MINISTERSTVO PRŮMYSLU A OBCHODU

EVROPSKÁ UNIE
EVROPSKÝ FOND PRO REGIONÁLNÍ ROZVOJ
INVESTICE DO VAŠÍ BUDOUCNOSTI

OPPI

Projekt:
energetická a kybernetická bezpečnost

I. etapa – aktualizace SVA

Praha 2013

TECHNOLOGICKÁ PLATFORMA
ENERGETICKÁ BEZPEČNOST ČR

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

– OBSAH –

Shrnutí I. etapy:

V rámci první etapy došlo k aktualizaci SVA ve všech plánovaných technologických oblastech. Tato aktualizace vyšla z kontextu zmapovaných iniciativ a dokumentů na národní i nadnárodní úrovni, které signalizují rostoucí význam tématu ochrany kritické infrastruktury a společenské odolnosti (resilience) a na ně navazující

přísun investic. Podobně byl rozpoznán trend narůstající potřeby efektivních procesů standardizace a certifikace.

Jednotlivé studie pokrývající technologické oblasti zmapovaly stav v daných segmentech a v rámci aktualizace SVA spočívající v jejím zúžení a její specifikaci identifikovaly konkrétní priority, jež budou v dalších fázích rozpracovány. Tyto priority vycházejí z identifikace nových hrozeb a požadavků na nové bezpečnostní a technologické systémy.

Vzhledem k proměně v realizačním týmu bude oblast sledování prvků kritické infrastruktury specifikována později, kdy se novým gestorem stane Řízení letového provozu ČR.

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			

PREAMBULE – ÚVOD DO PROBLEMATIKY

Tento materiál představuje výstup z první fáze naplňování SVA Technologické platformy Energetická bezpečnost (TPEB) ČR. Deklarovaným cílem TPEB je na základě SVA iniciovat výzkumné a vývojové projekty zaměřené na návrhy nových produktů, a služeb a to jak z hlediska technologického, tak i legislativně procesního. 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 stávající 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.

1. Shrnutí

Úvodní kontextuální kapitola poukázala na rostoucí význam ochrany kritické infrastruktury a společenské odolnosti (resilience), který lze vysledovat v národních, evropských i transatlantických strategických dokumentech. S rozpoznáním významu toho tématu pro (nad)národní obranu a bezpečnost přirozeně souvisí i nárůst potenciálních investic, které budou nadále stimulovány programy a iniciativami v rámci EU i NATO. Z hlediska stávající situace je patrné, že budoucí efektivní strategie v této oblasti bude vyžadovat vyšší míru mezinárodní koordinace a spolupráce. Nejen v tomto ohledu se jako zásadní jeví torba spolehlivých certifikátů a standardů stejně tak jako posílení standardizačních a certifikačních autorit, které v minulosti v některých souvislostech selhávaly.

Kapitola zabývající se oblastí komunikačních technologií zdůrazňuje jejich pojetí jako prostředku zabezpečení kritické infrastruktury stejně tak jako samotné infrastruktury. V kontextu komunikačních technologií jako kritické infrastruktury upozorňuje na potřebu věnovat pozornost výzkumu optimálního zálohování a zabezpečení činnosti komunikačních systémů a jejich optimálnímu autonomnímu napájení.

Kapitola věnující se kybernetické bezpečnosti se v širším slova smyslu zaměřuje na kybernetické hrozby pro systémy ve státní správě a samosprávě a v oblasti energetiky. Jako klíčové priority jsou identifikovány testování aplikací, systémů a prvků ICT infrastruktury vedoucí k závazné metodice či standardu, určení meziresortní koordinační rady pro zajištění vzájemné kompatibility a umožnění distribuovaných nouzových a obranných scénářů, či sestavení katalogu typických informačních aktiv, hrozeb, zranitelností, rizik a opatření s cílem řešit generická rizika plošně a efektivněji. V neposlední řadě vytvoření vzdělávacích programů pro veřejnost i profesionály pracující ve státním či privátním sektoru.

V oblasti fyzické bezpečnosti byla jako prioritní identifikována nutnost vytvoření legislativy, která by upravovala použití integračních platforem na objektech kritické infrastruktury s tím, že musí umožnit připojení a monitoring nadřízeného pracoviště monitorujícího objekty kritické infrastruktury, a to jednotným protokolem, který by zpracovával integrační nástroj monitoringu kritické infrastruktury. V návaznosti na vyjasněné legislativní prostředí by bylo možné projednat s vlastníky kritických infrastruktur koordinovaný přístup při zavádění těchto integračních platforem.

V oblasti sledování prvků kritické infrastruktury tento materiál předkládá úvodní návrh z University obrany. Vzhledem k různorodosti klíčových témat vyplývajících z této kapitoly se na ní bude v dalších etapách podílet více subjektů, zejména předpokládáme součinnost s Řízením letového provozu ČR, který prostřednictvím své zkušenosti lépe zachytí domácí i mezinárodní kontext stejně tak, jako jejich legislativní technologickou stránku.

2. Energetická a kybernetická bezpečnost v evropském kontextu

Cílem této kapitoly je představit kontext strategické výzkumné agendy TPEB. Hned v úvodu je třeba zdůraznit, že v rámci TPEB je energetická bezpečnost pojímána především s ohledem na ochranu kritické energetické infrastruktury. V tomto ohledu se agenda odlišuje od v ČR dominantního chápání energetické bezpečnosti, které se soustředí na bezpečnost dodávek v zahraničněpolitických a geopolitických souvislostech. V zaměření na kritickou infrastrukturu lze také nalézt inherentní propojení mezi energetickou a kybernetickou bezpečností. Jak bude naznačeno níže, problematiku kybernetické bezpečnosti lze vnímat jako páteřní v celé oblasti ochrany kritické infrastruktury.

Následující řádky nejprve představí současný strategický posun v chápání bezpečnostních priorit ve stávajícím globálním prostředí. Cílem bude poukázat na rostoucí relevanci či spíše urgenci řešení témat spojených s ochranou kritické (informační) infrastruktury. V dalším kroku se text zaměří na dynamicky se rozvíjející se iniciativy v rámci EU, které zásadním způsobem proměňují prostředí na úrovni EU i v samotných členských státech. Cílem bude poukázat na výzvy i příležitosti, které lze v kontextu vývoje EU iniciativ z pohledu ČR spatřovat. V neposlední řadě se pak text zaměří na situaci v České republice, která prozatím rozhodně nepatří k vůdčím státům v oblasti zabezpečení kritické (informační) infrastruktury.

3. Resilience (odolnost) jako vůdčí bezpečnostní koncept

Moderní společnosti jsou stále více závislé na infrastruktuře, ať už se jedná o fyzickou infrastrukturu či oblast více či méně virtuálních sítí, skrze které prochází obrovské množství informací. Technologicky stále více vyspělá infrastruktura v mnoha ohledech usnadňuje či spíše zefektivňuje nejrůznější lidské činnosti, nicméně rostoucí závislost na do značné míry nekontrolovatelné a neuhlídatelné infrastruktuře s sebou přináší i rostoucí míru nebezpečí a rizik, která mohou být výsledkem nezamýšlených procesů stejně tak jako intencionální činnosti.

Zhruba v posledním desetiletí si tuto skutečnost začínají uvědomovat i klíčové národní a nadnárodní instituce, přičemž především nadnárodní snahy prozatím přinesly pouze velmi limitované výsledky. Na druhou stranu lze však v pro ČR klíčovém euroatlantickém prostoru v posledních letech jednoznačně vysledovat snahu zefektivnit ochranu kritické infrastruktury. Do určité míry můžeme tento trend zasadit i do obecnější proměny chápání bezpečnosti. V drtivé většině evropských států v posledních letech (a ze střednědobé perspektivy od konce studené války) klesají výdaje na obranu chápanou v tradičním slova smyslu. Vyjma ekonomických důvodů spojených s ekonomickou krizí lze také především v Evropě identifikovat rostoucí neochotu podporovat vzdálené zahraniční mise. Fenomén posledních dvou desetiletí, který dobře charakterizuje metafora, podle které se o evropské bezpečnosti rozhoduje v Afghánistánu, přestává být společensky relevantní. Z politického hlediska se tak jeví obhajoba investic do „vzdálené“ obrany jako značně neperspektivní.

Lze tedy říci, že v posledních letech dochází k proměně národně-bezpečnostního paradigmatu. Zatímco konec studené války přinesl odklon od chápání národní obrany jako obrany teritoria a otevřel prostor pro „out of area missions“, současný proces velmi dobře zachycuje koncept tzv. resilience (odolnosti). Klíčovou již není obrana teritoria, ať

už v dané zemi či v dalekém Afghánistánu, ale stává se jí ochrana území, tedy ochrana obyvatelstva a infrastruktury, které se na daném území nacházejí. Doposud nesouvislé agendy jako reakce na přírodní katastrofy, kyberbezpečnost nebo protiraketová obrana jsou spojovány společným cílem, kterým je vyšší odolnost společnosti obývající tento vnitřní prostor. Zdroj rizik, proti kterým je třeba se obrnit, se přitom může nacházet kdekoliv: za branami, ale i tisíce kilometrů daleko či v kyberprostoru. Tento progresivní posun reflektují i klíčové euroatlantické strategické dokumenty. V rámci EU k původní Evropské bezpečnostní strategii (2003)[1] přibyla v roce 2010 i Strategie vnitřní bezpečnosti EU[2], která s pojmem společenské odolnosti efektivně pracuje. Méně známá je však skutečnost, že kritickou infrastrukturu a společenskou odolnost zmiňuje také poslední Strategická koncepce NATO přijatá v Lisabonu 2010.[3] **Ze strategického hlediska je orientace na ochranu kritické infrastruktury (a v širším slova smyslu na odolnost společnosti) jednoznačným klíčovým bezpečnostním trendem současnosti i budoucnosti v minimálně střednědobém horizontu. Strategický rámec bude bez pochyby určující při identifikaci potřeb a následné alokaci prostředků do výzkumu, vývoje, inovací, ale také do samotné implementace technologických řešení.**

Proměny chápání bezpečnostních priorit nereflektují pouze vnější skutečnosti, ale přirozeně reagují i na výskyt reálných problémů. Pád linky vysokého napětí na území Německa v listopadu 2006 vedl k velkým odstávkám proudu ve Francii, Itálii a zasáhl i některé části Belgie, Nizozemí, Rakouska, Španělska, Portugalska a určité dopady pocítili dokonce zákazníci až v Maroku. Celkově odstávky dodávek v krátkém čase postihly více než 10 milionů lidí. Black outy jsou dlouhodobým a poměrně častým problémem také v některých částech Spojených států.[4] Obrovské škody a sanační náklady přinesl také výbuch ropné plošiny Deepwater Horizon v Mexickém zálivu v dubnu 2010. Podle stále ještě neuzavřeného účtu společnost BP provozující plošinu zaplatila v rámci sanací a

[1] Rada EU (2009): Evropská bezpečnostní strategie: Bezpečná Evropa v lepším světě, < http://www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC7809568CSC.pdf>

[2] Evropská komise (2010): Communication from the Commission to the European Parliament and the Council of 22 November 2010 – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0050_en.htm>

[3] Strategická koncepce NATO (2010), <http://www.mzv.cz/jnp/cz/zahranicni_vztahy/bezpecnostni_politika/bezpecnostni_strategie_cr/aktivni_spoluprace_moderni_obrana.html>

[4] Centre for European Policy Studies (2010): Protecting Critical Infrastructure in the EU, *CEPS Task Report*, <http://www.ceps.eu/book/protecting-critical-infrastructure-eu>

odškodnění 41 mld. dolarů, přičemž její loňský zisk navíc klesl o necelou pětinu.[5] Podobně společnost Oxford Economics spočítala, že globální HDP poklesl o 5 mld dolarů v důsledku výpadku letecké dopravy, kterou omezila erupce islandské sopky v roce 2010. V roce 2008 World Economic Forum publikovalo studii, podle které v následujících deseti letech (2008-2018) existuje 20 % riziko zásadnějšího narušení kritické informační infrastruktury, jehož náklady by se mohly globálně vyšplhat ke 250 mld. dolarů.

Oblast kybernetické bezpečnosti představuje zcela odlišnou perspektivu. Podle poslední studie společnosti Norton (Norton Cybercrime Report 2012) se přímé náklady spojené s dopady kybernetických zločinů v roce 2012 globálně vyšplhaly na 110 miliard dolarů. Každou vteřinu se tak stává obětí kybernetického zločinu 18 lidí, což představuje zhruba 1,5 milionu obětí denně. V roce 2012 bylo poškozeno asi 556 milionu lidí, což představuje 46 % online populace.[6] Rostoucí urgenci pak naznačuje odhad, podle které bude v roce 2020 50 miliard „věcí" připojeno na internet.[7]

Média se v minulých letech významně věnovala některým kauzám, z nichž nejznámější jsou pravděpodobně dopady červa Stuxnet, který útočil na systémy průmyslové kontroly a řízení SCADA. Dle výzkumů vedených Microsoftem byl Stuxnet zřejmě mířen na íránská jaderná zařízení v Natanzu či Búšehru, neboť 2/3 z 45 tisíc napadených počítačů se nacházely v Íránu. Právě Stuxnet také mohl stát za odstávkou části centrifug v Natanzu v roce 2009.[8] Zprávy amerických zpravodajských služeb také naznačují, že státy jako Rusko či Čína vyvíjejí značné aktivity na poli cyber intelligence. Právě čínské aktivity se staly součástí jednání mezi USA a Čínou na nejvyšší úrovni. O čínské technologické vyspělosti a úrovni investic svědčí skutečnost, že Čínám a nejnižší úroveň infikovanosti malwarem ze 105 zemí, které pravidelně sleduje Microsoft Security Blog.[9] V případě Ruska nelze opomenout široce medialzovaný a zkoumaný kybernetický útok na Estonsko v roce 2007 či údajnou kybernetickou ofenzívu předcházející útoku na Gruzii v roce 2008.

---

[5] The Economist (2012): Schumpeter, 15th November

[6] Norton Cybercrime Report (2012), <http://us.norton.com/cybercrimereport>

[7] Clemente, Dave (2013): *Cyber Security and Global Interdependence*, Chatham House: THe Royal Institute of International Affairs

[8] Farwell, P. James, Rohozinski, Rafal (2011): Stuxnet and the Future of Cyberwar, *Survival*, 53, 1, pp. 23-40

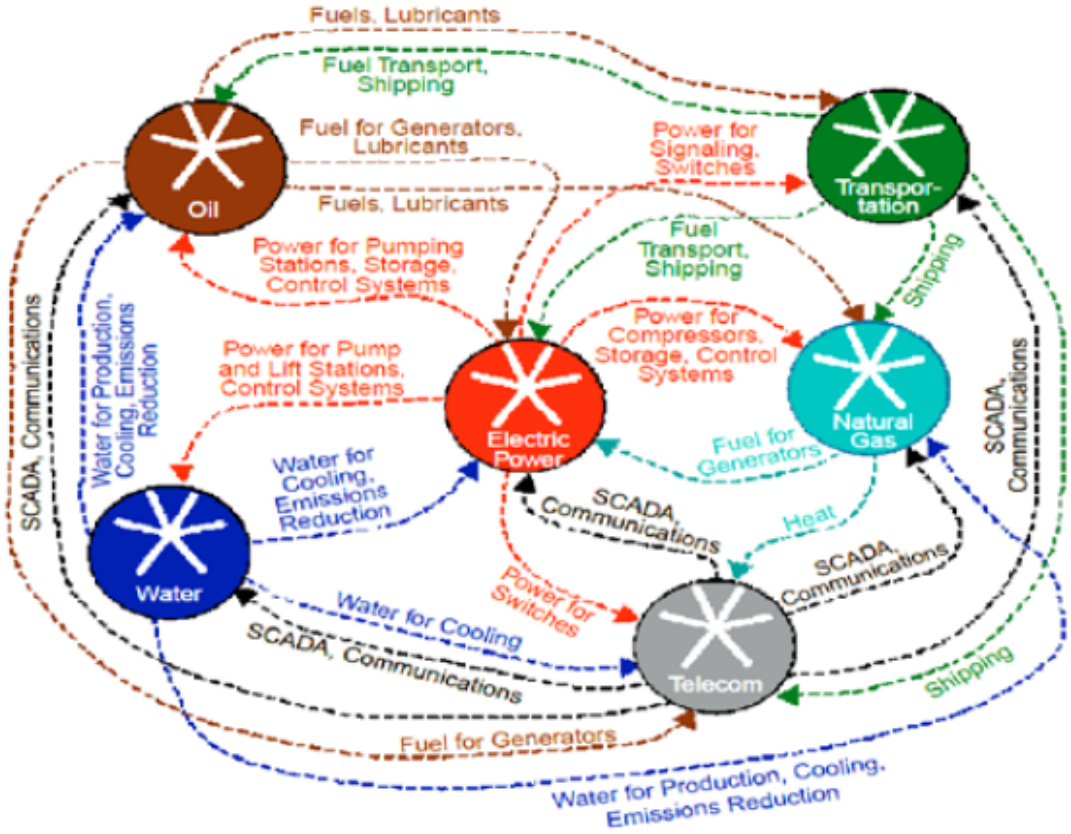
[9] Cilluffo, J., Frank (2013): *Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure*, Homeland Security Policy Institute, George Washington University, <http://www.gwumc.edu/hspi/policy/Meehan_Cilluffo%20Testimony%20March%202013.pdf>

Podobných informací, čísel a odhadů by bylo možné uvést celou řadu. V tomto kontextu mají ilustrovat potenciální reálné ekonomické dopady na státy či celé regiony. Podobné výzkumy navíc nezachycují potenciální společenské a politické dopady, které by mohly odpovídat dopadům konvenčních válek.

4. Klíčové výzvy v oblasti ochrany kritické infrastruktury

Rostoucí vzájemné propojení kritických infrastruktur jedním z klíčových charakteristik dané oblasti. V rámci jednotného vnitřního trhu EU a v návaznosti na dlouholetou snahu propojovat transevropské sítě (TEN) lze říci, že evropský prostor je provázaný relativně mnohem více než jiné světové regiony. Úrovni této provázanosti však prozatím neodpovídá míra koordinace a kooperace mezi členskými státy a institucemi EU. Tato skutečnost bude ještě rozebrána níže. Oblast kontroly kritické infrastruktury se také v posledních desetiletích proměnila v důsledku liberalizačních a privatizačních vln. V současnosti je zhruba 85 % kritické infrastruktury v privátních rukou.

Figure 1. Example of interdependencies between sectors



Source: Rinaldi et al. (2001).

Výše a níže uvedené náčrty[10] představují ukázku vzájemného propojení nejrůznějších oblastí kritické infrastruktury. Zároveň platí, že většina zmíněných systémů přirozeně překračuje národní hranice. Sektorová úroveň vzájemné závislosti je tak multiplikována geografickou vzájemnou závislostí, která byla výše ilustrována případem německého výpadku na lince vysokého napětí, který se projevil až v Maroku. Elementárně řečeno sebelépe připravená skupina států bude vždy tak silná jako její nejslabší člen či nejslabší stát v dosahu.

V návaznosti na výše zmíněné bychom jako klíčové výzvy mohli identifikovat:

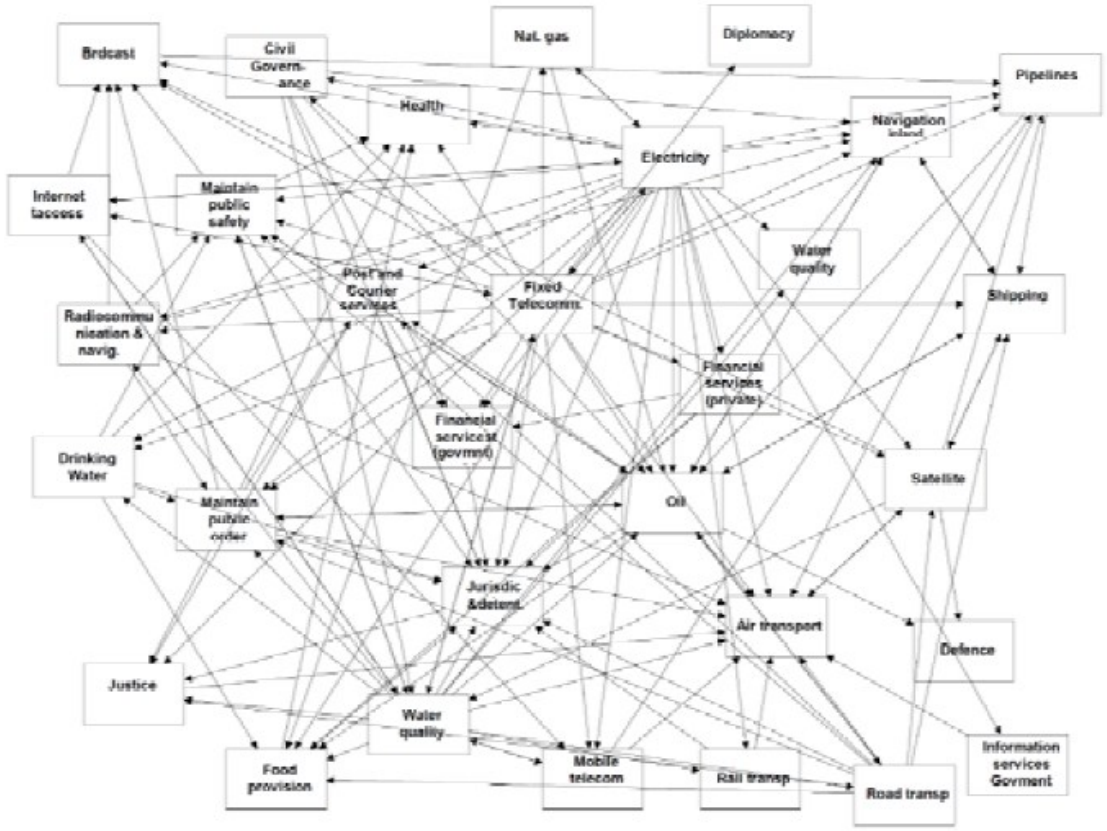
- **Střet privátní a veřejné sféry.** Jak už bylo zmíněno, většina kritické infrastruktury je v soukromých rukou, přičemž ale v podstatě celá odpovědnost za bezpečí společnosti leží na státu. Tato skutečnost vytváří

[10] Centre for European Policy Studies (2010): Protecting Critical Infrastructure in the EU, *CEPS Task Report,* <http://www.ceps.eu/book/protecting-critical-infrastructure-eu>

značný důraz na sdílení informací, které mohou leckdy mít citlivou povahu. Je evidentní, že efektivní řešení ochrany kritické infrastruktury může vznikat a existovat pouze na public-private platformách.

- **Neohraničenost**. U kritické infrastruktury a především pak u jejích informačních sektorů nelze identifikovat fyzické či politické hranice, které jsou klíčové pro určování právní, hmotné či třeba politické odpovědnosti. Tato charakteristika implikuje nutnost nadnárodních řešení v této oblasti.

Figure 4. Interdependencies



Source: Luiijf et al. (2008).

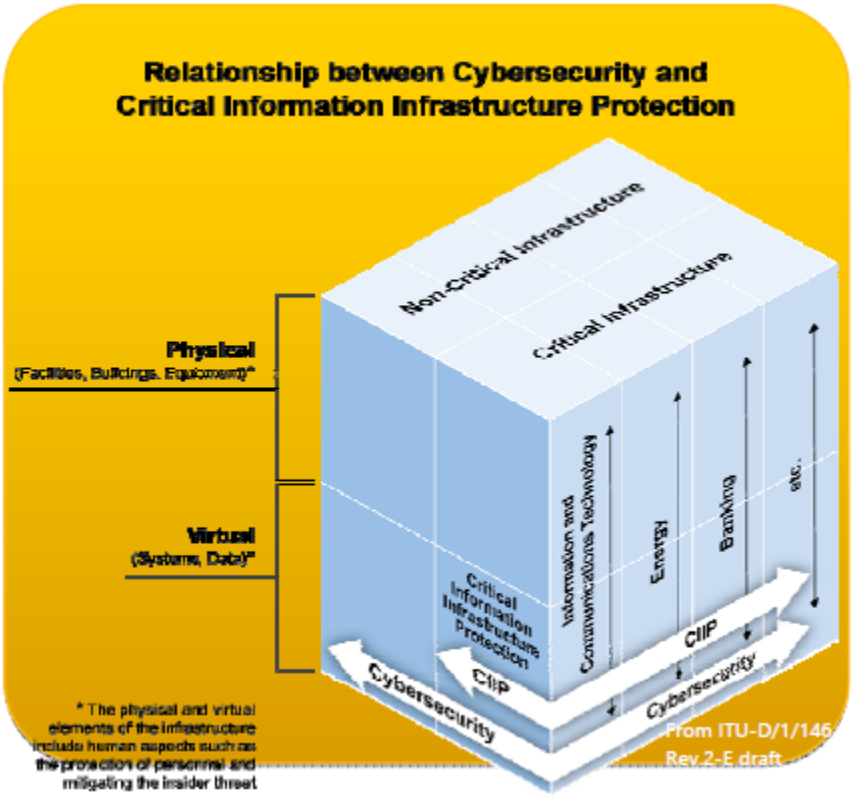
- **Síťová propojenost.** Kritická (informační) infrastruktura představuje obrovské množství vzájemně propojených, otevřených a dynamicky se rozvíjejících sítí, jejichž propojenost navíc dynamicky narůstá.
- **Komplexnost.** S výše uvedenými charakteristikami souvisí i komplexnost, která implikuje inherentní nepředvídatelnost a nestabilitu.
- **Zranitelnost.** Společenská závislost a citlivost informací dělají z kritické infrastruktury extrémně zajímavý cíl pro nejrůznější kriminálníky či

nepřátele. Je prozatím šťastným paradoxem, že naši závislot a schopnost odolnosti prozatím testují více přírodní katastrofy a havárie.

- **Lidský faktor.** I sebesofistikovanější systémy jsou závislé na lidském faktoru, přičemž platí, že nároky na něj samozřejmě se složitostí systémů stoupají.

Analytické debaty se v posledních letech věnovaly také zachycení vztahu mezi kritickou infrastrukturou a kritickou informační infrastrukturou. Samotná debata o kritické infrastruktuře má za sebou zhruba jednu dekádu, přičemž minimálně v první fázi diskuzí byla kritická informační infrastruktura pojímána jako součást (resp. podmnožina) kritické infrastruktury. V souvislosti s informačním technologickým vývojem se však tento vztah poněkud proměňuje, neboť kritická informační struktura se stává páteří systémů kritické infrastruktury. Tento trend potvrdila celá řada událostí posledních let, jejíž počátek můžeme hledat známého testu generátoru Aurora, který se podařilo poškodit pouze prostřednictvím IT technologií. Velkou pozornost si také získala zpráva, podle které ruské a čínské agentury dokázaly v dubnu a červnu 2009 penetrovat americkou elektrickou síť ovládanou North Americal Reliability Corporation (NERC). Právě poslední zmíněný případ otevřel v současnosti stále živou, a pro budoucnost evidentně klíčovou, diskuzi o významu a kvalitě bezpečnostních standardů v této oblasti. V tomto ohledu je třeba zdůraznit postupný přechod na SMART technologie, které se v americkém případě ukázaly jako velmi zranitelné. Bez zajímavosti ani nejsou mediálně vděčné případy, podle kterých se dostávají nechráněné čínské součástky do významných vojenských technologií. **Bez ohledu na možný reálný rozsah potenciálních problémů v medializovaných případech je zřejmé, že kromě technických řešení bude zcela zásadní posílit autorizační, certifikační a standardizační procesy i autority, které v některých případech vědomě či nevědomě selhaly.**

Figure 7. Cyber-security and CIIP



Source: Broda (2010).

5. Ochrana kritické infrastruktury v EU

Posledním impulsem pro celounijní iniciativy v oblasti ochrany kritické infrastruktury a resilience se staly teroristické útoky v Madridu a Londýně v červnu 2004, resp. červenci 2005. Prvním obecně formulovaným cílem bylo vytvořit strategii ochrany kritické infrastruktury, který byl později rozpracován ve Sdělení Komise Radě a Evropskému parlamentu - Ochrana kritické infrastruktury při boji proti terorismu.[11] Tento dokument poprvé v kontextu EU vymezil samotný pojem kritická infrastruktura, kterou definoval jako:

Kritické infrastruktury se skládají z hmotných zařízení a zařízení informační technologie, sítí, služeb a majetku, jejichž narušení nebo zničení by mělo vážný dopad na zdraví, bezpečnost, zabezpečení nebo hospodářský blahobyt občanů nebo efektivní fungování vlád v členských státech. Kritické infrastruktury se vyskytují v mnoha různých odvětvích hospodářství, včetně bankovnictví a finančnictví, dopravy a distribuce,

[11] Evropská komise (2004): Sdělení Komise Radě a Evropskému parlamentu - Ochrana kritické infrastruktury při boji proti terorismu, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52004DC0702:CS:HTML

energetiky, podniků veřejných služeb, zdravotnictví, dodávek potravin, komunikací a klíčových vládních služeb. Některé důležité prvky v těchto odvětvích nejsou „infrastruktura“ v pravém slova smyslu, nýbrž sítě nebo dodavatelské řetězce, které podporují dodávky důležitých výrobků nebo služeb. Například dodávky potravin nebo vody do našich hlavních městských oblastí závisí na některých klíčových zařízeních, ale také na komplexní síti producentů, zpracovatelů, výrobců, distributorů a maloobchodníků.

6. Mezi kritické infrastruktury patří:

- Energetická zařízení a sítě (např. elektrická energie, produkce ropy a plynu, skladová zařízení a rafinérie, přenosové a distribuční systémy)
- Komunikační a informační technologie (např. telekomunikace, vysílací systémy, software, hardware a sítě včetně Internetu)
- Finančnictví (např. bankovnictví, cenné papíry a investice)
- Zdravotnictví (např. nemocnice, zdravotnická zařízení a krevní banky, laboratoře a léčiva, pátrací a záchranné služby, pohotovostní služby)
- Potravinářství (např. bezpečnost, výrobní prostředky, velkoobchodní distribuce a potravinářský průmysl)
- Vodní hospodářství (např. přehrady, skladování, úprava a sítě)
- Doprava (např. letiště, přístavy, intermodální zařízení, železniční sítě a sítě veřejné hromadné dopravy, dopravní řídící systémy)
- Výroba, skladování a přeprava nebezpečných výrobků (např. chemických, biologických, radiologických a jaderných materiálů)
- Vláda (např. kritické služby, zařízení, informační sítě, majetek a klíčová státní místa a památky)

Tento dokument dále anticipoval několik hlavních stále se rozvíjejících evropských iniciativ v této oblasti – European Programme on Critical (EPCIP), Critical Infrastructure Warning Network (CIWIN) a European Network and Information Security Agency (ENISA).

7. European Programme for Critical Infrastructure Protection

EPCIP je de facto zastřešujícím programem pro řadu inciativ v oblasti ochrany kritické infrastruktury založeným Sdělením komise ze dne 12. 12. 2006[12] v návaznosti na Zelenou knihu o ochraně kritickém infrastruktury. Hlavním cílem EPCIPu je zlepšit kapacity v oblasti ochrany kritické infrastruktury v rámci celé EU i na úrovni jednotlivých členských států. Klíčovým tématem se vedle zlepšení kapacit stalo nastavení procesů sdílení informací a identifikace a analýza vzájemné závislosti. V tomto ohledu se jedním z prvních hmatatelných výsledků stalo vytvoření Výstražné informační sítě kritické infrastruktury (CIWIN), která představuje veřejný internetový chráněný informační a komunikační systém.[13] Původním záměrem Evropské komise bylo vytvoření komplexního komunikačního a informačního portálu, na kterém by se setkávaly údaje členských států o hrozbách, zranitelných místech i strategiích vedoucích k předcházení a řešení problematických situací. Z pohledu Evropské komise se měl systém postupně stát systémem včasného varování. K tomuto kroku však nedošlo kvůli odporu některých členských států (mj. i ČR). Z CIWINu se tak stává především informační a komunikační fórum, do kterého budou postupně zapojovány také národní instituce a subjekty zodpovědné na národní úrovni za jednotlivé prvky kritické infrastruktury.

Hlavním finančním nástrojem EPCIPu se stal evropský Zvláštní program: prevence, připravenost a zvládání následků teroristických útoků (2007–2013), který byl využíván k financování projektů sedmého rámcového programu z rozpočtového rámce EU pro roky 2007-2013. V novém rozpočtovém rámci došlo k zásadnímu navýšení prostředků pro DG Home Affairs, a to o zhruba 40 procent oproti předchozímu rozpočtovému rámci. Tuto skutečnost je třeba dát do souvislostí s proměnou chápání konceptu bezpečnosti zmíněnou v úvodní pasáži. Klíčovým nástrojem v novém období se stane tzv. Internal Security Fund, pro který vyhrazeno více než 4,6 mld. eur.[14]

[12] Evropská komise (2006): Sdělění komise o Evropském programu na ochranu kritické infrastruktury, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0786:FIN:CS:PDF

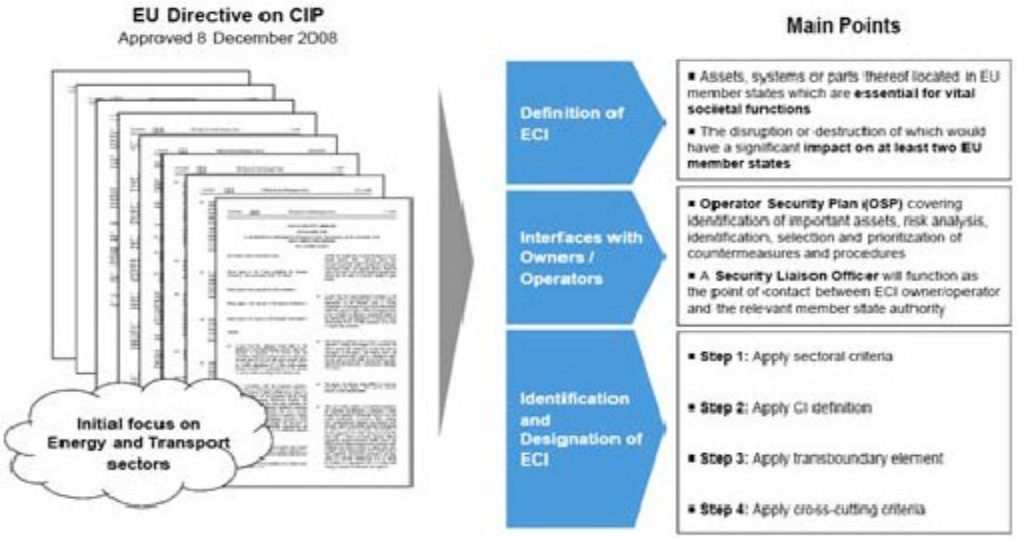
[13] Rada EU (2008): Návrh ROZHODNUTÍ RADY o výstražné informační síti kritické infrastruktury (CIWIN), http://ec.europa.eu/prelex/detail_dossier_real.cfm?CL=cs&DosId=197548

[14] DG Home Affairs (2013): Funding Home Affairs beyond 2013, http://ec.europa.eu/dgs/home-affairs/financing/fundings/funding-home-affairs-beyond-2013/index_en.htm

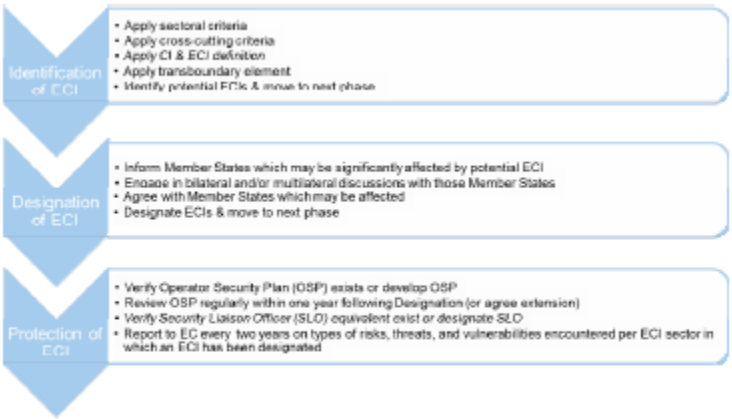
Nejvýznamnějším legislativním nástrojem se stala Směrnice 2008/114/ES,[15] jejímž cílem bylo zavézt postupy pro určování a označování evropských kritických infrastruktur a společný přístup k posouzení potřeby zvýšit ochranu těchto infrastruktur s cílem přispět k ochraně obyvatel. ČR implementovala tuto směrnici prostřednictvím změny zákona č. 240/2000 Sb. o krizovém řízení. Kromě legislativní úpravy také v dialogu se sousedními zeměmi ČR identifikovala evropskou kritickou infrastrukturu (pouze) v oblasti energetiky. Už z české zkušenosti je patrné, že směrnice nenaplnila původní ambice, které spočívaly v kompletní identifikaci a tzv. Evropské kritické infrastruktury a v přijetí mechanismů na její ochranu. V procesu schvalování směrnice došlo postupně k zúžení sektorů z původních 11 (energetika, jaderný průmysl, ICT, voda, potraviny, zdraví, finance, doprava, chemický průmysl, vesmír, výzkumné prostředky) na dva hlavní (energetika a doprava). Jako další sektor, ve kterém by měla být identifikována a designována evropská kritická infrastruktura, byl později zmíněn ICT.

Podle směrnice měly členské státy provést čtyřstupňovou analýzu na národní úrovni směřující k identifikaci a designaci evropské kritické infrastruktury (viz schéma) a poté ve spolupráci s vlastníky daných infrastruktur připravit tzv. Operator Security Plan (OSP) naznačující bezpečnostní opatření. Každý vlastník evropské kritické infrastruktury měl také určit Security Liaison Officera, který by se stal kontaktem pro evropské partnery.

[15] Rada EU (2008): Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:CS:PDF



Annex III směrnice přímo specifikoval tři fáze vedoucí k identifikaci, designaci a ochraně systémů evropské kritické infrastruktury. Většina členských států využila své vlastní národní seznamy kritické infrastruktury a z ní poté vytvářela seznam evropské kritické infrastruktury dle definice uvedené v čl 2 směrnice. Z celkového pohledu lze říci, že pro většinu zemí s rozvinutým systémem ochrany kritické infrastruktury směrnice nepředstavovala v podstatě žádnou přidanou hodnotu. Proces identifikace a designace evropské kritické infrastruktury v sektoru dopravy narážel na určitou disproporci mezi leteckým a námořním subsektorem a ostatními subsektory. Jedním ze závěrů analytických implementačních studií také byla skutečnost, že se nepodařio zcela zachytit vzájemnou provázanost a závislost jednotlivých sektorů a subsektorů, což mělo dopad na identifikační i designační fázi.



ECI Process

Z výsledků implementace je patrné, že směrnice neměla příliš pozitivní vliv stav ochrany kritické infrastruktury na evropské i národní úrovni. V konečném důsledku bylo identifikováno a designováno pouze několik evropských kritických infrastruktur a následně několik Operation Security Plans. Navíc žádná z transevropských energetických sítí nebyla identifikována jako evropská kritická infrastruktura, což svědčí o zcela neefektivní aplikaci metodologie uvedené v annexech směrnice. K pozitivním výsledkům naopak patří skutečnost, že se zvýšilo všeobecné povědomí o hrozbách spojených s kritickou infrastrukturou a do určité míry i ochota členských států spolupracovat v nadnárodním rámci na snahách o její ochranu.

Důkazem o rostoucím významu tématu ochrany kritické infrastruktury je i její začlenění do širších strategických plánů a dokumentů EU. V této souvislosti je třeba zmínit zejména Stockholmský program z roku 2009,[16] kde je snaha o redukci zranitelnosti EU v oblasti kritické infrastruktury uvedena jako jeden z hlavních cílů. Součástí Stockholmského programu je také výzva ke všem institucím i členským státům EU k prohlubování společných iniciativ v oblasti ochrany kritické infrastruktury a prohlubování resilience. Součástí tohoto procesu by měla být i evaluace a následná revize směrnice 2008/114/EC.

Ochrana kritické infrastruktury také hraje významnou roli ve Strategii vnitřní bezpečnosti EU. Strategie upozorňuje na nové kapacity v rámci kriminální či teroristické činnosti stejně tak jako na zranitelnost systémů kritické infrastruktury. Zároveň zdůrazňuje potřebu solidarity při reakcích na problémy i nutnost lepší prevence a připravenosti.[17] V tomto ohledu se jako klíčové jeví procesy risk assessmentu a risk managementu, které na unijní úrovni v podstatě absentují.

EPCIP je nadále rozvíjen sítí konzultačních a expertních skupin, které napomáhají sdílení a výměně informací a při identifikaci vzájemných závislostí. V neposlední řadě je možné v rámci EPCIPu využít i další nástroje fungující v rámci Evropské komise. V oblasti ochrany obyvatelstva lze využít kapacity Civil Protection Monitoring and Information Center, které je součástí varovných systémů Evropské komise využívaných

[16] Stockholmský program (2010): http://europa.eu/legislation_summaries/human_rights/fundamental_rights_within_european_union/jl0034_cs.htm

[17] Evropská komise (2010): Communication from the Commission to the European Parliament and the Council of 22 November 2010 – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, <http://europa.eu/legislation_summaries/justice_freedom_security/fight_against_organised_crime/jl0050_en.htm>

při koordinaci rychlé pomoci mezi členskými státy v případech havárií, přírodních katastrof či teroristických útoků.

V kontextu ochrany kritické infrastruktury se také často zapomíná na roli Rady EU v rámci Společné bezpečnostní a obranné politiky. Rostoucí relevance tématu ochrany kritické infrastruktury v oblasti zahraniční a bezpečnostní politiky EU opět potvrzuje trend zmíněný na počátku tohoto textu. Resilience a ochrana společnosti navazuje platformu vzájemné spolupráce členských států, která byla s odkazem na přírodní katastrofy zahájena v rámci ES už v roce 1987. Viditelnější strukturu představuje jednotka Civil Planning and Conduct Capability (CPCC), která byla vytvořena v rámci Evropské bezpečnostní a obranné politiky v roce 2000 pro podpor civilního plánování v oblasti krizového managementu EU. V kontextu lisabonských proměn struktury Rady došlo v roce 2009 ke spojení civilního a obranného ředitelství do Crisis Management and Planning Directorate, což reflektovalo silnější tendeci EU k civilní složce managementu konfliktů. Oblast kritické infrastruktury je v této souvislosti vnímána především v kontextu prevence přírodních katastrof a jejich managementu.

8. Ochrana kritické informační infrastruktury v EU

Pro oblast ochrany kritické informační infrastruktury platí zřejmě ještě více než pro ochranu ostatních infrastrukturních sítí, že v rámci UE existuje značná diverzita mezi přístupy jednotlivých členských států. Některé více spoléhají na aktivity privátního sektoru v oblasti resilience (Velká Británie), jiné naopak vytvořily národní instituce často na základě existujících národních obranných struktur (Švédsko, Francie). Výchozí myšlenku EU iniciativ tak představovaly snahy po koordinaci jednotlivých národních iniciativ a harmonizaci legislativních přístupů s cílem umožnit efektivnější sdílení dat.

V návaznosti na tyto myšlenky byla vytvořena agentura ENISA (European Network for Information Security), která se má stát určitou expertní platformou fungující jako center of excellence asistující Evropské komisi, členským státům i privátním aktérům při prevenci a řešení bezpečnostních problémů.[18] Hlavní náplní ENISY je sběr a vyhodnocování dat týkajících se bezpečnostních incidentů v EU. Tato činnost v oblasti analýzy rizika by měla stimulovat horizontální spolupráci členských

[18] Evropská komise (2007): Nařízení Evropského parlamentu a Rady, kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0861:FIN:CS:PDF

zemí a potřebnou výměnu informací, přičemž na vertikální ose se jako klíčová jeví spolupráce mezi veřejným a privátním sektorem.

Další aktivity ENISY směřují do oblasti zprostředkování procesů standardizace, jejímž cílem je skrze definování technických požadavků zajistit interoperabilitu sítí a informačních platforem. Specifické cíle ENISY byly rozpracovány v Akčním plánu,[19] který rozpracovává úkoly v celkem pěti oblastech. V oblasti *připravenosti a prevence* měly členské státy do konce roku 2011 zajistit fungování vládních skupin CERT (Computer Emergency Response Team), které se mají stát klíčovými složkami vnitrostátní schopnosti týkající se připravenosti, sdílení informací, koordinace a reakce. Zároveň tato kapitola zdůraznila potřebu další spolupráci mezi veřejným a soukromým sektorem prostřednictvím Evropského partnerství mezi veřejným a soukromým sektorem pro odolnost (E3PR).

V oblasti *detekce a reakce* klíčovou aktivitu představuje vytvoření Evropského systému pro varování a sdílení informací (EISAS), který by měl být přístupný i občanům či malým a středním podnikům. Mezi další významní aktivity v dalších oblastech pak patří například posílání spolupráce mezi vnitrastátními CERTy či odolnost a stabilita internet.

[19] Evropská komise (2009): Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection, "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

KOMUNIKAČNÍ TECHNOLOGIE

1. Analýza současného stavu

Strategická výzkumná agenda (SVA) Technologické platformy energetické bezpečnosti (TPEB) se věnuje popisu perspektivních oblastí výzkumu, vývoje a inovací v oblasti **komunikačních technologií** na stranách 12 až 16. Směry vývoje jsou zde predikovány na základě zevrubné analýzy současného legislativního rámce a současného stavu vývoje.

Na komunikační technologie lze pohlížet jako na **prostředek zabezpečení** kritické infrastruktury, a současně jako na samotnou **kritickou infrastrukturu**. V SVA TPEB je akcentován první pohled. Výzkum komunikačních technologií je nahlížen zejména z perspektivy zajištění fungování integrovaného záchranného systému, zabezpečení SMART technologií proti zneužití či zabezpečení infrastruktury lokální výměnou informací a vzdáleným řízením.

Právě potřeba vzdáleného řízení a koordinace fungování energetických a dalších kritických systémů (dodávky pitné vody a základních potravin) činí z komunikačních systémů samotnou kritickou infrastrukturu. Bez funkční komunikace totiž nelze optimalizovat dodávky energií a dalších kritických komodit. Aktualizace stávající SVA toto hledisko reflektuje (viz 2. kapitola).

K implementaci zabezpečené a vysoce spolehlivé komunikace lze využít standardní, komerčně dostupné technologie (systémy mobilních přenosů, kabelových přenosů, satelitních přenosů) nebo nestandardní uživatelsky orientované technologie. Standardní technologie jsou uživateli nabízeny formou služby. Tato služba je relativně levná a relativně spolehlivá, nicméně uživatel má omezené možnosti ovlivnit zabezpečení, spolehlivost a dostupnost spojení.

Uživatelsky orientovaná komunikace většinou využívá volných kmitočtových pásem k přenosu informace za podmínek, daných správcem rádiového spektra (Český telekomunikační úřad). Tato volnost nabízí široké možnosti strategického výzkumu.

Komunikační systémy jakou nedílná součást ochrany kritických infrastruktur i kritická infrastruktura sama jsou spravovány a rozvíjeny na úrovni Evropské unie (ochrana celoevropských infrastruktur, satelitní systém Galileo, globální telematické systémy, atd.), na úrovni více států jednoho regionu i na úrovni národní. Výzkum

komunikačních systémů na všech třech úrovních podporuje Evropská unie projekty rámcových programů.

2. Trendy výzkumu

Funkční komunikační systémy jsou naprosto nezbytnou podmínkou fungování všech současných systémů. Výhodou komunikačních systémů (na rozdíl od distribučních sítí strategických energií a surovin) je možnost jejich robustního zálohování a zabezpečení.

2.1. Jako příklad uveďme municipální propojení počítačových sítí:

1. Sítě jsou primárně propojeny optickými kabely. Optickým kabelem se šíří koherentní optická vlna. Optický kabel optickou vlnu izoluje od vlivu okolí a zamezuje neautorizovanému přístupu k přenášené informaci. Proto tento způsob propojení zajišťuje vysokou rychlost přenosu dat a vysokou spolehlivost spojení.
2. V případě přerušení optického kabelu (úmyslného či neúmyslného) lze spojení operativně a rychle nahradit bezkabelovým atmosférickým optickým spojem. Tento spoj je založen na šíření koherentní optické vlny volným prostorem (atmosférou). Vlastnosti spoje mohou být negativně ovlivněny stavem atmosféry (déšť, mlha), nicméně rychlost přenosu a nebezpečí neautorizovaného přístupu k přenášeným datům jsou srovnatelné s přenosem po optickém vláknu.
3. Pro případ nepříznivých atmosférických podmínek lze atmosférický optický spoj zálohovat spojem mikrovlnným. Mikrovlnný spoj je odolnější vůči nepříznivým atmosférickým podmínkám, nicméně rychlost přenosu a rezistence vůči neautorizovanému přístupu jsou mnohem nižší.

Považujeme-li komunikační systémy za kritickou infrastrukturu, je nutné věnovat pozornost **výzkumu optimálního zálohování a zabezpečení činnosti komunikačních systémů**. Na evropské úrovni je nutno řešit zabezpečení celoevropských systémů (páteřní počítačové sítě, satelitní systémy), na regionální úrovni zabezpečení regionálních systémů (systémy mobilních komunikací, systémy rádiového vysílání, telematické systémy).

Nutnou podmínkou fungování komunikačních systémů je spolehlivé zabezpečení jejich napájení. Považujeme-li komunikační systém za kritickou infrastrukturu, je

zapotřebí navrhnout autonomní způsob napájení. Jedině tak lze eliminovat závislost komunikačního systému na dalších kritických infrastrukturách.

Autonomní napájení komunikačních systémů lze realizovat jedním z níže uvedených způsobů nebo jejich kombinací:

1. Akumulovaná energie (baterie, palivové články, super-kapacitory);
2. Záložní zdroje energie (diesel-agregáty);
3. Přírodní zdroje energie (sluneční, vodní, větrná);
4. Bezdrátová dodávka energie ze vzdálených zdrojů.

Je-li komunikační systém kritickou infrastrukturou, je třeba iniciovat **výzkum optimálního autonomního napájení komunikačních systémů**.

2.2. Výzkum komunikace zprostředkované poskytovateli

Při přenosu informace pronajatými komunikačními kanály nebo standardními službami operátorů je jedinou možností zabezpečení přenášené informace její šifrování. Šifrování dat je druh kryptografie, který zabezpečuje elektronická data, a tím umožňuje chránit soukromí jejich vlastníka.

Existuje řada volně dostupných i licencovaných programů určených k šifrování dat. Některé programy na šifrování dat jsou přímo součástí operačního systému. Technologie BitLocker je součástí operačního systému Windows Vista a Windows 7. Mezi volně dostupné programy patří TrueCrypt, DiskCryptor, FileCryptor, a mnoho dalších.

Vznik nového šifrovacího nástroje vždy podnítí snahy o prolomení šifry a neautorizovaný přístup k přenášené informaci. Výzkum v oblasti šifrovacích nástrojů je tedy zaměřen na vývoj stále robustnějších metod šifrování. Nové metody šifrování bývají časem prolomeny, takže je nutné opět přijít s novou, robustnější metodou.

2.3. Výzkum uživatelsky orientované komunikace

Uživatelsky orientované komunikační systémy jsou systémy vyvíjené na míru zákazníkovi. V těchto systémech lze aplikovat vyspělé metody zabezpečení komunikace a zamezení neautorizovaného přístupu k přenášeným datům.

Obecně můžeme říci, že přenášenou informaci můžeme zabezpečit jedním z níže uvedených způsobů nebo jejich vzájemnou kombinací:

1. **Zabezpečení na úrovni signálů**. K zabezpečení slouží různé šifrovací techniky (znemožňují přečtení informace) a zabezpečovací kódy (umožňují obnovení informace při jejím částečném zničení).
2. **Zabezpečení na úrovni kmitočtu**. Přenášená informace je rozprostřena v širším kmitočtovém pásmu (*spread spectrum*) nebo se kmitočet přenosu náhodně v širším pásmu (*frequency hopping*). Obě techniky lze využít k zabezpečení přenosu (pseudo-náhodné změny kmitočtu znají pouze komunikující strany).
3. **Zabezpečení založené na prostorové a polarizační diverzitě**. Možnost napadnout bezdrátový komunikační spoj může být omezena využitím adaptivních antén (automatické tvarování směrové charakteristiky) a změnou polarizace elektromagnetické vlny.

2.4. Stávající výzkum sleduje zejména následující směry:

1. **Hardwarová akcelerace kryptografických algoritmů.** Kryptografické algoritmy naplňují specifické požadavky informační bezpečnosti jako integrita dat, důvěrnost a autenticita. Vykonávání kryptografických algoritmů integrovaných do SSL/TLS protokolů může být akcelerováno implementací krypto-systémů logickými poli FPGA. Hardwarová akcelerace kryptografických algoritmů přináší vyšší rychlost a vyšší úroveň kybernetické bezpečnosti.
2. **Zkoumání kybernetické bezpečnosti na komplexních modelech.** Jelikož kybernetické hrozby mohou mít komplexní dopad, jsou zkoumány více-pohledové přístupy k eliminaci hrozeb. Tyto přístupy jsou zkoumány na modelech, jež vycházejí z dynamiky systémů, technologie minimalizace technologických hrozeb a kybernetické teorie. Další zdokonalování těchto modelů umožňuje zlepšovat ochranu před kybernetickými hrozbami. K implementaci modelů lze s výhodou využít expertní systémy.
3. **Využití synergií v rozsáhlých systémech**. Ke zvýšení kybernetické bezpečnosti rozsáhlých systémů lze využít synergií mezi tokem informací, materiálů, energií, atd. Vhodný řídicí algoritmus, který optimalizuje dílčí toky, tak může narušení toku jedné komodity napravit díky synergii s toky ostatních komodit.
4. **Využití umělé inteligence**. Umělá inteligence vykazuje vysoký stupeň adaptivity, podobný živým bytostem. Právě vysoký stupeň adaptivity předurčuje umělou inteligenci k obraně proti kybernetickým útokům a dalším nebezpečím.

5. **Digitální forenzní metody** jsou analogií ke konvenčním forenzním metodám. Zaměřeny jsou však na digitální sítě a prokazování zločinů v těchto sítích. Výzkum využívá výsledků digitálních forenzních metod k posilování odolnosti stávajících systémů vůči kybernetickému zločinu.
6. **Omezení padělání digitálních podpisů a dalších autentizačních stop**. Zkušenost ukazuje, že nebezpeční padělání elektronického podpisu (sken běžného podpisu) je nesrovnatelně vyšší ve srovnání s padělaním podpisu konvenčního. Metody obrany jsou založeny na vodoznačení, evolučních algoritmech a doménových transformacích. Díky těmto metodám lze nebezpeční zneužití podpisů výrazně omezit.

Výše uvedený výčet přístupů ke zlepšování kybernetické bezpečnosti je více méně ilustrativní. Jak je vidět v databázi IEEE Xplore, v letech 2010 až 2013 byly otázky kybernetické bezpečnosti diskutovány ve více než 50 článcích v odborných časopisech a více než 200 příspěvcích na mezinárodních konferencích. Je tedy zřejmé, že se jedná o velmi aktuální téma.

2.5. Potenciál pro normotvorbu

Jako inspirace při přípravě norem zabezpečení komunikačních kanálů může sloužit přístup americké NIST (*National Institute of Standards and Technology*). V roce 1997 NIST oznámila, že chce nahradit stávající standard DES (*Data Encryption Standard*) standardem novým AES (*Advanced Encryption Standard*). NIST vyhlásila soutěž na zveřejnitelný šifrovací algoritmus, který by byl schopen chránit citlivá vládní data. 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.

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. V prvním kole bylo vybráno pět nejlepších návrhů (kompromis bezpečnosti, možnosti implementace a šíře aplikací), v druhém kole byl vybrán vítěz. Na základě vítězného návrhu byla v roce 2001 vytvořena odpovídající norma.

3. Závěry a doporučení

Komunikační systémy jako kritická infrastruktura i jako nástroj ochrany kritických infrastruktur jsou rozvíjeny na celoevropské úrovni, regionální úrovni i národní úrovni. Výzkum národních komunikačních systémů je dominantně podporován

z národních zdrojů (projekty Technologické agentury ČR, rezortních ministerstev a orgánů státní správy). Na výzkum celoevropských a regionálních komunikačních systémů lze získat podporu z evropských rámcových programů.

V letech 2007 až 2012 bylo z těchto rámcových programů podpořeno přes 100 projektů směřujících k prevenci, připravenosti a zvládání bezpečnostních hrozeb. Vlajkovým projektem byl ERNCIP (*European Reference Network for Critical Infrastructure Protection*).

Varovná informační síť kritické infrastruktury (CIWIN, *Critical Infrastructure Warning Information Network*) je dalším příkladem celoevropské aktivity. CIWIN je zabezpečený informační a komunikační systém na bázi internetu, který slouží k výměně informací vztažených k ochraně kritické infrastruktury (CIP, *Critical Infrastructure Protection*). CIWIN byla spuštěna v roce 2013.

Evropská komise bude podporovat projekty směřující k dalšímu rozvoji politik a metodik řízení rizik fungování kritické infrastruktury. Komise se bude snažit zpřístupnit všechny prostředky poskytované Centrem zpravodajských analýz (INTCEN, *Intelligence Analysis Centre*).

Snahou členských subjektů TPEB by měla být integrace do výzkumných konsorcií celoevropských projektů. K tomu lze využít:

- **Mezinárodní kontakty univerzit**. Univerzity se účastní řady projektů 7. rámcového programu, akcí mezinárodní spolupráce COST a dalších nadnárodních aktivit. Tyto kontakty lze zprostředkovat i dalším členům TPEB.
- **Globální působnost nadnárodních firem**. Nadnárodní společnosti, které mají dceřiné firmy v řadě zemí, mohou relativně snadno vytvořit kostru nadnárodního konsorcia pro řešení evropského projektu.
- **Podpora zástupců státní správy** reprezentujících Česko v mezinárodních organizacích a výborech těchto organizací.
- TPEB má díky členství univerzit, firem a veřejných subjektů jedinečnou šanci profitovat ze synergií těchto tří složek.
- Výsledky výzkumu vyplývající z řešení evropských projektů lze následně úspěšně lokalizovat na národní úrovni. Lokalizace může být financována

Technologickou agenturou ČR, CzechInvestem či dalšími národními poskytovateli veřejné podpory výzkumu a vývoje.

- Pro strategický výzkum komunikačních technologií bude výhodné nabídnout členství v TPEB malým a středním firmám, které se zabývají vývojem a výrobou komunikačních zařízení. Jako příklad uveďme:
- DCom, www.dcom.cz, mikrovlnná rádiová zařízení
- Racom, www.racom.eu, rádiové modemy
- Miracle Group, www.miracle.cz, optické bezdrátové spoje
- Alcoma, www.alcoma.cz, mikrovlnné bezdrátové spoje
- S nabídkou členství by mohly být osloveny další významné univerzity (ČVUT v Praze, Západočeská univerzita v Plzni), ústavy Akademie věd ČR (Ústav fotoniky a elektroniky, Ústav přístrojové techniky) atd. To by významně zvýšilo šance TPEB na zastoupení v konsorciích strategických celoevropských projektů.

FYZICKÁ BEZPEČNOST

1. Monitoring technických prostředků fyzické bezpečnosti kritické infrastruktury

Při již zmíněném zabezpečení datových sítí pro komunikaci s objekty kritické infrastruktury lze tyto výhodně využít k preventivnímu monitoringu odpovědnými orgány z hlediska bezpečnostních technologií. K tomu je nutné v prvé řadě provést monitoring stavu, potřeb a následně přijmout řešení.

1.1. Současný stav integrace bezpečnostních systémů v ČR

Integrace bezpečnostních systémů v České republice je vzhledem k zahraničí na poměrně vysoké úrovni. Vzhledem k poměrně bohatému mixu technologií od jednotlivých výrobců jsou v ČR na předních místech, co do počtu instalací především integrační platformy malých relativně lokálních firem, pro které není problém zaintegrovat technologie různých výrobců. Velcí nadnárodní výrobci integračních platform se z větší části zaměřují na integraci "svých" technologií.

Z uvedeného vyplývá, že určitá standardizace je v našich podmínkách celkem náročná, ne však nemožná.

Integrační platformy by se dali rozdělit do mnoha vzájemně se prolínajících skupin a to jak z hlediska topologie systému, tak z hlediska hloubky integrace, nebo například z hlediska typu komunikace s integrovanými technologiemi. V každém případě vždy se jedná o sumarizaci informací z jednotlivých technologií do jednoho celku.

Z používaných integračních platforem na našem trhu mohu uvést následující (seřazeno abecedně dle názvu produktu):

Název produktu:	Výrobce / země
ABI	SPIRIT / Slovensko
AlViS	SPIRIT / Slovensko
C4	Gamanet / Slovensko
Integra	Integoo / ČR

Latis Trade FIDES / ČR

MrGuard Colsys / ČR

SBI CGC / Slovensko

SiveillanceTM Vantage Siemens / Německo

SiveillanceTM Fusion Siemens / Německo

SMS PKE / Rakousko

Winpack Honeywell / Rakousko

2. Níže uvedené popisy systémů jsou převzaté texty od jednotlivých výrobců

2.1. ABI

ABI je software pro dálkovou správu, řízení a monitorování integrovaných systémů v samostatných budovách i rozsáhlých komplexech. Jedná se o modulární vícevrstvou aplikaci typu klient/server, která umožňuje snadnou práci z jakéhokoli počítače připojeného do sítě Internet/intranet a vybaveného libovolným webovým prohlížečem. Základními funkcemi ABI jsou centrální dálková správa uživatelů, ovládání a monitorování veškerých zabezpečovacích systémů a funkce pasport pro správu a údržbu budov. Díky svým unikátním funkcím Vám ABI umožní dosáhnout snížení finančních nákladů nutných na provoz obsluhovaných lokalit i snížení celkového počtu personálu potřebného pro vlastní obsluhu a provoz. ABI nabízí plnou otevřenost vůči integrovaným systémům od libovolných výrobců.

2.2. AlViS

AlVis je univerzální grafické vývojové prostředí určené na tvorbu aplikací monitorovacích a řídících systémů. Je výsledkem dlouhodobého vývoje a má za sebou množství úspěšných instalací jak na území České republiky a Slovenské republiky, tak i Polska, Rakouska a Ruska. Je vhodný všude tam, kde vzhledem k požadavkům obsluhy, složitosti sledovaného objektu, množství různých zařízení a prioritních úrovní, není možné bez použití počítačového systému dosáhnout přehledný flexibilní lehce adaptovatelný monitorovací, řídící a výstražný systém.

2.3. C4

C4 je integrační bezpečnostní systém, který zabezpečuje centralizované a víceuživatelské řešení pro správu zařízení objektové bezpečnosti. Uživateli poskytuje rozsáhlé nástroje pro:

Centrální správu bezpečnostních zařízení

Vizualizaci a monitoring zařízení

Automatizaci bezpečnostních procesů

Analýzu a vyhodnocování bezpečnostních informací

Centrální identity management

Podporu krizového managementu

Svou síťovou architekturou umožňuje sdílet informace týkající se provozu bezpečnostních zařízení více uživatelům. To samozřejmě výrazně zvyšuje efektivitu správy zařízení a podpůrných činností v rámci podniku.

Systém C4 je otevřený modulární systém, který umožňuje navrhnout instalaci dle požadavků zákazníka, od jednoduchých - monitorujících jednu samostatnou budovu, po robustní řešení monitorující různá bezpečnostní zařízení velké organizace ve všech jejích objektech bez ohledu na vzdálenost.

2.4. Integra

Událostmi řízený systém Integra 3 je nástrojem pro správu bezpečnosti a provozu budov a areálů. Tento systém zpracovává data z nejrůznějších zdrojů (od kamer a čidel přes docházkové systémy až po I/O moduly vrat, výtahů, výrobních zařízení apod.), vytváří z nich smysluplné informace (například, že v určité zóně došlo k narušení bezpečnosti, spustí akci), předkládá tyto informace srozumitelným způsobem na mapovém podkladu, společně s instrukcí jak v konkrétní situaci postupovat automaticky vytváří provozní deníky, včetně záznamů o událostech a reakcích ostrahy umožňuje jednotné vzdálené řízení technologií a zón areálu, nebo vzdálených objektů poskytuje další sofistikované funkce potřebné pro řízení dění v budově či areálu, plánování údržby, rychlé vyhledávání záznamu události apod.

2.5. LATIS

Integrační a monitorovací systém LATIS® SQL byl vyvinut na základě nejaktuálnějších HW i SW technologií. Do produktu byly převzaty všechny důležité vlastnosti, které se osvědčily již u jeho předchůdce – systému LATIS®, který si vydobyl renomé při provozu na mnoha komerčních instalacích, i při ostraze strategických armádních objektů.

Hlavním úkolem systému LATIS® SQL je zajistit integraci a monitoring všech technologií, které se v současné době používají k provozu v moderních budovách a technologických areálech. Těmito technologiemi jsou například elektronické zabezpečovací systémy (EZS), elektronické požární systémy (EPS), systémy elektronické kontroly vstupu (EKV), systémy MaR (ventilace a klimatizace, výtahy atd.), uzavřené televizní okruhy (CCTV) a další.

Pro efektivní funkci budovy nebo areálu jako celku je nejdůležitější dosáhnout jednak integraci všech systémů do jednotného a pro obsluhu přehledného a srozumitelného informačního systému a jednak umožnit vzájemnou vazbu informací mezi systémy tak, aby události identifikované jedněmi systémy vyvolávaly logické reakce jiných systémů.

Skutečné propojení činností jednotlivých systémů přináší teprve řídicí systém LATIS® SQL, který propojením s uvedenými technologiemi prostřednictvím jejich komunikačních kanálů integruje systémy do jednoho celku. Tato integrace přináší uživateli komfort umožňující efektivní provoz a správu z jednoho pracoviště, na kterém budou všechna data a informace přístupná v jednotné srozumitelné podobě.

2.6. Centrální monitorovací pracoviště MrGuard

Základem tohoto pracoviště je počítač typu PC se softwarovým vybavením umožňujícím monitorování stavu jednotlivých systémů (čidel, otevření dveří, stavu hlídání apod.).

K tomuto pracovišti je možné připojit ústředny EZS, EPS, a zařízení pro kontrolu vstupů. Obsluha je opticky i akusticky upozorněna na důležité události (např. poplachy, ale i jiné volně programovatelné stavy). Monitorovací pracoviště je možné využít i pro sledování stavu a vyhodnocování poplachů na vzdálených pracovištích, kde není stálá obsluha či ostraha. Pomocí modemů nebo prostřednictvím datové sítě je možné přenášet poplachová hlášení nebo hlášení o stavu jednotlivých prvků a částí objektů,

případně zobrazovat aktuální situaci graficky na mapě těchto objektů včetně zobrazení stavu čidel.

2.7. SBI

Produkt SBI (Secure Building Inteligence) je určen pro komplexní obsluhu bezpečnostních, provozních, technologických elektronických systémů. Představuje nejmodernější softwarové řešení v oblasti monitorování, řízení, správy systémů EZS, EPS, měření a regulace, CCTV, EKV, včetně komfortního vyhodnocení docházky. Program využívá progresivní softwarové technologie pro vytvoření aplikačního uživatelského prostředí v prostředí prohlížeče webových stránek Internet Explorer. Základem prostředí je databáze MS SQL (MSDE), která udržuje všechny databáze, tabulky a číselníky nezbytné pro provoz programu. Kompletní obsluhu, správu a údržbu programu je možné převést z jakéhokoliv PC s MS Internet Explorer připojeného prostřednictvím sítě LAN, WAN k databázovému serveru. Systém podporuje sběr dat z monitorovaných technologií jak pomoci rozhraní RS 232 (lokální připojení) i prostřednictvím sítí LAN, WAN s využitím komunikačního protokolu TCP / IP. Program je důsledně řešen jako modulární systém (uživatel volí, které moduly systému chce používat), včetně propracované správy připojených lokalit a technologií. Pro vizualizaci je zvoleno přehledné mapové zobrazení aktuální situace v objektu. Pro každého operátora je možné nastavit jiné aplikační prostředí, které není závislé na PC, kde je aktuálně operátor přihlášen. Operátorovi je na kterékoliv stanici automaticky vytvořené jeho aplikační prostředí, včetně jeho práv v systému SBI. Samozřejmostí databázového prostředí je komfortní systém logování všech aktivit - uživatelských i technologických. Program je určen především pro zákazníky, kteří mají objekty rozprostírající se v rámci velkého území a jednotlivé objekty jsou vybaveny datovou sítí. Z hlediska funkčnosti je SBI řešeno na klíč zákazníkovi.

2.8. SiveillanceTM Vantage

softwarové řešení pro kritickou veřejnou i firemní infrastrukturu. Tento software byl vyvinut pro řízení bezpečnostních systémů firem a institucí, u nichž představuje výpadek provozu ohrožení osob nebo velké finanční ztráty. SiveillanceTM Vantage tak najde uplatnění například v těžkém, chemickém nebo farmaceutickém průmyslu, v podnicích zabývajících se výrobou a distribucí energie, či ve veřejné, letecké a lodní dopravě. Software je výjimečný svou schopností podpory všech procesů a procedur moderní organizace s důrazem na bezpečnost a přizpůsobivostí vůči bezpečnostním předpisům konkrétní aplikace. SiveillanceTM Vantage snižuje rizika a následky

potenciálního nebezpečí pro provoz firem, což v důsledku přináší významnou finanční úsporu. Otevřená rozhraní umožňují do SiveillanceTM Vantage integrovat rozličné bezpečnostní systémy, jako například kontrolu vstupu, průmyslové televize, videoanalýzy, požární a bezpečnostní signalizace, tísňové hlásky a různé komunikační systémy. Tyto prostředky v kombinaci s řídicím jádrem systému představují výkonný a efektivní systém pro bezpečnostní management.

2.9. SiveillanceTM Fusion

sofistikovaná technologie pro komplexní bezpečnost

Nová platforma s názvem Siveillance Fusion pro komplexní zabezpečení objektů a lokalit. Siveillance Fusion řeší problematiku integrace bezpečnostních systémů kontroly vstupu, videa a zabezpečovací signalizace. Poskytuje kompletní přehled o situaci, nepřetržitě monitoruje potenciální hrozby a zvyšuje celkovou bezpečnost organizace.

2.10. SMS

Bezpečnostní řídící systém - integruje na výrobci nezávislé relevantní bezpečnostní systémy

SMS je počítačový řídící systém, který definuje nová měřítka. Samostatné bezpečnostní systémy jako digitální videosystém (DVS), přístupová kontrola, poplachové systémy, požární systémy, ozvučovaní systémy, programovatelné automaty atd. se sloučí do jednotné operátorské plochy. Nezávislá funkčnost těchto systémů tímto není ovlivněna.

SMS nabízí řešení na míru a garantuje bezpečnostnímu personálu přehled a jednoduchou manipulaci při co nejvyšší možné flexibilitě.

2.11. WINMAG

WINMAG je systém řízení a správy na bázi PC, speciálně vyvinutý pro požadavky bezpečnostních technologií.

WINMAG realizuje správu a vizualizaci EPS, EZS, systémů kontroly vstupu, digitálního záznamu videa a systému řízení únikových východů. Databáze a uživatelská pracovní plocha jsou vytvořeny dle běžných standardů. Hlášení se zobrazují graficky a v textové formě.

Technické aplikační možnosti WINMAGu jsou mnohostranné. Zahrnují rozsah od přehledně zobrazovaných hlášení až po aktivní řízení všech součástí bezpečnostní a

technologické správy budov. Na základě bezpečnostních sítí IGIS-Loop a essernet® je WINMAG profesionálním a komfortním řešením informačního a vizualizačního systému správy budov.

3. Vize vývoje v nejbližším období

V nejbližším období se předpokládá další posilování v oblasti integrace a tudíž i zvyšování rizika napadení bezpečnostních systémů z kyberprostoru. Je bezpodmínečně nutné aby do politiky zabezpečení datové infrastruktury byla zahrnuta i infrastruktura bezpečnostních technologií, které jsou čím dál tím více dalším uživatelem kyberprostoru.

Je však taktéž nutné chápat fyzickou bezpečnost jako další a neoddělitelnou vrstvu komplexní bezpečnosti kybernetické.

Moderní integrační nástroje fyzické bezpečnosti začnou čím dál tím více být mimo jiné i nástrojem pro řízení procesů v krizových situacích, sledování a vyhodnocování poruchovosti jednotlivých technologií a jejich prvků a dalších analytických procesů.

4. Doporučení a další postup

Pokud shrneme výše uvedené, stejný stav je i u provozovatelů KI. Stav integrace a přístup k fyzicke bezpzpečnosti je u jednotlivých organizací značně rozdílný. I v případě, že má o fyzickou bezpečnost provozovatel KI zájem je tato budována nesystematicky a nahodile. Z tohoto důvodu je mezi fyzickým zabezpečením jednotlivých provozovatelů KI značný rozdíl. V tomto případě složky zodpovědné za krizové řízení v okamžiku ohrožení objektů KI řeší až nastalou situaci a nemají průběžné informace o stavu minimálně nutné technologie fyzické bezpečnosti na jednotlivých objektech.

5. Stanovení možné cesty

Z uvedeného vyplývá, že určitým řešením by bylo vytvoření jednotné platformy, případně komunikačního protokolu, pro monitoring a případně částěné ovládání bezpečnostních systémů objektů KI nad jednotlivými integracemi (integračními platformami), která by zajišťovala sběr dat o stavu jednotlivých technologií a zároveň zabezpečovali preventivní přehled například o prováděných pravidelných kontrolách jednotlivých technologií

To předpokládá nutnost existence legislativy, která by upravovala použití integračních platforem na objektech KI s tím, že musí umožnit připojení a monitoring

nadřízeného pracoviště monitorujícího objekty KI (krajská ředitelství PČR?) a to jednotným protokolem, který by zpracovával integrační nástroj monitoringu KI (nutno vyvinout, či upravit stávající). V tomto bodě existuje průsečík s kybernetickou bezpečností (je nutný spolehlivý a bezpečný přenos těchto dat).

Pro zdárné naplnění těchto požadavků je nutné vytvořit i dostatečný legislativní nástroj, který by specifikoval použití jednotného protokolu, úroveň a pravidla instalace a následné servisní péče nejen o nadstavbový (integrační) nástroj, ale i o primární bezpečnostní technologii.

Aby byla zajištěna i ekonomická stránka tohoto projektu a následně je nutné vytvořit adekvátní pravidla financování. Toto může být zajištěno například povinným odvodem určitého procenta z plánovaných investičních akcí u každého provozovatele objektů KI a to do budování bezpečnostních systémů (včetně servisu a následné technické péče). K tomuto by byli jednotliví provozovatelé zavázáni například prováděcím předpisem k novele zákona o bezpečnosti KI.

6. Závěrem

V předchozích odstavcích byl popsán stávající a možný koncový stav. Pro zdárné naplňování výše uvedeného je bezpodmínečně nutné v první řadě vyvolat jednání s bezpečnostním managementem jednotlivých provozovatelů objektů KI a s nimi koordinovat další postupy tak, aby u těchto provozovatelů nedocházelo ke zbytečným nákladům a aby připravovaná legislativa a uvažované protokoly korespondovali co nejvíce s jejich potřebami a zvyklostmi.

OCHRANA KRITICKÉ INFRASTRUKTURY – MOŽNOSTI VYUŽITÍ UAV

1. Legislativa – doplněk bodu 3.3.2.1

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 a 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 řadu 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.

2. Základní definice předpisu.

2.1. Autonomní letadlo:

Bezpilotní letadlo, které neumožňuje zásah pilota do řízení letu.

2.2. 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.

2.3. Bezpilotní systém (UAS).

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

2.4. 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.

3. Rozsah působnosti

Doplněk 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 UCL 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 a okolní letový provoz.

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

Z uvedeného plyne, že bezpilotní letadlo po splnění příslušných požadavků může provádět např. letecké práce, letecké činnosti pro vlastní potřebu, rekreační a sportovní létání, atd.

4. Obecná specifikace činností

- 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 a činnost leteckých škol.
- Leteckou činností pro vlastní potřebu se rozumí lety, kterými zajišťuje právnická nebo fyzická osoba podnikatelskou nebo jinou činnost, k níž je oprávněna podle zvláštních předpisu. 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.

5. Bezpečnost.

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.

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.

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 a kontrolního spoje provede ukončení letu.

6. Letové prostory.

Let bezpilotního letadla a/nebo modelu letadla smí být prováděn jen v prostorech stanovených článkem 7 přílohy pokud UCL 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 a 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 a 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.

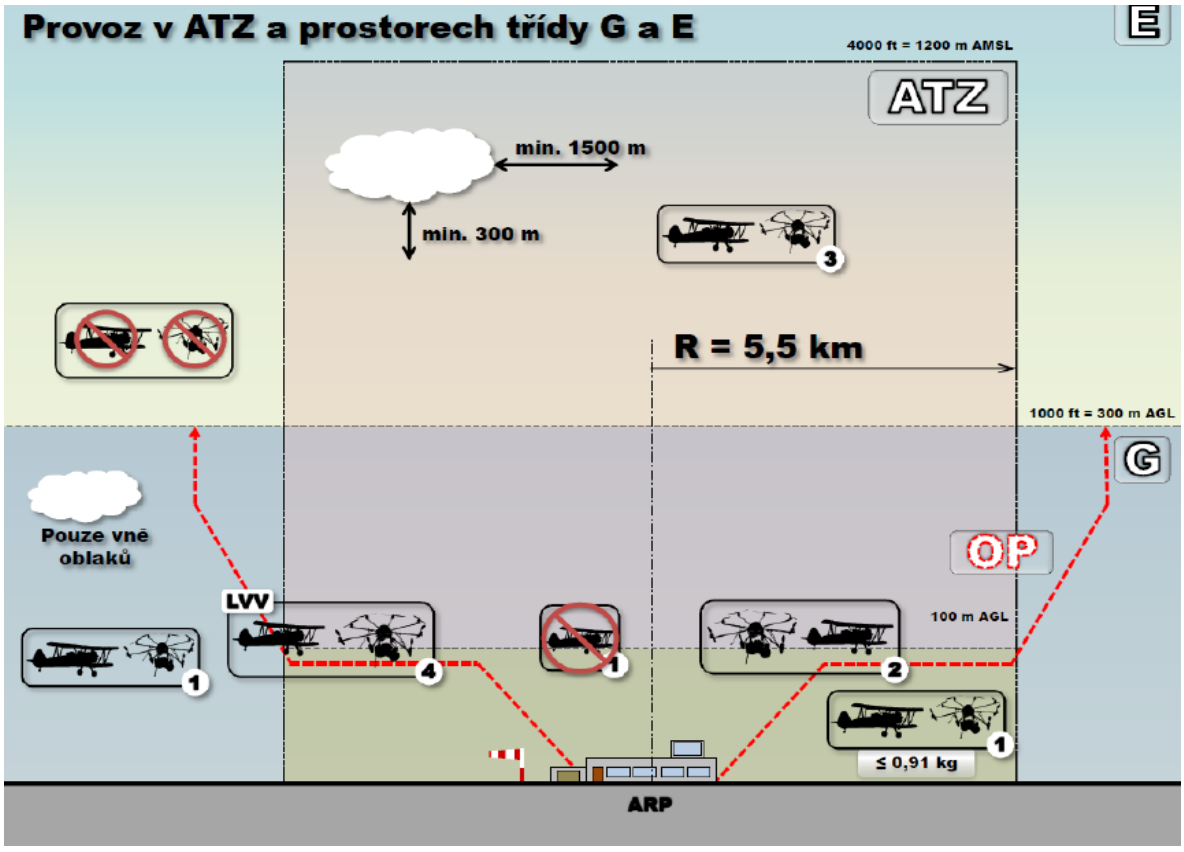
Autonomní bezpilotní letadlo nesmí být provozováno ve společném vzdušném prostoru.

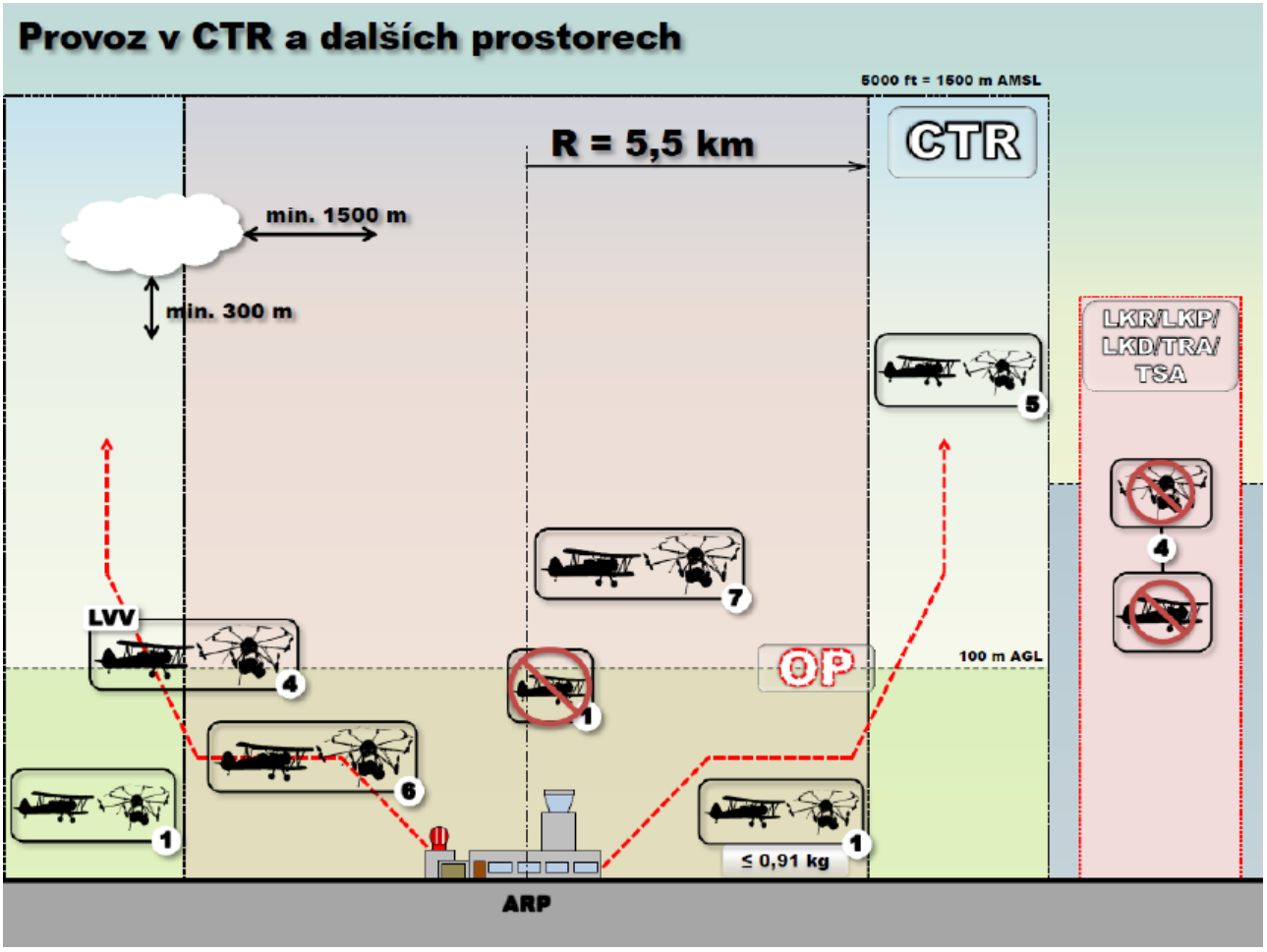
Modely letadel s maximální vzletovou hmotností do 20 kg

Bezpilotní letadla (tj. včetně modelů letadel s maximální vzletovou hmotností nad 20 kg)

CTR	Řízený okrsek letiště	**LKR**	Omezený prostor
ATZ	Letištní provozní zóna neřízeného letiště	**LKP**	Zakázaný prostor
OP	Ochranná pásma letišť	**LKD**	Nebezpečný prostor
G / E	Označení třídy vzdušného prostoru	**TSA**	Dočasně vyhrazený prostor
ARP	Vztažný bod letiště	**TRA**	Dočasně vymezený prostor
AMSL	Nadmořská výška	**AGL**	Nad úrovní země

1	Lety bez koordinace
2	Splnění podmínek provozovatele letiště (PL) + koordinace s letištní informační službou (AFIS)
3	Splnění podmínek PL + koordinace s AFIS
4	Souhlas/povolení Úřadu pro civilní letectví (ÚCL)
5	Letové povolení příslušného stanoviště řízení letového provozu (ŘLP). ŘLP může dále požadovat: stálé obousměrné spojení a odpovídač sekundárního radaru
6	Povolení ÚCL (nebo v případě leteckých prací (LP) koordinace s ŘLP + koordinace s PL). ŘLP může dále požadovat: stálé obousměrné spojení a odpovídač sekundárního radaru
7	Povolení ÚCL (nebo v případě LP koordinace s ŘLP + koordinace s PL) + letové povolení ŘLP. ŘLP může dále požadovat: stálé obousměrné spojení a odpovídač sekundárního radaru





7. Ostatní legislativa.

Provoz bezpilotního letadla musí být v souladu s 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.

Orgány a asociace působící v ČR

- Úřad civilního letectví
- Ministerstvo dopravy
- Asociace výrobců bezpilotních letounů.

ř.	maximální vzletová hmotnost	≤ 0,91 kg		> 0,91 kg a < 7 kg		7 – 20 kg		> 20 kg		bezpilotní letadlo provozované mimo dohled pilota
-	účel použití / požadavek	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	rekreačně sportovní	výdělečné, experimentální, výzkumné	
1	evidence letadla	ne	ano	ne	ano	ne	ano	ano	ano	ano
2	evidence pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
3	praktický a teoretický test pilota	ne	ano	ne	ano	ne	ano	ano	ano	ano
4	povolení k létání	ne	ano	ne	ano	ne	ano	ano	ano	ano
5	povolení k provádění LP a LČPVP	nelze	ano	nelze	ano	nelze	ano	nelze	ano	nelze
6	označení UA: ID štítek / ID štítek + pozn. značka	ne / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ne	ano / ano	ano / ano
7	min. ve vzdálenosti (m): vzlet, přistání / osoby, stavby / osídlený prostor	bezpečná	bezpečná	bezpečná	bezpečná	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150	bezpečná, ale minimálně 50/100/150
8	pojištění: běžný provoz / LVV (mil. Kč)	ne / 0,25	dle nař. č. 785/2004[1]	ne / 1	dle nař. č. 785/2004[1]	ne / 3	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]	dle nař. č. 785/2004[1]
9	dozor	ne	ne	ne	ne	ne	ne	ano	ano	ne
10	„failsafe" systém	ne	ano	ano	ano	ano	ano	ano	ano	ano
11	provozní příručka UAS	ne	ano	ne	ano	ne	ano	ne	ano	ne
12	hlášení událostí	ne	ano	ne	ano	ne	ano	ano	ano	ano

8. Návrhy dalšího postupu.

Navrhnout projekt zahrnující podrobný rozbor právních aspektů provozu UAS jehož cílem by bylo návrh změn platné legislativy v národních podmínkách a odstranění některých sporných nebo nevhodných bodů omezující využití systémů UAS. Dalším výstupem by byla schválená metodika pro realizaci letu.

Navrhnout projekt, jehož cílem by bylo vytvoření jednotných uznaných požadavků na piloty UAS včetně osnov výcviku a vytvoření pilotní školy pro tyto piloty.

Navrhnout projekt realizující rozbor kmitočtového pásma v oblasti řízení systémů UAS s cílem návrhu legislativní úpravy vymezující kmitočtový úsek (pásmo) pro tyto systémy.

9. Závěr:

Regulace bezpilotních letadel, včetně modelů letadel, je komplexním úkolem, kterým se zabývají státní správy také ostatních států světa s nejrůznějšími výsledky a praktickými zkušenostmi. Mezinárodní harmonizace, byť žádoucí a praktická, není v blízké budoucnosti realitou, ale pouhým přáním. Regulační rámce jdou napříč doslova všemi oblastmi letectví, včetně letové způsobilosti, provozu, způsobilosti personálu a neustále reagují na nové a nově zaváděné technologie a konstrukční principy.

Česká republika věnuje doméně bezpilotních systémů pozornost, kterou si zasluhuje a má nástroje jak pro koncepční budování regulačního rámce, tak pro jeho další modifikace s ohledem na provozní zkušenosti doma i v zahraničí. Směr dalšího vývoje proto záleží nejen na způsobu mezinárodní harmonizace a diskuzi zainteresovaných subjektů, ale také na odpovědnosti pilotů a provozovatelů.

Literatura:

http://lis.rlp.cz/predpisy/predpisy/dokumenty/L/L-2/data/effective/doplX.pdf

http://www.avbs.cz/index.php?page=download&kat=1

http://www.volny.cz/pavel.macek/regulace/PripominkySMCR.pdf

http://www.caa.cz/file/5965_2_1/download

http://www.caa.cz/navody/provoz-ostatnich-letadel-bez-pilota-na-palube

9.1. Technologie

V rámci České republiky bylo z různých zdrojů realizováno nebo se realizuje řada projektů v oblasti řízení systémů UAS umožňujících nebo alespoň předpokládaných umožnit integraci těchto systémů do jednotného vzdušného prostoru. Mezi některé lze vybrat následující:

9.1.1. FT-TA3/104 - *Výzkum a vývoj technologií pro řízení letu ultralehkých a lehkých letadel“.

Projekt řešil výzkum metod a high.end technologií pro rozpoznávání objektů určené pro systémy rychlé reakce lehkých a ultralehkých letadel a pro zvýšení bezpečnosti a komfortu letu. Navržené metody a technologie umožňují rozpoznávat í objekt ve složitých reálných scénách, měřit dálku a úhlové souřadnice a tyto předávat systémům rychlé reakce. Výsledky byly ověřeny na demonstračním vzorku a na prototypu systému pro zvýšení bezpečnosti letu.

9.1.2. FT-TA3/103 – „Výzkum high-end technologií a metod pro rozpoznávání pohybujících se objektů, stanovení parametrů pohybu objektů a pro systémy automatického sledování pohybujících se objektů“.

V projektu byl řešen výzkum metod a high.end technologií pro rozpoznání objektů, stanovení parametrů jejich pohybu a pro automatické sledování těchto objektů. Navržené metody a technologie umožňují rozpoznávat rychle se pohybující objekt ve složitých reálných scénách, měřit dálku a úhlové souřadnice a tyto předávat systémům automatického sledování. Výsledky byly ověřeny na ověřovacích vzorech pro použití v robotizaci, automatizaci, vojenských a bezpečnostních systémech.

9.1.3. FR-TI1/195 – „Výzkum a vývoj technologií pro inteligentní optické sledovací systémy“.

V projektu byl řešen výzkumu a vývoj technologií pro inteligentní optické sledovací systémy (IOSS), které umožňují detekci, rozpoznání a sledování několika objektů (cílů), nacházejících se současně v zorném poli optického systému, a to s důrazem na cíle mizivé (neočekávaně se objevující a rychle mizící za překážkami). Optický systém automaticky sleduje objekt - cíl a určuje jeho zeměpisné souřadnice, včetně extrapolace dráhy pohybu objektu při mizení za překážkou. Inteligentní optický systém umožňuje odesílání dat uživatelům. Inteligentní optické sledovací systémy jsou navrženy jako jednokamerové a dvoukamerové (stereoskopické), měřící dálku a souřadnice objektu (cíle).

9.1.4. TA02011092 – „Výzkum a vývoj technologií pro radiolokační mapovací a navigační systémy“.

Projekt se zaměřuje na výzkum a vývoj radiolokačního mapovacího a navigačního systému a rozšíření know-how v této oblasti v ČR. Tento integrovaný systém se skládá z radiolokační jednotky založené na technologii SAR (Synthetic Airborne Radar), z

inerciální navigační jednotky a řídicího modulu. Integrací uvedených modulů vznikne unikátní systém plnící funkci kontinuální navigace a získání obrazu terénu i za nepříznivých podmínek, kde stávající monitorovací a mapovací systémy již nefungují.

9.1.5. FI-IM4/022 - Výzkum, vývoj a zhotovení autonomního automatického padákového zásobovacího systému pro vojenské a humanitární účely.

Projekt realizoval výzkum matematického modelu řízení letu a umělé inteligence zásobovacího padáku pro vojenské a civilní použití. Cílem výzkumu a vývoje byla realizace zcela autonomního, vysoce sofistikovaného automatického padákového zásobovacího systému sloužícího pro zásobování vojenských jednotek v týlu nepřítele popř. sloužícího pro humanitární účely, včetně všech systému a podsystémů nutných pro obsluhu a diagnostiku.

9.1.6. FR-TI3/220 - Realizace letounu VUT 081 Kondor pro aplikaci optického monitorovacího systému a jeho ověření v reálných podmínkách.

Projekt je zaměřen na výrobu prototypu letounu VUT 081 Kondor a integrace pokročilého optického systému pro monitorování průmyslových sítí a produktovodů, bezpečnostní a dopravní pozorování. Dále pak ověření užitných vlastností celého systému na typických modelových misích monitorovacích letů. Návrh letounu vychází z letounu VUT 001 Marabu na kterém jsou provedeny konstrukční úpravy zejména trupu letounu, umožňující efektivní integraci optického monitorovacího systému a pracoviště operátora.

9.1.7. TRACK SYSTEM a.s., Čechova 1100, 50002 Hradec Králové

Vývoj, výroba a provozování víceúčelového bezpilotního vrtulníku HEROS (Helicopter Robotic System). Vrtulník je využitelný pro monitorování silničního provozu, detekce chemických látek a záření, hlídkování v chráněných oblastech a okolí státních hranic či letecké snímkování a filmování. Další uplatnění je v různých průmyslových či zemědělských aplikacích (monitorování elektrických vedení a produktovodů). Vrtulník je poháněn pístovým spalovacím motorem Rotax. Maximální rychlost letu dosahuje 181 km/h, cestovní rychlost je 139 km/h. Maximální vzletová hmotnost činí 456 kg, z čehož na užitečné zatížení připadá 120 kg. Palivová nádrž o objemu 114 l umožňuje dosáhnout vytrvalosti letu v délce až čtyř hodin.

9.1.8. FD-K3/097 - Digitální přenosový systém DATEX.

Projekt řešil digitální radiový přenos datových signálů mezi pozemní stanicí a UAV. Systém je navržen jako otevřený.

9.1.9. FR-TI1/090 - Pneumatický urychlovač pro start UAV (bezpilotního prostředku) hmotnostní kategorie do 70 kg.

V projektu byl řešen návrh a realizace pneumatického urychlovače pro zabezpečení vzletu UAV. Byl vypracován teoretický rozbor, návrh a realizace pneumatické části urychlovače, převodového ústrojí, rampy, nosného vozíku bezpilotního letounu a transportního přívěsu. Kromě odpovídající technické dokumentace bylo řešení ověřeno výrobou funkčního vzoru a provedením základních funkčních zkoušek.

Z uvedeného nástinu již ukončených nebo běžících projektů plyne, že se dané problematice věnuje poměrně značná pozornost. Problém je, že není proveden souhrnný a jasný přehled o již realizovaných projektech daný především roztříštěností jednak realizátorů tak i poskytovatelů.

9.2. Návrhy dalšího postupu.

Navrhnout projet řešící podrobné zmapování všech realizovaných nebo běžících projektů a to i příbuzných umožňující kromě přehledu o stavu navrhnout další směry ve vývoji a tyto rozvinout včetně legislativního rámce.

Navrhnout projekt – studii zabývající se analýzou prostředků UAV/UAS, a možností sledování těchto prostředků dostupnými prostředky včetně částečného ověření zjišťování a sledování.

Literatura:

http://www.isvav.cz/prepareProjectForm.do?projectResearchPlanFormSessionFilter=sessionOrDefault

KYBERNETICKÁ BEZPEČNOST OBECNĚ

1. Úvod

Kapitolou kybernetická bezpečnost zde chceme postihnout širší souvislosti bezpečnosti, související s faktem, že stále více osob, organizací i technologických systémů je připojeno do Internetu a je z této sítě ovlivnitelné jak pozitivně, tak negativně. Jde nám zde sice primárně o technický pohled na bezpečnost, ale do budoucna nelze zanedbat jak systémové (organizační), tak společenské (sociální) aspekty. Pro dlouhodobé řešení této oblasti není možné některou z těchto částí zanedbat.

Kybernetická bezpečnost je součástí širší bezpečnosti. Závislost fungování na počítačích propojených mezi sebou a do internetu, je skutečností prolínající všemi oblastmi. Díky tomu se jednotlivé oblasti bezpečnosti stále více prolínají a vzájemně ovlivňují. Fyzická bezpečnost s bezpečností v kyberprostoru, bezpečnost státu a bezpečí občanů, zabezpečení organizací a soukromí zaměstnanců. Z toho důvodu se v některých částech dotkneme i oblastí na první pohled nesourodých avšak pro hodnotný výsledek důležitých. Je již klasickou pravdou, že reálně je bezpečnost možno zlepšit pouze provázanými opatřeními technickými, organizačními a vzděláváním. Je třeba počítat s tím, že pokud by se incidenty vyskytovaly často, mohou mít citelný dopad nejen na přímo postižené organizace, ale také politický - na spokojenost občanů i ekonomický - národní hospodářství.

Různé oblasti fungování státu tedy musí účinně napomáhat celkové odolnosti společnosti vůči negativním událostem. Negativní událostí rozumíme jak záměrný útok, tak omyl, či chybu nebo technickou poruchu.

2. Kybernetická bezpečnost ve společnosti

2.1. Veřejnost

Osvěta široké veřejnosti je potřebná přinejmenším proto, aby se zvyšovala odolnost vůči poplašným zprávám a panice.

2.2. Školství

Základní vzdělání a orientace v pojmech a principech je třeba dostávat již od základních škol plošně. Bezpečí ve virtuálním světě se týká téměř každého, od dětí po seniory.

2.3. Státní správa a samospráva

Veřejné instituce pracují stále více pomocí informačních systémů a shromažďují stále více osobních, citlivých a jinak důležitých informací. Systémy se postupně propojují, do budoucna i centralizují, proto chyba jednoho úředníka může mít fatální dopady nejen na jednotlivce či firmu, ale také na celé území.

2.4. Průmysl a energetika

Velké i malé podniky jsou důležitým cílem naší práce v oblasti kybernetické bezpečnosti. Jejich ochrana je důležitá nejen z primárního důvodu, že jsou dodavatelem energií, bez kterých by chod státu zkolaboval, ale také proto, že bezpečnostní incidenty jim a potažmo státu mohou napáchat velké ekonomické škody.

2.5. Kritická infrastruktura

KI tematicky spadá do kapitoly Průmysl a energetika, avšak vzhledem k její důležitosti a pravděpodobnému podrobnějšímu rozpracování ji zařazujeme jako zvláštní kapitolu.

2.6. IZS

Je třeba definovat roli složek integrovaného záchranného systému v případech kybernetických útoků a posílit odolnost jich samých (regionální zejména krizové štáby, HZS, zdravotnická zařízení a další. PČR a AČR pravděpodobně řešeno má)

2.7. Legislativa a technická normalizace

Důležitost tématu kybernetické bezpečnosti je zakotvena v zákoně o kybernetické bezpečnosti, avšak je nutné pokračovat v prováděcích legislativních předpisech a participovat na tvorbě technických norem na národní i mezinárodní úrovni.

2.8. Vnější obrana

Není naší ambicí zde zpracovávat obranné strategie, avšak odolnost státu, společnosti, institucí atd vůči kybernetickým útokům a jejich následkům, je třeba řešit ve spolupráci s resortem obrany. V naší oblasti (téměř) neexistuje hraniční perimetr rozdělující vnitřní a vnější bezpečnost.

2.9. Mezinárodní prostředí

Evropská unie, USA a další státy v posledních letech kybernetickou bezpečnost zpracovávají v různých rovinách a intenzitě. Naší ambicí je tento vývoj nejen sledovat, ale také ovlivňovat.

3. Fungování infrastruktury z hlediska kybernetické bezpečnosti

Kybernetickou bezpečnost státu je třeba vnímat a řešit jako celek složený z mnoha vzájemně propojených částí. Každá z nich je důležitá a ohrožení každé z nich je ohrožením celku i v případě, že ostatní ohroženy nejsou. Vzájemná závislost je ale tak velká, že větší kolaps jedné části si nelze představit bez dopadu na části ostatní. Můžeme základně rozdělit do těchto oblastí:

- Kritická infrastruktura
- Média
- Podniky a další organizace
- Domácnosti a osoby

Kybernetická bezpečnost je relevantní téma pro celou kritickou infrastrukturu, jak je definována Ministerstvem vnitra: Kritickou infrastrukturou (KI) se rozumí výrobní a nevýrobní systémy a služby, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

- Výroba a distribuce energií
- Výroba a distribuce pitné vody a potravin
- Zdravotní péče
- Telekomunikace
- Veřejná správa
- Dopravní infrastruktura
- Odpadové hospodářství
- Bankovní a finanční sektor
- HZS, Policie ČR, Armáda ČR musí být do určité míry nezávislé, ale přesto jsou součástí (tzv. nouzové služby)

3.1. Média

Do kritické infrastruktury nejsou zařazena média, avšak dle našeho názoru je třeba věnovat jim také speciální pozornost, alespoň nejdůležitějším celoplošným, protože scénáře kybernetických útoků nemusí probíhat jen po technologické rovině, ale také prostřednictvím dezinformací a manipulace.

3.2. Podniky a další organizace

Pokud by došlo d dlouhodobějšímu výpadku či „jen“ znedůvěryhodnění některého široce využívaného systému či technologie, může to znatelně omezit fungování podniků a tím způsobit dopad do výkonu národního hospodářství.

3.3. Osoby a domácnost

Totéž co podniků, se do určité míry týká osob a domácností, které jsou nejsnáze manipulovatelné či zneužitelné.

Pokud se na kybernetickou bezpečnost podíváme jako na bezpečné fungování informačních systémů a infrastruktury, můžeme ji do určité míry řešit systematicky, dle již zavedených postupů, jako otázku důvěrnosti, dostupnosti a integrity. Tedy že se k systému a datům dostane jen ten, kdo k tomu má oprávnění, vždy když je to třeba a je jisté, že informace nejsou porušeny. Je třeba řešit nejen potenciální útoky, ale také chyby obsluhy a havárie technologií či následky incidentů v jiných oblastech. Další pravdou, která v této oblasti platí, je, že nebezpečím jsou také uživatelé a zařízení uvnitř systému.

Je třeba systematicky zvyšovat celkovou odolnost systémů a celé společnosti proti kybernetickým incidentům počínaje výchovou a vzděláváním, přes technická opatření až po přípravu a nácvik nouzových scénářů.

4. Kybernetické hrozby systémům státní správy a samosprávy

V této kapitole hodláme z hlediska informační / kybernetické bezpečnosti rozebrat stav a rizika informačních systémů využívaných pro veřejnou správu, identifikovat potenciál pro zlepšení a navrhnout konkrétní kroky.

Elektronizace systémů potřebných pro chod státu je již naprostou samozřejmostí. Stejně tak to platí o agendách úřadů jak centrálních, tak i místních. Často se zatím sice jedná o samostatné aplikace nenapojené na další systémy, ale i tak běží v sítích připojených k internetu, musíme je tedy považovat za napadnutelné. Míra jejich zabezpečení je v drtivé většině závislá na poctivosti a odborné znalosti těch, kteří stavěli infrastrukturu a programovali software. Nehovoříme zde samozřejmě o systémech

ministerstva obrany, ani policie a dalších speciálních složek, ale pouze o systémech běžných ministerstev, úřadů a zřizovaných organizací.

4.1. Systémy veřejné správy

V současné době probíhá vytváření centrálních registrů s cílem poskytovat je všem oprávněným organizacím. Toto je správný systémový krok, ale současně zvyšuje atraktivitu takového centrálního místa pro případné útočníky. I technická závada v takovém případě napáchá více škody, než kdyby k výpadku došlo u některého systému jednoho úřadu. Jedná se nejen o samovolný technologický pokrok, ale což je důležité, také jeden ze záměrů strategie Smart Administration - rozvoj a zavádění digitalizace agend veřejné správy (eGovernment, eHealth, eJustice, eCommerce, eBusiness, eSkills, eInclusion, eProcurement, eKultura, eLegislativa, eVzdělání apod.) a podpůrných nástrojů (úložiště, sítě), dále podpora a rozšíření elektronické identifikace – podpisu, plateb, totožnosti; a rozvoj informačních systémů Policie ČR, Integrovaného záchranného systému, bezpečnostních systémů v oblasti justice a vězeňství, dopravních systémů, varovných systémů apod. Mimo to je a zřejmě zůstane v provozu mnoho systémů pro jednotlivé úřady. Ty často běží u externího poskytovatele infrastruktury. Dalším typem jsou drobné aplikace vyvíjené nahodile např. pro potřeby jednoho oddělení určitého úřadu. Z hlediska způsobu provozu, jejich vlastníka a do určité míry i šíře dopadu, můžeme systémy rozčlenit na:

- Centrální sdílené informační systémy
- Systémy pro interní chod úřadů
- Drobné aplikace
- Pronajímané služby

Tyto skupiny obsahují:

4.1.1. Centrální sdílené informační systémy

Tyto systémy jsou provozovány technickým provozovatelem zpravidla jiným, než je jejich vlastník či garant. Jejich uživateli jsou různé subjekty, od úřadů, podniků po občany. Hrozeb vůči těmto systémům je mnoho, avšak díky profesionálnímu přístupu tvůrců a provozovatelů obsahují, doufejme, pouze nepatrné zranitelnosti a rizika napadení jsou tudíž akceptovatelná.

- Státní pokladna - MF
- Jednotné výplatní místo - MPSV

- Jednotné inkasní místo - MF
- ARES (Registr živnostenského podnikání, Obchodní rejstřík,…) - MSp
- Základní registr osob - ČSÚ
- Národní digitální archiv – MV
- Mapové a katastrální podklady – ČÚZK a PÚ
- Evidence obyvatel – MV
- Elektronické identifikační doklady (ePas, eOP, ePKP) – MV
- Evidence majetku státu – ÚZSVM
- ISDS, CzechPoint – MV
- Systémy pro potřeby IZS – MV
- Národní infrastruktura pro elektronické zadávání zakázek – NIPEZ
- Komunikační infrastruktura veřejné správy – MV
- Registr vozidel a související agendy – MD
- a další

4.1.2. Systémy pro interní chod úřadů

Tyto systémy jsou provozovány nejčastěji interně a jsou to buď specializované systémy pro určitý typ úřadů (např. pro radnice), nebo obecné. Díky tomu může být známo větší množství možností napadení, avšak obecně z toho plyne pouze riziko se středním dopadem na kybernetickou bezpečnost.

- Účetnictví
- Mzdy
- Majetek
- GIS
- Spisová služba
- A další

4.1.3. Drobné aplikace

Z různých dobrých i méně dobrých důvodů se můžeme setkat v organizacích veřejné z toho nevyjímaje s množstvím drobných aplikací ať už naprogramovaných

externí firmou, či interním pracovníkem IT, nebo dokonce samotným úředníkem (pro makra v MS Excel, MS Access či seznamy v MS Sharepoint je to velmi časté). Na takových aplikacích často stojí podstatná část určité agendy. Ačkoli se jedná o aplikace vytvářené často bez ohledu na bezpečnost, dostupnost a integritu dat, nelze jednoznačně říct, že je jejich vytváření a používání špatné. Pro analýzu informačních rizik v konkrétní organizaci bývají důležité, avšak z pohledu kybernetické bezpečnosti sledujeme spíše rizika se širším dopadem.

- Evidence čehokoli, kalkulátory atd….

4.1.4. Pronajímané služby

Do této skupiny patří či budou patřit systémy, které si organizace pronajme na určitou dobu od externího poskytovatele. Tento způsob bude pravděpodobně čím dál častější. Důvody jsou jak účetní – jde o provozní nikoli investiční náklady, tak technologické – mohu si vybrat a ihned začít používat optimální službu bez ohledu na mou technologickou vybavenost, tak také organizační – užívám a platím jen potřebný počet licencí, dokud je potřebuji. Takové systémy jsou vytvářeny různými firmami a je třeba předpokládat různou úroveň zabezpečení. Proto by bylo vhodné co nejdříve vytvořit praktickou i metodickou pomůcku, aby kontrola úrovně zabezpečení těchto systémů nebyla vždy jen na místním správci IT v organizaci.

KYBERNETICKÉ HROZBY V ENERGETICE

1. Základní přehled dělení kritické infrastruktury

Následující tabulka je přehledem dělení kritické infrastruktury dle amerického úřadu Department of Homeland Security, tak jak jej používají v řadě jimi vydaných analýz. Pro účely této analýzy je kladen důraz především na sektor energetický a komoditu elektřina.

Sektor	Průmysl
Energetika	Elektřina Plyn Ropa
ICT	Telekomunikace (včetně satelitů) Systémy vysílání radiových vln Softwarové a hardwarové sítě (Internet)
Doprava a transport	Vodní Letecká Železniční Silniční Logistická
Zdravotnictví	Ochrana zdraví Farmacie a očkování Laboratoře
Vodní systémy	Přehrady Zásobníky pitné vody Čistírny a distribuční systémy
Finance a pojišťovnictví	Banky Burzy Pojišťovny Finanční služby
Vláda a státní instituce	Vláda Parlament Justice Pohotovostní služby
Zemědělství a produkce potravin	Zemědělství Distribuční sítě
Média a kultura	Rozhlas Tisk Symbolické budovy

2. Definice kybernetických incidentů

V češtině není pevně zakotvena terminologie oboru kybernetické bezpečnosti, nicméně vzniká jistý úzus, jakým způsobem nahlížet na řadu diskutovaných událostí.

Prvně se události dají dělit na *aktivní,* tedy takové, které v danou dobu právě probíhají a mají konkrétní efekt na informační systémy. Mezi takové události se řadí: *incidenty* a *útoky*. Jedná se o konkrétní aktivity s tím rozdílem, že incidenty mohou být nezamýšleného charaktery, kdežto za útoky se považují takové incidenty, u nichž je

prokazatelný lidský úmysl. Řada odborníků se snaží vyhnout terminologii, která by byla přímo převzata z prostředí vojenské bezpečnostní agendy, nicméně právě fakt, že je možné útok militarizovat dává prostor tuto terminologii přebírat. Ve výsledku je možné používat méně konkrétní terminologii, která není tolik zavazující. Je vhodné na tento rozdíl poukázat, neboť v literatuře se zmíněné termíny užívají často velmi volně.

Druhou kategorií kybernetických událostí jsou tzv. *pasivní* události, do kterých lze zařadit např. *zranitelnost* nebo *hrozbu*. Zranitelnosti jsou vady na softwarovém nebo hardwarovém vybavení, které jsou známé nebo neznámé. Zranitelnosti nulového dne (0-day vulnerability) jsou pak zranitelnosti, o jejichž existenci nikdo doposud nevěděl. Jejich účelnost spočívá právě v možnosti útočníka zneužít takový nedostatek v návrhu kódu nebo tištěného spoje k provedení útoku. Zranitelnosti nulového dne by de facto neměly vykazovat kybernetické incidenty, budeme-li se u incidentu držet předpokladu jeho vzniku bez lidského úmyslu. Hrozbou jsou zranitelnosti známé, díky čemu je možné odhadnou míru rizika po dobu jejich odstraňování.

Dělení kybernetických událostí

Pasivní	Aktivní
Zranitelnost	Incident
Hrozba	Útok

3. Vyhodnocování rizika hrozby

Existuje celá řada metodik vyhodnocování rizik vhodná k aplikaci na kybernetické hrozby. Za nejvhodnější a nejjednodušší lze považovat formuli:

Hrozba = schopnost + úmysl + příležitost

Jak bylo zmíněno výše, hrozba ke svému naplnění vyžaduje aktéra. Míra rizika jejího naplnění vyplývá ze schopnosti aktéra zneužít zranitelnosti softwarové nebo hardwarové vrstvy, míry vážnosti úmyslu a uplatnění příležitosti v kontextu se zisky, vyplývající z daného útoku.

Hrozby lze vyhodnocovat v následující univerzální matici:[20]

Úroveň	**PROFIL HROZBY**

[20] Duggan, D. P., S. R. Thomas, C. K. K. Veitch, and L. Woodard. *Categorizing Threat: Building and Using a Generic Threat Matrix.* Albuquerque, NM: Sandia National Laboratories, 2007.

hrozby	Vazba k cíli			Zdroje			
	Intenzita	Tajnost	Čas	Technický personál	Znalost		
					Kyber	Kinetická	Přístup
1	Vysoká	Vysoká	Roky až dekády	Stovky	Vysoká	Vysoká	Vysoká
2	Vysoká	Vysoká	Roky až dekády	Desítky až stovky	Střední	Vysoká	Střední
3	Vysoká	Vysoká	Měsíce až roky	Desítky až stovky	Vysoká	Střední	Střední
4	Střední	Vysoká	Týdny až měsíce	Desítky	Vysoká	Střední	Střední
5	Vysoká	Střední	Týdny až měsíce	Desítky	Střední	Střední	Střední
6	Střední	Střední	Týdny až měsíce	Jednotky	Střední	Střední	Nízká
7	Střední	Střední	Měsíce až roky	Desítky	Nízká	Nízká	Nízká
8	Nízká	Nízká	Dny až týdny	Jednotky	Nízká	Nízká	Nízká

Existuje celá řada hrozeb, které jsou zneužitelné jednotlivci. Mezi takové hrozby tradičně patří DDoS útoky (Distributed Denial of Service), neboť botnet až o stovkách tisích zkompromitovaných počítačů nebo mobilních telefonů je možné zakoupit řádově za desítky až stovky amerických dolarů. V kontextu takového prostředí lze předpokládat, že útoky úrovně 8 mohou nastat i denně. Důkazem tomu je současná situace v USA, kde velké bankovní domy čelí denním útokům zcela záměrně po pracovní dobu. S obdobným rozsahem útoků jsme se v ČR zatím nesetkali, ale je zřejmé, že za obdobné situace není možné každý jednotlivý útok řešit individuálně, ale technologickou převahou nad útočníky – schopností ustát situaci vysokou *odolností* informačních systémů.

Analýza konkrétní hrozby by měla obsahovat takové indikátory, které by byly schopny popsat dostatečně objektivně každou jednotlivou hrozbu natolik přesně, aby ji bylo možno zařadit do vybrané úrovně obdobné matice. Každá úroveň hrozby by měla předpokládat určitou míru zásahu proti hrozbě, aby byly kapacity obranného týmu CERT (Computer Emergency Response Team) připraveny reagovat odpovídajícím způsobem. Je nutné vzít v potaz, že kybernetické útoky mohou mít charakter až miliónů incidentů za měsíc.

4. Zdroje hrozeb

Za zdroje hrozeb lze považovat především: vlády jiných států (1.-5. úroveň), teroristi (3.-8. úroveň), průmysloví špioni (1.-8. úroveň), skupiny organizovaného zločinu (3.-8. úroveň), hacktivisti (4.-8. úroveň) a hackeři (5.-8. úroveň).

5. Variace kybernetických útoků

Následující rozdělení útoků na čtyři oblasti je pouze jedním z mnoha možných způsobů, jak kybernetické útoky dělit. Každý z uvedených útoků využívá existující hrozby, resp. zranitelnosti cílených informačních systémů:

5.1. Čistě kybernetický útok

Útok, jehož původ i cíl se vyskytuje přímo v kyberprostoru. Jedná se např. o útok virem na data a jejich smazání, zpronevěření nebo modifikace. Tento typ útoku nemá žádné další (přímé a jednoznačné) důsledky na fyzický prostor. Typický příklad Saudi Aramco 2012.

5.2. Kybernetizovaný útok

Útok, jehož původ je v kybernetickém prostoru, např. virus, a důsledek jeho činnosti je zřetelný ve fyzickém světě. Takový typ útoku se většinou označuje za kybernetický, ale takové označení je svým způsobem zavádějící. Pokud lze otočit uzávěrem manuálně a důsledkem je např. exploze nahromaděného plynu, jedná se o čistou sabotáž. Pokud by takový útok byl veden z kybernetického prostoru, neboť uzávěry již nelze uzavírat jen ručně, jedná se jednoznačně pouze o vylepšení stejného typu sabotáže. Typický příklad Stuxnet 2010.

5.3. Kybernetický útok jako podpora konvenčnímu útoku

Jedná se o útok, jehož osamocené vedení by nemělo de facto žádné poškozující účinky. Za předpokladu, že taková činnost je podporou konvenčnímu kinetickému útoku, jedná se o součást takového útoku. Kompromitace protiletadlového systému a zajištění, že takový systém nezobrazí nálet stíhací letky, která následně vybombarduje tížený cíl, perfektně vystihuje tento typ útoku. Typický příklad Operace Orchard, Sýrie 2007.

5.4. Skrytá hardwarová hrozba

Je diskusí zda nezdokumentované instrukce plošného spoje (procesoru) v návrhu celého zařízení lze zařadit mezi kybernetické hrozby. Obecně se předpokládá, že ano, nicméně už samotný charakter této hrozby působí, že jej je možné srovnat s jakýmkoliv mechanickým poškozením. V takovém případě by se jednalo opět o sabotáž, jejíž

charakter nemusí mít vůbec kybernetický charakter, např. zařízení shoří a přestane fungovat. V jiném případě však mohou takové instrukce být prostředkem pro zneužití implementace malwaru přímo do takového zařízení a mít důsledek v kyberprostoru. V takovém případě by se o kybernetickou hrozbu jednat mělo. Typickým příkladem je rozšíření výrobku firmy Huawei a s ní spojené podezření, že se jedná o čínským státem kontrolovanou společnost, jenž může zásadně ovlivnit chod nespecifikovatelného rozsahu informačních technologií. Huawei je nyní jednou z nejrozšířeních síťových technologií především díky své velmi nízké ceně.

6. Historické momenty důležitých kybernetických útoků na energetickou infrastrukturu

6.1. Exploze plonovodu Urengoy–Surgut–Chelyabinsk

Nejspíše nejznámějším útokem na energetickou infrastrukturu je i přes řadu výhrad o kybernetickém původu útok na plynovod v Sovětském svazu v roce 1982. Spekulace jsou dodnes nevyjasněné, nicméně hlavním předpokládaným důvodem exploze, která byla ve své době považována za jednou z největších nenukleárních explozí, byla záměrná modifikace řídících systémů SCADA americkou tajnou službou CIA. Sovětský svaz tehdy nedisponoval vlastními technologiemi a proto nakoupil technologie od kanadské firmy, která spolupracovala se CIA. Řídící systémy záměrně přetlakovaly plynovod až po zprovoznění, což způsobilo na Sibiři ohromnou explozi. Tento útok lze považovat za kybernetizovaný útok, neboť jeho původ je čistě kybernetického charakteru a dopady byly zřetelné ve fyzickém světě.

6.2. Období klidu a blackout 2003

Dalších třicet let lze považovat z hlediska kybernetických hrozeb a útoků v energetickém sektoru za naprosto klidných. Probíhaly spekulace o kybernetickém původu blackoutu na východním pobřeží USA v roce 2003. Různé zdroje citovaly agenta Toma Donahue ze CIA, který měl doložit médiím v roce 2007 doklady o kybernetickém útoku. Realita je s velkou pravděpodobností taková, že bylo možné zpětně dohledat nestandardní zásahy do řídících systémů v průběhu blackoutu. Ty jsou ale připisovány pracovníkům snažících se zachránit situaci během již probíhajícího kaskádového efektu vypínání přetížených elektráren. Zdroje o Tomu Donahue jsou neověřitelné.

6.3. Moment probuzení – Saudi Aramco 2012

V roce 2012 došlo k objevení viru na pracovních stanicích zaměstnanců společnosti Saudi Aramco, která zajišťuje zásadní podíl světové dodávky ropy. Saudi

Aramco je často na prvním místě světového žebříčku hodnoty firem. Samotný útok byl proveden v den islámského svátku Lailat al Qadr, kdy 55 tis. zaměstnanců zůstalo doma, ale jeden vnitřní narušitel rozšířil ve vnitřní síti na míru připravený vir Shamoon. Jedná se doposud v dějinách o největší kybernetický útok, neboť smyslem viru nebylo jakkoliv zasahovat do řídících systémů, ale smazat veškerá data na harddiscích bez možnosti jejich obnovy. Vir tedy kromě mazání dokázal velmi sofistikovaně modifikovat kompletní magnetický povrch disku, výsledkem byl pouze mnohokrát uložený obrázek hořící americké vlajky, tím zajistili nemožnost obnovy dat jejich přepsáním. Reakcí vnitřních bezpečnostních pracovníků IT bylo odříznutí všech zaměstnanců od emailů a internetu, čímž se chod společnosti zastavil. Zpětně nebyly obnoveny ani tak zásadní data, jako objem již provedených dodávek a s nimi spárovaných plateb. Obnova, resp. výměna desítek tisích harddisků a instalace čistého operačního systému, trvala více jak týden. Výše z toho vyplývajících škod nebyla nikdy přesně vyčíslena. Útok je připisován Íránu, neboť obsahoval sebedesktrukční kód Wiper, který použily USA ve viru Flame, kterým stahovaly data z Iránu po několik let.

Tento útok prokázal, že není nutné manipulovat s řídícími systémy, aby se dosáhlo velmi vysokých finančních škod.

7. Zdroje hrozeb a útoků v energetickém sektoru

V roce 2011 americký DHS reportoval 198 útoků na energetický sektor, což je 10x více než rok předtím. V roce 2013 společnost PwC reportuje 10-49 útoků v posledním roce u 17% dotazovaných energetických společností, což je ve srovnání s rokem 2011 47% nárůst.[21]

Společnost Mandiant ve svém reportu APT1 o čínské špionážní jednotce „PLA unit 61398“ zmiňuje navýšení jejich aktivit každým rokem v násobcích (2006 jeden, 2007 čtyři, v roce 2012 již přes tisíc úspěšně napadených serverů). Mandiant to připisuje nejen zvýšené aktivitě této jednotky, ale i jejich zvyšující se schopností aktivity odhalovat. Samotná aktivita může jít do stovek. Odborníků má tato jednotka určitě stovky až tisíce s ohledem na velikost budovy, ve které s největší pravděpodobností sídlí.[22]

[21] www.pwc.com/en_GX/gx/oil-gas-energy/publications/assets/pwc-embedding-cyber-security-into-the-energy-ecosystem-pdf.pdf

[22] Manidant, *APT 1 Report.* Washington DC, 2013.

Nárůst rizik na energetický sektor roste každým rokem a je nutné je nehledat pouze v rizicích spojených s fyzickou destrukcí, tyto případy se řadí mezi ty výrazně sofistikovanější a s velkou pravděpodobností nebudou stát v popředí vysokých finančních ztrát, přestože budou jistě mediálně velmi exponované.

8. Největší hrozba – člověk (insider)

8.1. Zlomyslný vnitřní narušitel (Malicious insider)

Viry Shamoon (Saudi Aramco 2012) nebo Stuxnet (útok na íránské centrifugy v roce 2010) jsou odlišné typy útoků. První zmiňovaný je čistě kybernetický, druhý je typicky kybernetizovaný s dopady na fyzický svět. Oba viry však spojuje jeden společný jmenovatel, který nelze odstranit sebelepším firewall nebo antivirem – vnitřní narušitel se specifickými právy přístupu, které zneužije. Zpravidla se jedná o lidi s dvojím možným záměrem: finanční zisk za provedenou sabotáž nebo zcizení citlivých informací – průmyslová špionáž, druhým motivem může být msta z neuspokojivé kariéry, o tomto problému se hovoří čím dál častěji. Tito lidé mohou být sólisté, což bude spíše druhý případ nebo jednat na objednávku třetí osoby, což bude zpravidla první případ.

Ve výzkumu PwC je zmiňuje jako riziko 40% dotázaných firem, tedy první nejvyšší.

8.2. Hacktivisti

Mezi velmi závažně narůstající problém se řadí organizované skupiny motivované vlastními hodnotami nebo protestním přístupem. Tito lidé bývají zpravidla velmi mladí. Zatčení skupiny Lulzsec americkou FBI odhalilo, že nejschopnější hackeři byli ve věku kolem 15 let a přesto velmi dobře zorganizovaní. Doba náhodných náctiletých géniů ustává a stále více se svět potýká se de facto organizovaným zločinem, ačkoli motivovaným společenskými hodnotami – ochránci životní prostředí převládají. Lulzsec dostali za svou činnost trest v jednotkách let odnětí svobody, nicméně je zřejmé, že podobně schopní hackeři budou v budoucnu moci i díky medializaci býti najatí státem za účelem provedení státem sponzorovaného útoku. V létě roku 2012 skupina Anonymous zveřejnila přes tisíc emailových adres pracovníků ropných společností na protest s plány těžit v arktickém prostředí, především v severním ledovém oceánu.

Ve výzkumu PwC je zmiňuje jako riziko 32% dotázaných firem, tedy druhý nejvyšší.

8.3. Oportunističtí kriminálníci nebo organizované skupiny

Malware Gozi do doby rozprášení americkou FBI prokázal extrémně sofistikovanou schopnost neútočit na servery, ale přímo na počítače uživatelů, tedy bez vědomí banky. Gozi do přihlašovací stránky vložil několik dalších polí přímo v prohlížeči na uživatelské stanici, které banka nepožadovala. Stránka si přesto vyžádala kód přes mobilní telefon, byla připojená přes https a stejně graficky zobrazená, čímž uživatel neměl sebemenší tušení, že by se mohlo jednat o zkompromitovanou stránku. Následně se do banky normálně přihlásil, část dat šla během přihlášení ale do databáze hackerů aniž by to banka nebo uživatel dokázali rozpoznat. Podobným způsobem je možné zkompromitovat platební účty průmyslových firem, což by mohlo mít ohromné důsledky. Jedná se ale o velmi sofistikovaný typ útoku. Společnosti jej ve výše citovaném výzkumu nehodnotili, nicméně lze předpokládat, že právě ona sofistikovanost jej řadí na nižší příčky rizika.

8.4. Jeden průnik, více aktérů

Doba odhalení nového malwaru je někdy i rok a půl a více, přesto je škodlivého kódu zdokumentováno na 200 tis. druhů denně (Kaspersky Lab). Pokud se některým hackerům podaří napsat výrazně zajímavý a efektivní kód nebo objevit zranitelnost, která má vysokou pravděpodobnost nebýt odhalena, či se jedná o celý komplex obdobných zranitelností, pak je hackeři nemají problém sdílet. Kód Gozi je toho dokladem. Logika a algoritmy kódu byly nalezeny minimálně ve dvou programovacích jazycích různých autorů, sdílena byla pouze logika a je prokázáno, že za něj původnímu autorovi bylo zaplaceno.

9. Státem sponzorované útoky

V takových případech jsou útoky již posuzovány z hlediska mezinárodního práva a to zda byl nebo nebyl porušen článek 2(4) Charty OSN o zákazu použití nebo hrozby silou. To, zda došlo k naplnění jeho podstaty zpravidla rozhoduje stát samotný a v historii se tak ještě ani jednou nestalo, přestože řada útoků je přisouditelná konkrétním státním aktérům. Zařazení tohoto typu narušitele zde má svůj smysl, protože státem motivované útoky jsou a i nadále budou ty nejsofistikovanější, nejdéle trvající bez odhalení a připravovány stovkami až tisícovkami odborníků.

10. Technický charakter hrozeb a útoků

10.1. Architektura průmyslového ICT

Problém často nespočívá pouze v tom, že někdo má úmysl či motiv, nýbrž i v tom, že ten motiv lze snadno naplnit nabízenou příležitostí, jak bylo uvedeno v základní rovnici hrozby.

10.2. Napojení SCADA systémů na sítě TCP/IP

Překvapivě je celá řada SCADA systémů napojena a řízena přes sítě TCP/IP používající internetový protokol IPv4. V USA proběhla studie, která (i přes svou výraznou diskutovatelnost) došla k závěru, že kolem 7000 řídících jednotek (PLC – programmable logic controler) přímo zodpovědných např. za tlak v potrubí je dostupných volně přes internet. Diskutovatelná je především metoda výzkumu, která nebyla zveřejněna. Nicméně, že toho hackeři jsou schopni je obecně známo.

10.3. Centralizace architektury

Schopnost viru rozšířit se během jediného dne do celé sítě Saudi Aramco svědčí o její naprosté centralizaci. Společnost AKAMAI v USA např. při řešení DDoS útoků primárně sítě jejich klientů (bank) maximálně decentralizuje, rozděluje na sektory, vrstvy, výkonnější servery, honeypoty apod. Čelí DDoS útokům jako dennímu problému, nikoli jako překvapivému nárazovému útoku. Ten by ale maximální důraz na centralizaci jistě odrazil. Decentralizace je součást strategie odolnosti, na kterou je poukazováno s důrazem i v EU strategii kybernetické bezpečnosti.

10.4. Spear-phishing

Typickým protagonistou je již zmiňovaný kód Gozi. Jedná se o činnost, která dokonale skryje své nežádoucí cíle a zmate uživatele, který poskytne osobní informace nebo klikne na nežádoucí link, jenž po spuštění spustí v prohlížeči aktivní prvky. V energetickém sektoru se jedná např. o vir Night Dragon, který díky této technice získal osobní emaily a citlivé dokumenty vedoucích pracovníků energetických společností. Obdobným způsobem se lze dostat k přístupovým kódům nebo si otevřít zadní vrátka pro sofistikovanější práci v napadené síti, např. následně ovládat přímo řídící systémy. V takovém případě není nutné, aby tyto systémy byly postavené na TCP/IP architektuře.

10.5. Cloud-computing

Čím dál více společností začíná používat různé metody cloudového ukládání dat. Není nutné, aby používaly rozšířené populární nástroje, se kterými se již nese delší dobu

špatná pověst z hlediska jejich bezpečnosti. Typickým příkladem je Dropbox. Cloudové řešení má i své B2B dodavatele, nicméně ve většině případů funkčnost překrývá bezpečnost. Bezpečnostní požadavky průmyslového podniku zpravidla tyto společnosti z principu věci nejsou schopny dodat. Cloud je ale opět další metoda centralizace, ovšem této se do budoucna svět s velkou pravděpodobností nevyhne.

10.6. DDoS

DDoS útok se většinou používá pro vyřazení webového serveru z provozu, může ale sloužit k zaměstnání pracovníků, kteří se nebudou mít prostor zabývat jiným útokem, popř. si ho nevšimnou. Jsou ale zdokumentované útoky, např. v listopadu 2012 na 50Hz distribuční soustavu, která byla přímo řízená napadeným serverem. V praxi se nic nestalo, ale jedná se o příklad, že i servery řídící elektrickou distribuci již byly napadeny a to prostým DDoS útokem, který lze zakoupit za desítky dolarů na internetu.

10.7. Virus, worm, trojan

Jedná se o tradiční dělení škodlivého kódu. Vir se od wormu (červa) liší tím, že jeho kód se lepí na jiné spustitelné nebo jakkoliv v paměti operabilní soubory.

Worm je zpravidla výrazně větší a má podobu konkrétního souboru, lze fyzicky dohledat i když často velmi komplikovaně. Worm je naproti viru schopen vlastní operace, popř. replikace bez zásahu člověka. Např. se zreplikovat na všechny adresy v emailovém klientu. Wrom může zajistit zadní vrátka pro hackera, který následně získa kontrolu nad zkompromitovaným počítačem.

Trojan je zřetelný software, který ale dělá jiné věci, než které uživateli tvrdí. Typicky MacKeeper, který se pro uživatele tváří jako nástroj na odstranění malware, přičemž sám malware je a otevírá zadní vrátka pro připojení na C&C server (command & control), který ze zkompromitovaných počítačů vytváří botnet. Botnet následně může nasměrovat datový tok na jeden cíl – DdoS útok.

11. Trendy

Sledování celosvětových trendů nám může pomoci v identifikaci budoucích hrozeb. Zde nám jde o seznam těch v současnosti nejdůležitějších, nikoli o jejich hodnocení a řazení dle důležitosti.

- Zvyšující se dopad virtuálního světa do fyzického, jak pro organizace, tak pro jednotlivce > co se objeví na internetu, mívá závažný dopad do skutečného světa

ať je to pravda či není. Mnozí mohou podlehnout iluzi, že iluze je důležitější než skutečnost.

- Zvyšuje se četnost kybernetických útoků a jejich důvody jsou různé, nemusí jít „jen“ o explicitní nepřátelství, ale také o hru, souhru okolností, formu vlastní propagace atd. > následky pro organizace mohou být závažné až fatální, i v případech, že to původce útoku nezamýšlel.
- Roste výpočetní výkon, počet počítačů i jejich mobilita. To je velmi relevantní pro distribuované útoky či lámání kryptografické ochrany > miliardy čipů po celém světě mohou paralelně provádět určitou úlohu. Výpočetní výkon tak vlastně vzrostl o několik řádů nejen „obvyklým“ technologickým pokrokem, ale také způsobem použití
- Roste vliv médií a sociálních sítí > je naprosto reálné změnit názor veřejnosti, zmanipulovat určitou sociální skupinu a to velmi rychle a v podstatě levně. I toto zařazujeme mezi trendy relevantní pro identifikaci kybernetických hrozeb, protože tento trend je umožněn moderními informačními technologiemi a patří do „Cyber“ světa
- Rychle přicházejí (i odcházejí) nové technologie, aplikace, systémy. Je třeba umět rychle reagovat > dříve nepředstavitelná rychlost inovací jak pozitivních, tak negativních nástrojů sebou nese nutnost správného rozlišování a umění rychlé reakce. Nestačí se něco jednou naučit.
- Virtualizace infrastruktur (cloud atd…). Vaše data a systémy už spravuje někdo jiný. > Ono už to tak je od začátku, ale vlastní správce IT, „člověk, kterého jsem někdy viděl“, se přeci jen zdál být lépe na dosah. Vždy je třeba zabezpečit data a systémy systémově (=prokazatelně se nic nemůže stát), nikoli na základě důvěry „že se nic nestane“
- Zvyšuje se síla rozvojových zemí (BRICS) > ekonomickou expanzi bude doprovázet technologická a naše citlivá data možná brzy potečou například skrz ruský hardware do indického informačního systému placeného čínskými penězi.
- Přibývají různé místně i jinak blíže neohraničené ad hoc vzniklé zájmové skupiny s nezanedbatelnou silou a úsilím > již nemůžeme počítat s tradičním rozvržením a stabilitou „vlivu“. Nyní je možné se zanedbatelnými náklady působit obrovským vlivem. Jeden blog může být více než vlastnictví několika celostátních novin.

Téměř platí, že díky Internetu jen stačí chtít, proto momentální hnutí budou vznikat na cokoli a proti čemukoli, tedy i proti pořádku a bezpečnosti.

- Státy a firmy mají díky horší hospodářské situaci méně zdrojů na pokrytí případných následků > velký výpadek infrastruktury, blackoutem počínaje, přes problémy telefonní sítě, po kolaps administrativy by měl následky nejen z hlediska výpadku výkonu podniků, ale také zhoršením ratingu ČR jako země spolehlivé a bezpečné pro investory. Stát v současné době nemá finančně ani organizačně na to, aby tomuto zabránil, případně alespoň sanoval následky.
- Zvyšuje se mezera mezi potřebnými a reálnými znalostmi a schopnostmi vedoucích pracovníků i všech občanů > tak jak dříve bylo nutností umět se zbraní v ruce ochránit svoji rodinu a vlast, nyní to tak pár let nevypadalo, tak v kybersvětě je nutné umět sebe, rodinu, organizaci ochránit před tím, aby s námi, našimi daty někdo zacházel tak, jak sami nechceme. To vyžaduje nové znalosti na úrovní základního vzdělání, které se zatím nikde neučí.

12. Identifikace potenciálu pro normotvorbu

- Vytvoření praktického standardu například ve formě checklistu pro uživatele, vlastníky a provozovatele systémů ve veřejném sektoru.

13. Závěry a doporučení

Kybernetická bezpečnost je pro fungování veřejné správy důležitým tématem stejně jako pro systémy v energetice. Fakt, že se závažnější incidenty objevují jen zřídka, nás nesmí ukolébat. Za vhodné považujeme začít ve veřejném sektoru co nejdříve s těmito tyto kroky:

- Testování aplikací, systémů a prvků ICT infrastruktury z hlediska požadavků na bezpečnost, případně vytvoření standardu a metodického pokynu závazného pro veřejný sektor
- Určení meziresortní koordinační rady pro zajištění jak vzájemné kompatibility, tak umožnění distribuovaných nouzových a obranných scénářů
- Sestavení katalogu typických informačních aktiv, hrozeb, zranitelností, rizik a opatření, aby se generická rizika řešila plošně a efektivněji.

- Dlouhodobě se snažit eliminovat informační systémy a aplikace, které neprošly bezpečnostním auditem
- Vytvoření specifických vzdělávacích programů
  - pro zaměstnance organizací zahrnutých do KI
  - pro zaměstnance ve veřejném sektoru
  - pro veřejnost
- Sledovat a navazovat na činnost CERT, CSIRT a dalších iniciativ zabývajících se KB.

SHRNUTÍ I. ETAPY

V rámci první etapy došlo k aktualizaci SVA ve všech plánovaných technologických oblastech. Tato aktualizace vyšla z kontextu zmapovaných iniciativ a dokumentů na národní i nadnárodní úrovni, které signalizují rostoucí význam tématu ochrany kritické infrastruktury a společenské odolnosti (resilience) a na ně navazující přísun investic. Podobně byl rozpoznán trend narůstající potřeby efektivních procesů standardizace a certifikace.

Jednotlivé studie pokrývající technologické oblasti zmapovaly stav v daných segmentech a v rámci aktualizace SVA spočívající v jejím zúžení a její specifikaci identifikovaly konkrétní priority, jež budou v dalších fázích rozpracovány. Tyto priority vycházejí z identifikace nových hrozeb a požadavků na nové bezpečnostní a technologické systémy.

13.1. Komunikační technologie

V oblasti komunikačních technologií se v dalších fázích SVA zaměří na komunikační technologii jako kritickou infrastrukturu. Klíčové priority dalšího výzkumu budou představovat:

- Výzkum optimálního zálohování a zabezpečení činnosti komunikačních systémů;
- Výzkum optimálního autonomního napájení komunikačních systémů;

13.2. Kybernetická bezpčnost

Široká technologická oblast kybernetické bezpečnosti je v aktualizované SVA zúžena na kybernetické hrozby pro systémy ve státní správě a samosprávě a v oblasti energetiky. Jako klíčové priority lze označit:

- Metodiku analýzy a analýzu kybernetických rizik a hrozeb:
  - v energetickém sektoru
  - v oblasti smart gridů
  - v oblasti cloudových úložišť
- Vytvoření praktického standardu pro uživatele, vlastníky a provozovatele systémů ve veřejném sektoru;

- Sestavení katalogu typických informačních aktiv, hrozeb, zranitelností, rizik a opatření s cílem řešit generická rizika plošně a efektivněji;
- Možnosti aktivní kybernetické obrany jako strategického přístupu v rámci veřejného i soukromého sektoru;
- Analýza vývoje a možné budoucí podoby APT - Advanced Persistent Threat;
- Procesy stávající evropské normotvorby a metodiky

13.3. Fyzická bezpečnost

Oblast fyzické bezpečnosti se v návaznosti na analýzu stávajících systémů integračních platforem bezpečnostních systémů bude nadále zaměřovat na řešení hrozeb plynoucích z diverzity využívaných integračních platforem. Klíčovu prioritou pro další rozpracování bude:

- Analýza možností vytvoření jednotné platformy, případně komunikačního protokolu, pro monitoring a případně částečné ovládání bezpečnostních systémů objektů kritické infrastruktury nad jednotlivými integracemi (integračními platformami);
- Identifikace legislativních potřeb spojených s implementací nadřízených platforem;

13.4. Sledování prvků kritické infrastruktury

V rámci první etapy došlo k ukončení spolupráce s Univerzitou obrany. Gesci za tuto sekci včetně aktualizace SVA převezme Řízení letového provozu ČR.

PŘÍLOHA 1 – ZÁKLADNÍ PARAMETRY EVROPSKÉHO PŘÍSTUPU K OCHRANĚ KRITICKÉ INFRASTRUKTURY V NOVÉM ROZPOČTOVÉM OBDOBÍ 2014-2020

V návaznosti na strategické dokumenty věnuje EU stále větší pozornost oblasti vnitřní bezpečnosti. Vzhledem ke své povaze popsané v úvodní studii představuje problematika ochrany kritické (informační) infrastruktury zásadní téma vnitřní bezpečnosti a společenské odolnosti (resilienci). Politické proklamace a jejich zformulování do podoby strategických dokumentů z posledních let nadále stvrzují prioritizaci ochrany kritické (informační) infrastruktury. Logickou návazností na tento politicko-strategický posun je i úprava rozpočtových nástrojů a především navýšení finančních prostředků, které do této sféry budou směřovat. Následující řádky se budou věnovat novému přístupu ke klíčovému nástroji, který představuje European Programme for Critical Infrastructure Protection (EPCIP) a ve druhé části základním parametrům rozpočtového rámce, které se budou týkat ochrany kritické (informační) infrastruktury.

Základní parametry EPCIPu byly nadefinovány v roce 2006 v rámci comprehensive review zaměřeného na EPCIP a následně Směrnicí 2008/114/ES. Již v době schvalování směrnice bylo patrné, že její dopad bude spíše malý a nedojde tak k naplnění představ Evropské komise. Tuto skutečnost poté potvrdilo vyhodnocení implementace v jednotlivých členských zemích. Konkrétně hlavním cílem směrnice bylo přinutit členské státy EU, aby identifikovaly a designovaly tzv. Evropské kritické infrastruktury, jejichž ochrana měla být následně vylepšena. Tento proces se měl týkat především sektoru dopravy a energetiky. Výsledkem však bylo určení pouze 20 evropských kritických infrastruktur, což objektivně představuje pouhý zlomek reálných struktur s přeshraničním či dokonce celoevropským rozsahem. Například mezi těmito infrastrukturami nenajdeme žádné energetické přenosové sítě. K ještě menšímu počtu infrastruktur vznikly tzv. Operační bezpečnostní plány, které měly být nástrojem posilování ochrany těchto infrastruktur.

K zásadním přínosům směrnice tak patří především zvýšení obecného povědomí o hrozbách a rizicích spojených s kritickou infrastrukturou na úrovni stakeholderů a částečně i celé evropské společnosti. Podobně je také možné ocenit rozšíření debaty o kritické infrastruktuře do dalších sektorů jako je například zdravotní péče či finanční služby.

Konkrétní legislativní kroky, které by měly následovat v dalším období, nejsou prozatím zřejmé. V procesu hodnocení EPCIPu a výše zmíněné směrnice se však ukázalo, že doposud nebyla věnována dostatečná pozornost problematice vzájemné závislosti mezi kritickou infrastrukturou, průmyslem a státními aktéry. Podobně není nijak koncepčně promyšlena vzájemná závislost mezi jednotlivými sektory, které EPCIP rozeznává.

Další prioritu EPCIPu představovalo vytvoření internetové informační a komunikační platformy s názvem Critical Infrastructure Warning Information Network (CIWIN). Tento systém byl finálně spuštěn počátkem roku 2013, přičemž komise předpokládá, že jeho využití především ze strany členských stát postupně poroste. Prostřednictvím CIWINu by měly být sdíleny a vyhodnocovány informace týkající se panevropských kritických infrastruktur, CIWIN by se dále měl stát nástrojem analýzy rizik, na jeho platformu by se postupně mohly napojit národní systémy ochrany kritické infrastruktury a v neposlední řadě by měl sloužit jako zdroj informací o spolupráci s třetími zeměmi v této oblasti. Právě aktivnější externí spolupráce by se také měla stát náplní dalšího období, přičemž by mělo jít především o dva typy aktivit. V návaznosti na nařízení komise zřizující tzv. Instrument for Stability bude možné podporovat ochranu kritických infrastruktur ve třetích zemích v oblastech mezinárodní letecké a námořní dopravy, energetických distribučních sítí a elektronických a komunikačních sítí. V druhém sledu půjde u uzavření strategických partnerství s vyspělými zeměmi, především s Kanadou a USA.

V právě končícím rozpočtovém rámci byl hlavním nástrojem v oblasti ochrany kritické infrastruktury na úrovni EU Program prevence, připravenosti a zvládání následků teroristických útoků, v rámci kterého bylo podpořeno celkem 111 projektů, jejichž hodnota dosáhla 45 milionů eur. Z těchto 111 projektů se ochranou kritické infrastruktury zabývalo 70, krizovým managementem 32 a společnou agendou 9 projektů.

Mezi hlavní priority a následně náplň projektů patřilo prohloubení znalostí v oblasti ochrany kritické infrastruktury a definování politických priorit vycházejících z vědecké analýzy. Mnoho projektů se tak věnovalo metodologickým otázkám týkajícím se mechanismů včasného varování, analýzy hrozeb a rizik či modelování vzájemných závislostí, na něž by měly navazovat priority následujícího období, které se v současnosti formují. Zásadní vlajkový projekt pak představoval projekt zaměřený na identifikace a rozvoj evropských experimentálních kapacit s důrazem na jejich vzájemné propojování. Mezi takové kapacity patří například oblasti CBRN, zjišťování výbušnin, ochrany proti zemětřesením, kybernetické bezpečnosti a v neposlední řadě také oblast standardizačních opatření.

Dalších 40 projektů dotýkajících se ochrany kritické infrastruktury bylo financováno z kapitoly Bezpečnost v rámci 7. rámcového programu (FP7). Celkové prostředky investované v rámci nástupce FP 7 budou oproti minulému rozpočtovému období navýšeny o cca 40 %. Zatímco prostřednictvím FP 7 bylo v letech 2007-2013 proinvestováno 53,3 miliard eur, v rámci dalšího pokračování Horizontu 2020 překročí investice do výzkumu a inovací v letech 2014-2020 70 miliard eur. Lze tedy důvodně předpokládat, že i podpora výzkumu a inovací v obecně prioritizovaných tématech z oblasti vnitřní bezpečnosti zásadně vzroste.

Zásadní proměnou by měl projít i samotný základní přístup k rozvoji EPCIPu. Novou výchozí myšlenku představuje skutečnost, že by význam evropské dimenze měl být ukázán v rámci pilotních projektů zaměřených na čtyři evropské infrastruktury, které jsou z podstaty přeshraniční, pokrývají klíčové sektory dopravu, energetiku a vesmír a pilotní projekt podporují jejich vlastníci/operátoři.

První z navrhovaných infrastruktur představuje systém na řízení letového provozu Eurocontrol, který pomáhá řídit velmi hustou leteckou dopravu zejména nad západní a střední Evropou. Druhým pilotním projektem by se měl stát evropský globální satelitní navigační Galileo. Třetí a čtvrtou infrastrukturu pak představují elektrické a plynové přenosové sítě. Tyto sektory by měly být detailně zmapovány, přičemž důraz bude kladen také na vzájemnou propojenost a závislost. Analýza daných sektorů, z nichž by měly vzejít data a zkušenosti, které bude možné aplikovat v rámci rozvoje dalších evropských sektorů, bude dělena na tři pilíře – prevence, připravenost a reakce.

V rámci prvního pilíře bude pozornost zaměřena především na analýzu a zhodnocení rizik. Tyto aktivity by měly navázat na dosavadní znalosti získané z projektů FP 7 z kapitoly bezpečnosti, ale i životního prostředí. Zároveň by měly využít i dalších nástrojů popsaných například EU Cybersecurity Strategy. Následně by v rámci druhého pilíře měly být navrženy strategie posilující připravenost členských států a dalších relevantních aktérů. Komise počítá s vytvářením kontingenčních plánů, organizováním zátěžových testů, společných cvičení apod. V návaznosti na tyto procesy by mělo dojít k posílení mezinárodní spolupráce a zformování nadnárodních strategií, které mohou být přenositelné i do dalších sektorů.

Ve střednědobém horizontu by tak zkušenosti a znalosti nabyté v rámci pilotních projektů mohly vést ke zformování evropského přístupu k ochraně kritické infrastruktury, jehož počátky by se budovaly v regionech, kde členské státy budou mít zájem o přeshraniční spolupráci a kde již k mnoha přeshraničním aktivitám dochází. Komise také počítá s tím, že z níže zmíněných a nových rozpočtových nástrojů bude i přes značné navýšení prostředků

podpořeno méně projektů, přičemž bude kladen důraz na jejich mezisektorální a přeshraniční charakter.

Kromě již výše zmíněných prostředků distribuovaných v rámci Horizontu 2020 budou klíčové investice prováděny v rámci rozpočtu DG Home. V této kapitole nový rozpočet počítá se dvěma nástroji (oproti celkem šesti v minulém rozpočtovém období) – Asylovým a migračním fondem a pro tuto oblast relevantním Fondem vnitřní bezpečnosti. Právě tento nástroj nahradí původní finanční nástroj ve formě Programu prevence, připravenosti a zvládání následků teroristických útoků. Z celkového rozpočtu dosahujícího bezmála 11 miliard eur bude pro Fond vnitřní bezpečnosti alokováno zhruba 4,6 miliard eur a dalších 822 milionů eur bude investováno do chodu a rozvoje existujících IT systémů a agentur. Z celkového pohledu se rozpočet DG Home navýší o bezmála 40%, což představuje v relativních i absolutních hodnotách značný nárůst v porovnání s ostatními rozpočtovými kapitolami stejně tak jako v časové perspektivě.

PŘÍLOHA 2 – LIMITY PASIVNÍ KYBERNETICKÉ OBRANY

1. Úvod

Následující kapitola shrnuje současné nejznámější postupy a metody kybernetické ochrany či obrany. Účelem textu je především seznámit technicky méně obeznámené čtenáře s běžnými metodami, které jsou pro významnou část kybernetických hrozeb dostatečné a postavit je vedle precizně mířených útoků, na které tyto metody nestačí. Cílem tohoto textu tak není vůle zdiskreditovat běžné metody, nýbrž popsat bezpečnostní situaci v kyberprostoru z perspektivy, která jasně rozliší dvě základní obranné strategie: pasivní a aktivní a popíše je v kontextu jejich efektivního uplatnění. Tato perspektiva je důležitá především z důvodu prudce narůstající diskuse na téma aktivní kybernetické obrany, která v druhé etapě tohoto projektu je rozebíraná v několika studiích. Aktivní obrana je z principu aktivního počínání administrátorů, programátorů či operátoru extrémně časově náročná, je tedy zřejmé, že její uplatnění je možné pouze tehdy, pokud je již jisté podezření, které může vzejít např. z různých metod behaviorálních analýz. Takové analýzy se stále řadí mezi pasivní obrany, byť podstatně sofistikovanější.

Následující text popisuje základní metody pasivní obrany, podpůrnou alternativu v podobě behaviorální analýzy a připravuje půdu pro další studie, které budou již přímo zaměřeny na možnosti, metody a strategie aktivní kybernetické obrany. Limity pasivní obrany jsou názorně představeny ve studii zabývající se komparativní analýzou několika vybraných případů z minulosti, na kterých jsou diskutovány limity pasivní obrany a jasně znázorněny momenty, kdy je aktivní obrana nezbytná.

V konvenční fyzické obraně státu je pasivní obrana nejen deklarace síly, tedy odstrašení silou, zajišťující odstrašení potenciálního státního protivníka. Za odstrašující nástroj lze dnes považovat i komplexní mezinárodněprávní prostředí se souvisejícími sankcemi a nebo ekonomické zájmy všech zúčastněných. Debata proč od 2. sv. války nedošlo mezi demokratickými státy k závažnějšímu konfliktu dala prostor vzniku celé řady teoretických přístupů v oboru mezinárodních vztahů. Tyto přístupy mají společný jeden atribut a to je jistá míra *důvěry* v typický aspekt příslušeného teoretického přístupu. U realistů kladoucích důraz na relativní výhody ze spolupráce se jedná o *důvěru v existenci absolutní síly protivníka* v jeho atomových zbraních, popř. možné

reakci celé aliance aktivací článku 5 washingtonské smlouvy. U liberálů kladoucích důraz naopak na absolutní hodnoty se jedná o *důvěru v ekonomický, kapitalistický systém*, který je všem prospěšný, rozvinutý o teorii mezivládního systému, který propojuje zájmy korporací a vlád. U funkcionalistů se jedná o *důvěru v efekt přetékání* technologií mezi státy; pro účely tohoto textu se jedná o kritickou infrastrukturu a důvěru ve smysl jejího propojení. Ať už se na problém díváme jakýmkoliv prizmatem, vždy se jedná o důvěru v nějaké empiricky doložitelné jevy. Budeme-li akceptovat, že teoretické pohledy se snaží vysvětlit realitu kolem nás vždy jiným úhlem pohledu a jsou tak za svých určitých okolností platné, pak zde máme kombinaci důvěry v absolutní silu protivníka, důvěru ve smysl kooperovat a důvěru ve smysluplnost se vzájemně integrovat, což v kontextu rozvoje demokratických společností a celé evropské integrace vedlo k nebývalému míru na kontinentě. Jenže v kybernetické bezpečnosti tyto důvěry chybí z celé řady důvodů a i proto je celá diskuse o kybernetické bezpečnosti stále velmi mlhavá a bez teoretického rámce vysvětlující jeho dynamiku.

V kyberprostoru dochází k celé řadě změn tohoto vnímání. Z realistického hlediska dochází ke změnám v distribuci moci, jednotlivci rozhodnutí střetnout se s mocí státu mají díky kyberprostoru dosud nebývalé příležitosti změřit své síly. Specifická kvalifikace jednotlivce, tedy nestátního aktéra, postavená na extrémně specifických znalostech je naprosto klíčová bez ohledu na kapacity státu. Jednak většina států není na podobný střet připravená, ale i ty silné státy budující vlastní Cyber Command nemohou vytvořit bariéru v podobě fyzicky nainstalované linie tanků na bitevním poli proti hackerům v kyberprostoru přesvědčených udeřit na Achillovu patu moderní společnosti – kritickou infrastrukturu. Jistá změna v balanci moci je zde zřejmá. To pochopitelně platí i pro státní aktéry, kteří mají pro budování této kapacity výrazně větší prostředky a statisticky vyšší pravděpodobnost než jednotlivec, že těchto velmi specifických znalostí dosáhnou. Tento nevyrovnaný vztah je základem velmi efektivní síly na straně útočníka a velmi náročné obranné strategie na straně obránce.

Kyberprostor nikomu reálně nepatří, některé pohledy mu přisuzují status tzv. *global common*, veřejného statku, který nikdo nevlastní, neobhospodařuje, nechrání... jako celek. Kyberprostor je meta produktem dílčích zájmů v propojení konkrétních ICT, nicméně jako komplex vytváří celou řadu diskutabilních jevů s ještě diskutabilnějšími atributy.

Prvním, a tím nejzásadnějším, atributem je *absence důvěry* v zaběhlé pořádky ve světě reálném. Ať už se jedná o důvěru v jednání protivníka, problém nemožnosti

přisouzení útoku konkrétnímu aktérovi totiž protivníka dokonale maskuje a pokud vznikne podezření, není nic jednoduššího než svůj podíl zapřít, neboť důkazní proces je vždy silně nestabilní a neprůkazný. Interakce se tak výhradně odehrává v kyberprostoru bez ohledu na to, kdo za ní reálně stojí.

Debatuje se i jestli kyberprostor vůbec existuje či se jedná o pouhý abstraktní koncept, jehož adresování dílčí bezpečnostní problémy neřeší. Mezinárodní právo např. s kyberprostorem jako konceptem se specifickými vlastnostmi nepracuje. Tallinnský manuál pouze definuje kyberprostor jako teritorium generované infrastrukturou situovanou na území konkrétního státu.[23] V manuálu totiž nejde o definici kyberprostoru, nýbrž o přenesení zodpovědnosti, popř. o možnost jasně poukázat na intervenci do územní celistvosti státu, je-li tato infrastruktura napadena. Neexistuje tedy důvěra především ve vnitřní dynamiku kyberprostoru, protože ji dosud nikdo uspokojivě nepopsal. Celá řada jevů vykazuje absolutně anarchické jednání, i když ne vždy. Např. nedostatek této důvěry zajistil, že se Obama před nálety na Libyi rozhodl nepoužít kybernetický útok proti jejich vzdušné obraně – nechtěl riskovat odhalení kybernetické zbraně, kterou má jistě USA k dispozici.[24] Jinými slovy dynamika kyberprostoru jako konceptu je natolik tekutá, že lze jen těžko odhadnout důsledky aktu, který může tuto tekutou podobu výrazně ovlivnit, což použití každé specifické kybernetické zbraně zcela jistě způsobuje. Stuxnet budiž příkladem. Žádný ze států nemá zájem na prolomení jakési nepsané bariéry a mají k tomu řadu důvodů. Za prvé nechtějí odhalit své schopnosti v kybernetickém konfliktu, který je možné řešit konvenčně. Za druhé nevědí, jaké zbraně mají jejich velcí protivníci a nemíní s nimi měřit síly a riskovat svou citlivou kritickou infrastrukturu. Za třetí všechny kybernetické zbraně jsou „meč dvojího ostří", jejich použití dává okamžitě všem hráčům na šachovnici do ruky jimi dlouze, složitě a komplexně vyvíjený kód, který může být použit proti nim. Případ napadení ropné společnosti Saudi Aramco, během kterého došlo k vymazání cca 55tis. počítačů (některé zdroje mluví jen o 30tis.) řádově v minutách, budiž příkladem použití kódu Stuxnet na spojence Západu – Saudskou Arábii a především na cca 15% světové produkce ropy.

[23] CCDCOE, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York: Cambridge University Press, 2013).

[24] http://www.nytimes.com/2011/10/18/world/africa/cyber-warfare-against-libya-was-debated-by-us.html

Druhým atributem je neletální charakter de facto všech útoků. Thomas Rid[25] patří mezi velké kritiky přemrštěné sekuritizace kybernetických hrozeb, nicméně jeho analýza je nesmírně přínosná. Rid netvrdí, že k masivnímu konfliktu v kyberprostoru nemůže dojít, ale kritizuje používání termínu kyber válka s přirovnáním k významu slova konvenční válka vedená např. těžkou armádní technikou. Ve své analýze Rid představuje tři základní aspekty současné i budoucí kyber války a to je: sabotáž, špionáž a propaganda. Válka dle Rida (opírá se o teorii války Carla von Clausewitze) musí vykazovat tři základní atributy: být instrumentální – mít jasně definované cíle v podobě zájmu měnit chování oponenta – donutit ho se přizpůsobit našim požadavkům, mít politický podtext – být vedená státem nebo proti politickým hodnotám jiných států nebo guerillou proti státu a především být násilná. Právě násilí je to, co Rid v kybernetickém konfliktu silně kritizuje, protože tam přímé násilí absolutně schází. Instrumentalita je prokazatelná u sabotážních útoků a propaganda je typický DDoS útok. Rid tak termín kybernetická válka vidí spíše v kontextu významu termínu např. války proti rakovině.

Absence důvěry v běžný zažitý řád a neletální charakter zásadně mění dynamiku celého prostředí a předestírá jen těžko odhadnutelný budoucí vývoj. Důvěra je zásadní pro schopnost předvídat chování protivníka, popř. sázet, že potencionální protivník bude mít jisté limity, ať už v kontextu mezinárodního práva nebo nepsaných morálních civilizačních zásad. Ani jedno v kyberprostoru neplatí. Nulová letalita umožňuje de facto neomezené experimenty. Jen těžko odhalitelná identita útočníka pak zajistí, že i případné nehody v podobě omylem otevřené přehrady lze riskovat, neboť nevyvolá mezinárodní konflikt mezi státy, na což je současné mezinárodní právo zajišťující předcházení konfliktu krátké a absence důvěry v dynamice prostředí, systému, řádu či pravidel, resp. v neexistující režim, otevírá neomezené možnosti v duchu absolutní anarchie v kyberprostoru.

Výše popsané teoretické prostředí je důležité pro uchopení následující technicky orientované části. Primárně anarchické prostředí vytváří extrémní tlak na obranu, neboť útočníci mají neomezeného prostoru k experimentům díky absenci letality i problému přisouzení. Pasivní obrana tak dříve nebo později vždy útok propustí a to i bez ohledu na

[25] Thomas Rid, *Cyber War Will Not Take Place* (HURST C & Company PUBLISHERS Limited, 2013).

silně zkomplikované prostředí pro útočníka např. formou tzv. honeypotů, tedy matení útočníka.[26]

2. Dvě podoby útoku

Pro naše účely je vhodné rozdělit typy útoků do dvou kategorii. Celoplošné útoky (broadcast attacks) a cílené útoky (targetted attacks). Jedná se o zásadně odlišné přístupy, ačkoliv obě strategie využívají obdobných nástrojů a zranitelností.

Celoplošné útoky mají za cíl v co nejkratším čase dosáhnout co největšího pokrytí zkompromitovaných zařízení (PC, telefony, switche etc.), zatímco u cílených útoků je strategicky nežádoucí plošné šíření, neboť zvyšuje riziko odhalení dříve, než dojde k úspěšnému prolomení obrany v cíleném zařízení a jeho kompromitaci.

2.1. Celoplošné útoky

Cílem je zasáhnout co největší počet zařízení s neurčitým cílem. Tento strategický přístup zpravidla směřuje k vytvoření rozsáhlých botnetů, které jsou následně používány k cíleným útokům nebo ke sběru specifických dat, např. čísla kreditních karet na zkompromitovaných bankovních systémech. Čím větší počet zařízení je napadeno, tím větší je pravděpodobnost úspěšného útoku. Pokud uživatelé používají nevhodný prohlížeč a jejich bankovní instituce neví o zranitelnosti, kterou útočníci použijí, je takto možné velmi rychle získat poměrně rozsáhlé množství přístupových údajů.

Celoplošnými útoky jsou zpravidla zasažena ta zařízení, ve kterých se vyskytuje stejná zranitelnost. Tato zranitelnost může být nová (0-day vulnerability, dosud neodhalená zranitelnost), stejně tak je možné, a v tomto případě i velmi pravděpodobné, že se jedná o zranitelnosti již známé, nicméně z napadených zařízení neodhalené neodstraněné. Proti těmto typům útoků postačuje obrana běžnými prostředky, mezi které se řadí základní bezpečnostní „hygienické“ postupy. Jedná se o aktualizace používaného software, nainstalovaný antivirus, antispyware, dobře nakonfigurovaná firewall, špatně prolomitelná hesla apod.

Plošné útoky není vhodné podceňovat, neboť i přes jejich charakter nekonkrétního zacílení jsou schopny zásadně ovlivnit chod zařízení, které je součástí kritické infrastruktury. Příklad může být vir Slammer worm,[27] kterému se při jeho

[26] Kristin E. Heckman et al., "Active Cyber Defense with Denial and Deception: A cyber-Wargame Experiment," *Computers & Security* 37(2013).

[27] http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99

velikosti 365 bytů podařilo proniknout do jaderného zařízení v USA a díky nedostatečné bezpečnosti na straně administrátorů poškodit řadu řídích zařízení tak, že bylo nutné celý řídící systém vypnout. Na tomto viru je zajímavý fakt, že v den svého prudkého rozšíření se mu podařilo částečně zpomalit internet, ale díky své minimální velikosti, byl schopen se i na úplně přehlcených systémech dál multiplikovat a odesílat mailem na všechny adresáty v seznamu uživatele napadeného zařízení.

2.2. Cílené útoky

Cílené útoky oproti plošným se zaměřují spíše na neznámé zranitelnosti, které využijí poprvé. Jejich zneužití v plošném měřítku by s velkou pravděpodobností vedlo k jejich odhalení a odstranění výrobcem softwaru. Je tedy navýsost logické, že tento typ útoku bude citlivý, opatrný, málo četný a dílčími kroky povede ke kompromitaci klíčového zařízení pro naplnění strategických cílů útoku. Běžné aktualizace nebudou postačovat, protože využitá zranitelnost nebude známá a útočník bude zcela jistě volit takovou taktiku, aby obešel běžné bezpečnostní opatření. Antivirus též, jelikož útočníci snižují výskyt viru už např. jeho sebedestrukčními mechanismy, popř. jej píší natolik specificky, že je schopen vracet antiviru kompromitovanou zpětnou vazbu a tím znemožnit vlastní odhalení. Sofistikované viry jsou psány přímo tak, aby obešly celou plejádu antivirů. Mají zabudovanou obrany na každý konkrétní zvlášť a i z toho důvodu lze obdobnou míru sofistikovanosti přisuzovat spíše státu než nestátním aktérovi.[28] Antispyware ztrácí na významu ze stejných důvodů, jako u antiviru, nicméně je velmi předpokládatelné, že takový typ útoku nebude veden formou šíření kompromitovaného software. Firewall je zbytečná, neboť takový typ útoku bude dělat vše pro to, aby se dostal do cíleného zařízení co nejjednodušší a nejběžnější cestou. Např. tedy spuštěním skriptu na webové stránce nebo emailem, popř. do řídících systémů přes USB klíčenku (Stuxnet, Flame etc.).

Cílené útoky se řadí mezi ty typy útoků, které lze s nejvyšší mírou pravděpodobnosti očekávat při strategických útocích státním aktérem proti jinému státu, ale nelze zanedbávat vůli použít takových prostředků u mezinárodních korporací v jejich konkurenčním boji. Právě vůle zkompromitovat bezpečnostní opatření na SCADA systémech konkurence zajišťující např. chod turbíny ve vodní elektrárně je typickým příkladem, který byl již laboratorně úspěšně vyzkoušen. Nicméně cílené útoky stále patří, a do budoucna budou velmi pravděpodobně i nadále patřit, mezi ty méně

[28] Clement Guitton and Elaine Korzak, "The Sophistication Criterion for Attribution," *The RUSI Journal* 158, no. 4 (2013).

četné, ačkoliv s jistotou mezi ty vážnější. V případě, že se útočící strana rozhodne zkompromitovat specifický řídící systém a poškodit tak např. kritickou infrastrukturu, má dvojí možnost. Jednou variantou je ten samý řídící systém pořídit a ve spolupráci se zpravodajskou službou vytvořit co nejvíce podobné technické řešení v laboratorním prostředí, na kterém bude svoji vyvíjenou kybernetickou zbraň testovat. Druhou variantou, která bude skoro jistě vždy následovat po laboratorním testu, tuto zbraň nenápadně testovat na cíleném zařízení v ostrém provozu bez nápadného způsobování škod, pouze testovat, zda je možné na dálky systém kontrolovat. Přesně pro podobné momenty pasivní obrana je skoro úplně nepoužitelným strategickým přístupem a musí nastoupit obrana aktivní.

	ZRANITELNOSTI		**CÍLE**	**OBRANA**				
ÚTOKY	0-day	známé		strategie	aktualizace	antivirus	antispyware	firewall
celoplošné	☑	☑	mnoho	pasivní	☑	☑	☑	☑
cílené	☑		omezené	pasivní/aktivní	?	?	?	?

Tabulka 1 - Obranné metody proti celoplošným a cíleným útokům

3. Formy pasivní kybernetické obrany

Jak již bylo řečeno, řada forem pasivní obrany není dostatečně účinná proti cíleným útokům. Následuje rozbor několika těchto přístupů zvlášť a popis konkrétních problémů, které vyvstanou v případě, že je útok jednoznačně cílený. Je nutné vzít v potaz prvně strategické zájmy útočníka. Vezmeme-li si k analýze příklad útoku za účelem vytvoření botnetu. V našem scénáři se zaměříme na jeden konkrétní případ a to je zajištění botnetu k dlouhodobému využívání k DDoS útokům.

3.1. Detekce antivirem

Útočník k doručení svého kódu do cíleného počítače využívá viru a proto může stát před rizikem, že tento vir bude odhalen. Lze předpokládat, že pro účely botnetu je důležitější získat a udržet kontrolu nad co největším počtem počítačů. Zprvu však může být pro útočníka důležitější vyzkoušet si schopnost vůbec s jedním infikovaným počítačem vykonat tzv. pokus o DDoS útok. Útočník tedy použije dílčí kódy již jednou napsaného viru, který antiviry znají a jeho šířením zkompromituje pouze tu část počítačů, které nejsou dobře chráněny – získá čas, neboť nemusí psát vir, ale primárně C&C rozhraní (command and control), kterým bude ovládat ty počítače, které se mu podařilo díky nedostatečné bezpečnostní hygieně zkompromitovat. Detekce antivirem je velmi pravděpodobná, nicméně tomu předejít zde cílem nebylo. Část počítačů získal a

mikro-botnet kontroluje za pomocí využívání vhodné zranitelnosti, která mu umožnila si vytvořit zadní vrátka (backdoors) v síti zkompromitovaných počítačů.

Jakmile však zjistí, že „nálož" (payload) v cílených počítačích funguje, začne psát vlastní vir (carrier), pokud je důsledný a má i zkušenosti z toho, jak některé antiviry jeho původní vir odhalily, píše vir tak, aby dokázal antiviru čelit a oklamat jej. Výsledkem je, že antiviry nejsou schopny tento vir odhalit z celé řady důvodů: A) vir je psaný tak, aby jej antiviry nedokázaly snadno detekovat, B) je napsaný od prvního řádku a je-li programátor zručný, může mít i dva roky času než jej všechny antivirové firmy vůbec zaregistrují.[29]

Jedná se o náročnou práci, při plošných útocích je méně pravděpodobná. Nicméně, v případě, že útočníkovi nejde o statisticky uspokojivou velikost botnetu, ale o masivní botnet výrazně velkých rozměrů jakého jsme byli svědky během útoku na Spamhouse, pak je takový postup nadmíru pravděpodobný. Útok na Spamhouse na několik hodin možná i zpomalil internet na celém světě, nicméně od té doby se o takovém dopadu vedou debaty.[30] Jisté je, že útok byl v řádu 300Gbps v době, kdy rozsah 4-10Gbps byl považován za velký DDoS útok. K zajištění takového útoku bylo nutné riskovat při vytváření botnetu co nejméně, aby jeho velikost byla co největší. Obejití detekce antivirem je v tomto případě velmi pravděpodobná.

3.2. Aktualizace

Zájmem útočníka není využít známé či neznámé zranitelnosti k vykonání jednoho útoku, např. získání kontroly nad co největším počtem počítačů. Ztrátu kontroly jednou aktualizací a tudíž ztrátu kontroly nad celým botnetem si nemůže dovolit. Zájmem tudíž je udržet kontrolu nad co největším počtem počítačů, aby mohl realizovat DDoS útoky bez ohledu na plošné aktualizace. Útočník bude mít jednou napsaný kód ke kontrole těchto počítačů a rozhraní pomocí něhož tuto kontrolu vykonává vzdáleně využívajíc k tomu právě danou zranitelnost. Je tedy zřejmé, že využití zranitelnosti je pouze dílčí část a proto bude dělat vše pro to, aby v případě aktualizace zranitelnosti, byl připraven využít zranitelnosti jiné.

Pravidelnou aktualizací software na cíleném počítači je tedy možné zajistit jistou míru ochrany. Nicméně bude-li útočník mít zájem zranitelnost využívat, nebude ji

[29] http://www.theguardian.com/technology/2012/jun/17/flame-virus-online-security

[30] http://www.lupa.cz/clanky/kolem-nejvetsiho-utoku-na-internet-v-historii-sili-pochyby-media-naletela/

využívat často, aby nebyla odhalena. Pro udržení botnetu je takový přístup pochopitelně nesmyslný, nicméně pro cílené útoky velmi pravděpodobný a tak aktualizace takovému útoku nepomohou. Stuxnet využil až tří různých 0-day zranitelností, tedy těch, které do té doby nebyly odhaleny a proto nejspíše ani nebyly využívány.[31]

3.3. Firewall a antispyware nebo antimalware

Plošné útoky budou využívat statisticky pravděpodobných scénářů. Skrze firewall projde útočník tou nejvíce pravděpodobnou cestou a to přes porty, které se využívají pro běžné služby (HTTP, POP3, FTP...). Antispyware nebo antimalware budou fungovat opět při užití běžně dostupných hackerských nástrojů, hůře, budou-li psané na míru.

3.4. Reakce na incident – CERT/CSIRT týmy

Velkým trendem je budování týmu CERT či CSIRT[32] reagujících na incident. Jejich role je primárně ve schopnosti rozšířit co nejrychleji informaci o nutnosti aktualizovat konkrétní software, neboť se zjistilo, že zranitelnost v něm obsažená je používána k cílenému útoku tak, jak to precizně dělá např. dlouho fungující US-CERT[33] nebo vznikající český vládní CERT (GovCert)[34]. Nedílnou rolí těchto týmů je i kooperace při znovu zprovoznění napadených systémů, nicméně z logiky věci je zřejmé, že v tom primárně soukromí provozovatelé kritické infrastruktury mají vlastní komerční zájem. V tomto zájmu nehraje roli pouze ztráta zisku v době neprovozování služby, ale i důvěra ve spolehlivost jejich technického řešení, které u provozovatelů ICT je nesmírně citlivá.

Zásadním problémem tohoto přístupu je fakt, že CERT týmy reagují až v momentě, kdy k poškozujícímu incidentu došlo. Jejich rolí tak může být maximální míra osvěty v preventivní fázi, schopnost pomoci napadeném subjektu v případě, že již měly se stejným útokem zkušenost a tuto zkušenost přenesou, nicméně schopnost předvídat útoky a soustředit se na aktivní obranu je pro tyto týmy cizí. Dobře situaci ilustruje rozdíl rolí mezi US-CERT a US Cyber Command, kde druhý zmíněný nehraje roli pouze ofensivní kapacity, ale zcela jistě i monitoringu schopností protivníka, který se na

---

[31] James P. Farwell and Rafal Rohozinski, "Stuxnet and the Future of Cyber War," *Survival (00396338)* 53, no. 1 (2011).

[32] CERT – Computer emergency response team and CSIRT - Computer Security Incident Response Team. Pojem CERT je registrovanou známou Carnegiie Mellon University již z 80. let, z toho důvodu se začal používat termín CSIRT. Nicméně jejich poslání de facto totožné.

[33] Jeho limitovaná role vyplývá už z definice jejich cílů: „US-CERT's mission is to improve the nation's cybersecurity posture, coordinate cyber information sharing, and proactively manage cyber risks to the nation while protecting the constitutional rights of Americans." Vice viz www.us-cert.gov

[34] Český vládní CERT je zřízen pod patronací Nádoního bezpečnostního úřadu a jemu podřízeného Národního centra kybernetické bezpečnosti.

útok připravuje např. na honeypotu k tomu připraveném. Tuto americkou strategii akcentuje fakt, že současný ředitel US Cyber Command Keith Alexandr je též ředitelem zpravodajské služby NSA – National Security Agency.

3.5. Alternativní metody pasivní kybernetické obrany

Mezi v současnosti nejvíce diskutované alternativní metody obrany patří tzv. behaviorální analýzy. Důvodem k jejich vzniku je neúnosná míra nárůstu kybernetických útoků, které jsou perfektně cílené, těžko odhalitelné a především čím dál úspěšnější. Nárůst je v řádu tříciferných procent.[35] České státní instituce mají tendenci oddělovat kybernetickou kriminalitu (policie) od kybernetické bezpečnosti (NBÚ) či kybernetické obrany (ministerstvo obrany), aby si tak ochraňovaly rozsah svých kompetencí. Je to fatální chyba, protože právě obrovský nárůst kybernetické kriminality dává prostor rozvoji sofistikovaných kybernetických zbraní a dalšímu financování organizovaného zločinu, který se může stát rovnocenným soupeřem státu v kyberprostoru. Měly by tedy zcela zřetelně intenzivně kooperovat, což se v praxi děje jen víc na neformální úrovni než reálné spolupráci. Alternativní metody jsou však velmi praktickým nástrojem na sběr dat, které mohou tuto spolupráci stvrdit.

3.6. Proč používat behaviorální analýzy

Dobře provedené útoky jsou těžko odhalitelné už proto, že zpravidla využijí maximum běžných, legálních a otevřených cest, které musí být otevřené pro legitimní software. Tyto viry, malware nebo spyware tak působí, že jsou buď součástí již probíhajících procesů v zařízení nebo jsou samy o sobě nástrojem, který uživatel k něčemu potřebuje avšak konají řadu aktivit bez jeho vědomí. Na druhou stranu řada legitimního software kromě užívání otevřených cest ke vzdálené komunikaci nějaký standardním způsobem funguje na vlastním zařízením. Jestliže se software začne ve zlomku času chovat (dotazovat operačního systému, otevírat porty na internet, posílat neobvyklé objemy dat, pravidelně se připojovat na vzdálený server...) je možné toto nestandardní chování identifikovat a tím odhalit nežádoucí kód. Velká řada světových vývojářů pochopila před jakou výzvou stojí, zvlášť v řadách gigantů jako je např. Adobe, protože právě jejich software je zcela běžně zneužíván k šíření škodlivého kódu. Adobe se dostala už i do situace, že čínští hackeři našli 0-day zranitelnost v aktualizaci (patch), kterou jako vývojáři dostali v beta verzi k dispozici před jejím rozšířením. Jednalo se o

[35] „FireEye Advanced Threat Report – 1H“, http://www2.fireeye.com/advanced-threat-report-1h2012.html

banální aktualizaci Adobe Acrobat Reader. Díky objevené chybě pak dokázali zkompromitovat miliony počítačů řádově v sekundách, protože uživatel samotnou aktualizací otevřel zadní vrátka, na které byli útočníci připraveni. Jiný případ je velmi aktuální, kde se ale obdobně podařilo útočníkům získat na 3 miliony uživatelských účtů i s kreditními kartami a především zdrojový kód řady produktů Adobe, se kterými budou schopni dohledávat 0-day zranitelnosti s nebývalou snadností.[36]

To však nic nemění na tom, že daný software by měl vykazovat i nadále standardní chování, nicméně tou největší výzvou je, jak takové standardní chování identifikovat a následně spolehlivě potvrdit, aby nedocházelo k falešným poplachům. Falešný poplach je situace, kdy aplikace uživateli oznámí nestandardní chování a existenci škodlivého kódu, aniž by to byla pravda. Typicky tou situací může být oficiální aktualizace od vývojářů. Pokud budou existovat zadní vrátka, jak aplikaci oznámit, že se jedná o regulérní aktualizaci, jsou pochopitelně zneužitelná a v případě ukradení zdrojového kódu jako u výše uvedeného příkladu se tak absolutně nic nezmění, ba naopak.

Dohledávání anomálií není matematickou novinkou. Jedním z přístupů, který detekuje anomálie v datové síti se běžně používá např. u forem jako Amazon nebo Netflix k nabízení produktů „které by se nám mohly líbit." Jedná se o strojové učení, data-minig nástroje kombinované s teoriemi a metodologickými přístupy známými např. v oborech nervových systémů[37] nebo genetických algoritmů.[38] Nejobecnější popis současných metod detekce anomálií byla zpracována Chandolem a Banerjeem.[39]

3.7. Základní tvorba referenčního vzorce

Základní systém učení se dělí do dvou kategorií a někteří z nás jej znají běžně z používání běžné firewall ve Windows. Supervizovaný přístup předpokládá, že při vzniku anomálie ji systém zdokumentuje a obratem se dotáže uživatele, zda-li se jedná o anomálii, či jeho intencionální zásah. Rozhodnutí uživatele se uloží jako příklad a systém se v příštím případě už rozhodně sám na základě tohoto příkladu. Nesupervizovaný

[36] „Scam of the day – November 4, 2013 – Adobe update, its worse than you think." - http://scamicide.com/tag/adobe-acrobat-hacked/

[37] Z. Zhang, J. Li, C. Manikopoulos, J. Jorgenson, and J. Ucles, "HIDE: A Hierarchical Network Intrusion Detection System Using Statistical Preprocessing and Neural Network Classification," in *Proc. IEEE Workshop on Information Assurance and Security* (2001).

[38] C. Sinclair, L. Pierce, and S. Matzner, "An Application of Machine Learning to Network Intrusion Detection," in *Proc. Computer Security Applications Conference* (1999).

[39] V. Chandola, A. Banerjee, and V. Kumar, "Anomaly Detection: A Survey," *ACM Computing Surveys (CSUR)* 41 no. 3, Article 15 (2009).

přístup toto rozhodnutí dělá automaticky na základě dílčích vzorů již integrovaných v daném učícím se systému. Supervizovaný je podstatně spolehlivější a tudíž i žádoucí, nicméně dosti zásadně komplikuje práci uživatele a při přehlcení dotazy lze s jistotou předpokládat, že uživatel nerozhodne vždy vhodně. Tento systém učení vytvoří tzv. „zdravá data" a uloží je do „tréninkového souboru," který je následně používán jako referenční vzor. Typickým příkladem je spam filtr v podobě blacklistu, který se sdílí napříč celým internetem – Spamhouse.

Tuto základní metodu s referenčním rámcem lze ještě rozdělit do dvou skupin, o jedné třídě a o dvou třídách. Metoda jedné třídy testuje pouze zdravá data, zatímco metoda o dvou třídách umí rozpoznat mezi zdravými i škodlivými daty.[40] Přestože by behaviorální analýzy měly být neoddělitelnou součástí pasivní kybernetické obrany, ne vždy jí jsou. Nejedná se pouze o referenční rámec firewall na kancelářském počítači, daleko důležitější je mít obdobné rámce v industriálních zařízeních, což zdaleka není pravidlem, ačkoliv z celkového komplexu chování těchto systémů lze předpokládat, že by učící se systémy čelily výrazně menšímu počtu překážek, než u počítačů v kancelářích.

4. Závěr

V této studii bylo za cíl nastínit základní limity pasivní obrany jak z teoretického, tak metodického přístupu. Detailnější studie v druhé etapě projektu se již bude zabývat konkrétními behaviorálními metodami podrobněji. Závěrem je vhodné podotknout, že tyto systémy nejsou všespásné a pro účely obrany kritických systémů v kritické infrastruktuře je vhodné přistoupit i k aktivní obraně, kterou budeme rozebírat ve studiích druhé etapy též podrobněji. Pasivní obrana je nutnou a neoddělitelnou součástí kybernetické obrany. Nelze si představit vytvářet referenční rámce behaviorální analýzy nebo monitorovat chování hackera v honeypotovém prostředí bez perfektní hygieny při zabezpečování celého ICT i SCADA systémů.

[40] Amir Averbuch and Gabi Siboni, "The Classic Cyber Defense Methods Have Failed – What Comes Next?," *Military and Strategic Affairs* 5, no. 1 (2013).

PŘÍLOHA 3 – ANALÝZA KOMUNIKACE V BEZDRÁTOVÝCH SÍTÍCH

Tato studie je zaměřena na přehled stávajících komunikačních systémů a následně jejich zabezpečení. Pozornost je věnována bezdrátovým komunikačním systémům, které jsou z hlediska napadení potencionálně zranitelnější. Na závěr je stručné shrnutí a zhodnocení bezpečnostních rizik popisovaných komunikačních systémů.

1. Přehled komunikačních systémů

Komunikační systémy můžeme obecně rozdělit podle způsobu přenosu informace na:

- Pevné (Drátové)
- Bezdrátové

Tyto se pak mohou dále dělit podle technologie na:

- Optické (optické záření)
- Elektromagnetické (rádiové vlny)

Dále se budeme v této studii zabývat **bezdrátovými** komunikačními systémy.

2. Bezdrátové komunikační systémy

Zde opět záleží na způsobu přenosu informace mezi komunikujícími subjekty. Ty mohou být optické, rádiové nebo sonické. Pozornost bude věnována rádiovým komunikačním systémům.

Rádiové komunikační systémy se mohou dělit dle použité technologie. Nejznámější a nejběžněji používanými technologiemi jsou:

- **Buňkové** (typickým představitelem jsou sítě mobilních operátorů)
- **Bezdrátové počítačové sítě** (WLAN) běžně označované jako WiFi (dle standardu IEEE 802.11) Použití do vzdálenosti řádově desítek metrů.
- **Sítě pro osobní komunikaci** (PAN) typickým představitelem je Bluetooth, ZigBee. Použití do Vzdálenosti řádově jednotek metrů.

- **Satelitní** různé druhy satelitní komunikace VSAT atd..

2.1. Mobilní Sítě

Mobilní sítě jsou dnes dostupné téměř ve všech obydlených místech planety a jejich využívání stále narůstá. Díky snadné dostupnosti a spolehlivosti jsou intenzivně využívány nejen veřejností pro osobní použití, ale i korporacemi a vládními organizacemi pro přenos informací a sběr dat.

2.2. Mobilní sítě druhé generace (2G): (GSM, GPRS, EDGE)

Nejznámější a nejrozšířenější systém pro mobilní komunikace je systém druhé generace označovaný jako GSM. Ačkoliv jako takový poskytuje jen malé možnosti pro datové přenosy, tak implementací technologií pro paketově orientovaný přenos dat GPRS, EDGE nachází široké uplatnění. Přenosové rychlosti nejsou vhodné pro multimediální přenosy velkých objemů dat, ale pro přenos dat např. ze senzorů či řídících central pro např. telemetrii jsou parametry systému dostatečné.

2.2.1. GSM

Systém mobilních komunikací druhé generace (2G) je nejrozšířenějším buňkovým systémem na celém světě. Jeho největší využití je pro přenos hlasových hovorů, ale díky implementaci systémů technologií GPRS a EDGE zkvalitňuje mobilní datovou komunikaci. Základní komunikace probíhá v kmitočtovém pásmu UHF (900MHz a 1800 MHz) [1][4]. Přístup ke sdílenému rádiovému médiu využívá časové TDMA a kmitočtové dělení FDMA. Využívá duplexní provoz s frekvenčním dělením FDD komunikace směrem k uživateli tzv. uplinku a směrem do sítě tzv. downlinku. Kmitočet, na němž je realizován přenos je určen tzv. ARFCN číslem tedy číslem rádiového kanálu. Šířka použitého kanálu je 200 kHz.

Systém GSM byl vyvinut v devadesátých letech 20. století, a proto i požívané technologie k zabezpečení komunikace proti neoprávněnému narušení jsou z dnešního pohledu poměrně rizikové, a to především díky velice rychlému vývoji v oblasti výpočetní techniky [1][4].

2.2.2. GPRS

Implementací nových algoritmů a postupů do stávajícího systému GSM je možné zvýšit uživatelskou přenosovou rychlost teoreticky až na 133,6 kbit/s při využití všech 8 time slotů v TDMA rámci GSM systému. Reálně však dosahuje nižších hodnot typicky kolem 67 kbit/s. Záleží ovšem na aktuálním vytížení sítě a použitém kódovacím

schématu, které je závislé na kvalitě rádiového spojení mezi základnovou stanicí a uživatelskou jednotkou [1][4].

2.2.3. EDGE

Dalším stupněm ke zvýšení datové propustnosti mobilních sítí je systém EDGE označován také jako EGPRS. Tato technologie již přináší oproti GPRS i nutnou implementaci nového hardwaru. Díky použití vícestavové modulace 8-PSK umožnuje zvýšit spektrální účinnost a s využitím adaptabilních schémat pro modulaci a kódování je dosažitelná přenosová rychlost při kvalitním rádiovém spojení až 473,6 kbit/s při využití všech 8 time slotů v TDMA rámci GSM systému. Reálně však dosahuje nižších hodnot typicky kolem 240 kbit/s. Záleží ovšem na aktuálním vytížení sítě a použitém kódovacím a modulačním schématu, které je závislé na kvalitě rádiového spojení mezi základnovou stanicí a uživatelskou jednotkou [1][4].

2.3. Mobilní sítě třetí generace (3G): (UMTS, HSPA)

2.3.1. UMTS

Třetí generace systému pro mobilní komunikace (3G) přináší zcela nový princip komunikace. Využívá rozprostírání přenášeného signálu pomocí pseudonáhodných posloupností. Tato technologie byla původně vyvinuta armádou Spojených států amerických.

Systém využívá duplexní provoz s frekvenčním dělením FDD. Jeden kanál na jednom kmitočtu pro downlink a jeden kanál na jiném kmitočtu pro uplink, v nichž jsou přenášena všechna data. Všichni uživatelé tak ve stejný okamžik využívají stejný kmitočet a k jejich rozlišení ve sdíleném radiovém kanále je použité kódové dělení CDMA. V České republice je pro systém UMTS použito kmitočtové pásmo 2100 MHz konkrétně pro downlink 2110 – 2170 MHz a pro uplink 1920 – 1980 MHz. Šířka použitého kanálu je 5 MHz [2][3][4]. Pro uživatele je pak nejpodstatnější výrazné zvýšení datových přenosových rychlostí, které přináší především technologie jako HSPA.

Klasické UMTS dle standardu 3GPP Release 99 poskytuje datovou přenosovou rychlost k uživateli tzv. downlink (DL) i ve směru od uživatele do sítě tzv. uplink (UL) až 384 kbit/s. V současné době se však implementují do 3G sítí pokročilé technologie pro vysokorychlostní datové přenosy jako jsou HSPA, HSPA+ [2][3][4].

2.3.2. HSPA

Implementací technologií HSPA lze dosáhnout datových přenosových rychlostí v downlinku 14,4 Mbit/s a v uplinku 5,76 Mbit/s. Toho je dosaženo zavedením sdílených datových kanálů a pokročilejšími kódovacími metodami a více stavovými modulačními schématy [3][4][5].

2.3.3. HSPA+

Navazuje na principy použité pro HSPA implementuje další pokročilé technologie a principy jako je zavedení druhého kmitočtového kanálu (Dual Carrier), sdílených datových kanálů a pokročilejšími kódovacími metodami, vícestavovými modulačními schématy a MIMO technologiemi. Takto je možné zvýšit přenosové rychlosti teoreticky až na 64Mbit/s [3][4][6].

V současné době je možné v České republice reálně dosáhnout přenosových rychlostí kolem 10 Mbit/s. Opět je ovšem důležité nastavení sítě, kvalita spojení a vytíženost sítě.

2.4. Datové sítě dle standardu IEEE 802.xx

2.4.1. IEEE 802.11 (Wi-Fi) - Bezdrátové počítačové sítě WLAN

Standard pro bezdrátové komunikační sítě WLAN s označením IEEE 802.11 (známé pod komerčním názvem Wi-Fi) je široce rozšířenou bezdrátovou sítí v oblasti průmyslu i domácího použití. Označení 802.11 zahrnuje celou skupinu standardů (a/b/g/n…) založených na podobných základních principech [9].

Komunikace probíhá v bez licenčním kmitočtovém pásmu 2,4 GHz (802.11 b/g/n) případně pro některé standardy i v pásmu 5GHz (802.11 a/n).

Nejznámější jsou standardy IEEE 802.11b a IEEE 802.11g běžně používané především pro veřejný bezdrátový přístup k internetu a v současné době i moderní 802.11n.

Přístupová metoda, ke sdílenému rádiovému médiu využívaná ve všech standardech založených na IEEE 802.11, je označována jako CDMA/CA, tedy přístup k médiu s detekcí kolizí s využitím mechanismu naslouchání nosné [4][9].

2.4.2. IEEE 802.11a [9][10]

Komunikace probíhá v jednom z dvanácti kanálů 20 MHz širokých v kmitočtovém pásmu 5,15 – 5,825 GHz. Používá modulaci OFDM při použití 52 subnosných vnitřně

modulovaných fázově (BPSK nebo QPSK) nebo pomocí více stavové kvadraturní modulace (16QAM nebo 64QAM).

Dosahuje datových rychlostí až 54 Mbit/s, vzhledem k použitému 5GHz kmitočtovému pásmu není kompatibilní se standardy 802.11b/g, které pracují pouze v pásmu 2,4 GHz.

2.4.3. IEEE 802.11b [9][11]

Komunikace probíhá v jednom ze čtrnácti kanálů 20 MHz širokých v kmitočtovém pásmu 2,412 – 2,484 GHz. Používá modulaci DSSS s vnitřní modulací DBPSK, DQPSK nebo CCK. Dosahuje datových rychlostí až 11 Mbit/s.

2.4.4. IEEE 802.11g [9][12]

Používá modulaci OFDM v kanálech 20 MHz širokých při použití 52 subnosných vnitřně modulovaných fázově (BPSK nebo QPSK) nebo pomocí více stavové kvadraturní modulace (16QAM nebo 64QAM). Dosahuje datových rychlostí až 54 Mbit/s, přičemž musí splňovat zpětnou kompatibilitu se standardem 802.11b.

2.4.5. IEEE 802.11n [9][13]

Používá modulaci OFDM, v kanálech 20 nebo 40 MHz širokých v kmitočtovém pásmu 5,15 – 5,825 GHz. Dosahuje datových rychlostí až 72 Mbit/s pro kanál šířky 20 MHz a až 600Mbit/s pro kanál šířky 40 MHz a při použití MIMO technologie.

2.4.6. IEEE 802.15.1 (Bluetooth)

Využití především pro připojení různých bezdrátových zařízení na krátkou vzdálenost (handsfree, myš, klávesnice, autorádio, mobilní telefon). Podle maximálního vysílacího výkonu se zařízení dělí do třech výkonových tříd, které stanovují i jejich maximální teoretický dosah (1, 10 a 100m) [4].

Přenosové rychlosti dosahují hodnot od cca 721 kbit/s do 24 Mbit/s (pro 802.11 AMP) podle kategorie použitého zařízené, typicky je dosažitelná přenosová rychlost 1-3 Mbit/s. Komunikace v rádiovém prostředí jer založena na metodě kmitočtového skákání v rozprostřeném spektru tzv. FHSS, v bez licenčním kmitočtovém pásmu ISM 2,402 – 2,480 GHz na 79 kanálech s šířkou 1 MHz, přičemž změna nosného kmitočtu probíhá 1600 krát za sekundu [7][8].

3. Kybernetická bezpečnost komunikačních systémů

Níže jsou popsány základní mechanismy a principy zabezpečení výše popsaných komunikačních systémů.

3.1. Mobilní Sítě – 2G (GSM, GPRS, EDGE)

3.1.1. GSM

Mechanismy a základní principy použité v systému GSM jsou i dále převzaty v ostatních pokročilejších systémech, avšak úroveň jejich zabezpečení je vyšší než pro GSM. To je logickým vývojem, který je nezbytný pro zachování bezpečnosti související s rychlým vývojem výpočetní techniky a mechanismů prolomení zabezpečení.

GSM využívá tři základní zabezpečovací mechanismy:

- Utajení identity uživatele
- Autentifikace uživatele
- Šifrování

Utajení identity uživatele

ÚČEL: Zamezení možnosti zjištění identity uživatele a právě využívaných přiřazených síťových prostředků (hovory, data i signalizace) potencionálním narušitelem.

PRINCIP: Anonymity uživatele je dosaženo používáním dočasného identifikačního čísla tzv. TMSI (Temporary Mobile Subscriber Identification) namísto jedinečného čísla IMSI (International Mobile Subscriber Identification), které je pevně přiděleno jednotlivým SIM kartám. IMSI je používáno pouze při zapnutí telefonu (uživatelského zařízení) a jeho registraci do sítě. Poté je uživateli přiřazen identifikátor TMSI, který je dále využíván při komunikaci s prvky sítě [14]-[18].

Autentifikace uživatele

ÚČEL: Ověřit totožnost uživatele (pomocí algoritmů A3, A8) pro následnou šifrovanou komunikaci.

PRINCIP: Systém GSM využívá pro autentifikaci dva zabezpečovací algoritmy označované A3, A8, které jsou uloženy na SIM kartě mobilního zařízení a v Autentifikačním centru (AuC), které je součástí architektury sítě [14]-[18].

Šifrování dat

ÚČEL: Zajistit šifrovaný přenos dat rádiovým prostředím (algoritmus A5).

PRINCIP: Systém GSM využívá pro přenos informací rádiovým prostředím zabezpečovací algoritmus A5. Algoritmus A5 je uložen v mobilním zařízení a umožňuje šifrovat a dešifrovat přenášená data s využitím kódu vygenerovaného při autentifikaci uživatele. Podle 3GPP je standardizován pro šifrovaný přenos algoritmus A5 (A5/1, A5/2, A5/3, A5/4) [14]-[18].

3.1.2. GPRS

GPRS využívá podobných principů pro šifrování jako GSM, jen s přihlédnutím na paketový způsob přenosu informace.

Šifrování probíhá po autentifikaci, algoritmus používaný pro zabezpečení datového spojení GPRS je označován GEA (GEA1, GEA2, GEA3, GEA4). Liší se mírou zabezpečení podle generace standardu, a to v délce šifrovaného slova [14]-[18].

3.1.3. EDGE

Pro EDGE (EGPRS) je použit stejný princip zabezpečení jako pro GPRS [14]-[18].

3.2. Mobilní Sítě – 3G (UMTS, HSPA)

3.2.1. UMTS

Zachovává zabezpečovací principy využívané u GSM pro zpětnou kompatibilitu a dále je rozšiřuje.

Autentifikace komunikujících subjektů

Zachovává základní princip autentifikace dle GSM a dále jej rozšiřuje o vzájemné ověření a potvrzení identity sítě a uživatelského zařízení.

Kontrola integrity

Používá integritní kódy pro ověření věrohodnosti a původu komunikace probíhající mezi terminálem a sítí aby nedošlo ke zfalšování řídící komunikace (man-in-the-middle). Vzájemná domluva terminálu a sítě při výběru používaného integritního algoritmu a klíče pro komunikaci a možnost ověření. Šifrování komunikace není aktivní vždy, proto je nutné ověřit, že je terminál připojen ke skutečné základové stanici a ne k imitaci vytvořené útočníkem.

Šifrování

Šifrování uživatelských i signalizačních dat. Vzájemná domluva a potvrzení terminálu a sítě při výběru šifrovacího algoritmu a šifrovacího klíče. Algoritmus zvaný KASUMI (bloková šifra) je základem pro šifrovací a integritní algoritmy f8 a f9 [16][17][18].

Rizika:

- IMSI je při prvním přihlášení do sítě vysíláno "nechráněné" tedy jako holý text.
- Man-in-the-middle (útočník se vydává za falešnou základnovou stanici).
- Díky použití terminálů s otevřenými operačními systémy (např. Android) je možné nežádoucím SW získat přístup k citlivým informacím [16][17][18].

3.2.2. HSPA

Zachovává zabezpečovací principy využívané u GSM i UMTS pro zpětnou kompatibilitu a dále je rozšiřuje využitím složitějších ověřovacích mechanismů a principů šifrování přenášených dat, tak aby v ideálním případě znemožnily i nejmodernějším výpočetním technologiím prolomení zabezpečení.

Šifrování je založeno na algoritmech popsaných organizací 3GPP (www.3gpp.org) a obsahuje algoritmy jako UEA, UIA, EEA, EIA. Jejich detailní specifikace je online dostupná (http://www.3gpp.org/ftp/Specs/html-info/35-series.htm, http://www.etsi.org/index.php/services/security-algorithms/3gpp-algorithms).

3.3. Datové sítě dle standardu IEEE 802.xx

2.2.1 IEEE 802.11 (Wi-Fi) - Bezdrátové počítačové sítě WLAN

Standard pro bezdrátové komunikační sítě WLAN s označením IEEE 802.11 (známé pod komerčním názvem WiFi) obsahuje celou skupinu sítí WLAN (a/b/g/n), které jsou popsány výše. Ačkoliv využívají různé technologie rádiového rozhraní, mechanismy zabezpečení jsou shodné pro celou skupinu 802.11.

Dle standardu 802.11 [9] jsou definovány dvě základní třídy bezpečnostních mechanismů:

- RSNA (Robust Security Network Associations) algoritmy

- Pre-RSNA algoritmy

Pre-RSNA [9]

Jsou založené na protokolu WEP a neposkytují dostatečnou ochranu, a proto je jejich použití pouze doplňkové s RSNA. WEP je snadno prolomitelný.

WEP (Wired Equivalent Privacy) [9] – Algoritmus využívá symetrickou proudovou šifru RC4 o délce 40, 104 nebo 232 bitů s inicializačním vektorem o délce 24bitů. K šifrování i dešifrování je zapotřebí statický klíč, který je neměnný a je tak možné jej odposlechnout a prolomit zabezpečení.

Integrita – Integrita je zajištěna lineární hashovací funkcí CRC-32 (Cyclic Redundancy Check), která je společně s daty šifrována.

Autentifikace – Autentifikace je možná dvěma způsoby. První využívá sdíleného klíče, kdy je na výzvu přístupového bodu odeslána šifrovaná zpráva tajným klíčem odeslána a v přístupovém bodu ověřena. Druhý způsob využívá sdíleného klíče tzv. SSID, který je zaslán s požadavkem na přístup do sítě klientskou stanicí.

RSNA [9]

Rozšíření bezpečnosti implementací nových protokolů a algoritmů zvyšujících odolnost proti narušení sítě útočníkem, a to vylepšením autentifikace, integrity i šifrování. Podle použitých mechanismů šifer a protokolů se tyto nové mechanismy označují WPA a WPA2.

TKIP (Temporary Key Integrity Protocol) [9][20] – Použit v zabezpečovacím mechanismu **WPA**. Vylepšuje WEP kombinováním tajného klíče a inicializačního vektoru ještě před zpracováním v **RC4**. Používá dynamický klíč, který se mění v čase. Dále implementuje TKIP novou 64-bitovou kontrolu integrity a **PSK** (Pre-Shared Key) označován jako osobní režim, který implementuje 256 bitový klíč.

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol) [9][20] – Použit v zabezpečovacím mechanismu **WPA2** poskytující pokročilý stupeň zabezpečení. Zajišťuje autentifikaci, integritu, šifrování a ochranu proti útokům. Protokol CCMP je založen na 128-bitové blokové šifře **AES** (šifra Rijndael, 128-bitový klíč, 128-bitové bloky). Kontrola integrity je prováděna CBC-MAV s využitím MIC (Message Integrity Code).

BIP (Broadcast/Multicast Integrity Protocol) [9] – Protokol kontroly integrity a ochrany proti útoku zahlcení sítě pro skupinové adresování.

SAE (Simultaneous authentication of equals) [9] – Autentifikace při komunikaci s použitím hesla.

EAP (Extensible Authentification Protocol) – Autentizační metoda definující formáty zpráv pro přenos a používání klíčů.

3.3.1. Bluetooth (IEEE 802.15) [7]

Primární systémová ochrana proti kybernetickému napadení je založena na tzv. Secure Simple Pairing, který využívá párovací algoritmus s šestnáctimístným párovacím kódem (PIN), avšak pro starší zařízení je použit fixní čtyřmístný párovací kód bez algoritmu.

Secure Simple Pairing používá šifrovací algoritmus Diffie-Hellman založený na eliptických křivkách (ECDH). Ten vnáší silnou entropii do přenosu a zamezuje odposlechu i tzv. Man-In-The-Middle, tedy připojení k podvodnému zařízení namísto požadovaného. Šifrování dat je realizováno proudovou šifrou E0.

4. Zhodnocení bezpečnosti komunikačních systémů

Popsané bezdrátové komunikační systémy a jejich zabezpečení je pouze systémové a jeho bezpečnost je založena na základním předpokladu, důvěryhodnosti poskytovatele služeb (mobilní operátor, internetový provider), který má přístup i k citlivým informacím a zabezpečovacím mechanismům.

Pro zachování vysokého stupně zabezpečení je nutné základní systémové zabezpečovací mechanismy doplnit o pokročilé metody a techniky zabezpečení, které i při prolomení systémového zabezpečení použitého komunikačního systému poskytnou požadovanou ochranu citlivých dat a neprolomitelnost použitého doplňkového zabezpečení.

Šifrování komunikace v síti mobilních komunikací se zabývají i české firmy a v nabídce ochrany choulostivých informací jsou jak softwarové aplikace založené na OS Android, Symbian i pro platformu Java tak i přímo speciální uživatelské zařízení (mobilní telefony) případně externí paměťové karty s integrovaným šifrovacím softwarem. Mezi takovéto společnosti a produkty patří SAFECOM, CircleTech, Vertu, Probin. V těchto případech je ovšem nutné, aby měli obě strany zařízení podporující

daný způsob šifrování. Hlasové hovory jsou pak přenášeny jako VoIP (Voice over IP), tedy formou datových paketů, namísto běžně přenášených hlasových hovorů formou přepojování okruhů.

Pro zajištění ochrany tedy není vhodné spoléhat pouze na základní systémové zabezpečení, ale doplnit jej o zašifrování přenášených dat ještě před samotným přenosem používaným komunikačním systémem.

Návrh šifrovacího algoritmu uživatelských dat je pak vhodné vyvinout přímo na míru podle daného způsobu komunikace, množství přenášených dat a dalších individuálních potřeb.

Dalším aspektem podílejícím se na bezpečnosti je zajištění bezpečnosti fyzických segmentů sítě a lidských faktorů.

Pokud vezmeme v úvahu historické souvislosti, tak se osvědčil postup použití zcela „nového“ jazyka, nijak nesouvisejícího s jazykem, v němž komunikují subjekty, jak tomu bylo za druhé světové války v americké armádě a tzv. kódu Navajo. Pak není možné najít jakoukoliv souvislost se zašifrovaným slovem a jeho nešifrovanou podobou. V současné době jsou ovšem přenášena data (binární) a ne přímo písmena či znaky, proto je vhodné pro přenos použít více cest a více zdrojů, jejichž správnou kombinací (kterou znají pouze autentifikovaní uživatelé) lze získat původní zprávu.

REFERENCE

[1] Halonen, T., and et. All, GSM, GPRS and EDGE Performance: Evolution towards 3G/UMTS, 2nd Edition, UK: J. Wiley & Sons , 2003.

[2] 3GPP; Technical Specification Group Radio Access Network; Physical Layer – General Description (Release 11). 3GPP TS 25.201 v11.1.0, December 2012.

[3] 3GPP; Technical Specification Group Radio Access Network; User Equipment (UE) radio transmission and reception (FDD) (Release 11). 3GPP TS 25.101 v11.6.0, August 2013.

[4] Prokopec, J. Systémy mobilních komunikací: Sítě pro mobilní datové služby. VUT v Brně, Brno: 2012, 186 stran.

[5] 3GPP; Technical Specification Group Radio Access Network; High Speed Downlink Packet Access (HSDPA); Overall description; Stage 2(Release 11). 3GPP TS 25.308 v11.6.0, September 2013.

[6] 3GPP; Technical Specification Group Radio Access Network; High Speed Packet Access (HSPA) evolution; Frequency Division Duplex (Release 7). 3GPP TR 25.999 v7.1.0, March 2008.

[7] IEEE standard 802.15.1, Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specification for Wireless Personal Area Networks (WPANs), USA, June 2005.

[8] Specification of the Bluetooth System, Master Table of Contents & Compliance Requirements; covered core Package version 4.0, June 2010.

[9] IEEE standard 802.11, Wireless LAN Medium Access Control (MAC) and Physical Layer Specification, USA, March 2012.

[10] IEEE standard 802.11a, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification: High-Speed Physical Layer in the 5 GHz Band, USA, June 2003.

[11] IEEE standard 802.11b, Wireless LAN Medium Access Control (MAC) and Physical Layer Specification: Higher-Speed Physical Layer Extension in the 2.4 GHz Band, USA, September 1999.

[12] IEEE standard 802.11g, Wireless LAN Medium Access Control (MAC) and Physical Layer Specification; Amendment 4: Further Higher Data Rate Extension in the 2.4 GHz Band, USA, June 2003.

[13] IEEE standard 802.11n, Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification; Amendment 5: Enhancements for Higher Troughput, USA, September 2009.

[14] 3GPP; Technical Specification Group Services and System Aspects; Security Related Network Functions (Release 12). 3GPP TS 43.020 v12.0.0, March 2013.

[15] 3GPP; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/3 Encryption Algorithms for GSM and ECDS, and the

GEA3 Encryption Algorithm for GPRS; Document 1: A5/3 and GEA3 Specification (Release 11). 3GPP TS 55.216 v11.0.0, September 2012.

[16] 3GPP; Technical Specification Group Services and System Aspects; 3G Security; Specification of the A5/4 Encryption Algorithms for GSM and ECDS, and the GEA4 Encryption Algorithm for GPRS (Release 11). 3GPP TS 55.226 v11.0.0, September 2012.

[17] 3GPP; Technical Specification Group Services and System Aspects; 3G Security; Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 1: f8 and f9 specification (Release 11). 3GPP TS 35.201 v11.0.0, September 2012.

[18] Boman, K., and et. All, "UMTS Security", Electronics & Communication Engineering Journal, vol.14, no.5, October 2002.

[19] 3GPP; Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 11). 3GPP TS 33.102 v11.5.1, June 2013.

[20] IEEE standard 802.11i, Wireless LAN Medium Access Control (MAC) and Physical Layer Specification; Amendment 6: Medium Access Control (MAC) Security Enhancements, USA, July 2004.