menšího rozsahu polohy centráže letounu. Pro plnění těch úkolů, kdy je prvořadým požadavkem dolet a vytrvalost, obtížné sledování letounu ze země a mise má

především monitorovací a průzkumný charakter, je uvedené konstrukční řešení naopak velmi výhodné.

Navrhovaný systém hybridní pohonné jednotky „spalovací motor – el. generátor“ zažívá v současné době dynamický rozvoj především v pohonech v osobní automobilové technice. Většina světových výrobců vozidel se snaží představit své hybridní vozidlo, které disponuje nižší spotřebou a sníženou úrovně emisí. Tyto přednosti, klíčové v automobilní technice, nejsou pro pohon UAV prioritní a využitelné. Použití miniaturizované hybridní pohonné jednotky pro pohon UAV ve světě není známo. Námi navrhované řešení např. umožňuje na rozdíl od pohonu UAV s pístovým motorem snížit hmotnost nesených bateriových akumulátorů, které napájejí řídící a komunikační prostředky daného UAV. Námi navrhovaná hybridní pohonná jednotka pro UAV částečně nahrazuje i komplexní palubní energetický zdroj.

c) **Očekávané výsledky řešení a jejich přínos pro teorii a praxi obrany státu**

Realizací předloženého projektu vznikne databáze technických podkladů nezbytných pro návrh, výrobu a provozování vrtulových UAV v AČR tak, aby byly aktivně využitelné v projektu budování AČR „Voják 21 –tého století“. Pro návrh, vývoj a provozování všech typů vrtulových UAV představují znalosti aerodynamických charakteristik pohonné jednotky vrtule – spalovací motor resp. elektromotor nepostradatelné podklady, bez kterých nelze stanovit letové výkony, dolet ani vytrvalost letu daného UAV.

Letovými zkouškami dojde k verifikaci tohoto nestandardního koncepčního uspořádání nosné plochy UAV, které vícemotorové samokřídlo s hybridní pohonnou jednotkou představuje.

Letovými zkouškami se dosáhne zpřesnění numerických modelů UAV a software pro výpočet letových výkonů, doletu a vytrvalosti.

Vznikne lehká a výkonná (celk. hmot. přibl 5,5 kg s výkonem 1,6-2,2 kW/ 36-48V) kompaktní hybridní pohonná jednotka pro pohon UAV, kterou bude možné po úpravách využít i jako mobilní energetickou jednotku u dalších složek AČR.

Zvýší se kvalitativní úroveň a kapacita zkušební základny Katedry letecké a raketové techniky, Katedry elektrotechniky a Katedry komunikačních a informačních

systémů UO Brno v oblasti telemetrického přenosu informací, alternativních mobilních zdrojů elektrické energie a v oblasti průmyslové experimentální aerodynamiky.

Zkvalitní se příprava nových vědecko pedagogických pracovníků UO v oboru hybridních pohonů, aplikované průmyslové aerodynamiky, mechaniky letu, měření v letecké a raketové technice.

Výrazně se zvýší znalosti, odborná úroveň a praktické zkušenosti řešitele - vědecko pedagogických pracovníků řešitelských kateder, UO Brno.

d) **Předpokládaný způsob realizace výsledků projektu, případná specifikace jejich uživatelů** (uvede se konečná realizace výsledků projektu)

Způsob, jakým budou výsledky realizovány je již naznačený v předchozí části. Modernizace a dobudování zkušební základny bude sloužit prioritně k řešení vojenských požadavků resortu.

Znalosti získané z řešení hybridní mobilní pohonné jednotky, měření aerodynamických charakteristik vrtulí, aerodynamických a pevnostních výpočtů nosiče – modelu UAV budou aktivně využívané při praktických ukázkách ve výuce studentů – vojenských profesionálů, při odborných školeních a zdokonalovacích kurzech ostatních složek AČR.

Další významný způsob realizace výsledků z měření a zkoušení nosiče-modelu UAV s hybridní pohonnou jednotkou bude publikační činnost pracovníků UO v odborných vojenských i civilních periodikách a na vojenských vědeckých konferencích doma i v zahraničí.

Předpokládá se, že praktické výsledky z měření a zkoušení modelu UAV s hybridní pohonnou jednotkou budou využívány ve výuce studentů univerzity obrany a to jak v bakalářském, tak i v magisterském a doktorském studijním programu.

Realizace nejrůznějších úkolů ve prospěch AČR umožní těsnější vazbu mezi UO a ostatními útvary AČR při zabezpečování širokého spektra úkolů, které jsou na AČR kladeny.

Navrhovaný projekt „**Vývoj a realizace modelu UAV s hybridním pohonem**“ je zaměřený na návrh, realizaci a letovými zkouškami ověření nosiče-modelu UAV s koncepčním uspořádáním nosné plochy typu samokřídlo s hybridní pohonnou jednotkou (HPJ). Touto HPJ se rozumí systém složený s dvoutaktního spalovacího

motoru s generátorem, který vyrábí elektrickou energii pro hlavní pohon modelu UAV. Vlastní pohon UAV je realizovaný vícemotorovou elektromotory poháněnou vrtulovou pohonnou jednotku, která je paralelně s dalšími palubními zařízeními modelu UAV napájena přes záložní baterie z hlavní palubní energetické jednotky tj. spalovací motor-generátor.

Pro úspěšné řešení projektu je nutné upravit a doplnit budovaná specializovaná zkušební zařízení na zkoušení výkonových i řídících prvků elektropohonů a měření aerodynamických charakteristik vrtulových pohonných jednotek v aerodynamickém tunelu.

Realizace projektu umožní aktivní zapojení UO do řešení rezortních úkolů v oblasti hybridních pohonů, zkoušení a testování částí letecké techniky a umožní tím rozvinout spolupráci s tuzemskými i zahraničními odbornými pracovišti.

e) **Předpokládané přínosy** projektu v 1. až 5. roce po ukončení řešení projektu, jak se projeví u příjemce, u jednotlivých dalších účastníků projektu, popř. u uživatelů výsledků projektu (vyplnění této části není povinné)

Realizace projektu umožní aktivní zapojení UO a její odborných kateder do řešení dílčích úkolů v rámci projektu AČR „Voják 21-tého století“ v oblasti návrhu, vývoje a používání malých UAV s hybridním pohonem.

Uživatel výsledků projektu získá prostředek-nosič využitelný ve vojenských misích pro dlouhodobé monitorování zájmové oblasti, v civilním použití půjde o monitorování při dopravních zácpách ve městech a na klíčových dálničních komunikacích, při živelných pohromách – lesní požáry, záplavy rozsáhlých území, monitorování pohybu osob a techniky v oblastech umístění strategických energetických zásob, přenosových soustav, státní hranice atd.

PŘÍLOHA 1. – PRINCIPY A PERSPEKTIVY KYBERNETICKÉ BEZPEČNOSTI ČR Z PRÁVNÍHO HLEDISKA

Doc. JUDr. Radim Polčák, PhD.

1. POJEM KYBERNETICKÉ BEZPEČNOSTI

Kybernetická bezpečnost představuje originální právní problém, jehož řešení nemůže být předmětem standardních regulatorních postupů. Sama o sobě je kybernetická bezpečnost fiktivním právním fenoménem, který reálně neexistuje – kybernetika, informatika nebo bezpečnostní studia totiž sice pracují s pojmy jako počítačová bezpečnost, informační bezpečnost či síťová bezpečnost, avšak pojem kybernetické bezpečnosti doposud nemá technických ani společenskovědních definic či oborových kritérií. To ale samozřejmě neznamená, že není důvod se tímto pojmem zabývat. Byl totiž vytvořen jako právní konstrukt právě kvůli praktické potřebě pojmově vymezit kombinaci technických, organizačních a právních opatření, jejichž primárním cílem je zajištění bezpečnosti informační a komunikační infrastruktury.

Označení této problematiky tvořící relativně nový podobor práva informačních a komunikačních technologií specifickým a v jiných disciplínách doposud nepoužívaným pojmem má svůj evidentní význam především v tom, že žádný z doposud užívaných pojmů nevystihuje na jedné straně komplexní charakter předmětného problému při současném zúžení jeho materie specificky na problematiku informačních sítí resp. informačních systémů majících pro tyto sítě zásadní význam. Současně je pojmem kybernetická bezpečnost zdůrazněna též zájmová úroveň závažnosti objektu právní regulace, přičemž se věcná působnost příslušných právních pravidel a mandatorních technických opatření omezuje pouze na otázky mající význam vzhledem k veřejnému zájmu na fungování informační společnosti.

V případě užívání pojmu informační nebo počítačové bezpečnosti by bylo vždy třeba zdůraznit, že předmětná právní úprava (zejm. povinnosti plynoucí soukromoprávním subjektům) omezuje se na jedné straně výlučně na otázky infrastrukturní, jejichž řešení je ve veřejném zájmu. Rovněž by bylo třeba vždy zdůrazňovat, že se netýká pouze technických záležitostí, ale řeší též souvislosti organizační a společenské. Nemělo by pak zřejmě valného smyslu psát příkladně zákon

o počítačové bezpečnosti, v jehož úvodních ustanoveních by muselo být opakovaně zdůrazněno, že se z oboru počítačové bezpečnosti dotýká jen jeho malé části a naopak, že řeší řadu otázek, které s počítačovou bezpečností vůbec nesouvisejí.

Skutečnost, že pojem kybernetické bezpečnosti byl vytvořen pro potřeby založení specifické formy právní regulace, odráží se též ve výběru adekvátní regulační metody.

2. METODOLOGIE PRÁVA KYBERNETICKÉ BEZPEČNOSTI

Obecně lze v právním instrumentariu nalézt tři typy právních metod, a to metody pozitivistické, naturalistické a realistické (či pragmatické). Pozitivistické metody vyznačují se, stručně řečeno, oddělením pravidel od faktických informací . Znamená to mimo jiné, že pravidlo nemůže svým obsahem vycházet z faktické informace (výroku), ale je vždy vytvořeno jako originální informace. Fakticita se tedy v obsahu pravidel nijak neprojevuje a s fakty pracujeme pouze jako s faktory naplnění subsumpčních podmínek . Jinak řečeno je tedy v tomto metodologickém pojetí právo systémem originálně tvořených povinnostních informací – fakta jsou pro právo důležitá pouze co do rozhodování v otázce, zda právo pro konkrétní situace formuluje nějaká práva, povinnosti či dovolení (tj. v otázce, zda jsou ad hoc naplněny znaky hypotéz příslušných právních norem).

Obecně se oddělení faktických a povinnostních informací u právního pozitivismu projevuje absencí vztahu mezi právem a morálkou . Morálka jako faktická kategorie totiž nemůže v pozitivistickém pojetí práva ovlivňovat obsah právních pravidel . To samozřejmě neznamená, že právní pravidla musí být nutně amorální – jejich konstrukci ani aplikaci však morálka přímo neovlivňuje. V oboru práva informačních a komunikačních technologií se základní motiv pozitivistické metodologie projevuje neexistencí přímého vztahu mezi faktickou situací určité technologie (tj. jejími parametry, fungováním apod.) a obsahem právních pravidel regulujících její užití. Důsledná aplikace pozitivistické metodologie v tomto směru může vést k takovým důsledkům, kdy je právně formulován právně perfektní (bezvadný) takový právní předpis nebo takové soudní rozhodnutí, jejichž praktická aplikace je z nějakého praktického důvodu vyloučena – k tomu může dojít tehdy, jsou-li např. stanoveny nereálné požadavky na nějakou technologii, právo požaduje řešení, které téměř nelze organizačně zvládnout nebo je vyžadováno splnění takové povinnosti, která je z ekonomického hlediska absurdní. Z právě uvedeného plyne, že užití této metody k řešení problému kybernetické bezpečnosti není vhodné.

Druhou možností je naturalistická právní metodologie postavená ve vztahu k pozitivismu na zcela opačné tezi spojení faktických a povinnostních informací. Obecnou implikací této teze je možnost přímého dovození právních pravidel z morálky a jí odpovídající předpoklad, že objektivní právo je jen konstatováním existence přirozených pravidel (de facto přírodních zákonů) a že právotvorba není ve skutečnosti o originárním vytváření právních pravidel ale pouze o jejich nalézání. Aplikace naturalistické metodologie v právu informačních a komunikačních technologií vede k závěru formulovaného předním americkým konstitucionalistou Lawrencem Lessigem do postulátu, že totiž „kód je zákonem kyberprostoru. " Znamená to, že právo pro informační síť je resp. má být pouze dovozováno z technických pravidel definujících možnosti chování uživatele. Lessigem popsaná situace již v řadě situací reálně funguje. Především v případech, kdy brání uplatnění práva některý z právních nebo přirozených limitů (tj. např. otázka jurisdikce, absence věcné působnosti, vysoké náklady na výkon práva apod.), je kód skutečně dominantním normativním faktorem ovlivňujícím, často výlučně, chování uživatelů.

Z právě popsaného důvodu nelze s iusnaturalistickou metodologií pracovat pro potřeby řešení problému kybernetické bezpečnosti. Přijetí tohoto přístupu by totiž v prostředí informačních sítí znamenalo popření základní premisy, na níž stojí v současnosti legitimita práva, tj. že právo je legitimováno veřejným zájmem vyjádřeným prostřednictvím instituce státu. Iusnaturalistické pojetí přitom přisuzuje možnost definovat obsah právních pravidel subjektům majícím pod kontrolou technické parametry příslušných součástí informační sítě, z nichž většinou jde o soukromoprávní korporace.

Nikoli jen vylučovací metodou jeví se jako nejvhodnější k řešení problému kybernetické bezpečnosti metoda realistická . Je postavena na podobném předpokladu jako právní pozitivismus, tj. že obsah právních pravidel je originárně vytvářen a je zajišťován autoritou státu, avšak netrvá na důsledném oddělení právních pravidel od faktických informací. Zohlednění fakticity, ať technické, ekonomické nebo organizační, má formu omezení legislativních a aplikační výstupů o ty, které jsou, stručně řečeno, buďto objektivně nebo prakticky neproveditelné . Pragmatický zákon tedy počítá jen s takovými povinnostmi, které je reálně možno splnit bez větší zátěže pro povinné subjekty a soudní rozhodnutí je založeno na předpokladu reálné (nikoli ideální) společenské, technické a ekonomické situace.

Zřejmá nevýhoda realistické metodologie spočívá především v riziku relativizace právních hodnot a principů, neboť tam, kde se jejich důsledná aplikace odchyluje od toho, co považujeme za součást technické, společenské nebo ekonomické reality, prostě od nich ustoupíme. To může vést k Dworkinem kritizovanému postupnému úbytku ideálů a nebezpečí tvorby situací, kdy právo jen kopíruje požadavky ekonomické, technické nebo obecně společenské reality resp. toho, co je za realitu aktuálně považováno politickou mocí. Na druhou stranu však realistická metodologie poskytuje jako jediná z uvedených alternativ prakticky použitelná řešení pro situace vyznačující se značnou mírou technické, ekonomické či společenské složitosti a právě takovou situací je přitom současný stav informační společnosti . Udržení úrovně hodnot a principů, jakož i idealistického charakteru právních pravidel je přitom v tomto případě řešeno nikoli metodologicky ale institucionálně prostřednictvím legitimity orgánů veřejné moci zajišťujících tvorbu příslušných právních pravidel a jejich následnou implementaci .

3. PRINCIPY PRÁVNÍ ÚPRAVY KYBERNETICKÉ BEZPEČNOSTI ČR A EU

V českém právu i právu EU je specifická právní úprava kybernetické bezpečnosti v současné době ve stadiu návrhů základních normativních právních aktů. V České republice je to návrh zákona o kybernetické bezpečnosti (aktuálně sněmovní tisk 81/0 ze dne 10. 1. 2014), v EU je to návrh Směrnice o opatřeních k zajištění vysoké úrovně síťové a informační bezpečnosti - aktuálně COM(2013) 48 final, 2013/0027 (COD). Přestože vznikala nezávisle na sobě, sdílejí obě navržená řešení stejnou regulatorní strategii a z jejich struktury lze rovněž vyčíst prakticky obdobný systémový základ právních principů. Důvodová zpráva k zákonu o kybernetické bezpečnosti shrnuje tyto principy následovně :

- Princip technologické neutrality – na základě toho principu, jehož jedním z rozměrů je i tzv. síťová neutralita, dochází ke striktnímu oddělení obsahu komunikace od technologií používaných pro jeho ukládání nebo přenos. Informační a komunikační technologie jsou tedy neutrální vzhledem ke způsobu, kterým jsou používány. Důležitým aspektem technologické neutrality je rovněž nezávislost právního regulačního rámce na konkrétní technologii – právní regulace je tedy důsledně neutrální vůči produktům různých dodavatelů (žádný z nich nepreferuje ani nevylučuje).
- Princip ochrany informačního sebeurčení člověka – informační sebeurčení člověka zahrnuje nejrůznější základní informační práva, z

nichž pro kybernetickou bezpečnost jsou důležité především právo na ochranu soukromí, právo na ochranu osobních údajů, právo na svobodný přístup k informacím a právo na přístup ke službám informační společnosti (to vychází ze skutečnosti, že v dnešní době nelze žít plnohodnotný soukromý život bez toho, aby měl člověk možnost tyto služby využívat) .

- Princip ochrany nedistributivních práv – v tomto případě jde především o ochranu národní bezpečnosti a specificky pak o ochranu bezpečnosti prostředí, v němž dochází k realizaci informačních transakcí (k tomu podrobněji viz dole).
- Princip minimalizace státního donucení – v případě návrhu právní úpravy jde především o implementaci výstupního kritéria třetího prvku testu proporcionality , v němž je nutno hodnotit, zda je zásah do lidské svobody proveden jen v nezbytně nutné míře. Konkrétně jde o svobodu povinných subjektů volně užívat předmět jejich vlastnického práva (tj. jejich informační a komunikační infrastrukturu). Ve vztahu k člověku se návrh v tomto směru omezuje prakticky dokonale, neboť uživatelům služeb informační společnosti vůbec nezasahuje do jejich práv (zákon se netýká informačních práv uživatelů, nezasahuje do jejich soukromí ani jim neukládá žádná jiná omezení či povinnosti).
- Princip autonomie vůle regulovaných subjektů – tento princip se týká metody právní regulace a projevuje se stanovením cílových parametrů bez toho, aby právotvůrce nutil regulované subjekty k nějakému specifickému konkrétnímu řešení (subjekty si tedy volí způsob, jak cílového stavu dosáhnout v podmínkách, v nichž samy působí).
- Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství – tento princip označovaný v mezinárodním právu veřejném jako due dilligence týká se odpovědnosti státu za mezinárodně škodlivé následky jednání, k němuž dojde pod jeho suverénní jurisdikcí (viz dále).

Za zvláštní pozornost stojí především princip ochrany nedistributivních práv směřující především k ochraně infrastruktury tvořené službami informační společnosti. Nedistributivní charakter bezpečnosti je v tomto případě dán skutečností, že tuto hodnotu nelze distribuovat, tj. nelze konstatovat, že z její existenci přímo plynou konkrétní práva jednotlivým subjektům. Namísto toho má bezpečnost celostní charakter

(jde o ochranu prostředí jako celku) a práva k jeho ochraně vykonává výlučně stát podobně, jako je tomu např. v případě národní bezpečnosti nebo ochrany životního prostředí.

Je v tomto směru nutno zdůraznit, že bezpečnost obecně (tj. vč. kybernetické bezpečnosti) nepředstavuje hodnotu či relevantní zdroj legitimity právních norem sama o sobě. Jedná se jako u ostatních nedistributivních principů o akcesorický institut, jehož legitimita není dána přímo ale prostřednictvím primárních principů, k jejichž ochraně směřuje. Nelze tedy hovořit pouze o bezpečnosti bez dalšího resp. nelze jí per se odůvodňovat vznik nových právních povinností nebo obecně jakékoli zásahy do svobody subjektů. Bezpečnost jako taková pak nemůže být ani ve struktuře proporcionality přímo poměřována s ostatními (distributivními) právními principy jako např. s právem na vlastnictví, právem na svobodu projevu nebo právem na práci.

Namísto toho je třeba vždy řešit otázku, co je bezpečností chráněno, tj. jaká primární hodnota resp. jaký primární princip je příslušnými konkrétními bezpečnostními instituty zajištěn. Dominantním motivem české právní úpravy je přitom právo na informační sebeurčení.

Právo na informační sebeurčení vychází genericky z práva na soukromý život, tj. práva člověka na hodnotnou osobní existenci, a to jak vzhledem k vlastní integritě (důstojnosti), tak i vzhledem k možnostem zapojení do společnosti. Komponentou informačního sebeurčení, která s rostoucí penetrací běžného života službami informační společnosti nabyla na zásadní důležitosti, je ochrana soukromí, z níž se ještě v poslední době specificky vydělila ochrana osobních údajů. Bezpečnost této pasivní komponenty informačního sebeurčení má především charakter jistoty člověka ohledně rozumné míry zabezpečení soukromé informační sféry před násilnými vnějším vlivy.

Aktivní komponentou informačního sebeurčení, která má vzhledem ke kybernetické bezpečnosti přinejmenším srovnatelný význam jako ochrana soukromí a osobních údajů, je právo na komunikaci. Jeho podstatou je předpoklad, že člověk nemůže vést plnohodnotný soukromý život bez toho, aby měl možnost běžným způsobem interagovat s okolním světem, tj. především komunikovat formou, která je v příslušných sociokulturních reáliích obvyklá. V aktuálních podmínkách je tak tuto komponentu informačního sebeurčení možno přeložit jako právo na přístup k (fungujícím) službám informační společnosti.

Právě uvedené samozřejmě neznamená, že by stát měl povinnost zajistit všem subjektům dodávky služeb informační společnosti nebo že by uvedené služby měly být s garancí státu poskytovány bezplatně. Stát má však v situaci, kdy jsou tyto služby běžnou součástí soukromého lidského života, povinnost garantovat jejich dostupnost a na nejvyšší úrovni též jejich funkčnost. To v tomto případě mimo jiné znamená též povinnost státu zabezpečit tyto služby tak, aby mohly být poskytovány bez obav o jejich bezpečnost. Z právě uvedeného tedy plyne, že jen bezpečné služby informační společnosti mohou dát člověku prostor k nerušené realizaci jeho práva na informační sebeurčení.

S právě uvedeným též souvisí primární princip, který český návrh nijak zvlášť nezdůrazňuje, ale který má ve vztahu ke kybernetické bezpečnosti rovněž zásadní význam, tj. princip svobody projevu. Na rozdíl od informačního sebeurčení se v tomto případě jedná namísto aktivní soukromé komunikace o zabezpečení možnosti veřejně vyjádřit svůj názor a případně se účastnit obecného společenského nebo politického diskursu. Stejně jako v případě informačního sebeurčení je přitom možno konstatovat, že pouze bezpečně fungující služby informační společnosti mohou k takové účasti poskytnout adekvátní prostor .

Ostatní shora uvedené principy mají ve struktuře navrhované právní úpravy spíše implementační charakter. Princip technologické neutrality zdůrazněný hned na prvním místě týká se především skutečnosti, že česká právní úprava směřuje k zajištění funkčnosti informační a komunikační infrastruktury bez toho, aby se týkala komunikovaného obsahu . Právní povinnosti subjektů ani pravomoci založené zákonem Národnímu bezpečnostnímu úřadu se tedy z podstaty nemohou týkat informací tvořících obsah komunikace prostřednictvím služeb informační společnosti. Dalším aspektem technologické neutrality je v tomto případě skutečnost, že povinné technické standardy ani technická řešení přímo implementovaná na národní úrovni nebudou zvýhodňovat nebo upřednostňovat žádnou konkrétní proprietální technologii .

Princip autonomie vůle regulovaných subjektů a princip minimalizace státního donucení se vztahují především k osobní působnosti, rozsahu a míře obecnosti konkrétních právních povinností definovaných připravovanou právní úpravou. Navrhovaná právní úprava je minimalistická v tom směru, že se vztahuje pouze na omezený okruh subjektů, přičemž míra zátěže těchto subjektů specifickými povinnostmi odpovídá důležitosti jimi spravovaných systémů a míře jejich bezpečnostní expozice.

Zohlednění maximální autonomie vůle při formulaci povinností pro subjekty spadající do osobní působnosti navrhované právní úpravy má aspekt liberální i pragmatický. Vedle toho, že je inkorporace tohoto principu pro regulované subjekty přirozeně příznivá, neboť jim poskytuje maximální volnost při implementaci příslušných povinností. Vedle toho však tento princip zohledňuje i značnou rozmanitost informačních sítí a systémů, jichž se dotýká. Pokud by byla právní úprava rigorózní co do specifikace konkrétních povinností, znamenalo by to buďto definovat nespočet variant dle rozsahu a funkcí příslušných sítí a systémů nebo pracovat s předpokladem, že standardní zákonné varianty budou vyhovovat co do efektivity vynaložených investic pouze některým subjektům – to by v konečném důsledku vedlo na jedné straně k tomu, že by byly některé subjekty nuceny investovat prostředky do bezpečnostních opatření, která by byla vzhledem k charakteru příslušných systémů přehnaně rozsáhlá a jiné subjekty by naopak ani při splnění zákonných požadavků neochránily svoji infrastrukturu v dostatečném rozsahu. Namísto toho volí návrh zákona stanovení cílového stavu, tj. požadované úrovně funkčnosti bezpečnostních opatření, přičemž ponechává regulovaným subjektům relativní volnost ve volbě konkrétních nástrojů pro jeho dosažení. To ostatně odpovídá i jedné ze shora zmíněných komponent principu technologické neutrality, neboť zákonné podmínky lze splnit nespočtem typů různých bezpečnostních řešení založených na technologiích od různých vzájemně si konkurujících dodavatelů.

Druhým aspektem autonomie vůle je u připravované právní úpravy možnost dobrovolné spolupráce soukromoprávních subjektů s národním dohledovým pracovištěm. Přestože se tato zákonná konstrukce založená na autonomním rozhodnutí soukromoprávních subjektů spolupracovat s orgánem veřejné moci jeví být na první pohled absurdní, lze o tuto formu spolupráce očekávat velký zájem především mezi soukromoprávními subjekty, které jsou předmětem zvýšené bezpečnostní expozice, ať už jde o aktivistické útoky na jejich infrastrukturu, konkurenční boj, průmyslovou špionáž apod. Spoluprací s národním dohledovým pracovištěm mohou tyto subjekty získat nejen přehled o tom, jaká je v reálném čase bezpečnostní situace v české informační a komunikační infrastruktuře (a tím i schopnost reagovat na aktuální kybernetické hrozby v předstihu), ale mohou získávat i průběžnou metodickou a koordinační pomoc při řešení kybernetických bezpečnostních incidentů. Obecně pak pro subjekty nabízející služby informační společnosti bude dobrovolná spolupráce s národním dohledovým pracovištěm představovat nepochybně přidanou hodnotu, kterou budou moci prezentovat svým klientům.

Z hlediska soukromoprávních subjektů však má inkorporace principu autonomie vůle též jeden problematický aspekt, jehož důsledky jsou zásadně důležité též pro výstupy této studie. Připravovaná právní úprava totiž nepočítá s tím, že by měly mít subjekty povinnost nechat si ex ante schvalovat nebo nějak potvrzovat vlastní řešení kybernetické bezpečnosti vzhledem ke splnění standardních zákonných požadavků. Především u středních a velkých podniků a veřejnoprávních korporací investujících podstatné prostředky do rozvoje své informační a komunikační infrastruktury je přitom stěžejní otázkou tzv. compliance, tj. ex ante kontrolovaného plnění zákonných požadavků příslušné jurisdikce. Je totiž z ekonomického hlediska neúčelné pro tyto subjekty investovat do rozvoje vlastní infrastruktury určité prostředky a přitom nemít jistotu, že tyto investice negenerují nějaké právní riziko . Skutečnost, že zákon ve své struktuře neobsahuje explicitní povinnost certifikace nebo jiného schválení příslušných technických a organizačních řešení tedy je na první pohled pro regulované subjekty příznivá, neboť jim nevznikají další náklady spojené se schvalovacími procesy. Středním a velkým subjektům však může způsobit zvýšení míry rizikovosti jejich investic do informační a komunikační infrastruktury, neboť neposkytuje ex ante jistotu, že jimi implementovaná bezpečnostní řešení skutečně bezezbytku plní zákonné požadavky. Nabízí se samozřejmě řešení formou regresní odpovědnosti dodavatelů – takové řešení však již není otázkou compliance a pro střední a velké subjekty stále představuje právní a ekonomické riziko (viz dále).

Princip bdělosti ve vztahu k mezinárodnímu společenství a ostatním suverénním státům se v navrhované právní úpravě projevuje už samotnou skutečností, že se Česká republika snaží při vynaložení podstatného úsilí dostat pod kontrolu bezpečnostní problémy vyskytující se pod její jurisdikcí. Obecně totiž tento princip zakládá odpovědnost státu za škodlivé následky způsobené ostatním státům v důsledku porušení mezinárodního práva veřejného v situacích, kdy stát mohl takovému porušení zabránit. Stát může tedy odpovídat i za to, že neuplatňuje efektivně svou vlastní jurisdikci. V situaci, kdy je infrastruktury na území státu zneužito k provedení kybernetického útoku s dopady v zahraničí, mají postižené státy a mezinárodní společenství důvod ptát se, zda škodlivým následkům nebylo možno zabránit. Existují-li popsané způsoby, jak předejít kybernetickým útokům resp. zneužití informační a komunikační infrastruktury, a kdy je implementace nejrůznějších bezpečnostních opatření nejen technicky možná ale též ekonomicky a sociálně akceptovatelná, pak má stát typu České republiky nikoli pouze právo ale přímo povinnost vůči mezinárodnímu společenství řešit svou vlastní kybernetickou bezpečnost .

Jak plyne z výše uvedeného, není otázka právní úpravy kybernetické bezpečnosti záležitostí momentální módy nebo náhodného politického rozhodnutí. Jedná se o problém, k jehož řešení má Česká republika bezprostřední povinnost, a to vzhledem k ochraně základních práv, jakož i k ochraně svých mezinárodních závazků.

4. AKTUÁLNÍ STAV ČESKÉ LEGISLATIVY A LEGISLATIVY EU

Jak uvedeno shora, jsou evropská i česká legislativa kybernetické bezpečnosti ve stadiu příprav. Obě legislativní předlohy vznikaly na sobě nezávisle, jsou však podobné nejen co do výše zmíněných základních principů ale též co do konkrétních regulatorních řešení .

Prvním podstatným momentem obou navrhovaných úprav je existence centrálních dohledových center na úrovni členských států chránících veřejný zájem a spravovaných nebo zajišťovaných národními orgány veřejné moci. Evropská úprava přitom požaduje nejen zřízení národních dohledových pracovišť ale rovněž designaci orgánu veřejné moci vybaveného odpovídajícími pravomocemi, do jehož kompetence bude svěřena agenda kybernetické bezpečnosti. Tento orgán pak má své výlučné místo nejen v národním systému kybernetické bezpečnosti ale bude se též v rámci spolupráce s ostatními obdobnými orgány a orgány EU podílet na zajištění kybernetické bezpečnosti EU. Charakter kybernetické bezpečnosti (tj. skutečnost, že jde o specifickou bezpečnostní agendu) přitom vyžaduje, aby byl takový orgán nezávislý nejen na soukromé (podnikatelské) sféře ale též na místní politické moci. To samozřejmě neznamená, že by mělo jít o zcela specifickou instituci bez politické legitimity, ale že by měla být demokraticky legitimována bez současné permanentní závislosti na tom, jak bude vypadat momentální politická situace v příslušném členském státě. Institucionální řešení kybernetické bezpečnosti v České republice provedené usnesením vlády č. 781 ze dne 19. 10. 2011 tuto podmínku splňuje.

Architektura kybernetické bezpečnosti v připravované české právní úpravě počítá kromě institucionálního zajištění ústředním orgánem státní správy (tj. Národním bezpečnostním úřadem) a jím provozovaným vládním dohledovým pracovištěm též se soukromoprávním dohledovým pracovištěm označovaným jako národní CERT. Toto dohledové pracoviště nemá disponovat veřejnoprávními kompetencemi a má působit především jako koordinační středisko ve vztahu k soukromému sektoru . Předpokládá se přitom, že bude soukromý sektor spíše nakloněn dobrovolné spolupráci se soukromoprávní korporací stojící na téže korporátní úrovni než s vrchnostensky organizovaným orgánem veřejné moci. Soukromoprávní národní CERT se navíc může

účastnit mezinárodní výměny s obdobně organizovanými zahraničními pracovišti, přičemž soukromoprávní resp. akademická komunita, kterou tato pracoviště v mezinárodním měřítku tvoří, hledí na orgány veřejné moci spíše s a priori nedůvěrou - vládní CERT spravovaný a provozovaný přímo Národním bezpečnostním úřadem se naproti tomu může zapojit do mezinárodní spolupráce veřejnoprávních institucí, která je naopak uzavřena pro soukromou či akademickou sféru.

Návrh české právní úpravy je rovněž v porovnání s připravovanou evropskou směrnicí pochopitelně konkrétnější co do typologie jednotlivých povinností. Počítá především s povinností vybraných subjektů zavést a provozovat tzv. bezpečnostní opatření, tj. standardní formy zabezpečení vlastní resp. spravované informační a komunikační infrastruktury. Návrh zákona přitom není konkrétní co do technických partikularit (viz výše), ale pouze pro různé typy informačních systémů a sítí stanoví základní technické a organizační parametry – konkrétní forma jejich implementace je pak otázkou volby příslušných správců. Ex post povinnosti dopadající na různé typy subjektů spadající pod rozsah osobní působnosti zákona pak zahrnují především povinnost reagovat na obecné či konkrétní pokyny Národního bezpečnostního úřadu vydávané formou rozhodnutí nebo opatření obecné povahy.

Přestože mezi navrhovanou českou a evropskou právní úpravou nejsou žádné zásadní koncepční rozdíly, je možno nalézt několik poměrně podstatných partikulárních odlišností. Česká právní úprava pracuje se strukturou povinných subjektů zahrnující správce kritické informační a komunikační infrastruktury (tj. správce systémů a sítí zařazených mezi kritickou infrastrukturu státu), správce významných systémů a sítí (tj. veřejnoprávní subjekty spravující významné informační systémy veřejné správy resp. soukromoprávní správce systémů a sítí vysoké důležitosti) a dále pak, nespadají-li do některé z právě uvedených kategorií, poskytovatele služeb elektronických komunikací. Poslední z uvedených kategorií povinných subjektů nemá v české legislativní předloze přímo specifikovány žádné závažné povinnosti – prakticky jde pouze o povinnost oznámit kontaktní údaje pro případ vyhlášení mimořádného stavu, tj. stavu kybernetického nebezpečí. Až v případě vyhlášení mimořádného stavu pak mají tyto subjekty povinnost reagovat na obecné a konkrétní pokyny Národního bezpečnostního úřadu podobně jako více exponované ostatní skupiny povinných subjektů. Zatímco však český legislativní návrh pracuje s pojmem poskytovatelů služeb elektronických komunikací, pracuje evropská legislativní předloha s osobní působností na poskytovatele služeb informační společnosti. Tyto kategorie, přestože se částečně překrývají, mají velmi rozdílný rozsah – zatímco do rozsahu pojmu poskytovatelů služeb

informační společnosti nespadají poskytovatelé služeb elektronických komunikací spočívajících ve vysílání signálu, nezahrnuje naopak kategorie poskytovatelů služeb elektronických komunikací obrovskou masu služeb informační společnosti nelicencovaných národními telekomunikačními úřady. Typicky jde o valnou většinu běžně používaných služeb obsahových (např. informační portály), virálních (sociální sítě a služby typu user-generated content) nebo zprostředkovatelských (např. vyhledávače, instant messengery apod.) Nebudou-li pak tyto služby považovány v ČR za součást kritické informační a komunikační infrastruktury, nebude prakticky možno jejich správcům ukládat povinnosti k zajištění národní kybernetické bezpečnosti, to dokonce ani za stavu kybernetického nebezpečí.

Pokud by však česká právní úprava pracovala, podobně jako evropský návrh, s kategorií poskytovatelů služeb informační společnosti, byl by Národní bezpečnostní úřad vystaven řadě jen velmi obtížně řešitelných problémů při užití svých nařizovacích a sankčních pravomocí. Předně by bylo obtížné vůbec zmapovat tak širokou a nesourodou masu nejrůznějších služeb a jejich poskytovatelů, jejichž počty mohou u nás dosahovat stovek tisíc (zde je nutno připomenout, že za poskytovatele služby informační společnosti se např. bez ohledu na osobní status považuje též každý provozovatel webové stránky, která umožňuje publikaci uživatelských reakcí či komentářů). Je však v tomto směru každopádně otázkou, zda bude spíše evropská legislativní iniciativa ustupovat z extrémně rozsáhlé osobní působnosti nebo zda dojde ke spíše pravděpodobné postupné změně českého přístupu a ke hledání způsobů, jak kategorii poskytovatelů služeb informační společnosti (původně vytvořenou za zcela jiným účelem) regulatorně zvládnout.

Druhým podstatným rozdílem mezi českou a evropskou legislativní předlohou je řešení otázek souvisejících s postihem počítačové trestné činnosti (kyberkriminality). Česká právní úprava se v tomto směru důsledně drží metodického oddělení bezpečnostní agendy od agendy trestní a pouze připouští za předem daných podmínek využití údajů o kybernetických bezpečnostních incidentech pro vyšetřování a stíhání trestné činnosti orgány činnými v trestním řízení. Sám Národní bezpečnostní úřad ani žádné z dohledových pracovišť však nebude vykonávat úkony činné v trestním řízení ani nebude provádět zajišťování důkazů či ztotožňování osob. V tomto směru následuje česká právní úprava explicitně nevyjádřený ale v české republice extrémně silný princip institucionálního oddělení exekutivních agend obrany národní suverenity (svěřené Armádě ČR), vnitřní bezpečnosti státu (svěřené Bezpečnostní informační službě a Národnímu bezpečnostnímu úřadu), vnější bezpečnosti státu (svěřené Úřadu pro

zahraniční styky a informace) a ochrany zákonnosti (svěřené Policii České republiky a částečně dalším orgánům výkonné moci). V České republice tak je nemyslitelné, na rozdíl od řady tradičních demokracií západoevropského nebo severoamerického typu, aby se v jedné instituci kumulovaly pravomoci překračující hranice uvedených agend (typickými příklady jsou v tomto směru americké FBI nebo NSA).

Z uvedeného důvodu není vhodné, aby předpis zaměřený na problematiku národní kybernetické bezpečnosti řešil současně otázku vyšetřování nebo stíhání trestné činnosti nebo aby byly orgánu výkonné moci, jemuž je dána působnost na úseku kybernetické bezpečnosti, svěřeny analytické nebo vyšetřovací kompetence pro potřeby přípravného či soudního řízení trestního.

5. TÉMATA K DALŠÍMU ROZPRACOVÁNÍ S DŮRAZEM NA ÚLOHU TPEB

5.1. Certifikace a compliance check

Jak uvedeno shora, pracuje návrh české právní úpravy s principem autonomie vůle regulovaných subjektů. Jedním z projevů tohoto principu ve spojení s principem technologické neutrality je mandatorní stanovení cílových charakteristik bezpečnostních opatření (organizačních i technických) a ponechání konkrétní formy realizace na úvaze příslušného povinného subjektu. Vhodnost takového řešení je vedle obecně menší regulatorní zátěže pro povinné subjekty dána též skutečností, že příslušné bezpečnostní řešení může být vždy realizováno na míru konkrétního systému. Regulovaný subjekt má tedy praktickou volnost ve výběru architektury, technologie i dodavatelů. V řadě případů přitom nebude nutno realizovat žádné zásadní investice, neboť stávající bezpečnostní řešení často s rezervou odpovídají zákonným požadavkům a marginální náklady tak budou pouze otázkou doplnění bezpečnostních řešení o reportovací funkcionality resp. adaptace stávající dokumentace pro potřeby zákonného výkaznictví.

Určitou nevýhodou tohoto jinak vhodně zvoleného řešení však je skutečnost, že povinné subjekty budou mít jen omezenou míru právní jistoty ohledně otázky, zda právě jejich konkrétní řešení odpovídá zákonným požadavkům, tj. zda v případě kontroly ze strany Národního bezpečnostního úřadu nebudou shledány vzhledem k zákonným požadavkům nějaké nedostatky. Byť jsou totiž požadované parametry bezpečnostních opatření definovány s maximální mírou určitosti, nelze se, a to ani při konkretizaci jednotlivých parametrů formou podzákonných právních předpisů, ubránit relativně velké míře abstrakce a výsledné nejistoty plynoucí vedle relativně abstraktních

zákonných a podzákonných pojmů též z velkého množství různých organizačních a technických kritérií.

K relativní neurčitosti zákonných resp. podzákonných požadavků, byť snížené na nezbytně nutnou míru, pak ještě přistupuje určitá míra nejistoty ohledně implementace a následného provozu bezpečnostních opatření. Zákonné požadavky totiž nesměřují jen ke statické formě bezpečnostních opatření (tj. k jejich statickým formálním parametrům) ale též k jejich implementaci a fungování v reálném čase. I bezpečnostní řešení dostatečně dimenzované vzhledem k zákonným požadavkům totiž může ve svém výsledku porušovat zákonné podmínky kvůli neadekvátní implementaci nebo nedostatečné pozornosti vzhledem k jeho trvalému provozu.

Nejistota ohledně toho, zda projektované, pořízené, implementované a provozované bezpečnostní řešení splňuje zákonné parametry, představuje závažný problém především pro střední a velké podniky, jakož i pro veřejnoprávní korporace. U středních a velkých podniků jedná se především o otázku compliance, přičemž především nadnárodní korporace často řeší otázky a priori plnění zákonných požadavků v příslušných jurisdikcích jako naprostou prioritu. Aktuálně se to týká např. otázek ochrany osobních údajů, bezpečnosti práce, požární bezpečnosti, utajovaných informací apod. Pro podnik velkého rozsahu je totiž zásadně důležité vyčíslení nákladů na plnění právních povinností v příslušné jurisdikci a priori – jen tak s nimi totiž lze kalkulovat do finančních plánů. Situace, kdy je velká nebo střední korporace nucena kalkulovat potenciální náklady na plnění právních povinností a posteriori, vždy generuje značnou míru nejistoty, neboť právní odpovědnost (postih) se v komplexních případech jen velmi těžko odhaduje a těžké je i provést takovou kalkulaci do všech možných důsledků.

V případě připravované úpravy kybernetické bezpečnosti tak jde příkladně o to, jaké mohou být právní následky implementace a používání takového systému bezpečnostních opatření, o kterém se následně prokáže, že nesplňuje zákonné požadavky. U velkého nebo středního podniku je v tomto směru případná pokuta jen jedním z mnoha možných následků, neboť nezákonnou implementací mohou být způsobeny např. škody třetím osobám (v takovém případě jde totiž o škody vzniklé v důsledku porušení právní povinnosti) nebo může v důsledku nařízených opatření k nápravě dojít k omezení provozu či k potřebám zásadních organizačních změn.

Dokonce i tam, kde lze počítat s konkrétní výší např. pokut, náhrad škody nebo škod způsobených zastavením nebo omezením provozu, představuje u všech typů podnikatelských subjektů a posteriori řešení právní rizikovosti velmi nevítanou

alternativu. Není totiž žádným tajemstvím, že podnikatelské aktivity mohou být významně poškozeny už tím, že se orgány státní moci nějakou formou o příslušný podnik zajímají. Typicky pak může i pouhá kontrola nebo vyšetřování ze strany oprávněných orgánů státní moci způsobit jen těžko předvídatelné komplikace a vést ke ztrátám, jejichž hodnotu lze jen stěží předem vyčíslit. To platí samozřejmě i pro případy, kdy vyšetřování nebo kontrola nevedou ve vztahu k příslušnému orgánu veřejné moci k žádném sankčnímu důsledku, neboť i pouhá vrchnostenská přítomnost na kontrolovaných pracovištích může se negativně projevit na výkonu celého podniku.

U veřejnoprávních korporací je otázka a priori souladu s požadavky právního řádu ještě důležitější než u podnikatelských subjektů. V porovnání se soukromoprávními subjekty jde navíc o prioritní otázku bez ohledu na jejich velikost. Je-li totiž k pořízení nebo provozu bezpečnostních opatření užito veřejných prostředků, nelze riskovat dodatečnou kvalifikaci těchto opatření jako nesouladných se zákonnými požadavky. Lze navíc předpokládat, že investice veřejného sektoru do kybernetické bezpečnosti budou minimálně z podstatné části kryty prostředky z různých rozvojových projektů – příjemce takových prostředků si pak dvojnásob nemůže dovolit rizikovost investice vzhledem ke splnění zákonných požadavků resp. nemůže si dovolit riskovat situaci, kdy projektové prostředky použije způsobem, který je dodatečně (např. na základě kontroly) označen za nikoli souladný s platnou právní úpravou. Poskytovatel dotace má totiž v takovém případě právo či dokonce povinnost dovolávat se podmínek jejího poskytnutí a požadovat vrácení poskytnutých prostředků.

Z právě popsaných důvodů lze mezi středními a velkými soukromoprávními subjekty a veřejnými korporacemi očekávat velkou poptávku po a priori aprobačních procedurách poskytujících nezávislé ujištění příslušnému subjektu ohledně toho, že implementované resp. provozované řešení bezpečnostních opatření je v souladu s požadavky účinné právní úpravy. Objektivně ideální variantou řešení tohoto problému by byla zákonná certifikační procedura realizovaná přímo příslušným orgánem státní exekutivy (v českém právním prostředí zřejmě Národním bezpečnostním úřadem) nebo jím pověřeným a dozorovaným nezávislým expertním pracovištěm.

Skutečnost, že taková procedura není součástí struktury navrhované právní úpravy, však lze jen sotva vnímat jako chybu právotvůrce nebo jako pravou mezeru v právu. Taková procedura musela by totiž být podrobně a rigorózně upravena, aby nevzniklo riziko privatizace výkonu nedistributivních práv resp. aby nebyl indukován korupční potenciál. Je přitom jen velmi obtížné takovou rigorózní úpravu provést v

situaci, kdy jsou k dispozici v tomto ohledu jen velmi omezené zkušenosti (zde je nutno připomenout, že stávající komerční certifikační procedury zaměřují se především na problematiku organizačních opatření, nikoli už na technologie k zajištění kybernetické bezpečnosti nebo na spolupráci s centrálními dohledovými pracovišti). Zavedení státní certifikace by rovněž vyžadovalo důkladnou přípravu institucionální a personální a je třeba v tomto směru konstatovat, že na našem pracovním trhu zdaleka není přebytek pracovní síly disponující dostatečnou mírou kvalifikace v oboru kybernetické bezpečnosti a k tomu náležitě motivované za aktuálních platových podmínek ke vstupu do státní služby. Příprava adekvátní procedury by z hlediska organizačního i personálního vyžadovala takovou časovou a finanční dotaci, kterou si vzhledem k vývoji bezpečnostní situace nemůže v současné době Česká republika dovolit (kromě toho je třeba po bohatých našich legislativních zkušenostech připomenout, že nemá smysl uvádět v účinnost právní úpravu, na jejíž implementaci není státní exekutiva náležitě připravena).

Ve prospěch státního řešení certifikace může naopak hovořit pozitivní zkušenost s obdobnou procedurou v agendě ochrany utajovaných informací. Ani v tomto případě přitom nebylo možno ji realizovat okamžitě, ale příslušné kapacity se postupně vytvářely. Skutečnost, že v tomto případě nejde o korupčně exponovanou situaci, navíc ukazuje, že je speciálně v případě NBÚ možno předpokládat takovou kvalitu institucionálních opatření, která vzniku a rozvoji korupčního rizika účinně brání. V případě kybernetické bezpečnosti by navíc bylo možno v porovnání s technologiemi a postupy pro ochranu utajovaných informací učinit celý certifikační proces ještě transparentnějším (tj. vystavit jej ve větší míře veřejné kontrole v tomto případě vykonávané především dodavateli vzájemně konkurenčních bezpečnostních řešení) a lze tedy konstatovat, že korupční rizikovost by bylo možno v takovém případě prakticky vyloučit.

Problémem však každopádně zůstává shora konstatovaná a jen těžko unilaterálně řešitelná dlouhodobost náběhu veřejnoprávní certifikační procedury daná nutností vytvořit na straně NBÚ odborně zdatný a dostatečně robustní personální substrát . Jedinou variantou přímého zapojení orgánu veřejné moci do a priori certifikace bezpečnostních řešení tedy zůstává institucionální nebo produktová aprobace certifikační procedury realizované nezávislým subjektem s dostatečnou personální kapacitou, tj. akademickou institucí nebo komerčním poskytovatelem.

Role zájmových sdružení a organizací zajišťujících expertní spolupráci soukromého a veřejného sektoru typu TPEB je v tomto směru evidentní. Ve vzájemné spolupráci s orgány odpovědnými za výkon vrchnostenské správy na úseku kybernetické bezpečnosti (tj. u nás s Národním bezpečnostním úřadem) a nezávislými akademickými institucemi mohou tyto organizace pomoci s vytvořením nezávislých certifikačních procedur praeter legem, které nebudou mít vrchnostenský charakter, ale přesto poskytnou zájemcům z řad soukromého a veřejného sektoru nezávislé komplexní posouzení bezpečnostních opatření (zde v zákonném smyslu tj. včetně dokumentace, procedur apod.) vzhledem k zákonným a podzákonným požadavkům. Charakter zájmového sdružení v tomto případě kombinuje aspekt transparentnosti (tj. je jasné, že jde o aktivitu obchodní komunity) a profesní specializaci (tj. zaměření na konkrétní ekonomické odvětví) s legitimitou společného postupu, tj. nejde pouze o zájem jednoho podnikatele, ale aktivita sdružení odráží vůli vzájemně si konkurujících subjektů.

Takové certifikační procedury samozřejmě nebudou disponovat vrchnostenským charakterem a jejich výstupy nebudou zavazovat orgány veřejné moci při hodnocení souladu příslušných bezpečnostních řešení se zákonem a podzákonnými předpisy. Při nalezení adekvátního modelu spolupráce s vrchnostenskými orgány však lze tímto prostřednictvím docílit faktické akceptace těchto certifikačních procedur Národním bezpečnostním úřadem alespoň v procesním smyslu. Jinými slovy tedy takový certifikát nemůže sice absolutně ochránit příslušný subjekt před kontrolou nebo následnou sankcí, jeho udělení však může být při případné kontrole fakticky zohledněno. Zatímco tedy může být za běžných podmínek prováděna kontrola bezpečnostních opatření bez jakékoli presumpce, může Národní bezpečnostní úřad kontrolovat certifikovaná bezpečnostní řešení s presumpcí souladu. Takové procesní řešení může pak pragmaticky posloužit nejen povinným osobám, ale samotnému Národnímu bezpečnostnímu úřadu – logicky ale jeho implementace vyžaduje především vzájemnou důvěru, kterou může zajistit pouze skutečná nezávislost certifikační procedury, jakož i její vysoká odborná úroveň (obojí je v našem prostředí řešitelné v první řadě spoluprací s akademickými institucemi).

Především z hlediska povinných subjektů užívajících k investicím do pořízení nebo provozu bezpečnostních opatření veřejné prostředky (v tomto případě je lhostejno, zda jde o soukromoprávní nebo veřejnoprávní organizace) je shora popsané řešení vhodné i z důvodu možné inkorporace do zadávací dokumentace resp. do mandatorních požadavků na dodavatelská řešení. Namísto relativně neurčitých formulací ohledně souladu bezpečnostních opatření s platnou právní úpravou budou

tyto subjekty moci v implementačních nebo realizačních smlouvách využít ujednání odkazující na získání konkrétních typů certifikací a sjednat si tím vyšší míru právní jistoty (vedle dodavatele totiž v takovém případě garantuje soulad i nezávislá certifikační autorita uznaná vrchností i odbornou komunitou). Obdobná pak může být též situace u dlouhodobých outsourcingových kontraktů, kde požadavek na certifikaci příslušného bezpečnostního řešení na aktuálně účinný standard může být na straně odběratele adekvátně řešit jistotu ohledně průběžného plnění zákonných resp. podzákonných povinností, u nich lze oprávněně očekávat, že se budou v čase výrazně vyvíjet a měnit.

K právě uvedenému je nutno doplnit, že příslušná certifikační řešení zdaleka nemusí být unikátní nebo monopolní resp. že pro různé typy bezpečnostních řešení mohou fungovat různé procedury. Certifikace tak může být prováděna např. formou prověrky ve fázi projektu informačního systému nebo sítě, kontroly jeho implementace nebo provozních zkoušek jako součásti různých fází akceptace příslušných dodávek. Formu certifikace mohou mít též například i penetrační testy nebo jiné typy operačních prověrek běžících systémů nebo sítí – tento model může být využíván především u dlouhodobých outsourcingových kontraktů, přičemž odběratel může mít díky němu stálou kontrolu nad kvalitou dodávané služby a nad skutečností, že služba např. i po několika letech stále plní aktuální požadavky právní úpravy (v tomto směru je třeba připomenout relativně vysokou pravděpodobnost postupných změn požadavků na bezpečnostní opatření v návaznosti na obecný technický vývoj). Certifikací mohou konečně procházet vedle celých bezpečnostních řešení i jen dílčí systémy nebo dokonce jejich jednotlivé komponenty – typicky tak může být systém nebo síť podrobena experimentální bezpečnostní expozici v testovacím polygonu a na základě kvality její odezvy může být certifikační autoritou doporučena/nedoporučena pro nasazení v určitém typu informačního systému nebo sítě.

Bezpečnostní opatření mohou být tedy na základě navrhované právní úpravy šita na míru konkrétním systémům nebo sítím a zcela jistě se v praxi vyvine minimálně několik jejich standardních typů. Z tohoto důvodu je vhodné podporovat i takové certifikační iniciativy, které budou směřovány do konkrétních hospodářských resp. veřejnoprávních sektorů . Lze v tomto směru očekávat, že profesně resp. sektorově orientované iniciativy mohou být mnohem efektivnější při tvorbě řešení pro specifické typy bezpečnostních řešení – je přitom logické, že typická bezpečnostní řešení v justici se budou zřejmě na úrovni technické i organizační zásadně odlišovat od bezpečnostních opatření aplikovaných v oblasti justičních systémů a sítí. Profesně resp. sektorově

orientované iniciativy mohou v tomto směru přinést ve smyslu efektivity nejen odpovídající úroveň znalostí v oboru kybernetické bezpečnosti ale také poznatky ohledně specifických požadavků v příslušném odvětví nebo oboru.

Jako problematická jeví se konečně v současné situaci též rizika plynoucí z čistě podnikatelsky orientovaných iniciativ, které může indukovat shora popsaná poptávka. Nebude-li totiž problematika a priori aprobace bezpečnostních opatření řešena formou spolupráce orgánů veřejné moci, akademických institucí a odborně orientovaných soukromých iniciativ, vytvoří se tím prostředí pro živelný vznik samozvaných razítkovacích produktů. Bude pak extrémně složité dostat takový čistě ekonomicky motivovaný chaos do situace, kdy bude možno se na příslušné certifikáty či jiné formy potvrzení z odborného hlediska skutečně spolehnout. Jen těžko si pak lze představit, jaké praktické důsledky by mohla mít situace, kdy by aprobaci bezpečnostních opatření nezávisle prováděli např. jednotliví znalci (bude-li zachována současná situace ohledně podmínek pro výkon a odbornou úroveň znalecké činnosti).

Jak naznačeno shora, může být úloha zájmových sdružení typu TPEB v tomto směru zásadní. Zájmové sdružení tak může formulovat požadavky na certifikační produkty a pak aktivně za své členy spolupracovat při přípravě certifikačních procedur. Kontakty sdružení k politické a úřední moci přitom mohou pomoci při koordinaci přípravy oborových nebo i obecných certifikačních procedur a neformálně zprostředkovat i případné náměty a připomínky členů. Zatímco je jen velmi málo pravděpodobné, že by typicky Národní bezpečnostní úřad přímo spolupracoval na přípravě konkrétního komerčního certifikačního produktu nebo přímo komunikoval se všemi povinnými subjekty, lze naopak předpokládat, že pro něj mohou být sdružení typu TPEB relevantními partnery pro diskusi odborných nebo organizačních otázek (to se ostatně velmi pozitivně projevilo již při samotné přípravě návrhu zákona, která probíhala formou permanentní diskuse se všemi zúčastněnými subjekty často reprezentovanými právě různými svazy nebo sdruženími).

Po čistě obchodní linii může sdružení buďto samo podpořit vznik resp. vývoj vlastní certifikační procedury vhodné pro oborový segment svých členů nebo se může za užití svých odborných kapacit identifikovat vhodná řešení používaná v zahraničí (zde především v USA) a podílet se na jejich portování na tuzemské právní a technické podmínky .

V neposlední řadě pak může sdružení působit zpět na své vlastní členy v tom směru, aby se vyvarovali shora naznačených chyb nebo neefektivních investic a

poskytovat jim díky svému odbornému zázemí a kontaktům na akademickou obec poradenství a metodickou podporu. Právě efektivitu investic do bezpečnostních opatření je možno vidět jako hlavní motivační faktor pro spolupráci povinných subjektů formou zájmového sdružení a pro takto zprostředkovanou spolupráci s orgány veřejné moci a akademickou sférou – vedle toho, že jde de facto o spojení prostředků k pokrytí vysoce odborného zadání, které jednotlivé povinné subjekty nemají možnost samy adekvátně pokrýt, může vzájemná koordinace odborných aspektů výběru a implementace bezpečnostních opatření (to nejen ve smyslu technickém ale i např., ve formě doporučených postupů pro konstrukci smluvních dokumentů pro outsourcing, zadávací dokumentace k zakázkám apod.) výrazně pomoci chránit členy sdružení před duplicitními nebo vyloženě nesmyslnými projekty. V tomto směru je možno poukázat na známé případy z praxe v české elektroenergetice, kdy samotná příprava zákona o kybernetické bezpečnosti vyvolala paniku v tom směru, že bude jistě třeba masivních investic do oddělených komunikačních sítí, zcela nových zabezpečovacích systémů apod. – při adekvátním odborném zhodnocení vhodnosti a potřebnosti těchto investic z hlediska požadavků připravované právní úpravy přitom vychází najevo, že namísto stamilionových investic postačí často jen drobná adaptace existujících řešení s nutností investic o řád až zva nižších.

5.2. Aktivní obrana – best practices

K tématu aktivní obrany je nutno předeslat, že v současné době neexistuje žádná obecně uznávaná taxonomie jejích typických forem. Pokud už je téma aktivní obrany předmětem odborných publikací, zaměřuje se odborná debata buďto na technické aspekty konkrétních typů obranných opatření nebo na základní systematiku v rámci relativně úzce vymezených typů. Nelze však hovořit o žádné komplexní systematice a dokonce ani o definici, která by mohla pojem aktivních obranných opatření (aktivních protiopatření) alespoň rámcově popsat. Za této situace je problematika aktivní obrany logicky spíše vědeckým zadáním a měla by být řešena formou výzkumných aktivit a iniciativ. Jediným použitelným zárodkem obecné taxonomie aktivních protiopatření je tzv. Dagstuhlská taxonomie , která byla sestavena v rámci specializovaného semináře Leibnizovy nadace na podzim 2013 a reflektovala požadavky na systematiku z hlediska informatiky i právní vědy. Ani tato taxonomie však není prakticky použitená, neboť obsahuje pouze náznak základních kategorií a bude tedy nutno ji dále vyvíjet a doplňovat.

Aktuální praxe kybernetické bezpečnosti však nemůže čekat na výstupy vědeckých projektů, neboť aplikace aktivních protiopatření představuje v běžném

fungování služeb informační společnosti každodenní nutnost. Vzhledem k tomu, že prakticky užívaná aktivní protiopatření často zasahují do vlastnických či závazkových práv nebo dokonce naplňují formální znaky skutkových podstat trestných činů, představuje aktuální praxe jejich uplatňování prakticky výlučně šedou zónu. Podnikatelé, kteří tato opatření používají, tak činí skrytě. Dokonce ani technici vyvíjející a aplikující tato opatření na objednávku soukromoprávních subjektů často dokonce ani nejsou s těmito subjekty v žádném oficiálním právním vztahu.

Poněkud lepší je v tomto směru situace ve veřejném sektoru, přičemž typicky výkonné orgány mohou při užití aktivních protiopatření aplikovat obecná oprávnění založená jim v návaznosti na charakter chráněného zájmu. Ani v tomto případě však není situace úplně ideální, neboť při aplikaci obecných oprávnění často vyvstávají otázky ohledně rozsahu příslušných institutů. Orgány veřejné moci jsou rovněž v užití aktivních ochranných prostředků obecně omezeny mlhavými hranicemi vlastní institucionální legitimity – typicky tak armádní složky mohou užít svých extrémně širokých oprávnění pouze za situace, kdy jde o věc národní suverenity, bezpečnostní složky mohou aktivně jednat pouze v zájmu vnitřní nebo vnější národní bezpečnosti a orgány činné v trestním řízení mají manévrovací prostor vymezen agendou vyšetřování a stíhání trestných činů resp. ochranou veřejného pořádku.

Na jednoduchou otázku, jaké aktivní prostředky může užít policista zařazený do obvodního oddělení (je-li toho samozřejmě technicky schopen), když zjistí útok na web místního podnikatele, však neexistuje dokonce ani obecná odpověď. Podobně nejsme schopni odpovědět dokonce ani na mnohem prozaičtější otázky nemající ani charakter bezpečnostních problémů, typicky na otázku, jaké konkrétní aktivní prostředky lze použít při získávání elektronických důkazů z informační a komunikační infrastruktury.

Jak je však uvedeno shora, nemůžeme si dovolit reagovat na faktickou situaci jen pokrčením ramen a vývojem či tolerováním šedé zóny prakticky používaných, účinných a potřebných aktivních opatření, která však existují zcela mimo účinnou právní úpravu. Roli soukromoprávních iniciativ typu TPEB lze v tomto směru vidět především v komunikaci praktických potřeb a sběru a vyhodnocování informací ohledně prakticky používaných technik v různých odvětvích hospodářství a společenského života a v následném zpracovávání těchto poznatků do podoby technických resp. právovědných zadání pro další výzkum a legislativní praxi.

V porovnání se shora popsanou potřebou řešení certifikačních procedur však každopádně platí, že v otázce aktivní obrany nemáme prozatím k dispozici ani představu

ohledně konkrétních potřeb a z nich vycházejících zadání pro organizační, technickou nebo legislativní realizaci. O to víc je samozřejmě nutno tuto otázku aktivně zpracovávat a řešit – v tomto směru je však nutno připomenout, že nemá smysl začít pracovat na řešení jakýchkoli partikularit bez současné představy o smyslu a účelu aktivních protiopatření jako takových a o jejich reflexi základními principy, na nichž stojí náš právní řád.

5.3. Kybernetická bezpečnost jako agenda podpory investic

Jedním ze základních principů, na nichž stojí legitimita připravované české právní úpravy, je princip bdělosti vzhledem k ostatním státům a mezinárodnímu společenství. Vedle shora popsané, byť stále nikoli prakticky uplatňované, částečné přičitatelnosti kybernetického útoku státu neschopnému při vynaložení rozumného úsilí zabránit zneužití informační a komunikační infrastruktury pod vlastní jurisdikcí, projevuje se tento princip i mnohem bezprostředněji, a to ve vztahu k ochraně investic. Česká republika je vázána obecnými procedurálními pravidly řešení sporů mezi státy a soukromoprávními investory doplněnými řadou bilaterálních dohod o ochraně investic zakládající pravomoc příslušných rozhodčích institucí – tato právní úprava vede ve výsledku k možnému založení odpovědnosti České republiky za investice zmařené v důsledku nelegitimního výkonu státní moci resp. v důsledku toho, že stát příslušné investice adekvátně neochrání.

Ve vztahu ke kybernetické bezpečnosti je možno konstatovat, že investor má v našich geopolitických reáliích oprávněná očekávání nejen co do fyzické bezpečnosti ale též co do obecné funkčnosti služeb informační společnosti. V případě, že stát není schopen zajistit fungující informační a komunikační infrastrukturu, jedná se z hlediska investora nejen o faktor při rozhodování o samotné lokalizaci investice ale může se jednat i o důvod založení odpovědnosti státu v případě, že investice byla uskutečněna a informační a komunikační infrastruktura není v důsledku bezpečnostní expozice adekvátně funkční.

Jedná se o podobnou situaci, jako kdyby stát nejprve nalákal investory na fungující dopravní infrastrukturu – ta by ale po nějakém čase přestala být použitelnou v důsledku častého výskytu dopravních přestupků, které policie nezvládá řešit. Podobnost s dopravní infrastrukturou však z hlediska investic samozřejmě není úplná resp. z tohoto srovnání vychází jako dokonale absurdní zjištění, že kybernetická bezpečnost ještě není předmětem agendy investiční konkurenceschopnosti České republiky.

V porovnání s dopravní infrastrukturou je totiž potřeba investic do kybernetické bezpečnosti z hlediska nákladovosti o několik řádů méně náročnou. Současně lze poukázat na skutečnost, že bezpečně fungující informační a komunikační infrastruktura je relevantním faktorem lokalizace přesně těch typů investic, které jsou pro Českou republiku prioritní, tj. investic do oborů s vysokou mírou přidané hodnoty – naproti tomu investice do dopravní infrastruktury, nepoměrně ve všech směrech náročnější, zdaleka neindukují jen ten typ investičního potenciálu, o který má mít Česká republika zájem (namísto toho jde o investice do nekvalifikované mechanické práce nebo jen manipulace se zbožím typu montoven nebo logistických center). Z toho plyne, že je absurdní, pokud Česká republika investuje v režimu podpory investic do rozvoje silniční nebo železniční sítě, aniž by ve stejném režimu investovala do zajištění kybernetické bezpečnosti.

Úloha soukromoprávních iniciativ typu TPEB je v tomto směru evidentní především v otázkách přenosu informací mezi podnikatelským sektorem a veřejnou mocí. K náležitému nastavení resp. zaměření příslušných investic je totiž třeba především znát reálné potřeby adresátů investiční podpory. Platí přitom, že středně velcí a velcí mezinárodní investoři zpravidla nemají zájem o podporu nebo dokonce o zajištění interních systémů bezpečnosti informací. Naopak lze podle zahraničních zkušeností předpokládat, že adekvátní zaměření investiční podpory má vést k zajištění bezpečného fungování služeb informační společnosti a poskytovat v reálném čase metodiku a asistenci pro zvládání závažných kybernetických bezpečnostních incidentů s původem mimo příslušné podnikatelské subjekty.

Jinými slovy má z hlediska investora význam, pokud hostitelský stát investuje do nástrojů k obecnému zajištění bezpečného fungování informační a komunikační infrastruktury. V tomto směru je nutno připomenout, že investory vedle provozu jejich vlastních informační struktur zajímá též dostupnost informačních a komunikačních technologií ze strany jejich obchodních partnerů a široké veřejnosti, jakož i využití veřejně dostupných služeb informační společnosti k interním organizačním procesům (práce z domova, komunikace mezi pobočkami, provoz distančních spotřebitelských terminálů apod.) Organizace typu TPEB přitom mohou pomoci identifikovat konkrétní otázky v příslušných průmyslových odvětvích a koordinovat komunikaci mezi příslušnou obchodní komunitou a orgány veřejné moci.

Na základě zahraničních zkušeností je však v tomto případě nutno varovat před přístupem k řešení veřejné podpory investic jako k lobbyistické aktivitě. V tomto

případě je totiž třeba, aby byla tato agenda zpracovávána na straně orgánů veřejné moci nikoli pouze institucemi a agenturami zabývajícími se podporou exportu ale aby jakákoli řešení na úrovni veřejné správy implementována příslušným vrcholným exekutivním orgánem (v našem případě Národním bezpečnostním úřadem). Vrchnostenské orgány na úseku bezpečnosti jsou přitom nejen přirozeně rezistentní vůči obchodnímu lobbyingu a typicky u Národního bezpečnostního úřadu může lobbyistický přístup potenciálních investorů nebo obecně zájmových sdružení vyvolat dokonce alergickou reakci. Pokud se tedy bude TPEB nebo obdobné organizace zabývat zvyšováním úrovně národní kybernetické bezpečnosti nebo možnostmi konkrétních projektů v oblasti kybernetické bezpečnosti teleologicky orientovanými na podporu investic, je třeba k této agendě přistoupit jako k výměně odborných poznatků (nikoli jako k lobbyingu za předem připravená řešení).

Je tedy třeba v této otázce zřejmě poněkud změnit praxi zažitou ve střední a východní Evropě, že totiž podnikatelé, pokud investují do účasti v oborových sdruženích, očekávají výměnou za to okamžitý a přímý hospodářský prospěch, tj. bezprostřední prosazení svých obchodních zájmů či dokonce příliv zakázek. Výměna odborných poznatků, diskuse či spolupráce s orgánem veřejné moci na expertní bázi přitom může podnikateli přinést nepřímý pozitivní efekt, jehož přínos pro jeho obchodní aktivitu může být ještě násobně hodnotnější. Je pak problémem zmíněného našeho stereotypu, že naši podnikatelé jen neochotně přistupují na to, že by měli investovat personální a finanční zdroje do aktivity, která jim okamžitě žádný přímý prospěch nepřinese – na druhé straně se pak není čemu divit, pokud orgány veřejné moci typu NBÚ přistupují ke skupinovým nebo individuálním podnikatelským iniciativám odborného charakteru s a priori nedůvěrou.

Pozitivní příklady důvěryhodné, efektivní a oboustranně výhodné vzájemné spolupráce na odborné úrovni není každopádně nutno brát jen ze zahraničí, byť je tato forma účasti průmyslových podniků na řešení odborných otázek veřejnou mocí běžná například v Německu, Spojeném Království nebo USA. Příkladem dobré praxe může být i shora zmíněný proces přípravy věcného záměru a posléze i textu paragrafového znění zákona o kybernetické bezpečnosti, kde se podařilo vést věcný dialog mezi podnikatelskou sférou zastoupenou sdruženími nebo samostatně většími podniky a dotčenými veřejnoprávními korporacemi.

5.4. Kybernetická bezpečnost jako agenda rozvojové pomoci

V současné době existují mezi jednotlivými státy velké rozdíly co do formy a intenzity řešení problematiky národní kybernetické bezpečnosti. Nedávná studie UNODC ukázala v tomto směru nikoli překvapivé obrovské rozdíly mezi rozvojovými a rozvinutými státy zjednodušeně označované jako rozdíly mezi severem a jihem . Při následném projednávání výstupů této studie v rámci expertní skupiny UNODC pro kyberkriminalitu a kybernetickou bezpečnost byly tyto rozdíly nejen evidentní ale z nebývale ostré výměny názorů vyplynula potřeba zabývat se otázkou kybernetické bezpečnosti jako integrální součástí agendy rozvojové pomoci. Důležitost dostupnosti bezpečně fungující informační a komunikační infrastruktury je totiž možno srovnat s důležitostí ostatních základních společenských funkcionalit – vlády rozvojových států však nedisponují dostatečnými finančními ani technickými kapacitami k jejímu zajištění.

Z výše uvedeného plyne, že motivace rozvinutých států k investicím do bezpečnosti informační a komunikační infrastruktury v rozvojových státech má být motivována a legitimována stejnými morálními důvody jako např. potravinová pomoc nebo pomoc s rozvojem základní technické nebo dopravní infrastruktury. V tomto případě však nemusí být motivace rozvinutých států pouze morální resp. sociální, ale může jít o prostý důsledek prosté utilitaristické úvahy ekonomické resp. politické.

Obecně platí, že je z hlediska nákladovosti výhodnější pokrývat kybernetické bezpečnostní incidenty pokud možno co nejblíže místu jejich vzniku, a to z hlediska časového i geografického. Poskytují-li pak rozvojové země z důvodu neschopnosti investovat do bezpečnostních opatření něco jako bezpečné přístavy pro vznik a vývoj kybernetických bezpečnostních incidentů, je logicky zájmem cílových států (a většinou jde naopak právě o státy rozvinuté) pokrýt příslušná bezpečnostní rizika shora popsaným způsobem. Strategické zaměření rozvojové pomoci do sektoru kybernetické bezpečnosti přitom může nikoli jen zprostředkovaně ale přímo pomoci řešení bezpečnostní situace nejen ve státech, kam pomoc přímo směřuje ale možná i významnějším způsobem v zemích, kde se kybernetické bezpečnostní incidenty projevují. Dárce tedy v tomto případě chrání prostřednictvím své intervence sám sebe (podobně jako např. rozvojová pomoc směřující ke zvyšování kvality života vede ke snižování nelegální migrace a omezování následných problémů ekonomických, sociálních apod.)

Rozvojová pomoc v sektoru kybernetické bezpečnosti má speciálně v případě České republiky ještě další rozměr, a to podporu tuzemského výzkumu, vývoje a

průmyslu v oboru pokročilých informačních a komunikačních technologií. Česká republika se, dlužno říci i přes dosavadní absenci prakticky jakékoli veřejné podpory, dostala na špici v oboru kybernetické bezpečnosti, ať už jde o oblast primárního výzkumu (nikoli jen v oboru ICT, ale i v oboru práva, psychologie nebo sociálních věd), experimentálního a aplikovaného vývoje nebo i komerčních aplikací. Existuje tedy v současné době u nás řada akademických pracovišť a podnikatelských subjektů, jejichž výsledky jsou plně srovnatelné v mezinárodním (nikoli jen evropském) měřítku a mohou řešit nejen aktuální problémy naší národní kybernetické bezpečnosti, ale jsou použitelné prakticky v libovolném národním nebo nadnárodní prostřední. Zaměří-li se pak do toho sektoru prostředky určené na rozvojovou pomoc (tj. pokud budou české instituce díky českým rozvojovým programům řešit problémy kybernetické bezpečnosti rozvojových zemí), bude tímto způsobem možno obecně podporovat další rozvoj tohoto sektoru v České republice, to přitom bez toho, aby se jednalo o zakázanou veřejnou podporu nebo jinou formu zakázaného narušování tržního prostředí.

PŘÍLOHA 2. – AKTIVNÍ KYBERNETICKÁ OBRANA

1. Cíle studie

- Popsat souvislosti diskurzu okolo tzv. „aktivní kybernetické obrany“ (ACD).
- Identifikovat základní metody a principy ACD.
- Navrhnout podobu simulace, testující jak metody, tak použité technologie.

2. Úvodem ACD

Diskuse ohledně aktivní kybernetické obrany (dále jen ACD – active cyber defense) se začala intenzivně rozvíjet v letech 2010 – 2012. Anoncovaná konference CyCon zaměřená pouze na aktivní obranu organizovaná estonským centrem excelence zaměřeným na kybernetickou obranu (NATO CCD COE) na rok 2014 jen definitivně potvrzuje trend, kterým se bude kybernetická obrana (ochrana) dále vyvíjet. To s sebou nese řadu otázek i poměrně komplikovaných právních dilemat.

Prvně je nutné vysvětlit proč se v tomto kontextu již nepoužívá např. aktivní kybernetická ochrana či bezpečnost, ale přímo obrana. Zatímco v kontextu termínu „kybernetická bezpečnost“ používaného v obecném slova smyslu ve všech prostředích, kde se s problematikou bezpečnosti ICT lze setkat, se termín „obrana“ používá v armádním prostředí. I když se jedná de facto o stejnou formu ochrany jako v případě např. kritické infrastruktury, armádní kruhy mají tendenci bránit a ne chránit. Je to zajímavý jev, který je vidět v celé řadě zemí, Česká republika není výjimkou. Se vznikem konceptu ACD bylo již zřejmé, že jiný termín než „obrana“ použít ani nelze a to především proto, že ACD vyžaduje aktivní preemptivní činnost v kyberprostoru a tudíž předpokládá či přímo vyhledává potenciální útočníky.

Pojem „aktivní kybernetická obrana“ se poprvé uceleně objevil ve strategickém konceptu amerického ministerstva obrany jako: „synchronizovaná a v reálném čase proveditelná kapacita odhalit, objevit, analyzovat a usměrnit hrozby a zranitelnosti. Staví na tradičních přístupech obrany sítí a systémů ministerstva obrany uplatňujíce nejlepší zkušenosti. (...) k zastavení průniku předtím, než dojde ke škodě. Protože pokusy o průnik nelze vždy zastavit na hranici prostoru našich sítí, tato obrana se

zaměřuje na operace uvnitř těchto hranic pokročilými senzory k detekci, odhalení, zmapování a usměrnění nežádoucích aktivit.“ [18]

Drtivá většina nástrojů, které se používají v

Akcent na celou problematiku ACD se postupně budoval vždy v kontextu konkrétních incidentů, u kterých bylo čím dál více zřejmější, že jim nelze předcházet sebelepší pasivní kybernetickou ochranou. Pokud se útočník rozhodne, že chce dosáhnout svého cíle, tak jej jednoduše dosáhne. Není důležité, zda se jedná o útok státního nebo nestátního aktéra, i když je nasnadě úvaha, že silný stát s dostatečnými prostředky a špičkovým výzkumem v pozadí patří mezi nejvážnější aktéry. Organizovaný zločin však v této věci nehraje roli výrazně menší. Celý kriminální komplex za virem Zeus je toho jedním z důkazů, nicméně i operace Red October vykazuje rysy spíše extrémně sofistikovaného, decentralizovaného a odolného organizovaného zločinu prodávajícího zpravodajské informace státům. Proti takové hrozbě se nelze bránit zapnutou firewall, antivirem nebo i systémy detekující průnik – IDS. V kontextu této úvahy začaly státy s budováním strategického konceptu aktivní kybernetické obrany, ve kterém bude s velkou pravděpodobností USA na špici. Jejich US Cyber Command patří otevřeně do armádních struktur s cílem realizovat „všechny spektra vojenských operací v kybernetickém prostoru.“[19] Fakt, že USA míní do nově vzniklého vojenského útvaru intenzivně investovat potvrzuje jejich anoncování navýšení o tisíce zaměstnanců do roku 2016.[20]

Kyberprostor vykazuje řadu specifických vlastností, kterým jistě vévodí problém přisouzení útoku aktérovi. V prostředí, kde má útočník natolik navrch, že dodržením základních pravidel po sobě nezanechá žádné stopy, je zřejmé, že útočné činnosti budou nadřazené obranným.[21] Pasivní obrana má jednoduše natolik limitované možnosti, že v kombinaci s problémem přisouzení a obecnou dynamikou kyberprostoru akademici, vojenští stratégové, poradci a odborníci v oboru shodně došli k závěru, že aktivní obrana je jedinou logickou cestou, jak se vypořádat s rostoucí vážností a precizností

[18] DoD and US-DoD, *DEPARTMENT OF DEFENSE STRATEGY FOR OPERATING IN CYBERSPACE*.
[19] Ibid.
[20] Tilghman, “U.S. Cyber Command to Hire Thousands of Troops, Civilians | Federal Times | Federaltimes.com.”
[21] Steinbruner, *Proceedings of a Workshop on Deterring CyberAttack*, 90.

kybernetických incidentů.[22] To s sebou nese řadu úskalí, jejichž popis následuje v celé této studii.

2.1. Cyber-kill-chain – řetězec úkonů hackera vedoucí k cíli

Pro praktické porozumění postupu hackerů se používá různých modelů tzv. rozfázování, kterému se v angličtině již zažitým termínem říká „cyber-kill-chain." Různí analytici přišli s různými modely dle dílčích fází, které akcentují. Vesměs se ale jedná o jisté přípravné a rešeršní fáze přes samotný útok k získání kontroly po spuštění cílových akcí (někdy se uvádí v závěru udržení zkompromitovaného systému v moci hackerů). Cílem tohoto analytického rozfázování je především odlišit různé přístupy či reakce v různých fázích. Jak již bylo řečeno výše, americké ministerstvo obrany je připravené k celému spektru kybernetických operací i v momentě, kdy útočník pronikne do systému.

Je třeba vzít v úvahu, že jedná-li se např. o cílený průnik k získání kritických zpravodajských informací, které mohou být k dispozici i v systémech kritické infrastruktury, celý útok může být precizně zorchestrovanou operací trvající řádově desítky minut. Úplně stejně se však může jednat o měsíce aktivní APT (Advanced Persistent Threat, viz. níže.). Právě z důvodu široké variace možných útoků se přistupuje k aktivní kybernetické obraně, kdy zdokumentování útoku není řešením, ale je nutné se reálně vypořádat s probíhající situací, její neustálou změnou a též s inteligentními útočníky na straně druhé, které využijí všech strategických prostředků k dosažení svého cíle. Aktivní kybernetická obrana se tak nehodí pro standardní ochranu domácích počítačů, ale především tam, kde v kontextu elementárního risk modelu je vysoká hodnota motivace ze strany útočníka.

Prvně se tento analytický přístup objevil v práci zpracovávané v největší obranné korporaci na světě, Martin Lockheed,[23] výchozí model je následující:

[22] Lachow, "Active Cyber Defense - A Framework for Policymakers."
[23] Hutchins, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains."

Obrázek 7 – Cyber-kill-chain – výchozí model zpracovaný v Lockheed Martin v roce 2005

1. **Reconnaissance** (průzkum) – V této fázi útočníci vyhledávají vhodné cíle, spouští detektory zranitelností, hledají proniknutelné webové stránky, typicky sborníky z konferencí, kde jsou emaily na významné instituce a blízký přístup k technologiím a vyšším znalostem.

2. **Weaponization** (ozbrojení/specifické nabití) – Sestavování na míru vytvořeného trojského koně se specifickým kódem. V této fázi se využívá v anglickém jazyce přirovnání k nabití hlavice (payload) do nosiče (delivery unit). Nicméně v kontextu kybernetické zbraně (nástroje) se jedná o nastavení automatizovaného kódu pro specifické účely nebo cíle. Může se jednat o PDF soubor v mailu, MS Office dokumenty nebo i jen webovou stránku. Na OS X se dlouhodobě řeší problém s trojany v podobě softwaru, který se tváří naopak jako nástroj na jejich odstranění a vede se o tom široká debata.[24]

3. **Delivery** (doručení) – Přenesení nabitého nosiče k cíli. Lockheed Martin CSIRT identifikoval v letech 2004 až 2010 tři nejtypičtější metody doručení: email, webová stránka a USB klíčenka.

4. **Exploitation** (exploatace cíle) – Jedná se o fázi, kdy je kód zanesený do cílového počítače úspěšně spuštěn a podaří se mu využít dané zranitelnosti exploatací operačního systému nebo konkrétní aplikace. Může se tak stát bez přičinění uživatele, stejně tak může uživatel tradičněji kód spustit nebo může být zneužito tak běžných pomůcek, jako je automatické spouštění po vložení USB klíčenky a celý proces se odehraje na pozadí, aniž by o čemkoliv uživatel věděl.

5. **Installation** (instalace) – Trojan v tuto fázi otevírá zadní vrátka napadeného systému a kontaktuje útočníka o úspěšně provedené exploataci.

6. **Command & Control** (C2 neboli převzetí kontroly) – Hacker dostává zprávu o úspěšné exploataci a zajišťuje kontrolu nad počítačem. Nejedná

[24] MacKeeper nebo MaxDefender se navenek tváří, že odstraňují nainstalovaný malware. Bylo prokázáno, že samy dělají činnosti, které nejsou uživateli známé stejně jako že odstranily jiný malware.

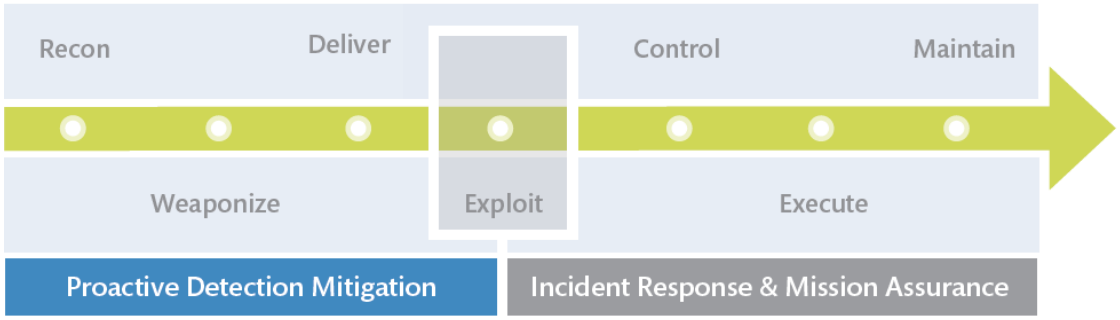
se o možnost hýbat myší na dálku, ale o možnost využívání zpravidla veškerých běžných prostředků cíleného počítače bez vědomí uživatele.

7. **Act** (actions on objectives – dosažení cíle) – Až v tuto chvíli hacker realizuje své konkrétní záměry, se kterými celou tuto útočnou operaci realizovali. Zpravidla se jedná o získání klíčových dat, nicméně samotné převzetí může být účelně použito i pro realizaci DDoS útoku. Takto zkompromitovanému počítači se říká – Zombie.

8. **Maintain** (udržení) – Někdy se jako poslední fáze uvádí udržení si zkompromitovaného počítače pod kontrolou, protože se předpokládá, že v citlivých systémech bude bezpečnostní tým podobné útoky odhalovat a reagovat na ně. Pak je potřeba znát dostatek právě existujících zranitelností, aby bylo možno v případě ztráty kontroly v jiné podobě celý systém obratem infiltrovat znovu.

Celý tento souhrn sedmi (osmi) kroků je kritický právě v tom, jakým způsobem je v každé fázi možné reagovat aktivity útočníka. Upevnění tohoto analytického modelu snižuje míru pravděpodobnosti úspěchu útočníka, informuje v pravou chvíli bezpečnostní obranné kapacity, usměrňuje významnost jednotlivých postupů a otevírá prostor pro implementaci řady proměnných, ze kterých je možné usuzovat vážnost konkrétních kroků útočníka a v reálném čase řídit obrannou operaci. V neposlední řadě tento postup přináší značné znalosti o metodách, dovednostech a vůli útočníka, ale též znalosti o zranitelnostech na straně oběti.

Od doby, kdy Lockheed Martin přišel s výše uvedeným modelem, objevilo se těchto řetězců více. Např. americká obranná společnost MITRE corporation nabízí následující, jen trošku rozšířenější, model:



Obrázek 8 – Cyber-kill-chain podle americké korporace MITRE.

Na tomto diagramu je velmi dobře vidět doba, kdy je nasazení nástrojů aktivní kybernetické obrany na místě bez ohledu na to, že je pochopitelně vhodné tento mix přístupů uplatňovat i po kompromitaci systému (viz. *Tabulka 1*). V každé fázi je důležité uplatnit vhodnou metodu nejen pro odvrácení útoku samotného, ale především pro získání času, který umožní získat klíčové znalosti pro odvrácení cíle celého útoku.

Navíc, ne vždy je uzavření celého systému v případě proniknutí možné. Řídící systémy SCADA (supervisory control and data acquisition) využívané v průmyslových podnicích je důležité udržet v chodu, nikoli bez průniku. Právě v těchto systémech je z titulu bezpečného provozu často velmi komplikované byť jen monitorování toku dat za účelem hledání anomálií, protože jakýkoliv zásah i za účelem bezpečnosti je pro provozovatele těchto systémů rizikem. Pokud vše funguje, není slovy jejich provozovatelů důvodu do těchto systémů zasahovat. O to víc jsou napadnutelné. I to bylo nejspíše důvodem, proč SCADA systémy společnosti Siemens byly i několik let po útoku virem Stuxnet stále provozované se stejnou zranitelností.[25]

	Proaktivní vhodná metoda			
Fáze útoku	**detekce**	**klam**	**terminace**	**reakce na incident**
Recon	✓			
Weaponize	✓			
Deliver	✓	✓		
Exploit	✓	✓	✓	✓
Control		✓	✓	✓
Execute			✓	✓
Maintain			✓	✓

Tabulka 1 – Vhodná metoda obrany ve vztahu k fázi útoku hackera.

[25] Collins and McCombie, "Stuxnet: The Emergence of a New Cyber Weapon and i."

3. Dělení aktivní obrany dle strategického přístupu

Existuje celá řada možných dělení aktivní kybernetické obrany, např. dle aktivity vykonávané obráncem nebo podoby útočníka, zda se jedná o státního aktéra či organizovanou zločineckou skupinu navíc po světě absolutně decentralizovanou. Jinak se bude připravovat obrana proti jednomu klíčovému průniku do systému, kde již samotná implementace škodlivého kódu v řádu vteřin může způsobit katastrofu, typicky třeba otevření přehrady. Že jsou důsledky takového útoku již jednoznačným použitím síly dle článku 2(4) Charty OSN bylo diskutováno,[26] to však nezabrání útočníkovi konat, zvlášť s minimální pravděpodobností odhalení. Jiný případ je kybernetická špionáž, která též patří do kategorie útoků, jenž se nepřestanou odehrávat na základě dobře nakonfigurované firewall nebo platných regulí mezinárodního práva. Ať se budeme na možnosti obrany dívat prizmatem typu útoku, možná lépe řečeno typem kybernetické operace, nebo charakterem útočníka, vždy se bude jednat o následující tři aktivity, které během aktivní kybernetické obrany bude obránce realizovat, buď v kombinaci nebo každou zvlášť:[27]

1. Detekce a forenzní analýza (detection and forensics)
2. Klamání (deception)
3. Terminace (termination)

Výše uvedené tři podoby aktivní obrany lze vnímat jako po sobě jdoucí přístupy či dílčí strategie, které se vzájemně nevylučují, ba naopak, doplňují. V případě hackerského útoku na nějaký informační systém se v IT bezpečnosti dlouhodobě řeší zranitelnosti tohoto systému, popř. nastane-li incident, tak jeho analýza a postup k odstranění zranitelností, které útok *umožnily*, nikoli však *způsobily*. Pokud zranitelností hacker zná několik, např. Stuxnet využíval tři,[28] pak odstranění této zranitelnosti snižuje pravděpodobnost úspěchu útočníka, nikoli však všechny jeho možnosti. Pokud útočník používá automatizované nástroje na vyhledávání zranitelností, které jsou volně dostupné, neboť se jedná de facto i o nástroj použitelný pro bezpečnostní techniky, pak má útočník výrazně navrch, proti obránci, který musí ručně aktualizovat systémy. Proti podobnému typu útoku – což je v podstatě každý záměrný útok – se nedá bránit konvenčními metodami bezpečnostní prevence.

[26] Schmitt, "International Law in Cyberspace: The Koh Speech An."
[27] Lachow, "Active Cyber Defense - A Framework for Policymakers."
[28] Rid, *Cyber War Will Not Take Place*.

4. Tři přístupy k aktivní obraně

4.1. Strategie detekce

V prvním případě se jedná o specifické detekční systémy. Typicky např. IDS – Intrusion Detection Systems, systémy detekující průnik do ICT infrastruktury, NIDS – Network Intrusion Detection System nebo IPS – Intrusion Prevention Systems, systémy aktivně preventivně předcházející průniku. Dalšími příklady detekčních metod jsou behaviorální analýzy, ačkoliv by se daly zařadit do výše dvou zmíněných. Behaviorální analýzy detekují anomálie v síti, které následně sleduje, analyzuje a dokumentuje. Díky těmto metodám se jednak dá odhalit celá řada aktivit, během kterých útočník pouze prozkoumává informační systém či síť před napadením, ale též odhalit a obráncům přiblížit schopnosti a dovednosti útočníků včetně odhadu jejich počtu.

Detekční metody jsou svým způsobem naprosto klíčové, protože řada napadených o tom, že někdo listuje jejich kritickými daty nebo ovládá jejich průmyslové systémy nemají potuchy i roky.[29] Operace Red October je jen jedním příkladem, kdy všichni z napadených o průniku nevěděli více jak pět let. Když se obdobné případy začaly objevovat pravidelně, vznikl termín APT – Advanced Persistent Threat. Termín poukazuje na typ útoku, během kterého útočník např. jen získá kontrolu nad cíleným zařízením, nicméně nic dalšího již (pravidelně) nevykonává, nebo jen velmi nenápadně, a tak se kompromitace špatně detekuje.

Následující tabulka pouze stručně nastiňuje výběr z komerčních produktů, které se řadí mezi NDIS systémy:

[29] Lachow, "Active Cyber Defense - A Framework for Policymakers."

Product	Vendor	Description
Enterprise Security for Communication and Collaboration	Trend Micro	Email, instant messaging, and collaboration systems connect your employees, partners, and customers, but they also open doors for cybercriminals. In...
Apani EpiForce	Apani Networks	Apani® EpiForce® is a software-based, cross-platform server isolation, encryption and access management solution that enables logical security zoning...
Cisco Catalyst 6500 Series Intrusion Detection System Module	Cisco Systems Inc	With the increased complexity of security threats, such as malicious Internet worms, denial of service (DoS) attacks, and e-business application...
Core Controller	Hewlett-Packard	Core network upgrades driven by data center consolidation, high performance computing and high bandwidth applications like video on demand and file...
Corero Top Layer IPS™	Corero Network Security	Top Layer IPS™ (Intrusion Prevention System) delivers the most comprehensive network protection compared to other IPS products. The company's IPS...
Digital Vaccine® Security Filter Service	Hewlett-Packard	In providing the vulnerability analysis for SANS every week, the TippingPoint DVLabs security team simultaneously develops new attack filters to address...

Obrázek 9 – Ukázka NDIS systémů. Více na http://mosaicsecurity.com/categories/60-network-intrusion-detection-system

Detekční systémy jsou naprosto klíčovou součástí spektra aktivní kybernetické obrany. Již dnes jich řada společností používá pro detekci anomálií v jejich síti, typicky banky. V případě nasazení virů jako je např. Zeus, který může pozměnit obsah stránek a tak z nich odesílat data, která si banka nepřála, aby bylo odeslány je přímo místo vhodné pro detekci anomálie. V případě, že se tak děje z počítače uživatele je pochopitelně pro banku nesmírně těžké takovou detekci realizovat, nicméně následné pokusy o přihlášení dle zkompromitovaných údajů v bance, popř. brute-force útoky na databáze karet jsou denní realitou. V takovém případě jsou detekční systémy anomálií v síti tím prvním, co umožňuje bezpečnostním specialistům odhalovat nevhodné chování na síti.[30]

Detekční systémy mohou fungovat s přednastavenými vzorci, nicméně nejvhodnější a nejspolehlivější metodou předcházející falešným alarmům je vytvoření si vlastního vzorce. Detekční systém po nějakou dobu monitoruje běžné chování na síti a vytvoří vzorec standardního průtoku dat. V případě, že je tento standard narušen, oznámí anomálii operátorovi.

Takový přístup má řadu úskalí, nastavení míru falešného alarmu je tím nejproblematičtějším. Nicméně v případě průmyslových podniků je velký prostor pro sbírání dat po poměrně dlouhou dobu a chod těchto systémů je z dlouhodobého hlediska

[30] Averbuch and Siboni, "The Classic Cyber Defense Methods Have Failed – Wh."

stabilní, inovuje se méně než webové servery a podléhá striktním regulacím, které jistou míru stability onoho vzorce zajišťují.

4.2. Strategie odepření a klamu

Třetí strategický přístup je starý jako lidstvo samo. Kromě toho, že je možné útočníkům nabídnout na míru připravené přihlašovací údaje do systému, které v případě použití spustí alarm a tak zajistí obráncům dokonalý přehled o aktivitě útočníka v předem připraveném zorchestrovaném scénáři, může se jednat též i o celé virtuální systémy, tzv. honey networks nebo pouze nastražené počítače, tzv. honey pots. Oklamání útočníka, který se domnívá, že právě pronikl do tíženého systému je poměrně jednoduchá, není však dlouhodobě spolehlivá. Je to stejná taktika, jakou volí útočníci, když se snaží uživatele přimět k otevření líbivého emailu, zatímco oni následně získávají kontrolu nad celým zařízením. Tyto metody lze zařadit i do pasivní obrany, nicméně budování honeypotů je již jistou mírou aktivity a proto je často řazena spíše mezi obranu aktivní.

Honeypoty jsou navržené k tomu, aby sesbíraly co nejvíce informací o útočníkovi a odhalily zranitelná místa na reálném systému. Některé soukromé společnosti se dokonce specializují přímo na sbírání zpravodajských informací o útočnících, aby napadený poznal motiv útočníka a dokázal útoku předcházet nebo lépe kategorizovat citlivá data.[31] Cílem těchto systémů je oklamat útočníka a přimět ho ke konkrétní předpověditelné aktivitě, která nahrává CND – obraně. Strategický přístup odepřením a klamem[32] je tou základnější metodou aktivní kybernetické obrany.

Honeynet je síť takových klamných počítačů zapojených do klamné sítě. Technicky je možné takovou síť klamných počítačů vytvořit kompletně ve virtuálním prostředí.[33] Subkategorií honeypotů jsou tzv. tarpit systémy, např. Labrea Tarpit. Jedná se o virtuální server, který se na venek tváří, že je umístěn dokonce přímo na adrese jako pravý server. Tyto servery obratem odesílají hodnověrné, za to extrémně zbytečné odpovědi na pokusy o připojení. Cílem je, že automatické prozkoumávání sítě se stává nepoužitelným, neboť tento systém precizně zahltí útočníkův log. Získává se tak velmi cenný čas pro obránce.[34]

[31] Příkladem může být např. CrowdStrike nebo Mandiant.
[32] Z anglického originálu „deny and deception."
[33] Qassrawi and Hongli, "Deception Methodology in Virtual Honeypots."
[34] Goh, "Intrusion Deception in Defense of Computer Systems."

V USA, konkrétně v korporaci MITRE, probíhal výzkum vedený Kristin Heckmanovou, jehož výsledkem bylo zjištění, že sebelepší honeypot, honey network (klamný virtuální ICT systém) nebo jakákoliv obrana v kontextu klamné obranné strategie (denial and deception strategy) informační systémy nikdy neubrání.[35] V průběhu tohoto experimentu byly nainstalovány klamné sítě ve virtuálním prostředí včetně celé infrastruktury a probíhala simulace útoku, celé operaci se říkalo Blackjack.

4.3. Strategie aktivní terminace

V prvním případě se jedná o tu nejtypičtější aktivní obranu, protiútok. Může se jednat o preemptivní úder, preventivní úder, ale také o implementaci vlastní logické bomby, která se zaktivuje v případě, že k útoku na připravovanou stranu dojde. Taková aktivace může okamžitě zhatit např. přenos ukradených dat nebo rozbít C&C infrastrukturu útočníka, kterého mimo jiné díky takové pasti je možné přistihnout činu.

Z objektivního hlediska je velmi komplikované odříznout útočníka od jeho infrastruktury. Je tedy nutné nahlížet celý problém aktivní terminace nikoli z radikální perspektivy „fyzické likvidace útočníkovy infrastruktury“, nábrž z perspektivy, jak útočníka odříznout od jeho prostředků, které používá k útoku.

Jedná-li se o DDoS útok, pak jsou možnosti terminace dvojí.

1. Nalezení serverů C&C (Command & Control), které útočník používá k ovládání botnetu.
    a. Tyto servery je možné buď též obdobným útokem vyřadit z provozu nebo
    b. je možné zasáhnout pouze ty infikované součásti serveru jakousi léčebnou metodou a tím tak odříznout útočníka od možnosti jej ovládat,
    c. kontaktovat provozovatele serveru s informací, že patří do sítě C&C serverů botnetu, obeznámit ho se zneužitou zranitelností a vyčkat až administrátor zasáhne sám.

[35] Heckman et al., “Active Cyber Defense with Denial and Deception: A .”

Prakticky budou všechny tyto metody komplikované, protože každý strategicky uvažující útočník bude C&C servery ovládat různými metodami, aby jej odhalení jedné metody neodřízlo od ovládání celého botnetu. I z toho důvodu je C&C serverů i několik.

2. Nezaměřit se na servery, ale na všechny zneužité zombie počítače, které jsou těmito servery ovládané. Komplikace vícero různých metod jejich ovládání uvedená výše, může být ještě komplikovanější zde, protože útočník může používat celé spektrum zranitelností a s velkou pravděpodobností bude.

To, že samotná terminace je komplexním problémem a není úplně snadné ji vykonat, ví své Microsoft, který se účastnil v nedávné době sesazení ZeroAccess botnetu.[36] Celé této akce se účastnila řada bezpečnostních firem, Microsoft, FBI atd. Je tedy zřejmé, že vypnutí botnetu není jednoduchým úkolem, jak z právního hlediska (zasahuje se s jistotou mimo území jednoho státu), tak z hlediska technického. Do budoucna lze jen předpokládat, že decentralizovaným ovládáním, psaním kódu trojských koní zneužívajícím nekonečné množství zranitelností bude tento úkol o poznání složitější.

V případě, že se jedná o specificky zaměřený útok na konkrétní systém v průmyslovém areálu, může být za terminaci považován byť i jediný zásah proti právě útočícímu počítači, ze kterého je útok prováděn. I taková situace může být značně komplikovaná, protože se může jednat o nastrčené zařízení mimo území státu, ve kterém se vyskytuje průmyslové zařízení a jakýkoliv zásah tak může mít komplikované legislativní důsledky. Útočník vědomý si tohoto dilematu může zneužít veřejně známé portály, jejichž terminace je jednoduše nemyslitelná. V takovém případě by bylo na místě odpojit průmyslový řídící systém, což je zase nemyslitelné pro jeho provozovatele. Dilemat je v takových chvílích tedy celá řada.

5. Simulace

5.1. Smysl simulace útoku

Vhodné uplatnění systémů, přístupů a metod aktivní kybernetické obrany není možné bez simulačních polygonů, testů na laboratorním prostředí a následném testovacím nasazení na ostrých systémech. Z části se jedná o separátní systémy, které mohou fungovat samy o sobě (detekční systémy, honeypoty) nebo o čistý counter-

[36] http://threatpost.com/microsoft-and-friends-take-down-zeroaccess-botnet/103122

hacking, který zase není možné (oficiálně) snadno uplatnit bez analýzy potenciálních právních důsledků takového jednání. Simulacemi je možné dosáhnout rozvinutí komplexní strategie obrany při využití celého spektra prostředků pro uplatnění v různých specifických situacích. Je zřejmé, že obrana na úrovni jaderné elektrárny bude mít značně odlišné možnosti než např. v případě obrany systémů řídících větrné elektrárny. V rámci tvorby této simulace by se TPEB měla změřit jen na SCADA systémy, které jsou dnes kriticky nechráněné, simulace na nich komplikované a zpravidla neprováděné.

Klíčové pro uplatnění tohoto modelu ochrany kritické infrastruktury je:

1. Návrh vhodného komplexu nasazených technologií.
2. Dohoda s konkrétním provozovatelem kritické infrastruktury, který by poskytl nutné především materiální prostředky.
3. Vytvoření vhodného modelu řízení celého nastaveného komplexu.
4. Vytvoření mapy standardního toku dat detekčními systémy.
5. Tvorba řady honeypotů, kam je možné případné anomálie rovnou směrovat a následně analyzovat.
6. Pro trénink týmu vytvořit řadu scénářů, kterým mohou čelit a rozvinout tak týmové dovednosti operátorů.
7. Připravit scénáře dílčích terminací až po scénář pohotovostního krizového protiútoku v případě jednoznačně cíleného útoku proti kritickým systémům.
8. Simulovat konkrétní útoky na takto připraveném simulačním prostředí do míry, kdy bude možné celý tento obranný model nasadit v praxi.
9. Vše perfektně zdokumentovat pro další případy tvorby obranného týmu a konfigurace vhodných nástrojů ACD na SCADA systémy.

5.2. Podoba simulace útoku na cíle kritické infrastruktury (SCADA)

Následující popis je elementárním návrhem simulace, která by měla být detailně rozpracována ve spolupráci s členem TPEB, jehož technologie se budou k simulaci uplatňovat a ve spoluprací s tím členem, který pro simulaci poskytne vhodnou infrastrukturu. Na místě je určitě i úzká spolupráce se dodavatelskými společnostmi

specifických využívaných systémů nad rámec produktů a řešení poskytnutých členy (Microsoft, Cisco, HP/DELL/IBM).

5.3. Cíle simulovaného útoku

- zjistit míru ochrany
- odhalit dílčí zranitelnosti na prvcích kritické infrastruktury
- vyzkoušet krizové procesní postupy personálu v případě napadení, popř. navrhnout jejich vylepšení
- simulovat více různě vážných incidentů
- celou simulaci provádět na separovaném SCADA systému

5.3.1. Organizace simulace

- **red team** – aktivní útočníci (crackers/hackers) v odděleném prostředí připojeném pouze k internetu (10 dnů)
- **blue team** – aktivní obránci na straně (5 dnů)
- **gray team** – pasivní účastníci provozu cvičení s infikovanými počítači (3 dny)

5.3.2. Cvičení rozdělené do pěti dnů:

- briefing/story behind, zbezpeční sítě a předinstalovaných systémů
- cvičení obrany první linie DMZ systémů, firewallů a otevřených systémů
- průnik do vnitřních řídích systémů, obrana a zajištění útočných kódů
- obrana před masivním DDOS, infiltrace teamu skrze techniky soc. inženýrství
- vyhodnocení a závěr cvičení

5.3.3. Hmotné prostředky pro pořádání cvičení:

- tři oddělené prostory vč. připojení na optickou městskou infrastruktůru
- virtuální datové centrum / polygon, operátorské stanice, telekomunikační zařízení na propojení koncových stanovišť

- internetová konektivita vč. autonomního systému registrovaného v RIPE.NET
- VoIP telefony, ústředna, vysálačky/scannery, GSM modemy
- Whiteboards pro každý team

5.3.4. Nároky na lidské zdroje:

- **RED TEAM** - 3-5 specialistů na UNIX/Windows/TELCO prostředí
- **BLUE TEAM** - 3-10 IT specialistů různých vědomostních oborů
- **GRAY TEAM** - bezpečnostní specialisté a hodnotitelé jednotlivých teamů

5.4. Průběh útoku

Den 1.

Pozadí: energetická společnost zabývající se výrobou, prodejem a distribucí energie, jejichž IT systém byl kompletně dodán na zakázku dodavatelskou servisní společnosti.

Dodaný systém:

- Síť rozdělená do čtyř aktivních zón: OTEVŘENÁ, SERVROVÁ (DMZ), UŽIVATELSKÁ, ŘÍDÍCÍ. Propojená IP protokolem a ochráněna velmi základně nenastavenými telco. zařízením
- OTEVŘENÁ – web společnosti
- SERVROVÁ – smtp/imap/pop3 protokoly
- UŽIVATELSKÁ – předinstalované pracovní stanice, WIFI zařízení
- ŘÍDÍCÍ – specializované a emulované řídící systémy (SCADA)

Úkol dne: zabezpečit a připravit síť na provoz v normálních podmínkách.

Den 2.

Cvičení obrany:

V průběhu dne bude docházet ke standardním průnikům přednastavených “děr” v systému a úkolem modrého teamu je nácvik zjištění tohoto průniku a kompromitování citlivých informací.

Den 3.

Průnik do vnitřních řídích systémů:

Zamezit průniku do vnitřní sítě, eventuálně zjistit pokusy a zajistit permanentní kontinuitu provozu řídících systémů. Zajištění kódu způsobující výpadky systémů.

Den 4.

Nácvik masivního DDOS – Obrana proti DOS/DDOS útokům na úrovni zabezpečení hraničních routerů, infiltrace kódu skrze techniky sociálního inženýrství, násilná degradace a kompromitace modrého teamu – virtuální likvidace nejschopnějšího personálu a zneužití jeho znalosti k prolomení vlastního teamu.

Den 5.

Vyhodnocení a závěr cvičení.

6. Předpoklady

Analýza používaného SW a HW vybavení cvičeného subjektu.

Vytvoření virtuálního duplikátu (1 měsíc).

Příprava 1 měsíc na organizaci operativních nácviků (exploits, předinstalované systémy, zapojení síťových prostředků atd.).

PŘÍLOHA 3. – KOMPARACE VÝZNAMNÝCH KYBERNETICKÝCH INCIDENTŮ

1. Rodina Zeus, Gozi, SpyEye a Citadel

Název	**Zeus**
Cíle	Zcizení peněz, bankovní instituce
Kategorie	Kybernetická kriminalita
Podoba kódu	Trojský kůň
Odhalen kdy	07 / 2007
Odhalen kým	FBI
Stav	Existující i v jiných podobách, zdrojový kód nadále volně k dispozici
Původ/smysl	Organizovaný zločin, ohromně rozšířený, schopný měnit svoji podobu
Specifické vlastnosti	Keystroke logging, form grabbing, phishing.
Formy infekce	Drive-by download – a) autorizovaným stažením aplikace bez obeznámení jejího fungování, b) nezáměrným stažením malware, spyware etc.
Rozsah	Jen v USA na 4 mil. počítačů, 1,5 mil. infekce jen přes Facebook
Výběr z napadených	V první řadě především běžní uživatelé Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek

Viry z této rodiny, jak je jim občas přezdíváno, jsou striktně zaměřeny na neoprávněné získávání přístupových údajů do finančních institucí. Tím nejzákladnějším způsobem je odezírání stisku tlačítek na klávesnici. V případě, že se banka dokázala proti takovému přístupu bránit např. tím, že žádá přepis zaslaného kódu na mobilní

telefon, není výjimkou, že kromě zcizení přihlašovacích údajů škodlivý kód zamění podobu webové stránky, doplní některé formuláře a po jejich vyplnění zašle hackerovi jejich obsah, který si je pečlivě ukládá do databáze. V takovém případě je možné pokračovat napadnutím mobilního telefonu a přeposílat i unikátní ověřovací kódy. Tento typ útoků se nazývá „man-in-the-middle." Název je odvozen od charakteristiky útoku, který je postaven na vložení nežádoucího formuláře, odezírací funkce atp. mezi uživatele a výslednou aplikaci. Nebezpečné na tomto typu útoku je právě fakt, že finanční instituce nemá vždy způsob, jak těmto útokům zamezit, protože nejsou vedeny přímo proti nim.[37]

Techniky kompromitace elektronických bankovních účtů se neustále zlepšují a doby tzv. script kiddies, tedy dětí experimentující s možnostmi bezpečnostních nedostatků dávno minuly. V tomto byznysu se pohybují nejen zkušení hackeři, ale i výrazně mladší, přesto velmi dovední, hackeři. Řadě z nich je kolem dvaceti let v době odhalení a souzení. Objem peněz, které tyto organizované skupiny jsou schopny zcizit se počítá již v řádu stamiliónů dolarů.

Z hlediska bezpečnosti státu jsou často tyto typy kriminální činnosti opomíjeny, jelikož tito útočníci přímo nenapadají systémy kritické infrastruktury (KI) nebo objekty důležité pro obranu státu (ODOS). Důsledkem je často jen povrchní znalost těchto technik u lidí, kteří se ochranou kritické infrastruktury zabývají a též jistá míra necitlivosti na typické phishingové útoky v prostředí průmyslového podniku. Techniky používané k získání osobních přihlašovacích údajů jsou důležité obecně, neboť poukazují na triky, které běžný uživatel, ale i velmi zkušený programátor, nemusí nebo nemůže snadno odhalit.

Dalším společným charakteristickým znakem této rodiny virů je vybudované celé infrastrukturní podsvětí,[38] které je pochopitelně kompletně decentralizované. Mezi prvky takové infrastruktury se řadí např. tzv. neprůstřelný hosting – „bulletproof servers" – který není zpravidla na jednom serveru, nýbrž rovnou na celém botnetu. Takový typ služby se nazývá crime-as-a-service.[39] Nicméně i konkrétní participanti na vývoji specifického kódu nebývají z jedné země, ale znají se pouze přes internet.

1.1. Hlavní charakteristiky viru Zeus a jeho historie

[37] Conroy, *Citadel and Gozi and Zeus, Oh My!*.

[38] Ibid.con

[39] Sood and Enbody, "Crimeware-as-a-service—A Survey of Commoditized Crimeware in the Underground Market."

Zeus patří mezi nejsofistikovanější škodlivé kódy na poli kybernetické kriminality. Jeho původní i současný účel je velmi prostý, získat od nepozorných uživatelů jejich přístupové údaje do internetového bankovnictví, následně převést libovolný objem peněz na účty zprostředkovatelů v zahraničí, kteří je různými běžnými způsoby zlegalizují a v jiných zemích od zprostředkovatelů vybrat významnou část takto zcizených peněz. Celkové škody mohou dosahovat až řádově stovky miliónů dolarů.

První zmínky o škodlivém kódu, který je schopen s extrémní úspěšností odezírat ze zkompromitovaných počítačů nejen formou phishingu, ale i prostým odezíráním z kláves, se objevila v roce 2007.[40] Zeus byl od počátku psán tak, aby byl schopen zmást antivirové ochrany, nicméně ve své době se jednalo o chování, které zatím nebylo v rozsáhlé míře pozorováno. FBI začala na případu pracovat od samého počátku, ale samotný zákrok lze datovat až do roku 2010, kdy bylo obviněno na 37 lidí.[41] Rozsah tohoto případu byl ve své době naprosto ojedinělý, jelikož původci kódu byli vystopování na Ukrajině, zprostředkovatelé ve Velké Británii, ale většina dalších přímo ve Spojených Státech, celkem na sto zapojených lidí, kterým se podařilo zcizit až $70 milónů ačkoliv neměli daleko k získání až $220 miliónů.[42] Věk obviněných se pohyboval především mezi 20-25 lety, i když někteří obvinění měli věk i nad 50 let. Hlavním obviněným hrozily až třicetileté žaláře, nicméně soudy přihlédly k jejich věku a výsledný verdikt se pohyboval v měsících kolem dvou let. Kristina Svechinskaya, která si díky svým svůdným fotografiím vysloužila označení nejsvůdnější hackerka v dějinách, nakonec podepsala přiznání s tím, že bude propuštěna po zaplacení $25.000 dolarů.[43] V této věci se hodně spekulovalo zda FBI neprojevila zájem o začlenění takto talentovaných mladých lidí do svých řad a nenabídla odsouzeným práci, což by jim obratem zajistilo i schopnost se z problémů vykoupit. Jedná se však o čisté spekulace.

Zásadnějším vývojem po tomto případu je rok 2011, kdy se původní zdrojový kód dostává na volný trh skrze hackerská fóra a jeho kompilace prokazuje perfektní schopnosti.[44] Obratem se tak kód dostává do komunity vývojářů, kteří jej mohou libovolně modifikovat a užívat, což má v první řadě za následek rozšíření o schopnost P2P distribuce vlastního zdrojového kódu, ale i operace v kyberprostoru za pomocí

[40] FINKLE, "Hackers Steal U.S. Government, Corporate Data from PCs | Reuters."
[41] FBI, "FBI — Manhattan U.S. Attorney Charges 37 Defendants Involved in Global Bank Fraud Schemes That Used 'Zeus Trojan' and Other Malware to Steal Millions of Dollars from U.S. Bank Accounts."
[42] BBC News, "More Than 100 Arrests, as FBI Uncovers Cyber Crime Ring."
[43] Ranjan, "The Hottest Hacker: Kristina Svechinskaya."
[44] Kruse, "Complete ZeuS Sourcecode Has Been Leaked to the Masses."

vlastního botnetu.[45] Zeus se tak vymyká svým původním tvůrcům, jeho podoba se libovolně mění a s tím i forma hrozby, kterou s sebou nese. Kód Zeus je i po šesti letech od jeho původního objevení stále k dispozici.[46]

1.2. Hlavní charakteristiky viru Gozi

Gozi je velmi podobným kódem výše zmiňovanému s tím rozdílem, že hlavní důraz byl kladen na doplňování reálných webových stránek prvky, které provozovatel, tedy zpravidla finanční instituce – banka, nezamýšlela do svého webu vložit. Tohoto vložení se dosahuje celou řadou bezpečnostních chyb v Internet Exploreru. Typickým příkladem je upozornění, že došlo k napadení stránek banky a proto je nutné, aby uživatel svou identitu potvrdil vyplněním celé řady klíčových osobních údajů do formulářů, které jsou graficky totožné s těmi, které uživatel dobře zná. Část takto vyplněných údajů se odesílá do banky, část rovnou na servery a do databází autorů kódu Gozi.[47] Následuje obdobný proces, jako u viru Zeus.

2. Slammer worm

Název	**Slammer worm**
Cíle	Neznámé
Kategorie	Necílený útok
Podoba kódu	Vir
Odhalen kdy	01 / 2003 – řádově minuty po spuštění
Odhalen kým	Nikdo konkrétní
Stav	Bezpečnostní záplata od Microsoftu zranitelnost vyřešila
Původ	Neznámý
Specifické vlastnosti	Přímé multiplikace sebe sama, nepřímé celosvětové zahlcení internetu
Formy	Specifická, distribuce v jediném packetu UDP na port

[45] Abuse.ch, "ZeuS Gets More Sophisticated Using P2P Techniques | Abuse.ch."
[46] Danhev, "New ZeuS Source Code Based Rootkit Available for Purchase on the Underground Market Webroot Threat Blog."
[47] Jackson, *Gozi Trojan | Dell SecureWorks*.jacks

infekce	1434
Rozsah	75 tis. serverů v řádu minut, 90% všech instalací na světě. Servery s MS SQL, dopad na provoz na letištích, bankoamaty, elektronické volby, jaderná elektrárna

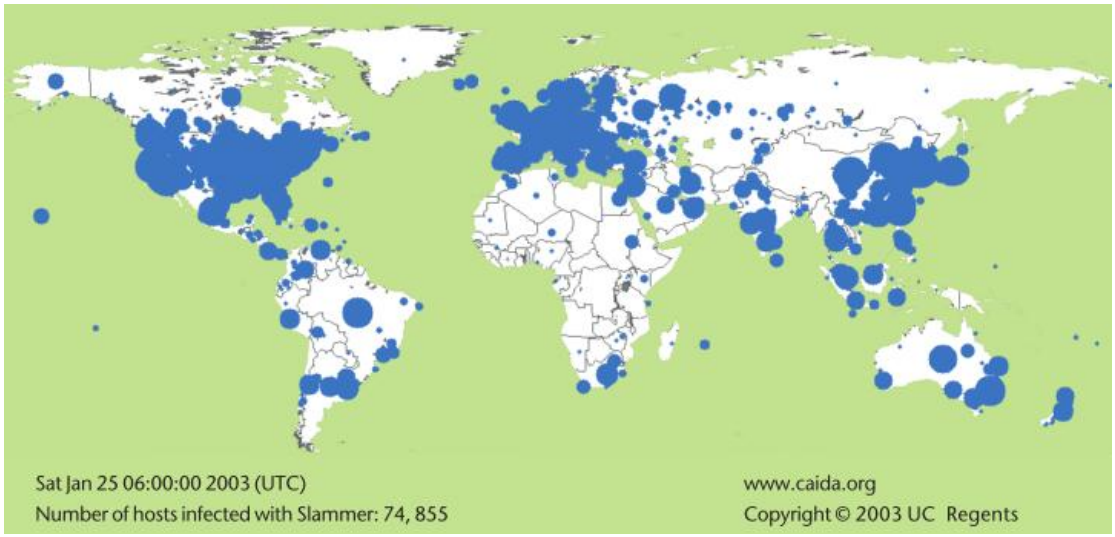
Slammer worm patří mezi jednoduché typy kódů, jejichž účinky jsou však poměrně dramatické. Velikost tohoto viru je pouhých 376B (bytů), jinými slovy kód má přesně 376 znaků. Pro srovnání prázdný Word dokument má velikost 20 tisíc bytů, tj. 20kB. Díky své velikosti se vejde do jednoho packetu IP protokolu, je tedy menší než prázdný email. 23. ledna 2003 se tomuto viru podařilo dostat do jaderné elektrárny Davis-Besse v Oak Harbor ve státě Ohio. K průniku došlo náhodou tím, že servisní firma propojila některé své systémy telefonní linkou T1 se systémy v elektrárně, která byla tou dobou ve dvouleté odstávce po jednom z nejvážnějších jaderných havárií v USA.

Tato událost byla čistě nahodilá. Slammer worm se začal šířit všemi směry toho samého dne, 23. ledna 2003. Využil k tomu bezpečnostní zranitelnost v SQL serveru od firmy Microsoft, v tzv. buffer overflow. Z tohoto místa byl schopen generovat náhodné IP adresy a multiplikovat se po internetu na další SQL servery Microsoftu, pokud na dané IP adrese byl nainstalován. V případě úspěchu nalezení dalšího SQL serveru se tak řetězovou reakcí dokázal v řádu minut šířit na libovolná místa na světě. Paradoxem je fakt, že Microsoft vydal bezpečnostní záplatu již půl roku před šířením viru Slammer worm, nicméně řada administrátorů, včetně těch v Microsoftu nebo elektrárne Davis-Besse, tuto záplatu nenainstalovala.[48] Zajímavostí je též způsob, jak se vir šířil. V normální komunikaci si síťová zařízení vyžádají komunikační kanál, který v případě přijetí protější stranou využijí k zaslání dat. V případě viru Slammer worm k tomuto požadavku nikdy nedošlo. Vir jednoduše využil možnosti odeslat jeden packet na port UDP 1434. Přestože protější strana takový packet nemusela mít zájem přijmout, samotný fakt, že se vir nacházel celý kompletně v jednom packetu, zajistil, že k infekci došlo.

Díky své minimální velikosti mohlo dojít na lince 100 Mbps až k 26 tisícům duplikací během jediné vteřiny. Fakticky tato míra během tří minut od jeho nasazení do sítě díky řetězové reakci narostla na neuvěřitelných 55 miliónů pokusů za vteřinu, celkově vir napadl na 75 tisíc serverů. Výsledkem tak obrovské míry šíření viru ve velmi krátké době byl celkový pokles rychlosti internetu, některé servery byly natolik

[48] Rid, *Cyber War Will Not Take Place*.t

zahlceny, že nedokázaly zpracovávat a odesílat jiná data, než packet s tímto virem. Jeho výhodou byla pravě minimální velikost v jednom packetu, čímž se jednalo o tu nejjednodušší operace pro napadený server a ten ji před ostatními upřednostnil. Slammer worm se stal nejrychleji se multiplikujícím se škodlivým kódem v historii. Dopady byly poměrně značné, přestože se jednalo pouze o narušení chodu internetu bez konkrétních jiných záměrů, např. mazání dat na serveru. Kromě již zmíněného napadení jaderné elektrárny došlo k výpadkům celých sítí, např. bankomatů nebo letišť, řada letů musela být zrušena, došlo i ke komplikacím během elektronických voleb.[49]



Obrázek 10 - Rozsah infekce po 30 minutách

Ačkoliv se tedy jedná o úžasnou ukázku schopnosti viru se multiplikovat na desetitisíce míst (desítky miliónů potencionálních cílů v jedné vteřině), nebyl prokázán viru záměr nést tzv. payload, kód, který by po doručení na místo způsobil škody. Nicméně už samotná schopnost zahltit komunikační linky způsobil podstatné výše zmíněn škody, důsledky v jaderné elektrárně ale byly ještě o poznání horší a tím se prokazují nezamýšlené důsledky takového typu viru, zopakujme o velikosti 376 bytů. Protože řídící systémy elektrárny byly přímo připojené ke kancelářské síti a ta doznala díky přehlcení virem kolapsu, zkolabovaly i některé řídící systémy. Je zřejmé, že takový přístup zajišťující monitoring řídících systémů na dálku by měl být read-only a tudíž by dopad na řídící systémy měl být nulový, praxe nejspíš byla taková, že i takto banální bezpečnostní opatření nepovažovali administrátoři za důležité. Zkolabované řídící

[49] Moore et al., "Inside the Slammer Worm."s

systémy měly na starosti měření teploty jádra reaktoru, chladící systémy a senzory měřící hladinu radiace.[50]

V případě, že se incident dotkne těchto řídících systémů, s velkou pravděpodobností se ještě nejedná o riziko ovládání jejich funkcí, nicméně manipulace s daty může ovlivnit chování personálu, jak se to např. dělo v případě jaderného zařízení v íránském Natanzu při útoku viru Stuxnet (viz. kapitola **Chyba! Nenalezen zdroj odkazů. – Chyba! Nenalezen zdroj odkazů.**) nebo kombinovaného útoku na syrský jaderný reaktor v syrksém regionu Deir ez-Zor (viz. kapitola **Chyba! Nenalezen zdroj odkazů. – Chyba! Nenalezen zdroj odkazů.**).

3. Operace Black Tulip (DigiNotar)

Název	**Operace Black Tulip – útok na společnost DigiNotar**
Cíle	Cílené na servery DigiNotar se záměrem získat certifikáty. Nezáměrný mohl být krach Diginotar a ztráta věrohodnosti
Kategorie	Cílený strategický útok
Podoba kódu	N/A
Odhalen kdy	27. srpna 2011, šest týdnů po útoku
Odhalen kým	Náhodně íránským uživatelem Alibo při kontrole gmailu
Stav	Certifikáty od DigiNotar nikdo neuznává, firma zkrachovala
Původ	Comodo Hacker, Írán. Patriot. Byla nařčena i americká NSA, která však tvrdí, že pouze poukázala na aktivitu cizí zpravodajské služby. Pozadí národního státu Írán velmi pravděpodobé.
Specifické vlastnosti	Útok spočíval ve vygenerování falešných certifikátů a jejich následného použití při vniknutí do zabezpečených systémů

[50] Poulsen, "Slammer Worm Crashed Ohio Nuke Plant Net • The Register."

Formy infekce	Jednalo se o přímý hacking konkrétního serveru, man-in-the-middle útok.
Rozsah	Miliony uživatelů, použití falešných certifikátů CIA, MI6, Mossad, Google, Skype, holandské vládní instituce.

Případ DigiNotar, certifikační autority vlastněné firmou VASCO Data Security International, je specifický tím, že se nejednalo o šíření škodlivého viru, či zneužití cizích počítačů malwarem, ani cílený útok na průmyslové zařízení nebo vykradení osobních údajů v bankách. Může se zdát, že útok na jednu relativně malou firmu nemůže mít globální dopady, ale opak je daleko pravděpodobnější. DigiNotar byl založen právě pro účely vydávání důvěrných certifikátů, primárně pro účely holandské vlády a administrativy, ale i pro soukromé účely. Tyto certifikační autority jsou často nazývány i jako TTP – „trusted third party," důvěrné třetí strany. Účelem je, že dva subjekty, kteří si chtějí s jistotou mezi sebou přenášet data, jako např. uživatel u svého domácího počítače a jeho banka, vloží důvěru do třetí strany, jejímž účelem je, že zajistí maximální kryptografické zabezpečení přenosu těchto dat. Že jsou data zašifrovaná je vidět ve webovém prohlížeči vedle adresy, zpravidla se tam zobrazí ikonka zámečku a po rozkliknutí detaily certifikátu a jeho původ. Je pochopitelně i na vývojářích prohlížečů, aby prohlížeče byly napsány tak, že akceptují jen ty ověřitelné certifikáty.

Certifikáty jsou buď přímo poskytované ze strany banky, prohlížeč jej akceptuje a dojde k přenosu šifrovaných dat. Nicméně i elektronický podpis v sobě obsahuje certifikát. Jeho užití je tedy poměrně dost plošné, ačkoli si to řada uživatelů neuvědomuje. Došlo tak k narušení tak zásadních služeb, jako je elektronické podávání daní nebo automobilový registr.[51]

Důvěra je v této věci naprosto zásadní, neboť právě důvěra ve schopnost těchto autorit a jejich kryptografických dovedností je základem důvěry mezi uživatelem a bankou. Právě tato důvěra byla natolik porušena, že DigiNotar zkrachoval ještě týž měsíc po odhalení útoku kompromitující server generující tyto certifikáty. Zpracování reportu bylo zprvu problematické, nejprve holandský kurátor přímo zakázal zveřejňovaní těchto citlivých údajů, neboť se domníval, že by mohlo dojít na další požadavky v neprospěch firmy DigiNotar a tím narušení celé sítě důvěry mezi subjekty. Nakonec byl zpracován

[51] Rid, *Cyber War Will Not Take Place*, 26.

report na žádost holandské telekomunikační autority OPTA,[52] do jisté míry obdoba českého ČTÚ. Tento report nebyl nikdy oficiálně zveřejněn. I soud odmítl na základě volného přístupu k informacím report zveřejnit s argumentem, že by narušil obchodní tajemství.[53] Obecně se mezi odborníky spíše drží názor, že celá tato obstrukce s reportem je dílem opravdu vážného narušení důvěry a další možné následky jsou natolik nevyzpytatelné, že je lepší klíčové informace prostě nezveřejnit. Následně však vznikl report na objednávku firmy DigiNotar[54] a jeho hutná aktualizace na objednávku holandského ministerstva vnitra.[55]

Dne 10. července 2011 se neznámý hacker naboural do serverů této společnosti a začal generovat certifikáty, kterých ve výsledku vygeneroval na 531. Mezi organizace, které byly zasaženy falešně vygenerovanými certifikáty se řadí i např. CIA, Mossad, MI6, Skype, Google. Devět dní následně firma DigiNotar odhalila bezpečnostní incident ve svých systémech, ale tuto informaci nezveřejnila. Původně vydala technické hlášení o neplatnosti cca 230 certifikátů, které přestaly prohlížeče nebo jiné aplikace akceptovat.[56] Zajímavé je, že Google neměl s DigiNotar žádnou smlouvu, to však nebránilo, aby hacker zneužil tuto autoritu, vygeneroval certifikát a použil jej v prohlížeči, který následně akceptováním DigiNotaru jako certifikační autority přístup do emailu umožnil. To samé se pochopitelně týká přístupu do systémů zmiňovaných zpravodajských služeb. Pro oboje účely je ale nutné kromě certifikátu mít i přihlašovací údaje, což není těžké získat, je-li takto zkompromitovaný prohlížeč a celá komunikace je šifrovaná kódem hackerovi známým.

Netrvalo dlouho, konkrétně dva dny o reportu íránského uživatele Alibo na adresu Googlu o podezřelém chování Chromu,[57] a všechny zásadní prohlížeče, Internet Explorer, Firefox i Chrome do pondělí byly aktualizovány a uživatelům v případě zneužitého certifikátu zobrazily varování. To bylo 29. srpna, dne 20. září v reakci na oznámení holandského ministerstva vnitra, že jejich webové služby nemohou být nadále důvěrně používány, firma DigiNotar vyhlásila bankrot.

[52] Onafhankelijke Post en Telecommunicatie Autoriteit, která ukončila svou činnosti v roce 2013, kdy byla inkorporována do tzv. Autority pro trh a spotřebitele.

[53] Winter, "Curator Diginotar Vreest Meer Claims | Nu.nl/diginotar | Het Laatste Nieuws Het Eerst Op Nu.nl."

[54] Hans et al., "Black Tulip Report of the Investigation into the DigiNotar Certificate Authority Breach."

[55] Prins, "DigiNotar Certificate Authority Breach."

[56] Ibid.

[57] Ibid., 7.

Diskuse nad účelem je širší. Hledat účel v zájmu zdiskreditovat DigiNotar je vcelku pochopitelné, nicméně tomu by nenasvědčoval fakt, že drtivá většina zkompromitovaných certifikátů byla použita z Íránu, viz. *Obrázek 11 - Oblasti, ze kterých bylo použito zkompromitovaných certifikátů*, konkrétně se jedná o 99%. Ostatní se jevily jako anonymizované IP adresy např. v síti TOR.[58] Některé využité techniky dle citovaného prvního reportu z podzimu 2011 byly poměrně amatérské, jiné však naopak velmi profesionální. Zároveň bylo možné vysledovat jistou míru spojitosti s vyšetřováním jiného útoku z března 2011, který byl přiřknut íránskému hackerovi Comodo. Samotný fakt, že bylo na 99% zkompromitovaných certifikátů v Íránu, je velmi pravděpodobné, že cílem útoku bylo sledování soukromé korespondence, tomu by nasvědčovala kompromitace takových služeb jako je Gmail nebo Skype.

Obrázek 11 - Oblasti, ze kterých bylo použito zkompromitovaných certifikátů

Je až k podivu, že firma, pro kterou je důvěra a tedy jistota, že nedojde ke kompromitaci jejich dat, neměla zajištěné naprosto zásadní a jednoduché bezpečnostní opatření. Na serverech byla nainstalovaná firewall pouze centrálně, antivirus nebyl vůbec, aplikace nebyly aktualizované, zároveň však měly instalované pokročilé obranné nástroje, jako jsou tzv. IDS – intrusion detection systems, ačkoliv průniku nezabránily. Není též jasné, proč nebyly instalované centrální logovací nástroje, což mohlo útočníkům po nějakou dobu velmi usnadnit zametání stop.[59] Tyto výše uvedené nedostatky způsobily, že byly zkompromitovány všechny servery do posledního.[60] Jedná se o typickou ukázkou „špatné bezpečnostní hygieny“, kterou v české republice bude možné

[58] Ibid., 8.
[59] Ibid., 9.
[60] Hans et al., “Black Tulip Report of the Investigation into the DigiNotar Certificate Authority Breach.”

do jisté míry předejít respektováním připravované vyhlášky k Zákonu o kybernetické bezpečnosti Národního bezpečnostního úřadu. Vyhláška stojí primárně na standardech ISO 270xx.[61]

Celkovým závěrem operace Black Tulip je pravděpodobně zájem íránských autorit ve sledování služeb, které nemají původ v Íránu. Je to pochopitelně spekulace, nicméně 99% zkompromitovaných certifikátů na území Íránu tomu nasvědčuje. Jestli to byl pouze osamělý útok Comodo Hackera jako íránského patriota je otázkou.[62] Existují spekulace o útoku ze strany americké NSA, která se následně k věci vyjádřila pouze tak, že informovala o související aktivitě cizích zpravodajských služeb, čímž pouze poukazovala na možnou kompromitaci v blízké budoucnosti.[63]

Závěrem k DigiNotar[64] je nutné podotknout, že takto jasně strategicky cílený typ útoku za cílem připravit o důvěru subjekty spolu na internetu běžně komunikující je alarmující. Zvláště tehdy, stane-li se obdobný typ útoku relativně běžným. Pokud se ve zkompromitované autoritě najde vnitřní nepřítel se zájmem prodat citlivé informace, pak se obdobnému útoku dá jen těžko předejít.

4. Red October

Název	**Operace Red October**
Cíle	Získání zpravodajských informací
Kategorie	Kybernetická špionážní operace
Podoba kódu	Trojský kůň, virus, malware.
Odhalen kdy	Říjen 2012, operace probíhala od 2007
Odhalen kým	Kaspersky Lab
Stav	Operace je stále aktivní, dosud zcizen neznámý objem

[61] K datu psaní tohoto textu nebyl Zákon o kybernetické bezpečnosti, ani související vyhláška v platnosti. Jsou dostupné pouze

[62] Jeho řadu vyjádření je možné nalézt na http://pastebin.com/u/comodohacker , dostupnost zkontrolována 30.11.2013

[63] Rouwhorst, "No, the NSA Was Not Behind the DigiNotar Hack | Koen Rouwhorst."

[64] Na serveru lupa.cz vyšlo poměrně detailní shrnutí k čemu tehdy došlo i ve srovnání s útokem na autoritu Comodo z března 2011: Peterka, "Kauza DigiNotar, Aneb: Když Certifikační Autorita Ztratí Důvěru - Lupa.cz."

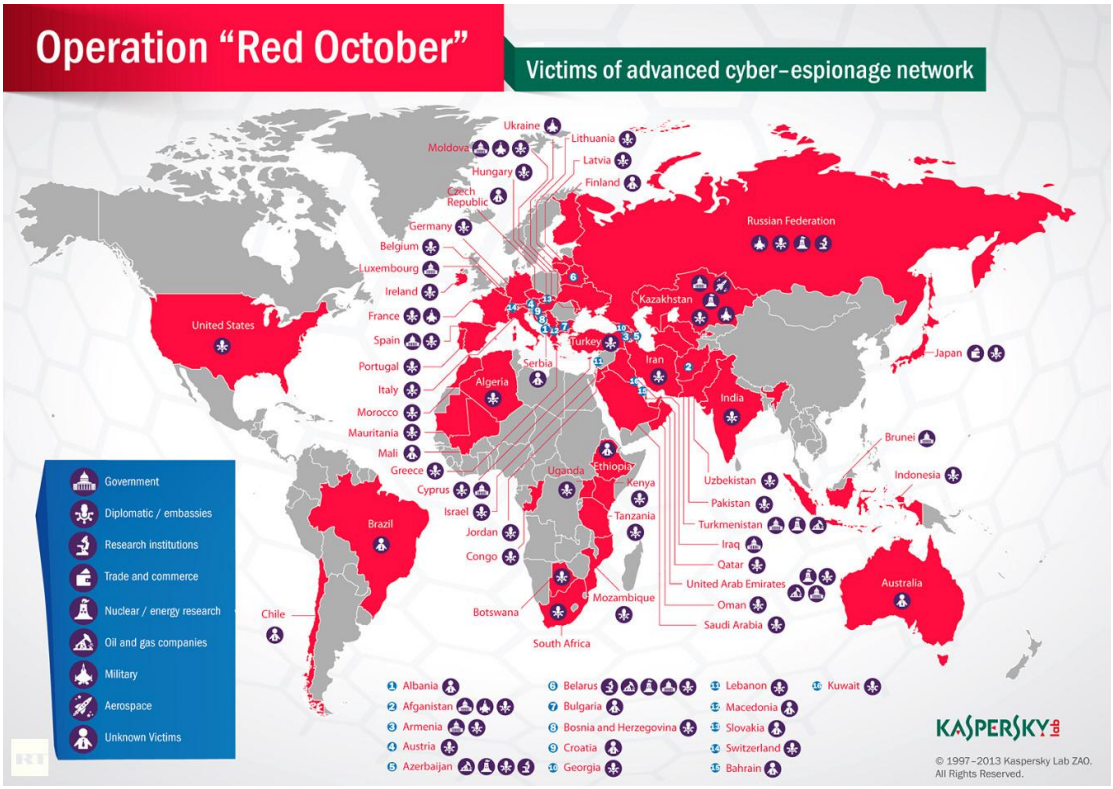
	citlivých vládních informací řady zemí.
Původ	Rusky mluvící původ dle komentářů v kódu, jinak nejasné. Podpora národním státem nepotvrzena, je ale velmi pravděpodobná.
Specifické vlastnosti	Útok spočíval v kompromitaci vládních zdrojů, energetického sektoru včetně jaderné energetiky, letecký průmysl. Celý komplex nástrojů, které spolu dokonale komunikovaly.
Formy infekce	Celé spektrum.
Rozsah	Celý svět, desítky tisíc počítačů včetně klasifikovaných sítí.

Operace Red October patří mezi největší kyber-špionážní operace současnosti. Její rozsah je natolik obrovský, že patří oprávněně mezi současné události potvrzující vážnost a hlavně efektivitu kybernetické špionáže. Už samotná doba pěti let trvající operace bez odhalení je alarmující, bnutno poto. Pokud toto číslo porovnáme s odhalením v DigiNotar, které trvalo řádově dny, je zjevné, že míra vůle po sobě zahladit stopy byla obrovská. Rámci řešení problému přisouzení kybernetického útoku ke konkrétnímu státu vzniká představa, především mezi politiky, policy makery a jinými odborníky, že míra sofistikovanosti by jistou berličkou být mohla. Nicméně to nebylo potvrzeno z řady důvodů, především není jasné, co v kontextu kybernetických hrozeb či operací je už natolik sofistikované.[65] Některé dopady mohou být obrovské na základě jen chytrého použití velmi dobře dostupného kódu, což by se dalo přisoudit např. kódu Zeus. V případě takto komplexních špionážních operacích je faktorem přisuzujícím původ státu spíše logicky odvozený smysl získání zkompromitovaných informací. Zde se jedná o vládní instituce a klíčové průmyslové podniky, konkrétně osm oblastí: vládní, dilomatické včetně ambasád, komerční a obchodní, jaderný a energetický výzkum, ropný a plynový průmysl, letecký průmysl, vojenské instalace.

Cílem celé operace je především východní Evropa, bývalé státy SSSR, ale i jeho satelity včetně České republiky. Cílem nejsou jen konkrétní datové uložiště, ale mobilní

[65] Guitton and Korzak, "The Sophistication Criterion for Attribution."

telefony, iPady a jiné kapesní zařízení, které umožňují útočníkům lépe odsledovat např. přístupové údaje do citlivých systémů.



Obrázek 12 - Rozsah operace Red October, zdroj: Kaspersky Lab

Technicky byla operace zajištěna opět poměrně sofistikovaně. Existuje vrstva zkompromitovaných serverů, cca 60 speciálních domén, databáze hesel, celá plejáda nástrojů, malwarů a dalších dílčích pomůcek, které umožňují jak kompromitaci napadených počítačů, tak jejich kontrolu, tento celý ekosystém se nazývá Rocra.[66] Jednotlivé nástroje na kompromitaci (exploits) byly pravděpodobně vyvíjeny čínskými hackery, zatímco celé moduly ekosystému Rocra byly napsány rusky mluvícími hackery. Celý systém je velmi odolný, při pokusu odstranit jeden C&C server[67] se komunikace

[66] GReAT, "The 'Red October' Campaign - An Advanced Cyber Espionage Network Targeting Diplomatic and Government Agencies - Securelist."

[67] Command & Control server, zařízení pod kontrolou útočníka sloužící k dalším účelům, zpravidla ke kontrole a zneužívání počítačů, které vykonávají rizikové útoky. V případě odhalení, útočník příjde o jeden takový C&C server, ale nikoli o nadvládu na celou infrastrukturou.

přesune jinam na jiné alternativní komunikační kanály. Síť je tak poměrně nerozbitná a i z toho důvodu je celá operace i nadále aktivní.

Způsoby kompromitace uživatelských stanic se řadí mezi ty nejprimitivnější, nejspíše také ty nejefektivnější. Kromě klasického phishingu se jedná i o infikované emaily a především o Word či Excel dokumenty v příloze,[68] po jejichž otevření dojde k infekci a zanesení škodlivého kódu. Ten oproti příkladu Slammer worm není bezúčelný, ale otevírá zadní vrátka k celému spektru operací. Na druhou stranu celá infrastruktura je naopak velmi sofistikovaná. Moduly kompromitující mobilní telefony (Windows Mobile, iPhone a Nokia) se nainstalují do napadeného počítače a čekají až uživatel svůj mobilní telefon připojí. V případě, že se tak stane, se aktivizuje a začne s telefonem otevřeně operovat. Stáhne maximální objem dat, zabalí je do balíku a odešle skrze vlastní komunikační kanály na C&C server odkud si je vyzvedne útočník. Celý řetězec až k útočníkovi je prakticky neodhalitelný, nicméně jeho struktura je viditelná.[69]

Mezi typické ukázky operací, které se ve zkompromitované počítači odehrají patří např.: stáhnout hesla uložená v prohlížeči včetně historie navštívených stránek, stáhni konfigurace účtů v Outlooku, udělej strom složek a index všech uložených souborů, najdi konfigurace dostupných síťových zařízení CISCO, replikuj se po síti na další zařízení a po instalaci zašli potvrzení o úspěšné kompromitaci na IP atd. Obdobných typů operací zjištěný malware dělá celou řadu.[70]

Jedná se tedy o dobře propracovanou kampaň s decentralizovanými prvky, která může sloužit jako dobře propracovaná síť kybernetické špionáže přisouditelná konkrétnímu státu, nicméně to se nepotvrdilo, ačkoliv to pochopitelně obdobné otázky otevírá. Tím, že získávání informací není přesně cíleno, diskutuje se možnost soukromého zájmu obdobné špionáže a následného prodeje těchto informací zpravodajským službám.[71] Jiná perspektiva nabízí, že by podobně sofistikovaná kybernetická špionáž mohla být demonstrací síly konkrétního státu, to by se potvrdilo tehdy, pokud by se konkrétní stát přihlásil k autorství alespoň nepřímo. Případ Stuxnetu (viz. kapitola **Chyba! Nenalezen zdroj odkazů.** – **Chyba! Nenalezen zdroj odkazů.**) je tím, kde je autorství v podstatě jasné ačkoliv se k němu oficiálně USA ani Izrael nehlásí.

[68] Ibid.
[69] Ibid.
[70] Ibid.
[71] Gomez, "Operation Red October Fuels Debate over Cyber Espionage | East Asia Forum."

Jejich diplomaté však v uzavřených kruzích o Stuxnetu mluví a ze strategického hlediska je takové autorství odvoditelné. To v případě operace Red October není.

5. Estonská kyber válka

Název	**Estonská kyber válka**
Cíle	Demonstrace síly, nejspíše morální trest za přesun sochy rudoarmějce, znemožnění chodu státu
Kategorie	Útok na státní suverenitu
Podoba kódu	DDoS útok
Odhalen kdy	Nebylo třeba jej odhalovat, trval 27.4. – 18.5. 2013
Odhalen kým	Stát nefungoval, odhalení tak lze přisoudit estonským autoritám
Stav	Skončil 18.5., Estonsko je již na podobné útoky připravené
Původ	Většina útoku pocházela z Ruska, nicméně řada útočících zařízení byla umístěna i v USA.
Specifické vlastnosti	Gradující DDoS útoky, které postupně znemožnily chod státní správy. Občas prolnuté záměnami webových stránek, web defacement. Spamming na vládní emailové schránky.
Formy infekce	Pouze DDoS útoky.
Rozsah	Vládní instituce v Estonsku, kritická infrastruktura.

Útoky na Estonsko v roce 2007 patří symbolicky do historie jako ukázka, kdy využití pouze kybernetických nástrojů pouze v kyberprostoru může zcela zásadně ovlivnit chod státu. Celá událost je v kontextu historie poměrně značně přehodnocena a i samotní zaměstnanci např. ministerstva obrany dnes poukazují na fakt, že Estonsko hraje perfektně roli oběti. To však nic nemění na tom, že nic obdobného se v historii doposud nestalo.

Politické pozadí celé události je poměrně prosté. Estonsko mělo v historickém centru Tallinnu umístěnou sochu rudoarmějce, který měl symbolizovat osvobození Estonska od nacistů. Faktem je, že Estonsko tvrdě bojovalo za svou nezávislost na Rusku ještě dávno předtím, než přišli nacisté. Jaan Poska je např. osobností, kterou Estonci ve své historii vnímají jako klíčového vyjednavače o estonskou nezávislost již v roce 1918, kdy Estonsko po první světové válce zažilo své první dny nezávislosti, jež muselo před Ruskem tvrdě obhajovat. Estonci tak jen těžko budou vnímat sochu rudoarmějce jako symbol osvobození a toto téma se po znovu vyhlášení nezávislosti v roce 1991 stalo aktuálním.

PŘÍLOHA 4. – SCADA SYSTÉMY

1. Úvod

Kritické infrastruktury zajišťující dodávky energie, vody, paliva či dopravní systémy jsou ve velké míře řízeny tzv. SCADA (Supervisory Control and Data Acquisition) systémy. Tyto výpočetní systémy zajišťují správnou funkci, řízení a dohled průmyslových procesů. Dřívější struktura komunikační sítě SCADA systémů byla izolovaná od vnějších sítí. Vlivem přechodu SCADA systémů z izolovaných sítí na otevřené (připojení do veřejné sítě Internet), dochází k výraznému zvýšení rizika kybernetických útoků. Jednotlivé segmenty SCADA systému mohou být propojovány rozdílnými komunikačními technologiemi (Ethernet, směrové rádiové spoje, optické spoje atd.) a zvyšují tak komplexnost vytvořené sítě.

K zajištění kybernetické bezpečnosti řídicích systémů je nutné vytvoření komunikačních protokolů, které budou splňovat nároky moderních bezpečnostních standardů, tak aby byly relevantní pro všechny implementované komunikační technologie. Nejedná se však pouze o technologické řešení, ale i o metodiku správy a používání komunikačních sítí a výpočetních technologií.

Problematikou bezpečnosti informačních technologií se také zabývá v rámci EU organizace ENISA, doporučuje zavádění bezpečnostních patchů rozšiřujících standard ISO/IEC 27002, další doporučení vydává americký institut NIST v sérii doporučení SP 800.

2. Struktura SCADA systémů

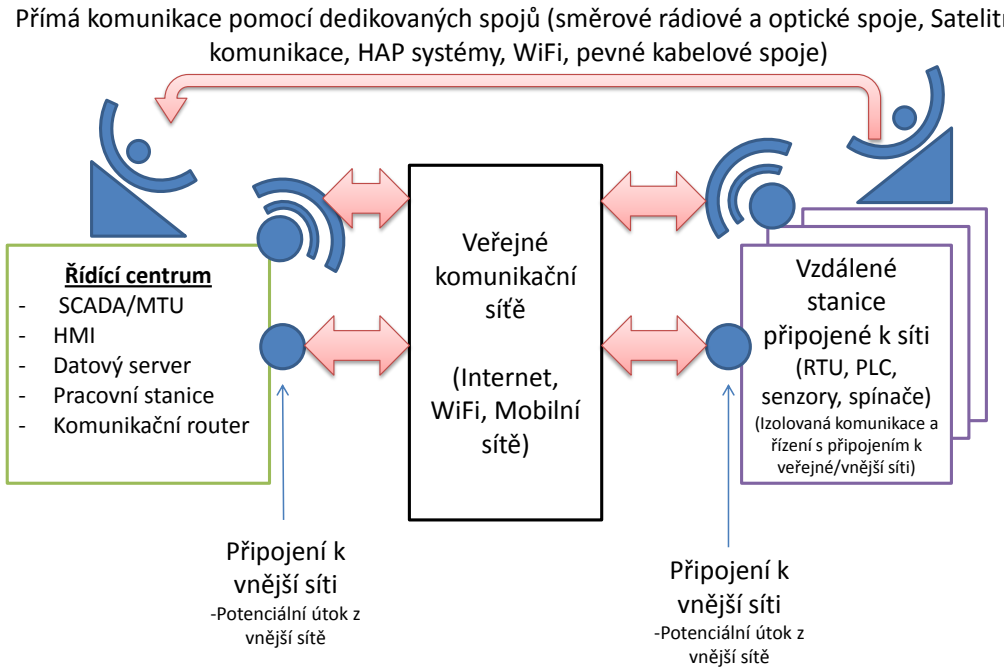
Struktura SCADA systémů může být velmi komplexní a je určena individuálními nároky a potřebami řídících subjektů. Obecná struktura SCADA systémů vychází z popisu v dokumentu NIST SP800-82 a je členěna do tří obecných částí. Jedná se o: Řídící centrum, komunikační sítě a Vzdálené stanice jak je naznačeno na Obr. 1. Jednotlivé části jsou složeny z komponent zajišťujících požadovanou funkci. Seznam a popis komponent je uveden níže.

- **Řídící centrum** - Zajišťuje řízení a sběr dat. Kromě níže popsaných součástí obsahuje datové a aplikační servery, databáze a další zařízení jako jsou komunikační routery, zajišťující propojení s dalšími části sítě.

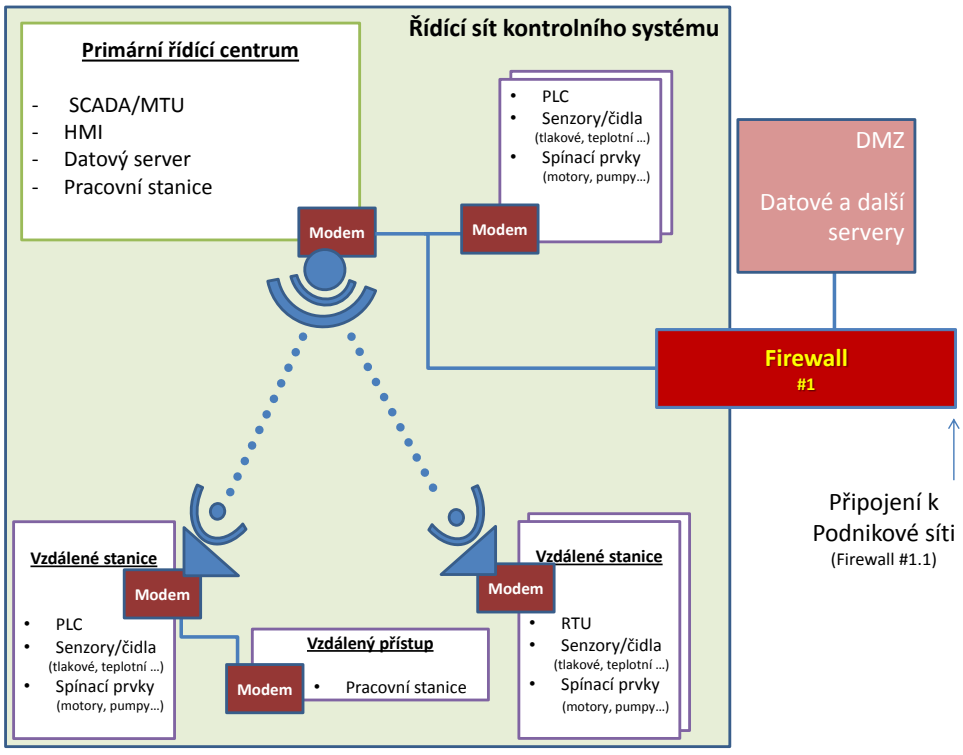
- **MTU** (Main Terminal Unit – Hlavní řídící jednotka) také označován jako **SCADA server**, v síťové topologii se jedná o řídící jednotka typu „Master“.
- **HMI a Pracovní stanice** jsou řídící komponenty obsluhované lidmi. Bývají lokálně spojeny s řídícím centrem, ale stejně tak mohou být umístěny i na vzdáleném místě.

- **Vzdálené stanice** - Zajišťují obsluhu a řízení lokálně připojených zařízení, mezi něž patří různé senzory, čidla či detektory stejně tak jako mechanické ovládací prvky např. spínače, motory nebo čerpadla. (obsluhovaná zařízení se liší podle konkrétního typu průmyslového odvětví).
  - **RTU** (Remote Terminal Unit) vzdálená řídící jednotka sloužící pro sběr a předávání dat do řídící jednotky (SCADA/MTU). Umožňují vzdálenou správu.
  - **PLC** (Programovatelný logický kontrolér) je průmyslový výpočetní systém vykonává stejné funkce jako RTU. Slouží k řízení základních logických funkcí, které vykonávají lokální procesy (senzory, spínače, motory). Jedná se o ekonomičtější a flexibilnější řešení než RTU, které jsou více komplexní.
- **Komunikační sítě** – zajišťují propojení jednotlivých segmentů a umožňují jejich vzájemnou komunikaci, řízení a další nezbytné funkce. Komunikační sítě jsou komplexní a jsou složeny z různých vzájemně propojených technologií, tak aby zajistily spolehlivé spojení.
  - **Komunikační routery** zajištují propojení jednotlivých typů sítí (lokální a rozlehlé sítě)
  - **Firewally** ochraňují zařízení v síti. Monitorují a řídí komunikaci podle přednastavených pravidel.
  - **Modemy** modemy slouží k přeměmě sériového datového signálu (vysílaného na datových sítích) na signál, který je možné vysílat na sítích slouřících k propojení např. vzdálených zařízeních (bezdrátový přenos, optické spoje…)
  - **DMZ (Demilitary Zone)** označuje je oddělený sítový segment připojený přímo k firewallu. Obsahuje např. datové servery, k nimž (informacím,

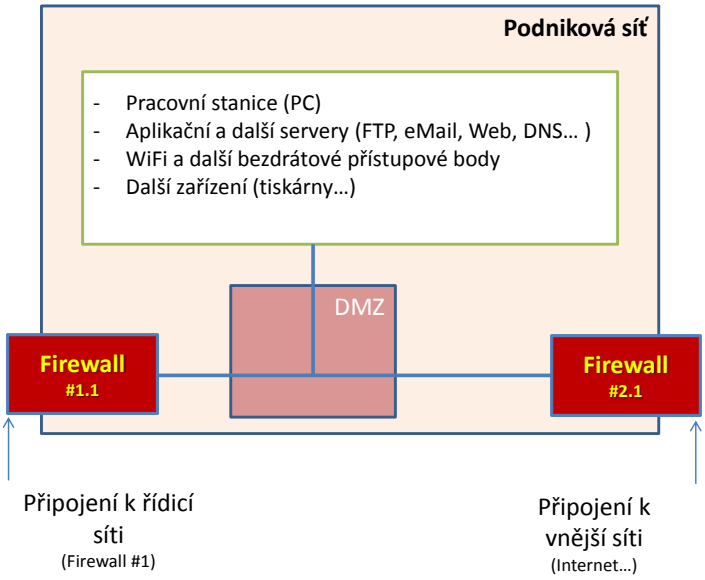
které obsahují) je potřeba přistupovat z oblastí mimo řídící síť (např. z korporátní sítě nebo vzdálené pracovní stanice).



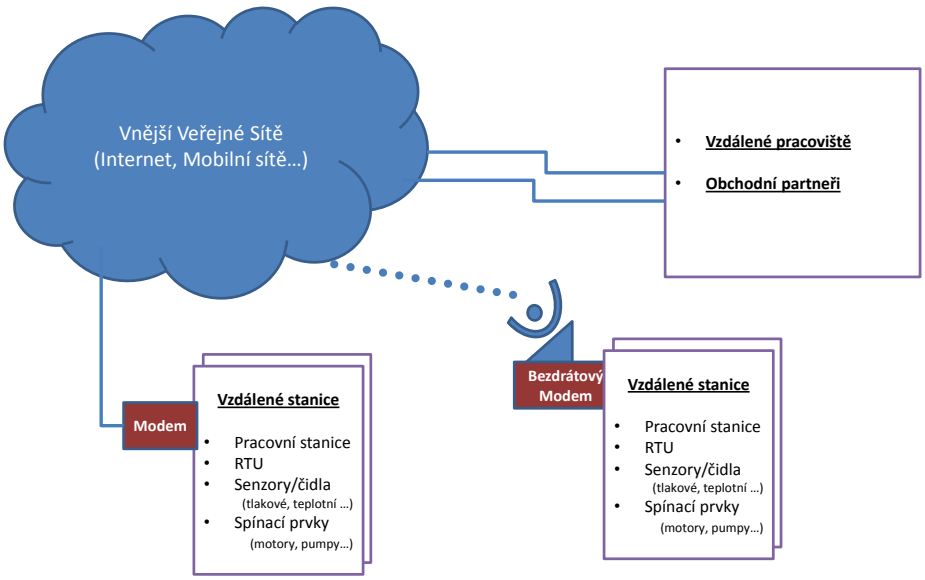
- **Obr. 1 Obecná struktura SCADA systému a vzájemné propojení jeho připojení součástí.**



- **Obr. 2 Struktura sítě řídicího systému SCADA**



- **Obr. 3 Struktura podnikové sítě pro připojení SCADA**



-

- **Obr. 4 Připojení vzdálených stanic pomocí veřejné sítě ke SCADA**

Komunikační protokoly

Komunikační protokoly používané v tzv. „legacy“ SCADA systémech nevyhovují bezpečnostním požadavkům (byly vyvinuty pro izolované SCADA systémy)

- ***Modbus***
  - Řídící soustavy průmyslových zařízení.
  - Otevřený paralelní protokol založený na komunikaci master/slave.
  - Komunikace různých zařízení (PLC, dotyk. Displ, I/O rozhraní…)
  - RS-232, RS-422, RS-485, Ethernet
- ***RP570***
  - Komunikační protokol sloužící ke komunikaci mezi uživatelským počítačem a vzdálenými stanicemi
- ***Profibus***
  - Průmyslová sběrnice
  - Automatizace výrobních linek
  - Master/slave

Standartní protokoly s podporou TCP/IP založené na Ethernetové síti (také představují bezpečnostní rizika, protože v sobě nezahrnují bezpečnostnímechanizmy) jež jsou využívány ve SCADA systémech.

- ***IEC 60870-5*** (ČSN EN 60870) je protocol sloužící k přenosu telemetrických dat. Zahrnuje specifikace IEC 60870-5-1 až IEC 60870-5-5 a dále

IEC 60870-5-101 až IEC 60870-5-104. Stručný popis vybraných součástí je uveden níže.

- -**101**: mechanismy přenosu dat pro sériové linky
- -**104**: mechanismy pro použití ve stávajících komunikačních sítích (Ethernet)
- Systémy dálkového ovládání zařízení a soustav
- Komunikace RTUs a další inteligentní elektronická zařízení (IED)

- Komunikace na aplikační vrstvě
    - Časová synchronizace a přenos souborů
- použití především v elektroenergetice

- ***IEC 61850*** (ČSN EN 61850) Zahrnuje specifikace IEC 61850-1 až

IEC 61850-10. Stručný popis vybraných součástí je uveden níže.

- Komunikace v energetice na rozvodnách, kde dochází k přepínání kilovatových výkonů, jejich součástí a dalších prvků (dispečink, elektrárna…)
- Ochrana a dohled nad provozem rozvodny včetně měření a regulace

- ***DNP3*** (IEC 60870) Stručný popis vybraných součástí je uveden níže.

- Protokol pro sériový přenos dat v rámci RTU a mezi RTU a řídící stanicí (akvizice měřených dat, řídící příkazy)
- použití především v petrochemii, farmacii, potravinářství, vodárny, elektrárny
- RS-232, RS-485, Ethernet, TCP/IP, UDP, optická vlákna

3. Bezpečnostní mechanizmy SCADA systémů a komunikačních protokolů

- Standardy skupiny IEC 62351 (IEC 62351-1 až IEC 62351-11) definují požadavky na bezpečnostní mechanizmy pro komunikaci v rámci SCADA systémů např. pro protokoly podle normy IEC 60870 (DNP3); IEC 61850, jak je naznačeno v Příloze 1.
    - Kryptografické protokoly IEC 62351–3 a IEC 62351-4 definují mechanismy zajišťující autentifikaci, integritu, utajení a ochranu proti neautorizované modifikaci komunikace (podvrhům) při komunikaci mezi koncovými segmenty.
    - IEC 62351 – 5 definuje bezpečnostní mechanizmy pro IEC 60870-5 (DNP3).

  - IEC 62351 – 6 definuje bezpečnostní mechanizmy pro IEC 60850 (VLAN pro

    GOOSE, RFC2030 pro SNTP)

- Standardy pro kybernetickou bezpečnost Průmyslových Řídicích Systémů (ICS) ve spojených státech (US) podle série doporučení institutu NIST (NIST SP 800):
  - **NIST SP 800-30** Guide for Conducting Risk Assessment
  - **NIST SP 800-37** Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach
  - **NIST SP 800-53, Rev 4** Security and Privacy Controls for Federal Information Systems and Organizations
  - **NIST SP 800-60** Guide for Mapping Types of Information and Information Systems to Security Categories
  - **NIST SP 800-70** National Checklist Program for IT Products: Guidelines for Checklist Users and Developers
  - **NIST SP 800-82** Guide to Industrial Control Systems Security

- (Pro komunikaci v rámci SCADA systémů jsou využity kromě dedikovaných technologií (viz. Protokoly SCADA) také veřejné komunikační sítě a běžně používané technologie a standardy. Doporučení podle US organizace NIST
  - Sítě pro mobilní komunikaci (GPRS/ EDGE/ HSPA/ LTE)
    - Rizika spojená s nárůstem použití mobilních telefonů (Android…)
    - Doporučení pro bezpečnost v US: NIST SP800-124
  - Bezdrátové datové sítě založené standardu IEEE 802.11 (Wi-Fi), 802.15 Bluetooth

- Doporučení pro bezpečnost v US: NIST SP800-121

- Pevné datové sítě založené na standardu IEEE 802.3 (Ethernet)

  - Doporučení pro bezpečnost v US: NIST SP800-114

- Další organizace zabývající se standardy pro kybernetickou bezpečnost Průmyslových Řídicích Systémů (ICS) je organizace ISA:

  - **ISA-99 /IEC 62443**

  - **ISASecure**–Certification of ICS devices and system

- **Zabezpečení funkčnosti sítě, spojení a protokolů**

Pro zajištění dostatečně robustné a odolné sítě je nutné vytvářet redundantní spojení v topologii, které zajistí spolehlivost spojení i při výpadku části sítě. Doporučené protokoly RSTP (Rapid Spanning Tree Protocol) na lokální síti mezi stanicemi, OSPF (Open Shortest Path First) na interní síti a VRRP (Virtual Router Redundancy Protocol) pro redundantní záložní propojení routerů.

Další zvýšení bezpečnosti je možné dosáhnout využitím virtuální sítě VLAN (Virtual Local Area Network) a protokolů IPv6, OSPFv3 (RFC 2740) SNMPv3 (RFC 3826), které poskytují vlasní mechanismy autentifikace a šifrování.

Filtrování MAC a IP adres na firewallech umožňuje přístup jen definovaných zažízení.

Pro zajištění hierarchického rozhodování při přidělování sítových prostředků na síťových prvcích je potřeba proiritizovat vysílané zprávy z důvodu zajištění nízké latence a požadované kvality příslušných služeb. Implementace mechanizmů založených na IP adresách a IEEE 802.1p.

- **Zabezpečení autentifikace zařízení a uživatele**

Implementace autentifikačního serveru např. RADIUS (Remote Authentification Dial-In User Service) (RFC 2865 a 2866) využívá IEEE 802.1x s podporou autentifikačního protokolu EAP hraje zásadní roli pro uživatelskou autentifikaci v celém systému. Rozhoduje o individuálním potvrzení autorizace a přidělení požadovaného přístupu.

Kryptografické protokoly využívající hashovací mechanismy by měly splňovat doporučení FIPS.

Pro přidělování a řízení privilegií, která jsou přidělována uživatelům je využíváno RBAC (Role Based Access Control), který IEC TC57 WG15 definuje pro použití ve SCADA systémech.

Komunikace na úrovni administrátora musí být zabezpečená. Doporučení pro nahrazení metod Telnet, HTTPS a HTTP metodami, které vyhovují bezpečnostním požadavkům: SSHv2 a RFC 2818.

- **Firewally**

Bezpečnostní doporučení NIST SP 800-41 pro firewally. Ve SCADA systémech musí být firewall implementován do řídící i korporátní-podnikové sítě. Bezpodmínečné je implementace funkce IDS (Industrial Detection System) a použití konceptu DMZ v nichž jsou umístěny datové servery přístupné z vnější sítě tak, aby byly odděleny od řídícího centra a nemohlo dojít z narušení řídící sítě.

- **IPsec a Virtuální sítě VPN**

IPsec označuje bezpečnostní rozšíření IP protokolu. Použití virtuální sítě VPN v rámci sítě založené na IP protokolu (Ethernet) dojde k vytvoření virtuálního tunelu, v němž jsou data přenášena zabezpečeně. Pro implementaci je možné použít oba protokoly IPv4 i IPv6. Detailní popis zabezpečených protokolů je vydáván organizací IETF v dokumentech RFC 4301 – RFC 4309.

V případě použití zabezpečení SCADA komunikace podle IEC 62351 je použití IPsec redundantní.

- **Bezdrátové připojení**

Pro zajištění bezpečného bezdrátového připojení podle IEEE 802.11 (Wi-Fi) je potřeba používat pokročilé šifrovací mechanizmy AES. Pro autentifikaci pak IEEE 802.1x a uživatelské certifikáty.

4. Bezpečnostní rizika

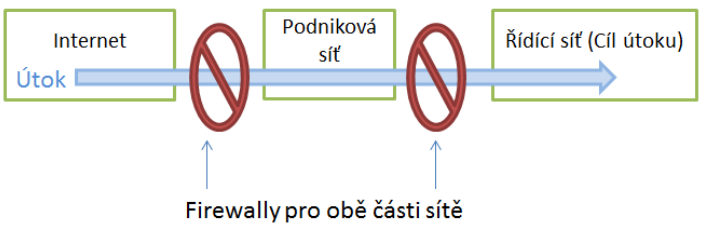
Zajištění bezpečnosti komplexní informačních a řídicích systémů vyžaduje zavedení rozsáhlých bezpečnostních mechanizmů a postupů. Tyto musejí obsáhnout jak technologické řešení, tak i metodiku správy informačních sítí a školení zaměstnanců.

Podle doporučení organizace IEC jsou bezpečnostní rizika rozděleny následovně:

- Neúmyslné hrozby
    - Závada na zařízení
    - Nedbalost obsluhy
    - Přírodní katastrofy
    - Bezpečnostní poruchy
- Cílené hrozby
    - Nespokojený zaměstnanec
    - Průmyslová špionáž
    - Vandalizmus
    - Kybernetické útoky
    - Počítačová viry a červy
    - Krádeže
    - Terorizmus
        - **Narušení**

Níže jsou stručně uvedeny potenciální hrozby spojené s přechodem SCADA systémů z izolovaných sítí na otevřené (připojení do veřejné sítě Internet). Detailnější struktura hrozeb je vyobrazena v Příloze 3.

- Front Door (Internet) : Postupy a principy infiltrace jsou „standartní“



- **Obr. 4 Struktura průběhu narušení SCADA systému**

- Back Door (fyzické narušení infrastruktury)

  - Poškození (vyřazení) komunikačního zařízení
  - „Nakažení“ nebo poškození komunikačního zařízení
    - (Modemy, Acces Pointy, kabely….)

- - Vnější útoky
  - Škodlivý program (počítačový virus/červ) - přímo vyvíjený pro narušení konkrétních řídící systémů
  - DOS (Denial of Services) – zahlcení komunikačního serveru
  - Spoofing – prolomeni autentifikace komunikace (narušení řídících informací)
  - Replay – opakované zasláni zachycených dat systémové komunikace (Zahlcení, neočekávaná data)
  - Man-in-the-Midle : zachycení–zarušení-záměna-vysílání systémové komunikace (narušení modifikovanými daty)

5. Závěr

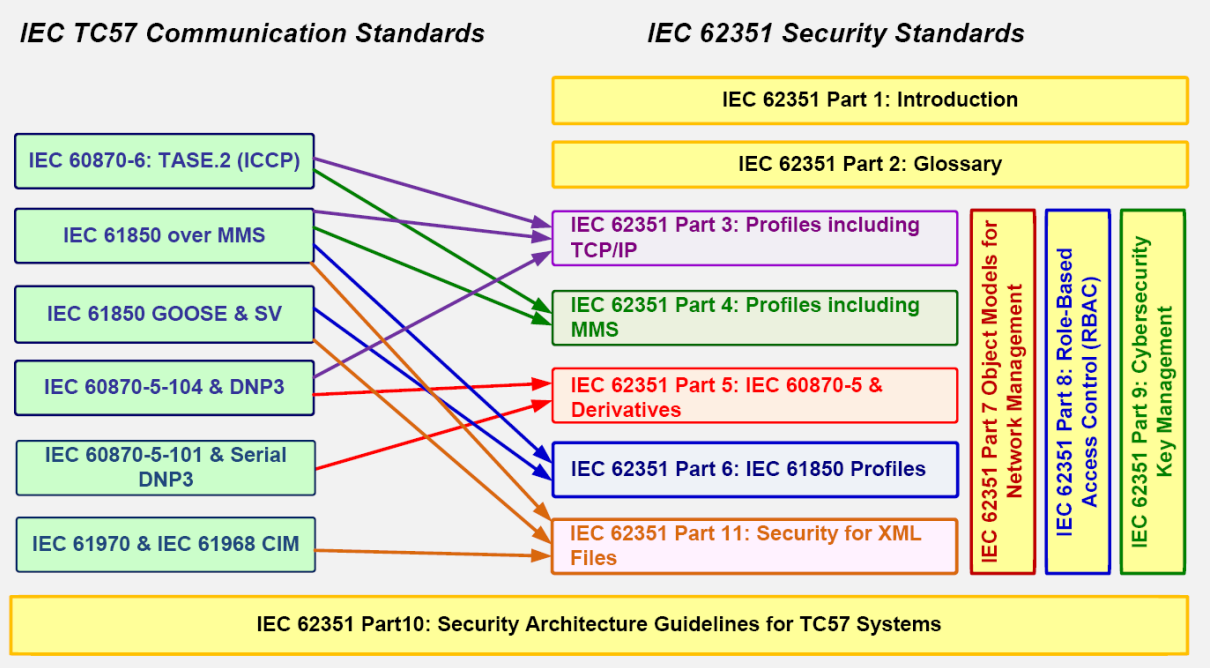
Cílem studie byla analýza komunikačních standardů a technologií používaných ve SCADA systémech z hlediska kybernetické bezpečnosti. Byly popsány komunikační protokoly a standardy používané ve SCADA systémech stejně tak jako mechanizmy a technologie sloužící k vytvoření bezpečné komplexní a otevřené sítě SCADA systému.

Klasická koncepce uzavřeného (izolovaného) SCADA systému využívá protokoly, které nesplňují nebo dokonce neobsahují žádné bezpečnostní požadavky a mechanizmy (Modbus, RP570, Profibus, IEC 60870, IEC 61850). Moderní koncept však vyžaduje propojení SCADA systémů s vnějšími komunikačními sítěmi, proto je nutné zavádět nové bezpečné komunikační protokoly, bezpečnostní standardy a mechanizmy.

Problematikou bezpečnosti komunikace v rámci SCADA systémů se zabývá mnoho subjektů. Patří mezi ně americký institut NIST v doporučeních série NIST SP-800, další je mezinárodní organizace IEC v doporučeních IEC 62351, mezi další patří organizace ISA v doporučeních ISA-99, mezi další organizace zabývající se kybernetickou bezpečností patří ENISA, NERC.

6. Příloha 1

Začlenění komunikačních standardů IEC 60870, IEC 61850 do zabezpečeného standardu IEC 62351

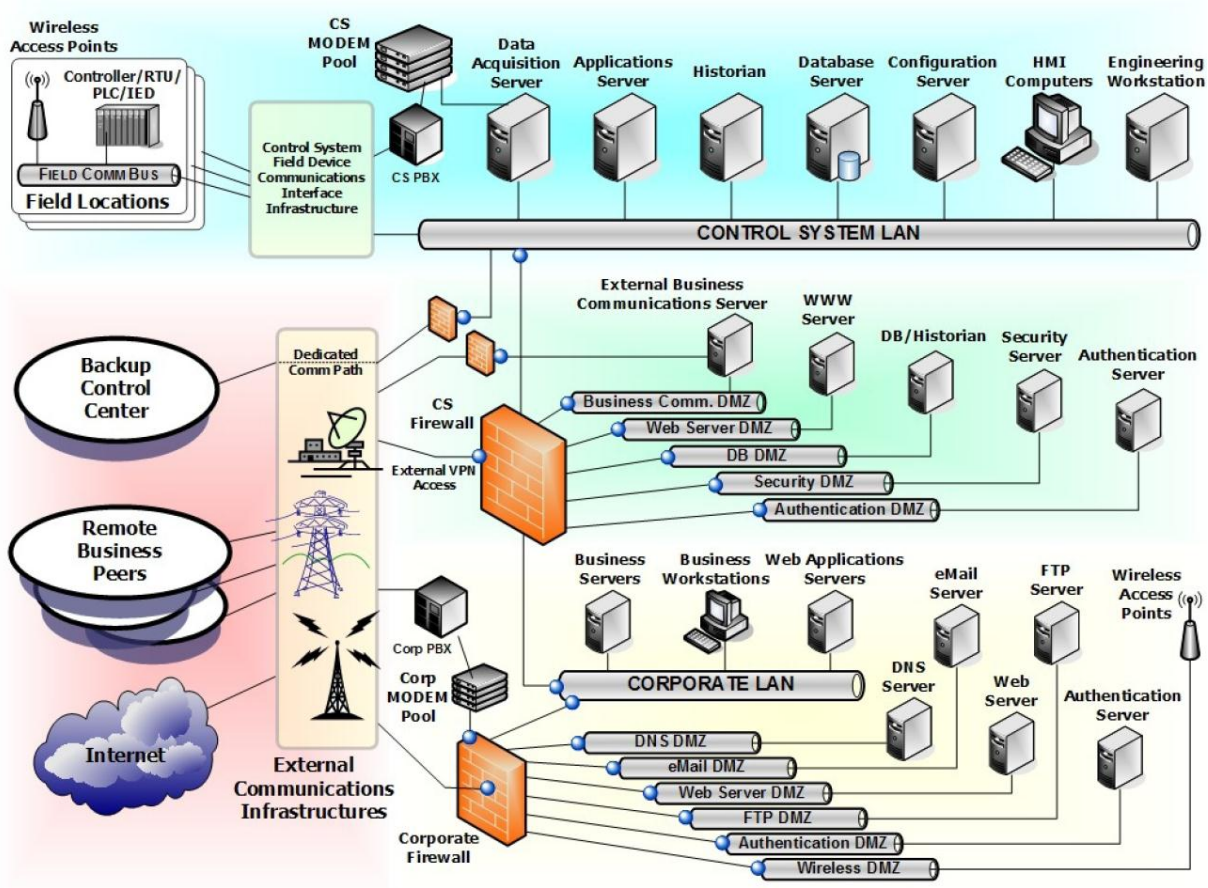


Převzato z

Cleveland, F.; IEC TC57 WG15: IEC 62351 Securitty Standards for the Power System Information Infrastructure, International Electrotechnical Commission, June 2012

7. Příloha 2

Komplexní struktura SCADA systému podle NIST SP 800-82 s implementovanými bezpečnostními mechanizmy.

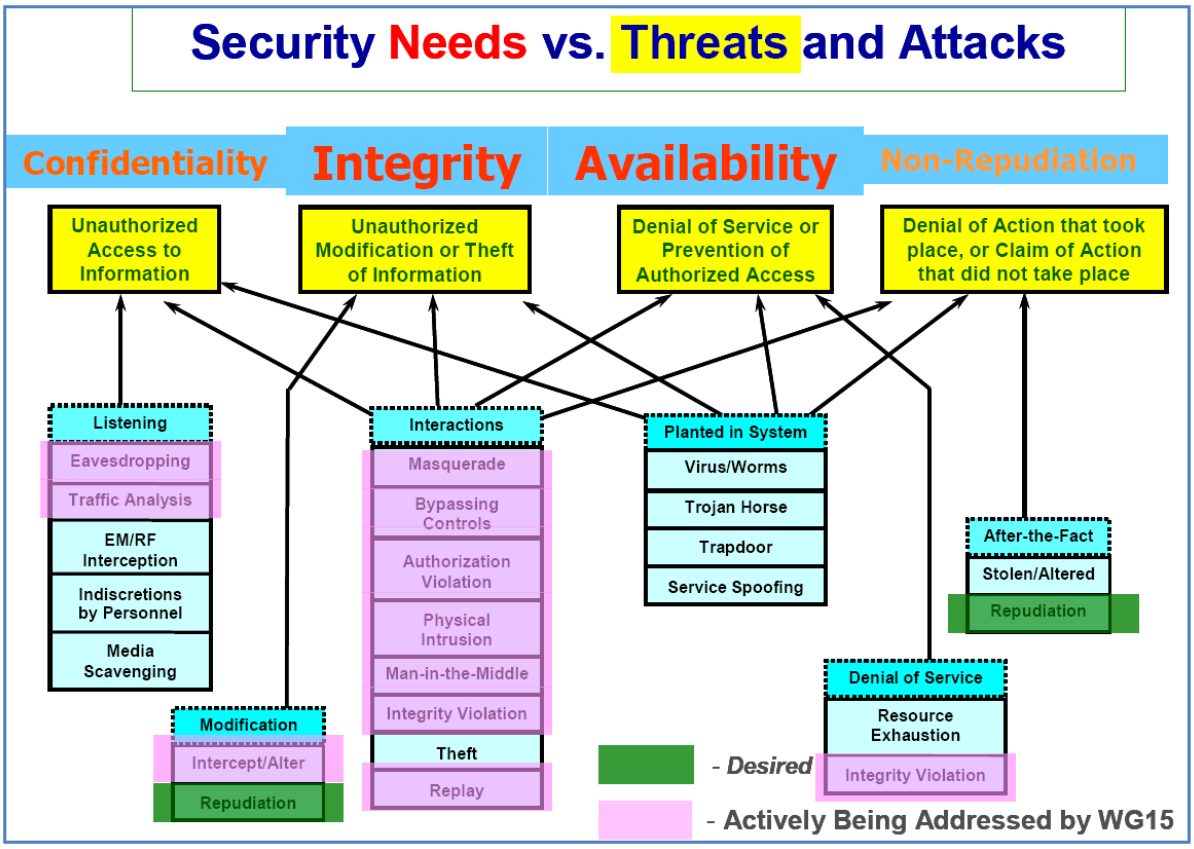


Převzato z

Stouffer, K; Falco, J; Scarfone, K. NIST SP 800-82: Guide to Industrial Control Systems (ICS) Security, Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programable Logic Controllers, National Institute of Standards and Technology (NIST), June 2011.

8. Příloha 3

Bezpečnostní požadavky, hrozby a možné útoky podle doporučení standardu IEC 62351 WG15



Převzato z

Cleveland, F.; IEC TC57 WG15: IEC 62351 Securitty Standards for the Power System Information Infrastructure, International Electrotechnical Commission, June 2012

PŘÍLOHA 5. – SMART GRID – KOMUNIKAČNÍ PROTOKOLY A BEZPEČNOSTNÍ RIZIKA

Ing. Lukáš Klozar

1. Úvod

Koncept Smart Grid představuje novou možnost inteligentního měření, přesného monitorování a interaktivního řízení služeb poskytovaných dodavatelem např. elektriské energie zákazníkovi (spotřebiteli). Stejně tak tento koncept přináší zcela nové možnosti efektivního řešení dynamických změn v síti. Rozvoj digitálních komunikačních a informačních technologií umožňuje propojení a vysokorychlostní komunikaci mezi jednotlivými segmenty sitě tak, aby bylo možné účinně reagovat na aktuální potřeby v reálném čase. Toto řešení však díky decentralizovanému prtovozu a vzájemném propojení představuje bezpečnostní rizika. Software i hardware se může stát cílem útoku. I pouhá záměna přenášených informací kritických infrastruktur může způsobit vážné nebezpečí.

Vzrůstající požadavky na infrastrukturu systémů dodávky elektrické energie přináší zvyšující se počet nových technologií jako elektrická vozidla, obnovitelné zdroje elektrické energie, které už nejsou centralizované, ale distribuované např. na budovách a dodávají elektřinu nerovnoměrně podle aktuálních klimatických podmínek. Koncept Smart Grid odhaluje nové způsoby chytrého ekologického, efektivního a udržitelného způsobu vypořádání se s těmito vzrůstajícími potřebami.

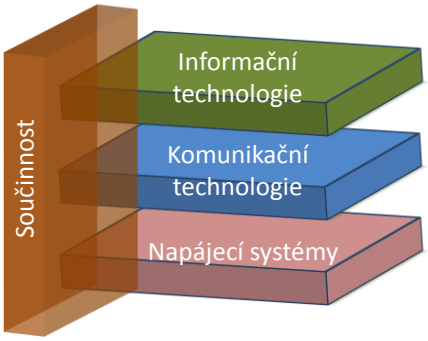
Moderní technologie umožní inteligentní způsob správy a dynamické řízení jednotlivých součástí distribuční energetické sítě tak, aby bylo možné reagovat na dynamické změny v sítí (změna spotřeby i produkce el. energie během dne) a zvýšila se efektivita provozu.

Problematikou konceptu Smart Grid se zabývá celá čada organizací CEN, ENISA, ETSI, IEEE, NIST, NISTIR, IEFT, CENELEC, ISA a další. Tyto organizace vytvářejí standardy, doporučení a metodické postupy spojené s dílčími problémy integrace.

2. Struktura Konceptu Smart Grid

Strukturu konceptu Smart Grid je možné rozdělit na tři základní oblasti, jejichž vzájemná součinnost je výchozím bodem standardizace. Další standardizační proces pak

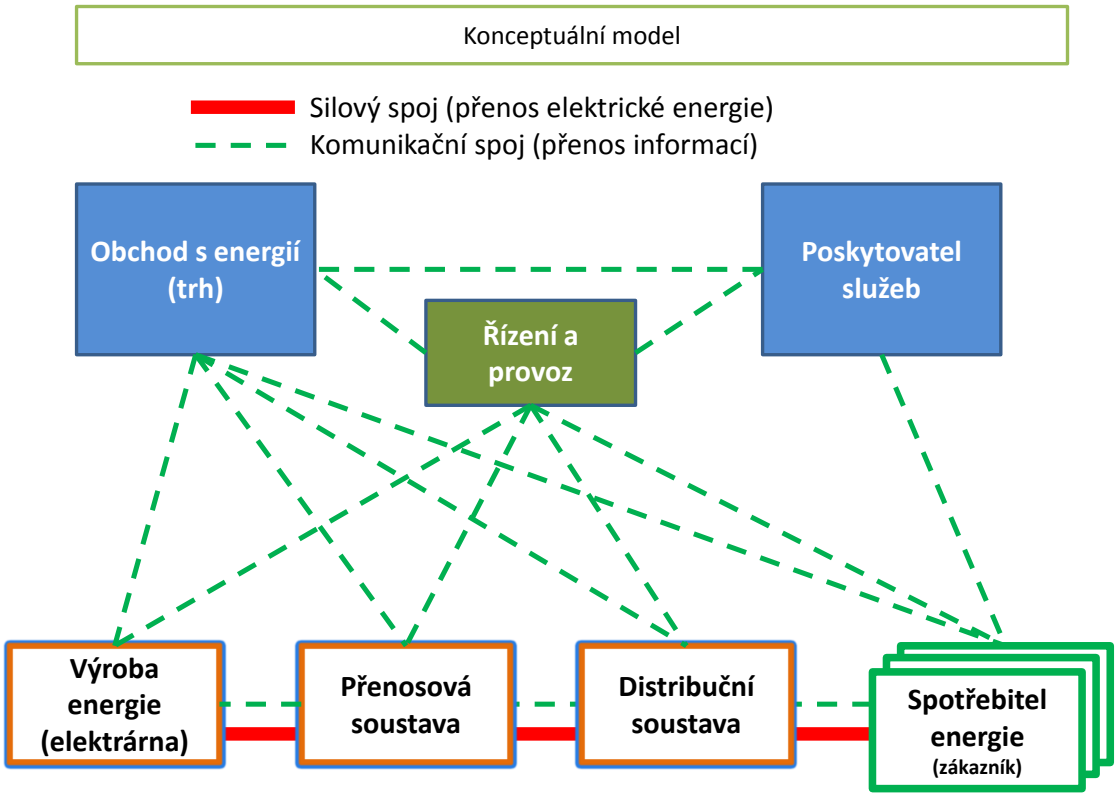
probíhá pro jednotlivé oblasti aby bylo močné začleňovat do sítě technologie různých výrobců. Na obrázku XXX jsou tři základní oblasti jejichž součinnost je nutné standardizovat jsou:



Obr. 1 Technologické oblasti součinnosti

- Napájecí systémy (popisují fyzické oblasti sítě od elektrárny až po zákazníka)
- Komunikační technologie (popisují technologie zajišťující propojení a přenos informací)
- Informační technologie (popisují technologie a způsoby řízení procesů a přenosu dat)

Konceptuální model na Obrázku 2 definuje jednotlivé domény oblastí a jejich vzájemné vazby.



(Mohou být součástí komplexních SCADA systémů)

- Technologie smart gridů využívá velké množství zařízení (např. senzorů). Tato zařízení, často od různých výrobců, ovšem můžou znamenat hrozbu pro bezpečnost celé sítě.

3. Standardy pro Smart Grid

Níže jsou uvedeny organizace podílející se na tvorbě standardů pro koncept Smart Grid.

3.1. ANSI C12. Smart Grid

- **ANSI C12.1-2008** Standard for Electric Meters Cod efor Electricity Metering

- **ANSI C12.18-2006/IEEE P1701/MC1218** Protocol Specification for ANSI Type 2 Optical Port

3.2. CEN-CENELEC-ETSI Smart Grid Coordination Group (SG-CG)

Organizace CEN, CENELEC a ETSI zveřejnily výsledky společné práce (**Final Report of the CEN/CENELEC/ETSI Joint Working Group on Standards for Smart Grids**) v oblasti vývoje standardů pro koncept Smart Grid. Doporučení v jednotlivých oblastech architektury systému, tvorby standardů a bezpečnosti vycházejí z těchto standardů:

- ISO/IEC 27001:2005
- ISO/IEC 27002:2005
- IEC 62351
- NERC CIP V4 (US standardy)
- NISTR-7628-2010 (US standardy)

3.3. NIST

NIST and SGIP (Smart Grid Interoperability Panel) CSWG (Cyber Security Working Group).

- **NIST SP 1108:** NIST Framework and Roadmap for Smart Grid Interoperability
- **NIST Priority Action Plan 2:** Guidelines for Assessing Wireless Standards for Smart Grid Applications
- **NIST SP800-39:** Managing Information Security Risk: Organization, Mission, and Information System View
- **NIST SP800-53:** Recommended Security Controls for Federal Information Systems
- **NIST SP800-82:** Guide to Industrial Control Systems (ICS) Security

3.4. NISTIR

- **NISTIR 7628** Security for metering standards DLMS/COSEM

- **NISTIR 7761** NISTs Guideline for Assessing Wireless Standards for Smart Grid Aplications
- **NISTIR 7823**: Advanced Metering Infrastructure Smart Meter Upgradeability Test Framework

3.5. ETSI (ETSI M2M Smart Grid)

Standard pro systémy mobilní komunikace mezi něž patří systémy GSM, UMTS (3G), LTE. Implementace tzv. Machine-2-Machine (M2M) komuikace, tedy komunikace mezi stroji pomocí mobilní komunikační sítě (např. pro interaktivní bezdrátové připojení inteligentních senzorů, spínačů a čidel s řídicím systémem).

- **ETSI 10269** Machine to Machine communications (M2M); Smart Metering USE Cases
- **ETSI 102.935** Machine-To-Machine Applicability of M2M architecture to Smart Grid Networks, Impact of Smart Grids on M2M platform
- **OSGP**

3.6. IEC (IEC SG3 (Strategic Group 3))

Na oblast konceptu Smart Grid jsou zaměřeny následující skupiny standardů.

IEC TC13

Zaměření na standardizaci pro Smart Grid v oblasti komunikace s chytrou měřící strukturou sítě elektrické energie.

- **IEC 62056** Security for metering standards DLMS/COSEM

IEC TC57 (WG15)

Zaměření na standardizaci v oblasti průmyslový řídících systémů jako např. SCADA.

- **IEC 62351**

IEC TC65

Zaměření na standardizaci v oblasti průmyslový měřících a řídících procesů.

- **IEC 62443** (based on ISA SP99)
- **IEC 62541** OPC UA

3.7. IETF

- **IETF RFC 6272** Internet protocols for Smart Grid

3.8. IEEE

V rámci organizace IEEE byl ustanoven výbor SCC21 (IEEE Standards Coordinating Committee 21), který je pověřen tvorbou standardů, doporučení a koordinací pro oblast palivových článků, fotovoltaniky, distribuovaného způsobu výroby energie a způsobů akumulace energie. SCC21 spojuje dvě oblasti. První oblast nese označení standardu IEEE 1547 a zabývá se oblastí vzájemného propojování všech částí konceptu Smart Grid (jak je naznačeno na Obrázku 1 a v Příloze 1). Druhá oblast pod označením standardu IEEE 2030 se zabývá součinností a principy vzájemné komunikace jednotlivých oblastí konceptu Smart Grid (jak je naznačeno na Obrázku 1 a v Příloze 1).

- **IEEE P2030/ IEEE P2030-2011** Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power Systém (EPS), and End-Use Applications and Loads
- **IEEE 1547** Standard for Interconnecting Distributed Resources with Electric Power Systems
- IEEE 1547.1 až IEEE 1547.10
- **IEEE P1775/1.9.7,** March 2009 IEEE Standard for Power Line Communication Equipment – EMC Requirements – Testing and Measuring Methods
- **IEEE P1601** Broadband Communications Over Power Lines MAC and PHY protocols
- **IEEE 1686**: Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
- **IEEE 802 series**
  - IEEE 802.11i: Wireless Security
  - IEEE 802.1X: Port based Network Access Control
  - IEEE 802.1AE: MAC security

- IEEE 802.AR: Secure Device Identity

3.9. ISO

- ISO 27000: Information Security Standards

3.10. ISA

- ISA SP99 Cybersecurity mitigation for industrial and bulk power generation stations

4. Komunikační protokoly

Komunikační protokoly musejí zajistit součinnost a bezpečnost všech připojených součástí. Nutnost existence komunikační vazby na páteřní komunikační systém.

4.1. OSGP (Open Smart Grid Protocol) (ETSI GS OSG 001)

- Komunikace na aplikační vrstvě nezávislá na komunikačním médiu
- Využívá komunikaci typu master/slave, kdy centrální jednotka iniciuje komunikaci.
- Při komunikaci mezi centrální jednotkou a vzdáleným zařízením, které podporuje protokol OSGP, je využíváno časového multiplexu TDM.
- Využívají komunikační protokol **EN14908,** který zajišťuje autentifikaci, nikoli však šifrování
- Implementace vlastního šifrování a autentifikace je řešeno dopňkově na aplikační vrstvě
- Jedinečný statický 94-bitový OMA klíč (OMAK) pro každé zařízení je po připojení nahrazen sdíleným OMA klíčem přiděleným řídící jednotkou.
- Algoritmy autentifikace jsou navrženy tak, aby

- Bezpečnostní doporučení pro komunikaci vychází z norem j ISO 27001, ISO 27002, ISA99.
- Standardy pro komunikační protokoly a kybernetickou bezpečnost Smart Gridů v US:
  - NISTIR 7628

- FIPS 140 – Standard pro kryptografickou ochranu

5. Komunikační systémy

(Pro komunikaci konceptu Smart Grid jsou využity kromě dedikovaných technologií také veřejné komunikační sítě a běžně používané technologie a standardy. Metodické pokyny a doporučení pro použití bezdrátových komunikačních technologií v konceptu Smart Grid zveřejnila organizace NIST v dokumentu

- Sítě pro mobilní komunikaci (GPRS/ EDGE/ HSPA/ LTE)
    - Rizika spojená s nárůstem použití mobilních telefonů (Android…)
    - Doporučení pro bezpečnost v US: NIST SP800-124
- Bezdrátové datové sítě založené standardu IEEE 802.11 (WiFi) , 802.15 Bluetooth
    - Doporučení pro bezpečnost v US: NIST SP800-121
- Pevné datové sítě založené standardu IEEE 802.3 (Ethernet)
    - Doporučení pro bezpečnost v US: NIST SP800-114,

Pro bezdrátové sítě vydal institut NIST dokument zabývající se technickými aspekty použití bezdrátových technologií pro Smart Grid:

NISTIR 7761: NIST Priority Action Plan 2**,** NISTs Guideline for Assessing Wireless Standards for Smart Grid Aplications

Komunikace v rámci větrných elektráren definována podle: IEC 61400-25, NIST PAP 16

6. Bezpečnostní rizika

Kybernetická bezpečnost Smart Gridu je podle dokumentu NIST SP800-82 blízce spjata s Průmyslovými řídicími systémy (mezi něž patří i systémy SCADA). Na druhou stranu se ve Smart Gridech objevuje další aspekt a tím je právě interakce se zákazníkem, jehož okamžité požadavky je třeba vyhodnocovat a zpracovávat. K tomuto účelu je potřeba využívat osobních informací zákazníka, které jsou přenášeny přes nezabezpečené prostředí veřejných sítí (dost často bezdrátově).

Dva hlavní důvody bezbztností standardizace v oblasti kybernetické bezpečnosti Smart Gridu:

- Spolehlivost dodávek
    - Zajištění spolehlivosti poskytovaných služeb kritické infrastruktury implementací moderních komunikačních technologií otevírá nové možnosti správy a řízení systému, ale současně přináší rizika útoku a s tím spojené hrozby.
- Ochrana osobních údajů zákazníka
    - Koncept Smart Grid přináší přímé propojení koncového zákazníka a dodavatele komunikačním rozhraním, namísto klasického konceptu, kdy bylo spojení realizováno pouze pomocí rozvodné a distribuční sítě.

Samotná oblast komunikace v závislosti na typu přenášené informace je v dokumentech vydanými organizacemi CEN-CENELEC-ETSI je rozdělena do dvou oblastí (tříd). CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Information Security.

- Osobní informace
    - Protože je pro interakci systému v konceptu Smart Grid nutné pracovat (přenášet v komunikační síti) s osobními informacemi zákazníků, vyžadují tato data speciální ochranný přístup.
    - Oblast ochrany osobních informací musí splňovat zákonné požadavky pro práci s osobními informacemi.
- Systémové informace
    - Zde jsou definovány systémové informace potřebné pro správnou funkci celého systému pracujícího na konceptu Smart Grid (dne se jedná o např. přihlašovací údaje, šifrovací klíče a jiné administrátorské a obchodní informace).

Jak je uvedeno v úvodu, vlivem decentralizace a transfromace systémové sítě z izolované na otevřenou (připojení do veřejné sítě Internet), dochází k riziku vnějších kybernetických útoků.

7. Závěr

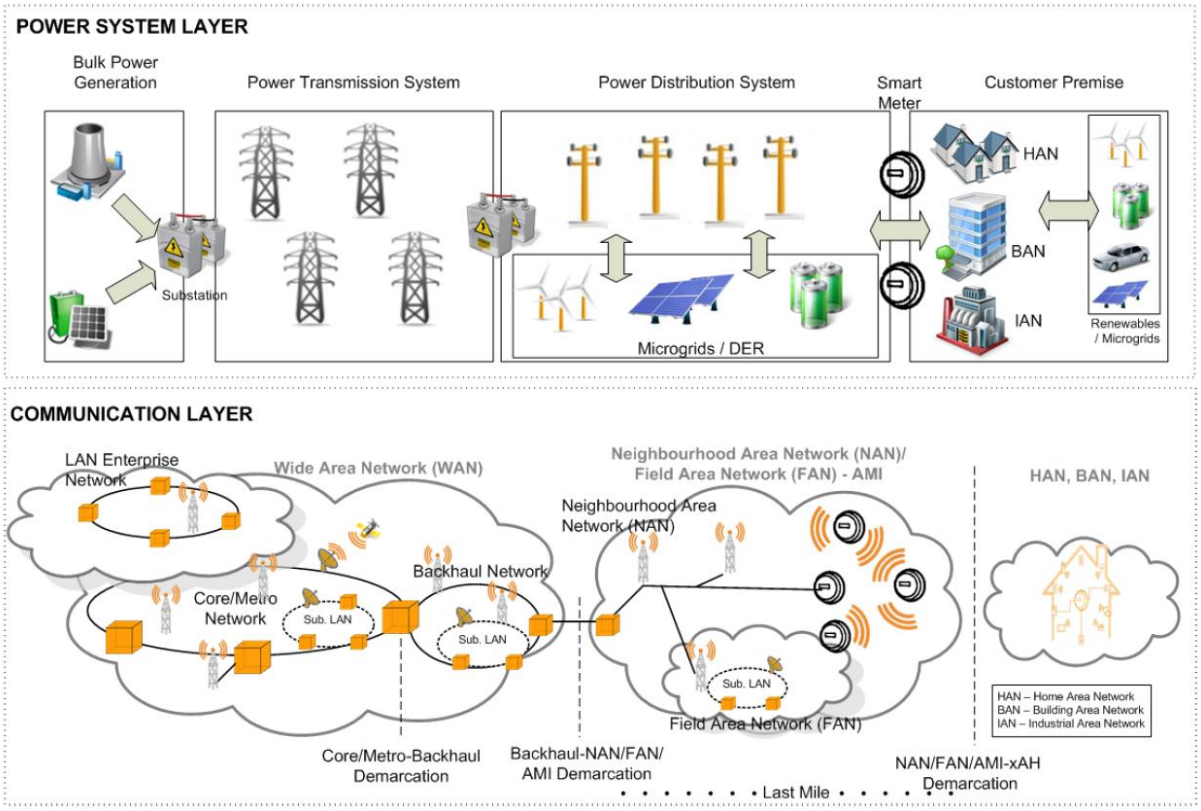
Koncept inteligentního měřícího a řídicího systému kritických infrastruktur jako je např. dodávka elektrické energie, který bude interaktivně propojovat všechny oblasti a domény spojené s výrobou, rozvodem, distribucí, prodejem i spotřebou energie, označovaný jako Smart Grid, je nevyhnutelným krokem k uspokojení vyvíjejících se nároků volného trhu. Důkazem toho, že koncept Smart Grid bude implementován do stávajícího konceptu řízení kritických infrastruktur naznačuje intenzivní zájem mnoha mezinárodních organizací (ANSI, CEN, ETSI, IEEE, 3GPP, ITU-T, NIST, NISTIR, IEFT, CENELEC, IEC, ISA…). Tyto organizace vytvářejí standardy, doporučení a metodické postupy spojené s dílčími problémi integrace.

Přijetí komplexních standardů definujících způsoby součinnosti a komunikace chytrých sítí je nevyhutelným krokem. Jinak by nebylo možné integrovat různá technologická řešení čímž by se snížila efektivita řízení a správy.

Cílem studie byla analýza standardizačního procesu v oblasti Smart Grid. Byly popsány standardy v rámci jednotlivých organizacích podílejících se na přípravě a návrhu technologického řešení konceptu Smart Grid. Byly identifikovány jednotlivé technologické oblasti, které je nutné koordinovaně propojovat, aby bylo možné vytvoření efektivního bezpečného způsobu chytrého řítení. Dále byly definovány bezpečnostní rizika spojené s nutností přenášet osobní a systémové informace komunikační sítí.

8. Příloha 1

Schéma přenosové sítě elektrické energie a komunikační infrastruktura pro implementaci konceptu Smart Grid.



Převzato z

IEEE P2030 Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power Systém (EPS), and End-Use Applications and Loads, 2010.

9. Příloha 2

Schéma rozvodné sítě v ČR podle údajů ČEPS