SOUHRNNÁ INFORMACE
O STAVU KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE
A PŘEDOPKLADY JEJÍHO ZAJIŠTĚNÍ NA OBDOBÍ 2011- 2015

KYBERNETICKÁ BEZPEČNOST[1]: PRIORITA BEZPEČNOSTI ČR

Trvale stoupá objem a důležitost zpracovávaných, přenášených, sdílených a uchovávaných dat. Data a systémy na jejich zpracování představují aktiva velké hodnoty pro jejich vlastníky a uživatele. Počítačový průmysl je sám o sobě velmi dynamickou oblastí hospodářství řady zemí. Vážné narušení počítačového průmyslu by negativně ovlivnilo celosvětové hospodářství.

V moderní společnosti je téměř vše, od zdravotnictví, přes dopravu a bankovnictví, až po vojenské složky, závislé na počítačových sítích. Kyberprostor – virtuální svět v prostředí počítačových sítí – umožňuje chod světa reálného: hospodářství, veřejného i soukromého sektoru, a usnadňuje život lidí vůbec. Internet je využíván nejenom jako pracovní nástroj, ale stává se součástí každodenního života moderního člověka.

Stále větší část mezilidské komunikace, která se v předchozí době byla zajišťována formou přímých telefonních hovorů, cestou listovní komunikace, nebo přímým kontaktem, je nahrazována komunikací virtuální (e-mail, sociální sítě atd.). Dochází k masovému využívání mobilní komunikace a bezdrátových přenosů dat. V kyberprostoru se odráží veškeré společenské aktivity, vznikají zde virtuální komunity, do značné míry nezávislé na reálném světě a postrádající elementární pravidla chování.

Snahou vlád moderního světa je vytváření rovných podmínek a příležitostí pro začlenění všech skupin obyvatel do společnosti. Nové technologie znamenají příležitost pro vytváření moderní a efektivní veřejné správy. Hovoří se o tzv. konceptu e-Inclusion, tedy o využití technologií pro realizaci principu rovnosti příležitostí. Dosažení ”informační gramotnosti” může být pro sebevíc znevýhodněné skupiny obyvatel (např. v závislosti na věku, zdravotním stavu, odlehlosti místa pobytu atd.) prostředkem k uplatnění na trhu práce.

[1] Pojem „kybernetická bezpečnost“ je v rámci dokumentu chápán jako pracovní zastřešující termín, který se v žádném ohledu neomezuje např. pouze na problematiku vojenství (není např. chápán jako synonymum termínu „kybernetická obrana“, „Cyber Defence“, CD).

Banky ve stále větší míře přecházejí na stále složitější počítačové zpracování finančních operací. Stále běžnější je používání Internetu i pro finanční operace. Mohutný rozmach prožívá domácí elektronika, která může být propojena s počítači a jejich periferiemi. Mobilní telefony, herní konsole, televizní přijímače jsou dnes terminálem celé řady služeb, ještě donedávna přístupných pouze prostřednictvím výpočetní techniky.

Poskytování řady služeb souvisí s požadavkem na trvalou dostupnost, tj. nepřetržitost, spolehlivost služby (fungování energetických sítí, připojení k Internetu). Nárůst používání konkrétních technologií v denním životě společnosti přímo souvisí s frekvencí jejich zneužívání. Stále větší část kriminální a neetické činnosti se orientuje na zneužití vyspělých informačních a komunikačních technologií. Počet činů, při kterých je užita vyspělá technologie, nebo činů, které jsou proti takové technologii zaměřeny, stoupá, a bude stoupat i nadále. Trvale se zvyšuje závažnost těchto incidentů, počet jejich obětí a objem materiálních ztrát jimi způsobených.

S tím, jak stále více údajů je uloženo v informačních a komunikačních systémech (a roste povědomí o jejich ceně), roste zájem zločinců o obsah těchto nosičů informací (např. útoky na různé finanční instituce, na ”elektronické obchody”, krádeže zdravotních záznamů).

Samotný princip, na kterém je kyberprostor postaven, vytváří podmínky pro to, aby útočníci byli vždy o krok napřed před obránci. Pod pojmem útočník se můžou skrývat útočníci s různou motivací:

- Amatéři s touhou dokázat si, že umí zaútočit na nějaký informační systém
- Odborníci s ekonomickou motivací – často ve službách organizovaného zločinu
- Odborníci s ideologickou motivací – prosazující náboženské, politické a podobné zájmy
- Odborníci ve službách státu – kyberšpionáž, armádní jednotky pro kybernetický boj apod.

Moderní technologie se vyznačují vlastnostmi, které znamenají nejenom výhodu pro uživatele, ale i pro útočníky s nepoctivými úmysly. Tyto technologie například:

- Umožňují globální dostupnost. To zvětšuje vzdálenost mezi útočníkem a napadeným, a umožňuje, aby útočník uskutečňoval svou činnost ze vzdáleného místa. Rovněž je možné, aby členové útočící skupiny byli v neustálém kontaktu, i když se nacházejí v různých částech světa.
- Jsou rychlé. To umožňuje útočníkům velmi rychle přenášet (kopírovat, ničit, pozměňovat) velké objemy dat.
- Zajišťují značnou míru anonymity. V obrovském množství zpráv přenášených elektronickými médii je navíc velmi nízká pravděpodobnost zachycení konkrétní zprávy, pokud není o okolnostech jejího zaslání nic předem známo.
- Jsou relativně levné a jejich používání je snadné. Ceny výpočetní techniky neustále klesají, a tak jsou dosažitelnější pro stále širší skupinu obyvatel. Ovládání takové techniky je stále více uživatelsky vstřícné a nevyžaduje zvláštní vzdělání a zkušenosti.
- Nastolují značnou asymetrii mezi ”útočníky” a ”obránci”. Útočník je tím, kdo volí cíl, okamžik a metodu útoku. Přitom zpravidla směřuje k tomu, aby s minimální snahou docílil maximálního efektu. Opatření, která by útok proti kybernetickým systémům ztížila, jsou oproti tomu velmi nákladná.

Kyberkriminalita bývá označována za typickou kriminalitu ”bílých límečků”, tedy osob, pro které je mnohem jednodušší nelegální činnost v kyberprostoru, než například páchání kriminality v ”reálném světě”. Zde bezúhonná osoba může v kyberprostoru páchat závažnou trestnou nebo neetickou činnost.

Nelegálních aktivit v kybernetickém prostředí je obecně odhaleno jen velmi malé procento. Poměr mezi spáchanými a odhalenými incidenty může podle některých expertů činit až 20 000 : 1. Mnoho institucí neohlásí útok z obavy ze ztráty prestiže, případně z obavy před odlivem klientů, to platí zejména pro finanční ústavy.

V souvislosti s trvale se zvyšující potenciální zranitelností moderní společnosti je třeba zmínit skutečnost, že za posledních 20 let řada společností zavedla systémy ”Digital Control Systems” (DCS) a ”Supervisory Control and Data Acquisition Systems” (SCADA). Ty slouží ke kontrole klíčových procesů a funkcí kyberprostoru, jež bylo do té doby třeba vykonávat ručně. DCS a SCADA slouží ve vodohospodářství, dopravě, energetice, zdravotnictví apod. Podíl Internetu na celkovém objemu přenosu řídících informací mezi stroji stoupá a stále bude stoupat. Takto přenesené informace jsou tudíž náchylnější ke zneužití. Kolaps řídicích systémů SCADA by znamenal i pro ”nekybernetické” části kritické infrastruktury nedozírné následky. Útočník by mohl převzít kontrolu nad klíčovými a vzájemně propojenými součástmi kritické infrastruktury (přehrady, vodovody, energetika, klimatizace v tunelech, letecká doprava a doprava vůbec, družicové systémy, jaderná zařízení, armádní systémy atd.), a touto cestou buď vydírat konkrétní oběť, organizaci, stát nebo přímo způsobit ztráty na životech a na majetku.

Zřejmý je i možný dopad kybernetického incidentu na finanční sektor (nefungují bankomaty a bezhotovostní platby, klesne důvěra v bankovní služby, burzy, pojišťovnictví atd.). Kybernetický útok velkého rozsahu by zároveň zpravidla omezil možnost využívat telekomunikační síť, včetně služeb tísňového volání.

Závažnější incident, uskutečněný v kyberprostoru, by mohl znamenat nemalé ”snížení kvality života” moderní společnosti, v extrémním případě i konec moderního způsobu života v dnešním smyslu slova s hospodářskými a politickými dopady. Lze konstatovat, že útoky prostřednictvím počítačových sítí představují hrozbu, srovnatelnou s účinky zbraní hromadného ničení.[2]

Významný aspektem je již zmíněná asymetrie kybernetického útoku, kdy několik málo specialistů může s relativně malými náklady poškodit hospodářství technicky vyspělého státu natolik, že si jeho obnova může vyžádat roky. Bez ochrany kyberprostoru ztratí efekt další dílčí bezpečnostní strategie. Případný katastrofický scénář by s vysokou pravděpodobností znamenal ohrožení základních civilizačních výdobytků (kolaps komunikačních a informačních sítí, komplikace pro finanční služby a další služby, u kterých je požadována spolehlivost, respektive de facto všechny aktivity, „řízené počítačem“).

[2] viz Lisabonský summit NATO v listopadu 2010.

Skutečnost, že kybernetický útok může zasáhnout mnoho obětí na řadě míst světa najednou bez ohledu na geografickou polohu (přičemž přírodní překážky a vzdálenost zde nehrají roli), a zapříčinit tak dalekosáhlé dopady na reálný svět, činí takový scénář přitažlivý nejen pro teroristické skupiny, ale i pro nezávislé jednající vyděrače.[3]

Již dnes řada států intenzivně studuje potenciál informační války. Pro některé země přitom hraje klíčovou roli zjištění, že jejich síly by jen stěží mohly uspět ve standardním vojenském střetu s nejvyspělejšími státy světa (např. zeměmi Severoatlantické aliance). Proto ubírají své aktivity směrem k možnostem boje v kyberprostoru. Informační válku je možné označit za specifickou (personálně a materiálně relativně nenáročnou, lacinou) asymetrickou strategii, kdy nezjištěný[4] nebo překvapivý útok prostřednictvím Internetu může podkopat obranyschopnost o poznání silnějšího a "bohatšího" protivníka. Uvedený aspekt je sledován i v rámci nadnárodních vojenských struktur, včetně Severoatlantické aliance. V rámci Aliance byl vybudován tzv. Center of Excellence for Cyber Defence (CoECD), umístěnýv Estonsku.[5]

Kyberprostor se také stal ideálním prostředím pro už vyzkoušené metody informačního boje. Ty jsou se stále vzrůstající frekvencí využívány ve vnitrostátním i mezinárodním kontextu (psychologické či dezinformační operace, zaměřené na modifikaci smýšlení širokých mas, během volebního boje apod.). To poskytuje řadu možností extremistickým a teroristickým skupinám i jednotlivcům:

- Rychlé a skryté utajené komunikace s anonymní identitou (vzájemná výměna informací a pokynů).
- Šíření propagandy, získávání a mobilizace nových aktivistů, sympatizantů či sponzorů; obhajoba a podněcování páchání kriminálních činů.

[3] Je třeba podotknout, že stále rostoucí propojenost světa a vzájemná závislost všech složek moderní civilizace, omezuje do nemalé míry možnost státy iniciovaných kybernetických útoků. Dokonce i tzv. "zločinné státy" jsou do té míry zapojeny do globálních počítačových sítí, že kolaps světových finančních trhů, který by masový kybernetický útok patrně způsobil, by negativně dopadl i na ně. Uvedená skutečnost by však nemusela odradit nestátní aktéry, jako jsou nadnárodní teroristické skupiny. Jim mohou být výkyvy světové ekonomiky lhostejné, respektive právě o ně mohou usilovat.

[4] Vojenská operace v kyberprostoru zpravidla nestojí o publicitu.

[5] V říjnu 2008 toto pracoviště získalo plnou akreditaci Severoatlantické aliance. Případné zapojení České republiky do fungování nově budovaného střediska v Estonsku je třeba ještě diskutovat na meziresortní úrovni.

- Získávání informací všeho druhu, včetně údajů o potenciálních cílech útoku.

Internet a moderní informační a komunikační technologie jako celek umožňují různým zájmovým skupinám (extremistům, teroristům, organizovanému zločinu) vytváření globálních organizačních sítí nového typu. Takové struktury mohou být, na rozdíl od ”tradičních skupin”, volnější, méně hierarchické. Jednotlivé teroristické buňky mohou být po všech stránkách autonomní, a zároveň připravené ke společné akci. Internet zároveň propojuje různé názorové skupiny (politicky, nábožensky či etnicky motivovaní extrémisté, respektive teroristé) a umožňuje jejich presentaci a vzájemnou konfrontaci. Vytváří tak ideální prostředí pro vyhrocení tzv. ”střetu civilizací”. Tyto organizace se stahují do pro ně „ bezpečného“ kyberprostoru, tzn. Špatně chráněného kyberprostoru.

DOSAVADNÍ KONCEPČNÍ MATERIÁLY, ZABÝVAJÍCÍ SE TÉMATEM KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Vláda České republiky se ve snaze maximálně využít potenciál moderních informačních a komunikačních technologií rozhodla nově definovat cíle státu v oblasti tzv. informační společnosti a v oblasti telekomunikací a formulovat novou strategii státu pro nadcházející období. Na rozdíl od původního přístupu, kdy byly koncepce v obou oblastech zpracovány samostatně (formou dokumentů ”Státní informační politika: cesta k informační společnosti” a ”Národní telekomunikační politika”), se vláda rozhodla respektovat úzkou provázanost a všeobecný trend konvergence obou těchto oblastí. V roce 2004 tak bych schválen strategický a koncepční dokument s názvem ”Státní informační a komunikační politika e-Česko 2006”.[6] Samotným názvem materiálu vláda reflektuje také přeměnu někdejšího oboru *telekomunikací* na *elektronické komunikace*.

V uvedeném kontextu byly stanoveny čtyři prioritní oblasti vládních aktivit:

- Dostupné a bezpečné komunikační služby.
- Informační vzdělanost.
- Moderní veřejné služby on-line.
- Dynamické prostředí pro elektronické podnikání.

S cílem posílení informační bezpečnosti v oblasti komunikační a informační infrastruktury České republiky a v souladu s § 4 odst. 1 písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy, jsou zpracovávány návrhy strategických dokumentů v oblasti ochrany Informačních systémů veřejné správy České republiky (ISVS ČR), a to i z hlediska jejich možného ohrožení teroristickým útokem.

[6] Přitom je však třeba konstatovat, že žádný z uvedených materiálů neřeší problematiku možných hrozeb komplexně, ale soustřeďuje se pouze na určité dílčí kroky v oblasti zajišťování kybernetické bezpečnosti, bez úsilí o vytvoření programu studia a analýz možných nebezpečí, o nějž by bylo vhodné jakékoli dílčí kroky odvíjet.

Jedná se zejména o následující dokumenty:

- ”Národní strategie informační bezpečnosti České republiky”, která stanovuje úkoly v oblasti vytváření důvěryhodných informačních a komunikačních systémů v podmínkách České republiky a na ní navazující ”Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky” (schválen usnesením vlády č. 677 z roku 2007).
- Návrh nařízení vlády k realizaci úkolů stanovených ”Národní strategií informační bezpečnosti České republiky” ze strany orgánů a organizací veřejné správy a subjektů kritické infrastruktury.
- ”Koncepce přenosu klasifikovaných informací komunikační infrastrukturou veřejné správy České republiky”, který reaguje na trvale se zvyšující požadavky přenosu určitých, zvlášť chráněných, informací stanovených právními předpisy.[7] Dokument navrhuje řešení prostřednictvím integrace informačních systémů do univerzálně použitelného bezpečného komunikačního systému veřejné správy, s přístupem do sítí ostatních zemí Evropské unie.
- ”Bezpečnostní politika přenosu klasifikovaných informací komunikační infrastrukturou veřejné správy České republiky”, popisující, v souladu s usnesením Bezpečnostní rady státu ze dne 18. listopadu 2003 č. 84, bezpečnostní cíle komunikační infrastruktury veřejné správy a způsoby jejich dosažení, stejně jako základní řídící struktury systému, jejich roli a oblast odpovědnosti při prosazování uvedených bezpečnostních principů. Obsah dokumentu je koncipován tak, aby výsledný systém vyhovoval bezpečnostním požadavkům komunikačního systému Evropské unie S-TESTA a informačních systémů krizového řízení České republiky.
- Novela zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů (zákon č. 439/2004 Sb.), §13, odstavec 2, který hovoří o tom, že správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.

[7] Množství těchto předpisů a nejednotnost jejich výkladu vede k projekci a realizaci řady účelově orientovaných a aplikačně závislých systémů.

- ”Návrh úrovní zabezpečení informačních systémů nezbytných pro chod kritické infrastruktury České republiky”. Na základě zadání, vyplývajícího z usnesení Bezpečnostní rady státu ze dne 27. května 2003 č. 59, předložilo v roce 2004 Ministerstvo informatiky úvodní studii citovaného materiálu, která přibližuje strategické požadavky na technické řešení zadání a požadavky na součinnost mezi resorty. Ministerstvo informatiky, ve spolupráci s Národním bezpečnostním úřadem, vyvíjelo činnost v oblasti ujednocení systému bezpečnostní klasifikace informací a následně přiřazení požadavku na zajištění odpovídajícího stupně bezpečnostní odolnosti jednotlivým informačním a komunikačním systémům nebo subsystémům.
- Informace klasifikované do kategorie utajovaných informací (viz zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti) jsou v České republice v současné době zpracovávány v několika desítkách informačních systémů, z nichž část je realizována jako systémy samostatných osobních počítačů bez síťového propojení, část zahrnuje lokální počítačové sítě (LAN) bez propojení s jinými sítěmi a část je realizována jako rozlehlé počítačové sítě (např. propojení několika LAN v různých lokalitách, propojení se zastupitelskými úřady ČR v zahraničí atd.).[8] Česká republika je napojena i na systémy, propojující členské země Evropské unie (Extranet, COREU, BdL) a NATO (Cronos, Minerva) a další mezinárodní organizace. Ve všech těchto případech je zajištěna adekvátní ochrana utajovaných informací a systémů samotných, v souladu s výše uvedeným zákonem a k němu příslušnými vyhláškami. Jednotlivé systémy jsou certifikovány Národním bezpečnostním úřadem, přičemž podmínkou pro vydání certifikátu je i zajištění ochrany komunikace certifikovanými kryptografickými prostředky a ochrana systému před útoky z externího prostředí. Součástí ochrany je vždy i antivirová ochrana. Možnost teroristického útoku kybernetickými prostředky nebo běžného napadení uvedených systémů je v zásadě eliminována. Mezi

[8] Nakládání s utajovanými informacemi se v České republice řídí následujícími právními předpisy: zákon č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti; vyhláška č. 523/2005 o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínících komor, vyhláška 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací, vyhláška 525/2005 o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací, vyhláška 528/2005 o fyzické bezpečnosti a certifikaci technických prostředků.

zbytková ohrožení jsou zařazena také ohrožení, související s působením hrozeb typu živelní pohroma a útok hrubou silou. Odpovídající ochrana proti tomuto riziku je těžko realizovatelná, neboť by se neobešla bez vysokých investičních nákladů a narážela by i na stavební omezení (památková ochrana objektů apod.).

- Otázce informační bezpečnosti se věnuje i „Bezpečnostní strategie České republiky“, která konstatuje, že „rozsáhlé úniky strategicky důležitých informací či zásahy do informačních systémů státních institucí nebo podniků a společností, které zajišťují základní funkce společnosti a státu, mohou ohrozit nejen strategické, ale i životní zájmy České republiky“.
- Aspektu e-Governmentu se aktuálně věnuje dokument „Strategie rozvoje pro informační společnost“, který operuje s následující vizí: Vláda vytýčila základní směřování ke zkvalitňování veřejné správy ve strategii efektivní veřejná správa a přátelské veřejné služby (Smart Administration). Materiál navazuje na analytické poznatky této strategie, rozvíjí a specifikuje její cíle v oblasti podpory e-Governmentu a racionalizuje využívání informačních a komunikačních technologií ve veřejné správě. Budování e-Governmentu a rozvoj služeb pro informační společnost není izolovaným úkolem. Úzce souvisí s racionalizací procesů a zaváděním moderních manažerských nástrojů ve veřejné správě, stejně jako se zkvalitňováním tvorby politik a právního prostředí. Tato vize rovněž hovoří o tom, že Česká republika se chce stát jedním z pěti nejlepších členských států Unie, co se týče zavádění principů e-Governmentu.

Dopad výše uvedených strategických dokumentů na bezpečnostní prostředí České republiky je zatím velmi nevyvážený. Dosud se úspěšně dařilo vyřešit spíše konkrétní respektive technologické aspekty problematiky, nikoli její směřování jako celku.

- Dokument ”Národní strategie informační bezpečnosti České republiky” byl v kontextu kompetenčních změn (zániku Ministerstva informatiky) opakovaně přehodnocován, avšak do současnosti nebyla řada jím stanovených úkolů

splněna (například co se týče problematiky vybudování vládního pracoviště typu CERT).

- Zatím není dořešena problematika definice Kritické informační infrastruktury
- V České republice rovněž nebylo jednoznačně stanoveno, který subjekt definuje závazné bezpečnostní požadavky pro informační systémy, ve kterých jsou provozovány vnitrostátní neutajované databáze.

Rámec úkolů Ministerstva vnitra v oblasti boje proti kybernetickým incidentům stanovilo usnesení vlády České republiky ze dne 23. října 2000 č. 1044, k dokumentu "Aktualizovaná koncepce boje proti organizovanému zločinu". Jeho prostřednictvím bylo Ministerstvu vnitra uloženo "*průběžně koncepčně řešit potírání organizovaných zločineckých aktivit v oblasti informačních technologií*".

Z tohoto důvodu byl v roce 2001 vypracován a schválen materiál "Koncepce boje proti trestné činnosti v oblasti informačních technologií", vycházející z konkrétních poznatků policejní práce v příslušné oblasti. Z nejdůležitějších úkolů z *Harmonogramu opatření* zmíněného materiálu je třeba zmínit následující:

- Zajistit podmínky pro další rozvoj (včetně materiálního a personálního posilování) struktur, přímo zapojených do potírání informační kriminality.
- Rozšiřovat a podporovat spolupráci policejních orgánů se zpravodajskými službami a nevládními neziskovými subjekty, zabývajícími se problematikou boje proti některým aspektům informační kriminality.
- Vypracovat principy plánu ochrany státních a některých strategicky důležitých nestátních informačních systémů.
- Vypracovat projekt hlásného systému pro trestnou činnost v oblasti informačních technologií.
- Iniciovat vznik a podporovat činnost sdružení kvalifikovaných odborníků, informujících ostatní zainteresované aktéry o bezpečnostních problémech a reagujících na probíhající útoky.
- Vypracovat projekt vzdělávání a doškolování orgánů činných v trestním řízení, s důrazem na objasňování trestné činnosti v oblasti informačních technologií (včetně přípravy výukových materiálů).

- Vyvíjet a zavádět forenzní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení.
- Podporovat nezávislou výzkumnou, publicistickou a dokumentaristickou činnost, zabývající se kybernetickými incidenty.
- Provádět osvětu a propagaci náležitého chování nejširší i odborné veřejnosti, související s bojem proti informační kriminalitě.
- Sledovat aktivity mezinárodních a nadnárodních organizací v oblasti boje proti trestné činnosti v oblasti informačních technologií. Aktivně se zúčastňovat mezinárodních akcí, týkajících se boje proti informační kriminalitě.

Podobně jako zmíněné dokumenty, i výše jejich uvedených ambicí byly naplněny jen částečně.

HLAVNÍ ÚKOLY K ŘEŠENÍ KYBERNETICKÉ BEZPEČNOSTI V ČESKÉ REPUBLICE

Ačkoli kybernetická spolu s informační bezpečností je bez nadsázky jednou z klíčových témat současnosti, tato problematika není v rámci České republiky komplexně řešena. Vzhledem k tomu, že veřejnou moc lze uplatňovat výlučně na základě a v mezích zákona a naopak soukromým osobám lze ukládat povinnosti pouze zákonem, se jeví dlouhodobé spolehnutí se na více či méně dobrovolné formy spolupráce nebo dokonce vnitřní organizace nejen státních, ale i soukromoprávních subjektů jako nedostatečné. V souvislosti s tím je nutno mimo jiné:

1. Deklarovat finanční a lidské zdroje, které se budou efektivně podílet na eliminaci kybernetických hrozeb v ČR a v návaznosti na plnění úkolů v rámci EU a NATO.[9]
2. Provést „audit“ aktuálně platné legislativy, související s otázkami kybernetické bezpečnosti a navrhnout její změny, doplnění.
3. Provést „audit“ norem souvisejících s kybernetickou bezpečností a zajistit jejich implementaci do informačních systémů veřejné správy a systémů kritické infrastruktury.
4. Vybudovat síť pracovišť typu CERT a posílit a zefektivnit tak detekci a reakce při řešení kybernetických incidentů. Cílem je také zefektivnění možností represe.
5. Využít možnosti delegace některých aktivit (např. Národní CSIRT).
6. Definovat kritickou informační infrastrukturu (vytvořit přehled subjektů, spadajících do kritické informační infrastruktury, detailně vymezit rozsah působnosti v této oblasti mezi ústředními orgány státní správy).
7. Aktivně se zapojit do mezinárodní spolupráce a výměny informací v oblasti kybernetické bezpečnosti.
8. Zajistit trvalé zvyšování úrovně povědomí široké veřejnosti o kybernetických hrozbách. Zajistit také trvalé zvyšování odborné úrovně v této oblasti u všech zainteresovaných složek – orgány činné v trestním řízení, vedoucí pracovníci,

[9] V souvislosti s budováním kybernetické obrany v ČR a v rámci NATO

techničtí pracovníci. Zavést systém vzdělávání v oblasti kybernetické bezpečnosti na všech stupních škol.

9. Zajistit travlou spolupráci se soukromou a akademickou sférou

Téma je o to více aktuální, protože probíhá celá řada kroků v oblasti přibližování veřejné správy občanům pod heslem „rychle, levně, spolehlivě“ (vytváření tzv. Czech Pointů, respektive celosvětově jedinečný projekt tzv. datových schránek). Všechny tyto kroky by mohly být jediným závažnějším incidentem znevěrohodněny a trvalo by roky, než by se podařilo důvěru veřejnosti znovu získat.

Mezi nejvíce zainteresovanými subjekty (Ministerstvo vnitra, Ministerstvo obrany, Ministerstvo zahraničí, Národní bezpečnostní úřad, Český telekomunikační úřad, zpravodajské služby) bylo dosaženo shody o tom, že uvedené otázky zasluhují prioritní pozornost.

Existující kapacity jednotlivých subjektů veřejné sféry v rámci České republiky sice v řadě ohledů drží krok se světovým standardem (co se týče teoretického a expertního přístupu), přesto v této oblasti existuje nemalý potenciál pro zlepšení.

PERSPEKTIVA ŘEŠENÍ AKTUÁLNÍ SITUACE V ČESKÉ REPUBLICE

Je třeba akceptovat skutečnost, že kybernetické hrozby se staly latentní, trvalou a všudypřítomnou hrozbou ohrožující celou společnost.

Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí České republiky. Ochromení počítačových sítí, jako jednoho z klíčových prvků kritické infrastruktury, by znamenalo řadu vážných důsledků, mohlo by například oslabit důvěru veřejnosti nejenom například v koncept e-Govermentu, ale ve schopnost státu zajistit standardní chod systémů potřebných pro život. Vyloučit nelze ani ztráty na životech, zapříčiněné politicky či jinak motivovanými.

Je třeba zdůraznit, že se jedná o interdisciplinární problém, zahrnující nejenom oblast technologickou, ale i sociální, psychologickou a právně-legislativní. Nedílnou součástí posílení kybernetické bezpečnosti České republiky je přitom aspekt bezpečnosti při respektování ochrany základních svobod uživatelů Internetu.

Jedině při překlenutí existujících slabin bude možné dostát ambicím České republiky v oblasti zavádění moderních informačních a komunikačních technologií a čelit aktuálním bezpečnostním výzvám XXI. století.[10]

[10] Viz „ Akční plán pro oblast kybernetické bezpečnosti ČR“.

Současný stav kybernetické bezpečnosti ve světě

Globální charakter ICT má z hlediska kybernetické bezpečnosti za důsledek, že okolím daného systému je celá globální ICT, a tedy k zajištění bezpečnosti vlastního systému nestačí jen lokální opatření, ale je třeba zvýšit bezpečnost celé ICT. Tento problém již nemá čistě technický charakter, ale stává se globálním problémem, řešeným na národní i mezinárodní úrovni. Podstatu kybernetické bezpečnosti dobře vystihují směrnice Guidelines for the Security of Information Systems, vydané OECD v červenci 2002, které zdůraznily, že je třeba podporovat vývoj bezpečnostní kultury, tj. soustředit se na bezpečnost při vývoji informačních systémů a sítí a osvojit si nové způsoby myšlení a chování při používání informačních systémů a sítí. Směrnice postuluje 9 základních principů, z nichž je třeba vycházet při řešení kybernetické bezpečnosti systémů. (Z těchto principů vychází a podrobnější jejich rozpracovává mezinárodní standard ISO / IEC 27001 a podobné principy obsahují i několik mezinárodní / národní metodické dokumenty.).

1. Bezpečnostní povědomí (awareness). Všichni zúčastnění [11] by si měli uvědomovat potřebu kybernetické a informační bezpečnosti a také toho co mohou udělat pro zlepšování bezpečnosti.

2. Odpovědnost (responsibility). Všichni zúčastnění jsou zodpovědní (přiměřeně úkolům, které v systému plní) za bezpečnost informačních systémů a sítí.

3. Reakce (response). Zúčastnění by měli jednat rychle a koordinovaně aby zabránili vzniku bezpečnostního incidentu, včas ho odhalili a adekvátně na něj odpověděly.

4. Etika (ethics). Zúčastnění by měli respektovat legitimní zájmy ostatních.

5. Demokracie (democracy). Bezpečnost informačních systémů a sítí by měla být kompatibilní se základními hodnotami demokratické společnosti, tj. musí být zachována svoboda myšlení, výměny idejí, volného toku informací, důvěrnosti informace a ochrany osobních údajů.

[11] pod zúčastněnými Směrnice OECD chápou tvůrce, majitele, správce a uživatele informačních systémů a sítí

6. Odhad rizik (risk assessment). Zúčastnění by měli provádět analýzy rizik, a poukazovat na ohrožení a možné dopady na systém a přijmout řešení adekvátní zjištěným rizikům.

7. Návrh a implementace bezpečnosti (Security design and implementation).
Zúčastnění by měli chápat bezpečnost jako podstatný prvek informačních systémů a sítí; tj. bezpečnost systému je třeba zohlednit už ve fázi jeho návrhu, vybrat a implementovat vhodná bezpečnostní opatření, odpovídající hodnotám, které mají chránit.

8. Řízení (Security management). Zúčastnění by měli uplatňovat komplexní přístup k řízení kybernetické a informační bezpečnosti. Řízení kybernetické a informační bezpečnosti by mělo být založeno na analýze rizik, mělo by být dynamické a zahrnovat všechny úrovně činností lidí působících v systému a všechny aspekty jejich operací.

9. Přehodnocení (Reassessment). Dotčené subjekty by měly přehodnocovat bezpečnost informačních systémů a sítí a provádět nezbytné změny bezpečnostních politik, praktik, opatření a procedur, aby odpovídaly vyvíjejícím se a nově bezpečnostním hrozbám. Směrnice OECD nejsou závazným dokumentem a mají pouze charakter doporučení.

Hodnocení bezpečnosti a budování bezpečných systémů

Potřebnou úroveň kybernetické bezpečnosti nelze dosáhnout přijímáním ad hoc řešení, ale musí být uplatňován systematický přístup. Průkopníkem v oblasti kybernetické bezpečnosti byly USA. Americké Ministerstvo obrany prakticky iniciovalo konstituování kybernetické bezpečnosti jako samostatné oblasti prohlášením projektu na zabezpečení svých počítačů již v roce 1977. Druhou institucí, která sehrála významnou úlohu v kybernetické bezpečnosti, byl americký National Institute of Standards and Technology, NIST (dříve National Bureau of Standards, NBS), který se na základě zákona (Brooks Act, 1965) stal institucí

odpovědnou za návrh a vývoj federálních norem stanovujících podmínky pro výběr a používání výpočetní techniky. NIST se zaměřil na dva klíčové směry:

- Návrh norem pro počítačovou kryptografii

- Norem pro vytváření a hodnocení zabezpečených počítačových systémů.

V roce 1981 byla NSA pověřena zajištěním všech systémů v působnosti Ministerstva obrany USA a vzniklo Computer Security Center, které se později (1985) změnilo na National Computer Security Center (NCSC) zajišťující počítačové systémy federální vlády. CSC vypracovalo dokument Trusted Computer System Evaluation Criteria, známou jako Orange Book, která poskytovala kritéria pro hodnocení důvěryhodnosti (stupně zabezpečení) hodnoceného systému. Orange book byla první ze série publikací věnovaných zajištění systémů (Rainbow series) vydanou americkým Ministerstvem obrany. V roce 1987 byl přijat Computer security act, kterým byly redukovány pravomoci NCSC na oblast národních (klasifikovaných) systémů. Všechny ostatní systémy byly převedeny do pravomoci NIST, který v koordinaci s NSA odpovídá za zpracování norem a směrnic týkajících se zabezpečení počítačů ve všech oblastech kromě zpracování některých vojenských a zpravodajských informací. Významným krokem, posilujícím odpovědnost NIST za oblast kybernetické a informační bezpečnosti bylo přijetí Federal Information Security Management Act (FISMA) v roce 2002. Také další informačně vyspělé státy vytvářely podobná kritéria na budování a hodnocení bezpečných systémů (Kanada, Velká Británie).

Globalizace ICT a potřeba kompatibilních bezpečnostních řešení vedla k harmonizaci národních kritérií nejprve do podoby Information Technology Security Evaluation Criteria (ITSEC)[12] a později se do mezinárodního standardizačního projektu zapojily i USA a Kanada. Výsledkem byl mezinárodní standard ISO / IEC 15408, známý jako Commnon Criteria for Information Technology Security Evaluation. Common Criteria umožňují definovat bezpečnostní požadavky na vyvíjený systém. Jsou velmi rozsáhlé a neposkytují návody na řešení bezpečnostních

[12] Německo, Francie, Holandsko

problémů při provozu systémů. Těmto problémům je věnován mezinárodní standard ISO / IEC 27001, který pochází z britského standardu BS7799 a je zaměřen na řízení kybernetickou a informační bezpečnosti. Většina současných ICT systémů je navržených a implementovaných jako otevřené systémy (tj. systémy, které jsou otevřeny pro komunikaci s jinými systémy), a proto normalizace bezpečnostních mechanismů ICT nabývá stále větší význam. Zpočátku požadavky na standardizaci určovaly státní orgány, ale přijaté normy zaostávaly za rozvojem technologií, a proto později iniciativu ve standardizaci převzali výrobci a uživatelé ICT.

Klíčové organizace ve standardizaci kybernetické a informační bezpečnosti jsou ISO (ISO společně s IEC vytvořila Joint Technical Committee (JTC1) pro tvorbu norem v oblasti ICT, v jehož rámci působí podvýbor SC 27 zabývající se normami z oblasti kybernetické a informační bezpečnosti) a americký NIST. Standardy v oblasti kybernetické a informační bezpečnosti vydává i ETSI, CEN, ECMA, CCITT, IEEE prostřednictvím ANSI, SWIFT pro finanční instituce. Některé obecně uznávané standardy spravují soukromé instituce (RSA Laboratories standardy pro PKI a elektronický podpis - PKCS), jiné jsou před formálním zpracováním do podoby standardu zveřejňované k veřejnému připomínkovému ve formě RFC (request for comments). Kromě stálých standardizačních organizací vznikají normalizační iniciativy na řešení specializovaných otázek (EESSI - elektronický podpis a PKI). V normách je zahuštěné mimořádně cenné poznání vysoce kvalifikovaných odborníků, ale zpracovat jej do použitelné podoby je s ohledem na počet a rozmanitost existujících standardů netriviální úkol.

Mezinárodní aktivity

Bezpečnostní problémy přesahují možnosti řešení na lokální úrovni a vyžadují mezinárodní koordinaci. Do řešení aktuálních kybernetických bezpečnostních problémů se zapojují významné mezinárodní organizace, jako je OSN, OECD, EU a G8; na půdě mezinárodních organizací tvoří vzorové zákony (UNCITRAL, Zákon o elektronickém podpisu), metodické materiály (OECD, Směrnice), Rada Evropy přijala Convention on Cybercrime, rovněž EU přijala několik dokumentů k závažným bezpečnostním problémům. Tyto dokumenty tvoří rámec, který je třeba naplnit konkrétními aktivitami. Vedle zmíněných standardizačních činností k nim patří činnosti zaměřené na prevenci resp. řešení bezpečnostních incidentů. V roce 1988 jako odpověď na první globální útok na Internet vznikl v USA CERT Coordination Center (známý jako the CERT / CC původně nazývaný Computer Emergency Response Team), následně se síť pracovišť CERT a CSIRT (Computer Security Incident Response Team) rychlé rozšířila po celém světě. [13] Během následujících let pracoviště CERT podstatně rozšířily svou působnost. Z pouhé podpory při řešení bezpečnostních incidentů se staly komplexními poskytovateli bezpečnostních služeb, včetně preventivních služeb jako varování, bezpečnostní poradenství, školení a služby spojené s řízením bezpečnosti. Reakcí na potřebu přípravy vysoce kvalifikovaných odborníků v kybernetické a informační bezpečnosti byl vznik Mezinárodní asociace certifikovaných auditorů informačních systémů, IDAC (Information Systems Audit and Control Association), která sdružuje auditory a manažery, stará se o jejich odborný růst a pořádá každoročně zkoušky pro nové adepty. Kybernetická a informační bezpečnost se stala i specializací v rámci informatického vzdělávání, EUCIP (European Certification of Informatics Profesionals) připravila vzdělávání pro profesionály v kybernetické a informační bezpečnosti. IFIP (International Federation for Information Processing) má speciální výbor (Technical committee 11) zaměřený na oblast kybernetické a informační bezpečnosti, který koordinuje výzkumné a vzdělávací aktivity v této oblasti.

Organizace Severoatlantické smlouvy (NATO) technicky řeší pouze ochranu aliančních, tedy společných informačních a komunikačních technologií. Ochrana na

[13] ENISA uvádí, že v Evropě je více jak 100 týmů CERT/CSIRT

národní úrovni zůstává v kompetenci jednotlivých členských zemí. NATO nicméně může v rámci konzultací dle článku 4 Washingtonské smlouvy působit jako fórum pro řešení kyberútoků na jednotlivé členské země a koordinovat společnou reakci na takové útoky.

Vývoj v oblasti kybernetické bezpečnosti v mezinárodním měřítku je v současné době nesmírně dynamický, stejně tak jako je dynamické zvyšování povědomí o kybernetických hrozbách v jednotlivých zemích i na úrovni mezinárodních institucí. Pro postihnutí tohoto vývoje a zjištění v maximální míře „současného“stavu je nutno provést důkladnou analýzu. Tato bude provedena v nejbližších týdnech.

Dodatek 1: Právní předpisy, které je nezbytné přehodnotit v souvislosti s otázkou kybernetické bezpečnosti v České republice

- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.
- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů
- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů
- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů;
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů;
- Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů
- Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů
- Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů;
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností a o změně některých zákonů, ve znění pozdějších předpisů
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů
- Zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění zákona č. 306/2009 Sb.
- Usnesení vlády č. 624 ze dne 20. června 2001, o pravidlech, zásadách a

způsobu zabezpečování kontroly užívaní počítačových programů;

- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor
- Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací
- Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES

Dodatek 2: Příklady kybernetických incidentů ve světě

- Útok na yahoo.com, amazon.com, buy.com, eBay.com a cnn.com, který proběhl ve dnech 7. a 8. února 2000, zapříčinil finanční ztráty v řádu desítek miliónů dolarů.
- V dubnu a květnu 2001, po kolizi amerického letounu s letounem Čínské lidové republiky, došlo mezi internetovými aktivisty z obou zemí k celé řadě vzájemných útoků.
- Dne 19. června 2001 bylo více než 359 000 serverů během 13 hodin infikováno virem Code Red. Koncem srpna 2001 se objevily zdokonalené viry Code Red II a III, jimiž bylo infikováno asi 975 000 serverů. Viry například zapříčinily výpadek serverů japonských aerolinií, zpožděno bylo 55 letů. Celková ztráta, způsobená virem a jeho mutacemi přesáhla 2,4 miliardy dolarů.
- Dne 21. října 2002 byly útoku vystaveny základní servery Internetu (tzv. DNS). Pozadí útoku nebylo vyjasněno. Z celkem 13 serverů (většina z nich sídlí v USA, v centrálách konkrétních universit) jich bylo 8 na určitou dobu vyřazeno z provozu.
- V říjnu 2006 se uskutečnil průnik extremistů do počítačové aplikace, která ovládá bezpečnostní kamery na letišti v Anchorage na Aljašce.
- V květnu 2007 kulminovala internetová blokáda Estonska. Uvedený incident ohrozil kritickou informační infrastrukturu celého státu. Estonsko je přitom ”internetově” nesmírně pokročilou zemí. Je průkopníkem při zavádění e-Governmentu a je prostřednictvím kyberprostoru silně zranitelné. Vlnou tzv. DDoS (*Distributed Denial of Service*) byly internetové servery zahlceny požadavky na služby a dočasně zkolabovaly.[14]
- V srpnu a září 2007 se do širšího povědomí dostaly útoky na servery umístěné v Německu a v USA, připisované hackerům ve službách Čínské lidové

[14] Incident nastolil řadu otázek i z hlediska mezinárodního práva: V současnosti totiž například Severoatlantická aliance nedefinuje internetové útoky jako vojenskou akci. To znamená, že ustanovení článku 5 Washingtonské smlouvy, se na zemi, která se stala terčem kybernetického útoku, nevztahují. Nicméně, aliance může v případě takového útoku využít konzultací dle článku 4 Washingtonské smlouvy.

republiky. Podobné incidenty jsou od té doby opakovaně avizovány z řady míst světa.

- V červnu 2008 se uskutečnil koordinovaný kybernetický útok na množství webových serverů v Litvě. V srpnu 2008 se obdobný scénář opakoval v Gruzii (v kontextu bojů o Jižní Osetii).
- V roce 2010 byly virem Stuxnet poškozeny centrifugy pro obohacování uranu v Íránu
- V roce 2011 byl rozbit botnet, který 10 let shromažďoval údaje o bankovních účtech a kreditních kartách. Bylo do něj zapojeno 2,3 milionů počítačů
- V roce 2011 byly napadeny servery státní správy v Číně
- Napadání serverů státních institucí a organizací v demokratických státech i velmi neutrálních (namátkou Rakousko) se stalo běžným

Dodatek 3: Ekonomické aspekty projektu budování kybernetické ochrany ČR jako součásti kybernetické bezpečnosti České republiky

Definice kybernetické ochrany

Kybernetickou ochranu (dále jen KO) lze definovat jako *ochranu informačního nebo jiného systému, řízeného počítačem, před*

- *kybernetickým nebo fyzickým útokem protivníka, který jej chce ochromit nebo manipulovat s ním tak, aby způsobil škodu,*
- *přístupem protivníků, kteří chtějí získat, narušit, poškodit nebo zničit cenné informace anebo složky řízeného systému, a to včetně zabránění přístupu k nim* (v tradičním pojetí bezpečnosti IT jde o důvěrnost, integritu a dostupnost dat).

Řízení KO obsahuje vždy hlavní složky, realizované zpravidla jako jeho jednotlivé subsystémy:

- řízení aktiv, jež jsou ohroženy kybernetickými útoky a jejichž poškození představuje hlavní dopad incidentů,
- řízení služeb, které představují procesy a jejich vlastníky, podílející se na všech hlavních krocích, realizované ochrany od prevence přes monitorování, detekci, analýzu, lokalizaci útočníků až po nápravná opatření a případné zahrnutí nových poznatků do ochranného systému,
- řízení kvality, nezbytné pro udržení co nejvyšší úrovně spolehlivosti, funkceschopnosti, použitelnosti, efektivnosti a schopnosti reagovat na technologicky a znalostně rozvinuté incidenty libovolného měřítka a rozsahu,
- řízení bezpečnosti, zajišťující maximální možnou míru ochrany vlastního systému kybernetické bezpečnosti proti infiltraci nežádoucích prvků, proniknutí do systému a jeho monitorování, analýze a poškození či alespoň degradaci funkci, v nejhorším případě prozrazení principů a důležitých složek ochranných procesů útočníkům.

Služby kybernetické ochrany

Podstatnou složkou kvality a účinnosti ochrany je *řízení služeb.* Pro posuzování kvality je nezbytná kvalifikace úrovně služeb. Pro účely specifikace projektového záměru a dalšího vývoje je vhodné specifikovat základní charakteristiky:

Úroveň	*Název*	*Charakteristika*
1	Řízení infrastruktury na zajištění kybernetické ochrany ČR	Řízení, správa a kontrola infrastruktury, monitorování činnosti jednotlivých prvků, audit postupů řízení dílčích složek, **definice služeb KO pro jednotlivé složky**, publikace a komunikace.
2	Řízení služeb KO ČR a jejich správa	**Řízení očekávaných situací jednotlivých složek řízeného systému,** průběžný monitoring bezpečnostního stavu, audit výkonnost a spolehlivosti služeb KO, měření dostupnosti, prověřování simulacemi.
3	Řízení přidané hodnoty KO pro stát v jednotlivých oblastech	**Harmonizace služeb KO optimalizací procesů dílčích složek a jejich interface.** Proaktivní postupy KO, analýzy statistik s návrhy na další rozvoj aktivity jednotlivých složek. Využití vhodných technologických prvků na podporu systému řízení kybernetické ochrany ČR.

Službou kybernetické ochrany je třeba rozumět „produkt“, poskytnutý odpovědným kompetentním prvkem systému kybernetické ochrany České republiky (SKOČR) „spotřebiteli“. Produktem se rozumí podpora nebo pomoc při řešení situace hrozícího nebo uskutečněného kybernetického bezpečnostního incidentu v rámci

specifikovaných pravidel, odpovědností a pravomocí SKOČR. Spotřebitelem lze rozumět místo, které buď samo iniciovalo požadavek na příslušnou službu anebo bylo adresně upozorněno na žádoucí převzetí služby hierarchicky nadřazeným prvkem. Službou v naznačeném významu je tedy nutno rozumět *vztah poskytovatele a spotřebitele*, nejde tedy o dodávku zboží, ať už hmotného nebo nehmotného (licence, autorská práva atp.).

Infrastrukturou kybernetické ochrany budeme rozumět souhrn všech řídících, výkonných, kontrolních a dohledových složek, technických prvků, dat, informací, know-how, procesů, pravidel a kompetencí, uplatňovaných v systému řízení kybernetické ochrany ČR.

Efektivnost kybernetické ochrany

Obrana proti kybernetickému ohrožení bude o to lepší, o co lepší bude vlastní řízení IT: snaha o *zvýšení efektivnosti ochrany proti kybernetickým útokům musí jít ruku v ruce se snahou* ***zvyšovat kvalitu a úroveň služeb IT: čím vyšší úroveň řízení služeb IT, tím efektivnější budou obranná opatření proti kybernetickému napadení.*** To však musí být současně doplněno o další nezbytné aktivity, zajišťující potřebný komplex postupů, procesů a potřebný výběr nástrojů, sloužících k maximální efektivnosti celého ochranného systému proti kybernetickému napadení. Celý systém je tak silný, jak silný je jeho nejslabší článek, což v jisté analogii je použitelné i pro efektivnost.

Podmínky kvalitního řízení a efektivnosti KO lze potom shrnout jako požadavky na důslednou a kvalitní specifikaci, klasifikaci, realizaci, aplikaci a neustálé zdokonalování jak celého systému, tak již zmíněných hlavních složek systému kybernetické ochrany :

- systém řízení kybernetické ochrany ČR včetně jeho hlavních subsystémů -
    - sub systému řízení aktiv,
    - subsystému řízení služeb,
    - subsystému řízení kvality IT i KO,

- subsystému řízení bezpečnosti.

Pro všechny zmíněné oblasti je nutno využít dostupné standardy včetně postupů nejlepší praxe.

Ekonomická východiska projektu

Odhad žádoucích nákladů na ochranu aktiv ČR

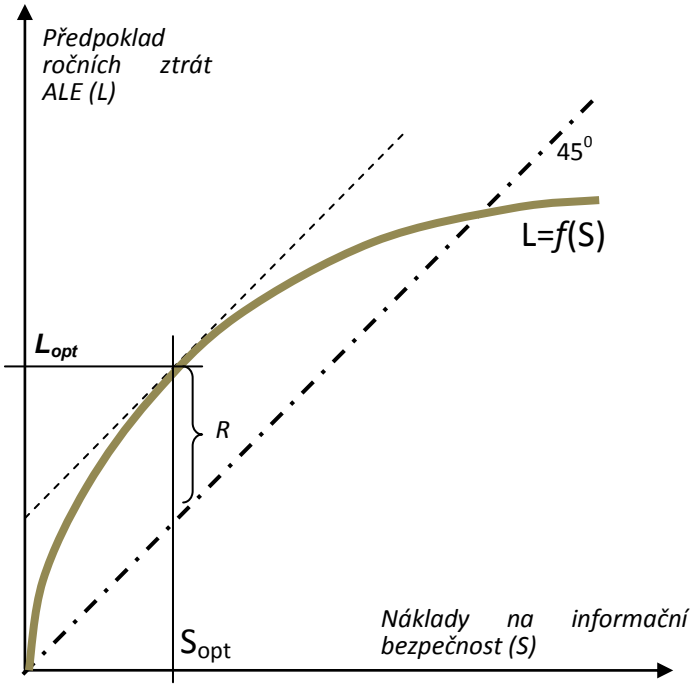
Orientační údaje pro odpovídající volbu strategických opatření v oblasti kybernetické ochrany je nutno získat z vhodného modelu. Jedním z vhodných zdrojů je tzv. *model rizikové neutrality*[15].

V prezentovaném modelu rizikové neutrality je vztah pravděpodobnosti ročních ztrát a nákladů na bezpečnost zobrazen tzv. kouřovou křivkou: kouř stoupá nejprve kolmo, aby pak byl sloupec kouře odkláněn prouděním vzduchu.

Riziková neutralita staví na tom, že organizace přestane zvyšovat náklady na ochranu tehdy, kdy jednotková hodnota zvýšení nákladů odpovídá redukci ročních ztrát, která je menší než jedna.

Čerchovaná čára z výchozího bodu pod úhlem 45^0 představuje stavy, kdy by S = L. Optimální hodnotou nákladů na bezpečnost je v tomto případě v bodě S_{opt}, kde tangenta funkce f(S) je rovna jedné (tečna křivky je rovnoběžná s čerchovanou čárou). Tento bod určuje předpokládané roční ztráty R = Lopt – Sopt, což označuje maximální rozdíl přínosů a nákladů!

[15] LAWRENCE A. GORDON and MARTIN P. LOEB: The Economics of Information Security Investment, , University of Maryland, ACM Transactions on Information and System Security, Vol. 5, No. 4, November 2002



Jádrem modelu Gordon-Loeb je ekonomický rámec, který umožňuje stanovit optimální investice na ochranu dané množiny informací (informačních aktiv). Výsledkem řešení tohoto modelu je zjištění, že náklady na ochranu mohou představovat pouze malý zlomek potenciálních ztrát. Model totiž naznačuje, že je neekonomické vkládat do ochrany proti kybernetickým útokům více, než 37% předpokládaných ztrát. Současně model poukazuje na to, že optimální úroveň prostředků, věnovaných na ochranu se nezvyšuje vždy, kdy vzrůstá míra ohrožení.

Organizace tedy mohou zvyšovat míru návratnosti vložených prostředků do ochrany investicemi do informační bezpečnosti činností, které jsou směrovány na zlepšení informační bezpečnosti množiny informací, která má střední úroveň ohrožení!

Z dosavadních zjištění[16] lze pak převzít rámcový údaj o vhodné míře nákladů na ochranu před kybernetickými útoky v úrovni zhruba ve výši 5% celkových nákladů na ICT.

[16] Viz též:

Bob Violino, "Survey Report– The Security Team – IT Organizations Are Making Security a Primary Job Function," Network Computing, Sept. 25, 2003 (Secure Enterprise survey finds that 5% is the median security expenditure);

Robert D. Austin and Christopher A.R. Darby, "The Myth of Secure Computing," Harvard Business Review, June 2003, p. 121 (the average company spends 5% to 10% of its IT budget on security);

Computer Economics Inc., 2003 Information Systems Spending, p. 11-1 (security software and hardware alone account for 2.8% of total IT budgets).

Rámcová kalkulace míry ekonomické úrovně KO

Z publikovaných statistik vyplývá, že ČR má v oblasti ICT 2,3% pracovníků ze všech zaměstnanců, zatímco např. Dánsko, Nizozemsko, Švýcarsko, Švédsko mají **přes 3%.** Z naznačeného lze očekávat, že postupně počet pracovníků ICT v ČR vzroste.

Ze služeb ICT přispělo v roce 2008 na tvorbu HDP 1,79%, a to z celkového objemu ICT služeb 142 mld. Kč. Použijeme-li v předchozí kapitole uvedený procentní podíl celkového objemu 5%, z uvedeného objemu služeb to odpovídá 7,1 mld. Kč.

Pro orientaci naznačíme potenciální odhadovanou strukturu této částky, věnované na ochranu:

Oblast využití 7.1 mld. Kč	*%*	*podíl mil. Kč*
Státní organizace, instituce a orgány v oblasti KO působící	40	2 840
Soukromé (firemní) složky, působící v KO	35	2 485
Akademická oblast	18	1 278
Výzkum a vývoj	7	497
Celkem	100	7 100

Uvažovaná odpovídající úroveň nákladů na projekt Budování kybernetické ochrany České republiky je v ročním objemu cca 300 mil. Kč (viz dále). Projekt tedy představuje v ročních nákladech pouze cca 4% potřebných (žádoucích) celkových nákladů na KO z celkového objemu ICT služeb, resp. 10% z nákladů, které by měly být vynaloženy na KO ve státní sféře.

Hlavní kritéria projektového záměru

Struktura hlavních aktivit

Současná úroveň analýzy problematiky umožňuje pouze rámcový pohled na projekt a jeho strukturu. Vzhledem k charakteru projektu, předpokládanému vývoji řešení i uvažovaném okruhu partnerů projektu je pro zamýšlený projekt uvažováno využití všech disponibilních zdrojů. V případě tohoto projektového záměru je nezbytné využít:

- všech dostupných finančních zdrojů pro krytí projektu: v tomto období je to zejména oblast Evropských strukturálních fondů s pokrytím vybraných složek i z jiných (plánovaných, zajištěných) zdrojů,

- všech disponibilních odborných kapacit kompetentních pracovníků v dané oblasti KO,
- možného partnerství všech kvalifikovaných organizací, organizačních složek státních orgánů, vybraných akademických pracovišť a dalších.

Rámcovou strukturu jednotlivých (hlavních) projekčních aktivit projektu Budování kybernetické ochrany České republiky (dále jen BUKO) tvoří:

1	Organizace, plánování, řízení a koordinace projektu
2	Efektivní řízení kybernetické bezpečnosti a řízení rizik
3	Vnitrostátní koordinace a komunikace mezi zainteresovanými veřejnými subjekty
4	Mezinárodní spolupráce – zastupování ČR v mezinárodních orgánech a institucích
5	Legislativní rámec (zákon)
6	Standardizace (revize standardů), aplikace nejlepší praxe
7	Konkurenceschopnost české ekonomiky
8	Rozšiřování národní kompetence, aplikace a rozvoj odpovídající technologie
9	Osvěta a vzdělávání, budování povědomí o kybernetické bezpečnosti, efektivní PR
10	Vytváření bezpečného a stabilního prostředí, aktivní udržování trvalé odolnosti (cvičení)
11	Partnerství s komerční a akademickou sférou
12	Zajištění ochrany státní a kritické informační a komunikační infrastruktury státu
13	Podpora ochrany lidských práv a svobod

Odhad členění nákladové struktury BUKO

Tab. I představuje předpokládané aktivity projektu. Každá z uvedených aktivit je komplexním projektem, tvořeným dílčími aktivitami s přiřazením odpovídajících zdrojů kapacit, finančních prostředků a časového rámce.

Aktivity pro realizaci budování kybernetické ochrany ČR		***Celk.***	*2012*	*2013*	*2014*	*2015*	*%*
Tab. I	Odhad celkových nákladů (mil. Kč)	**1253**	251	313	363	326	100
BUKO1	Organizace, plánování, řízení a koordinace projektu	**113**	23	28	33	29	9
BUKO2	Efektivní řízení kybernetické bezpečnosti a řízení rizik	**138**	28	34	40	36	11
BUKO3	Vnitrostátní koordinace a komunikace mezi zainteresovanými veřejnými subjekty	**38**	8	9	11	10	3
BUKO4	Mezinárodní spolupráce – zastupování ČR v mezinárodních orgánech a institucích	**50**	10	13	15	13	4
BUKO5	Legislativní rámec (zákon)	**25**	5	6	7	7	2
BUKO6	Standardizace (revize standardů), aplikace nejlepší praxe	**50**	10	13	15	13	4
BUKO7	Konkurenceschopnost české ekonomiky	**150**	30	38	44	39	12
BUKO8	Rozšiřování národní kompetence, aplikace a rozvoj odpovídající technologie	**213**	43	53	62	55	17
BUKO9	Osvěta a vzdělávání, budování povědomí o kybernetické bezpečnosti, efektivní PR	**88**	18	22	25	23	7
BUKO10	Vytváření bezpečného a stabilního prostředí, aktivní udržování trvalé odolnosti (cvičení)	**75**	15	19	22	20	6
BUKO11	Partnerství s komerční a akademickou sférou	**125**	25	31	36	33	10
BUKO12	Zajištění ochrany státní a kritické informační a komunikační infrastruktury státu	**163**	33	41	47	42	13
BUKO13	Podpora ochrany lidských práv a svobod	**25**	5	6	7	7	2
BUKO		**%**	20	25	29	26	100

Kumulovaný finanční rozpočet

Pro posouzení adekvátnosti jednotlivých složek je nezbytné provést korekci naznačených finančních objemů na jednotlivé třídy nákladů. Tab. II uvádí odhadovanou strukturu navrženého nákladového členění BUKO (z Tab. I) s tím, že investice nejsou v nákladech zohledněny a pro potřeby projektu jsou uvažovány v této koncepční fázi jako *služby.*

Tab. II **Rozpočet mil.Kč období 2012 - 2015**

kód		%	mil. Kč	BUKO1	BUKO2	BUKO3	BUKO4	BUKO5	BUKO6	BUKO7	BUKO8	BUKO9	BUKO10	BUKO11	BUKO12	BUKO13	BUKO
01	os. náklady	55	689,2	62,02	75,81	20,67	27,57	13,78	27,57	82,70	117,16	48,24	41,35	68,92	89,59	13,78	689,15
02	cestovné	2	25,1	2,26	2,76	0,75	1,00	0,50	1,00	3,01	4,26	1,75	1,50	2,51	3,26	0,50	25,06
03	zařízení	2	25,1	2,26	2,76	0,75	1,00	0,50	1,00	3,01	4,26	1,75	1,50	2,51	3,26	0,50	25,06
04	kancelář	3	37,6	3,38	4,13	1,13	1,50	0,75	1,50	4,51	6,39	2,63	2,26	3,76	4,89	0,75	37,59
05	služby	35	438,6	39,47	48,24	13,16	17,54	8,77	17,54	52,63	74,55	30,70	26,31	43,86	57,01	8,77	438,55
06	staveb. úpravy	0	0,0	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00	0,00
07	podpora	1	12,5	1,13	1,38	0,38	0,50	0,25	0,50	1,50	2,13	0,88	0,75	1,25	1,63	0,25	12,53
08	ze smlouvy	2	25,1	2,26	2,76	0,75	1,00	0,50	1,00	3,01	4,26	1,75	1,50	2,51	3,26	0,50	25,06
		100	**1253,0**	112,77	137,83	37,59	50,12	25,06	50,12	150,36	213,01	87,71	75,18	125,30	162,89	25,06	1253,00
			mil. Kč	113,00	138,00	38,00	50,00	25,00	50,00	150,00	213,00	88,00	75,00	125,00	163,00	25,00	**1253,00**
			%	9	11	3	4	2	4	12	17	7	6	10	13	2	100

Předběžný odhad objemu služeb

Z Tab. I a Tab. II lze stanovit podrobnější pohled na struktur služeb pro jednotlivé aktivity.

Předběžný rozpočet služeb (hrubý odhad)

Tab. III

	2012	2013	2014	2015	Celk.mil.K	%
BUKO1	7,9	9,9	11,4	10,3	**39,5**	**9**
BUKO2	9,6	12,1	14,0	12,5	**48,2**	**11**
BUKO3	2,6	3,3	3,8	3,4	**13,2**	**3**
BUKO4	3,5	4,4	5,1	4,6	**17,5**	**4**
BUKO5	1,8	2,2	2,5	2,3	**8,8**	**2**
BUKO6	3,5	4,4	5,1	4,6	**17,5**	**4**
BUKO7	10,5	13,2	15,3	13,7	**52,6**	**12**
BUKO8	14,9	18,6	21,6	19,4	**74,6**	**17**
BUKO9	6,1	7,7	8,9	8,0	**30,7**	**7**
BUKO10	5,3	6,6	7,6	6,8	**26,3**	**6**
BUKO11	8,8	11,0	12,7	11,4	**43,9**	**10**
BUKO12	11,4	14,3	16,5	14,8	**57,0**	**13**
BUKO13	1,8	2,2	2,5	2,3	**8,8**	**2**
BUKO	87,710	109,638	127,180	114,023	**438,550**	**-73,0**
%	**20**	**25**	**29**	**26**	**100**	

Odhad rozpočtu vlastních nákladů

Pokud od rozpočtovaných nákladů ve struktuře BUKO odečteme objemy služeb, bude výsledný rozpočet představovat vlastní náklady (Tab. IV)

Předběžný rozpočet vl. nákladů (mimo služby)

Tab. IV

	2012	2013	2014	2015	mil.Kč
BUKO1	14,7	18,3	21,3	19,1	**73,3**
BUKO2	17,9	22,4	26,0	23,3	**89,6**
BUKO3	4,9	6,1	7,1	6,4	**24,4**
BUKO4	6,5	8,1	9,4	8,5	**32,6**
BUKO5	3,3	4,1	4,7	4,2	**16,3**
BUKO6	6,5	8,1	9,4	8,5	**32,6**
BUKO7	19,5	24,4	28,3	25,4	**97,7**
BUKO8	27,7	34,6	40,2	36,0	**138,5**
BUKO9	11,4	14,3	16,5	14,8	**57,0**
BUKO10	9,8	12,2	14,2	12,7	**48,9**
BUKO11	16,3	20,4	23,6	21,2	**81,4**
BUKO12	21,2	26,5	30,7	27,5	**105,9**
BUKO13	3,3	4,1	4,7	4,2	**16,3**
BUKO	162,9	203,6	236,2	211,8	**814,5**
%	**0**	**0**	**0**	**0**	**-100**

Hrubý nástin kapacit

Pro ilustraci řešitelského potenciálu je proveden výpočet FTE (Full Time Equivalent) na uvedené vlastní náklady. Předpokladem je kalkulovaný objem osobních nákladů 0,750 mil. Kč/osobu/rok (viz Tab. V)

Hrubý nástin kapacit FTE (člr)

Tab. V

	2012	2013	2014	2015	Celkem FTE člr.
BUKO1	16.54	20.67	23.98	21.50	82.70
BUKO2	20.22	25.27	29.31	26.28	101.08
BUKO3	5.51	6.89	7.99	7.17	27.57
BUKO4	7.35	9.19	10.66	9.56	36.75
BUKO5	3.68	4.59	5.33	4.78	18.38
BUKO6	7.35	9.19	10.66	9.56	36.75
BUKO7	22.05	27.57	31.98	28.67	110.26
BUKO8	31.24	39.05	45.30	40.61	156.21
BUKO9	12.86	16.08	18.65	16.72	64.32
BUKO10	11.03	13.78	15.99	14.33	55.13
BUKO11	18.38	22.97	26.65	23.89	91.89
BUKO12	23.89	29.86	34.64	31.06	119.45
BUKO13	3.68	4.59	5.33	4.78	18.38
BUKO	183.77	229.72	266.47	238.91	918.87

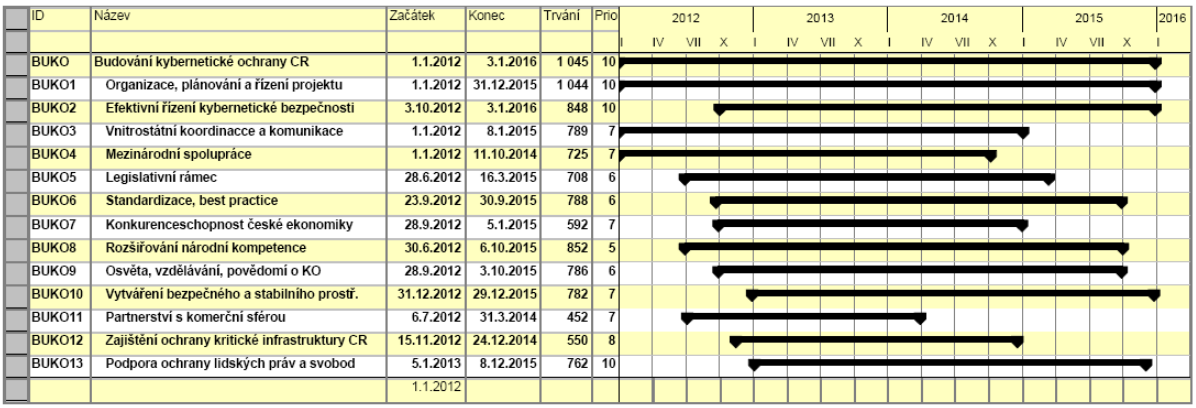
Harmonogram

Prezentovaná úroveň časového rámce je podmíněna řadou okolností, které nelze kvalifikovaně posoudit. Z tohoto důvodu je každé podrobnější plánování spekulativní a jeho vypovídací schopnost relativně nízká.

I s vědomím těchto omezení zařazujeme nástin časového rámce s tím, že jeho skutečná podoba by se měla s vývojem přípravy projektu aktualizovat, zpřesňovat a prohlubovat jeho rozlišovací úroveň.

Harmonogram_BUKO_v1.0.rmp - Gantt Chart

ID	Název	Začátek	Konec	Trvání	Prio
BUKO	Budování kybernetické ochrany CR	1.1.2012	3.1.2016	1 045	10
BUKO1	Organizace, plánování a řízení projektu	1.1.2012	31.12.2015	1 044	10
BUKO2	Efektivní řízení kybernetické bezpečnosti	3.10.2012	3.1.2016	848	10
BUKO3	Vnitrostátní koordinacce a komunikace	1.1.2012	8.1.2015	789	7
BUKO4	Mezinárodní spolupráce	1.1.2012	11.10.2014	725	7
BUKO5	Legislativní rámec	28.6.2012	16.3.2015	708	6
BUKO6	Standardizace, best practice	23.9.2012	30.9.2015	788	6
BUKO7	Konkurenceschopnost české ekonomiky	28.9.2012	5.1.2015	592	7
BUKO8	Rozšiřování národní kompetence	30.6.2012	6.10.2015	852	5
BUKO9	Osvěta, vzdělávání, povědomí o KO	28.9.2012	3.10.2015	786	6
BUKO10	Vytváření bezpečného a stabilního prostř.	31.12.2012	29.12.2015	782	7
BUKO11	Partnerství s komerční sférou	6.7.2012	31.3.2014	452	7
BUKO12	Zajištění ochrany kritické infrastruktury CR	15.11.2012	24.12.2014	550	8
BUKO13	Podpora ochrany lidských práv a svobod	5.1.2013	8.12.2015	762	10
		1.1.2012			



Dodatek 4: Základní právní předpisy vytvářející legislativní rámec (výběr):

- ústavní zákon č. 1/1993 Sb., Ústava České republiky,
- ústavní zákon č. 2/1993 Sb., Listina základních práv a svobod,
- zákon č. 101/2000 Sb., o ochraně osobních údajů.,
- zákon č. 106/1999 Sb., o svobodném přístupu k informacím,
- zákon č. 227/2000 Sb., o elektronickém podpisu, včetně navazujících prováděcích vyhlášek,
- zákon č. 365/2000 Sb., o informačních systémech veřejné správy,
- zákon č . 480/2004 Sb., o některých službách informační společnosti,
- zákon č. 127/2005 Sb., o elektronických komunikacích,
- zákon č. 273/2008 Sb., o Policii České republiky,
- zákon č. 40/2009 Sb., trestní zákoník,
- zákon č. 141/1961 Sb., o trestním řízení soudním,
- zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů (krizový zákon),
- zákon č. 111/2009 Sb., o základních registrech,
- zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů,
- zákon č. 21/1992 Sb., o bankách,
- zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů,
- zákon č. 89/1995 Sb., o státní statistické službě,
- zákon č. 153/1994 Sb., o zpravodajských službách České republiky,
- zákon č. 6/1993 Sb., o České národní bance.

Stěžejní prováděcí předpisy:

- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor
- Vyhláška č. 524/2005 Sb., o zajištění kryptografické ochrany utajovaných informací
- Vyhláška č. 525/2005 Sb., o provádění certifikace při zabezpečování kryptografické ochrany utajovaných informací
- Vyhláška č. 526/2005 Sb., o stanovení vzorů používaných v oblasti průmyslové bezpečnosti a o seznamech písemností a jejich náležitostech nutných k ověření splnění podmínek pro vydání osvědčení podnikatele a o způsobu podání žádosti podnikatele (vyhláška o průmyslové bezpečnosti), ve znění vyhlášky č. 11/2008 Sb.
- Vyhláška č. 527/2005 Sb., o stanovení vzorů v oblasti personální bezpečnosti a bezpečnostní způsobilosti a o seznamech písemností přikládaných k žádosti o vydání osvědčení fyzické osoby a k žádosti o doklad o bezpečnostní způsobilosti fyzické osoby a o způsobu podání těchto žádostí (vyhláška o personální bezpečnosti)
- Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění vyhlášky č. 19/2008 Sb.
- Vyhláška č. 529/2005 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, ve znění vyhlášky č. 55/2008 Sb.

Předpisy EU:

- Smlouva o fungování Evropské unie
- Smlouva o Evropské unii
- Listina základních práv Evropské unie
- Směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy
- Směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů
- Směrnice Evropského parlamentu a Rady 1999/5/ES ze dne 9. března 1999 o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody
- Směrnice Evropského parlamentu a Rady 2006/123/ES ze dne 12. prosince 2006 o službách na vnitřním trhu
- Směrnice Evropského parlamentu a Rady 1997/66/ES ze dne 15. prosince 1997 o zpracování osobních dat a ochraně soukromí v telekomunikačním sektoru
- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích)
- Směrnice Rady ze dne 14. května 1991 o právní ochraně počítačových programů
- Rozhodnutí Rady 2001/264/ES ze dne 19. března 2001, kterým se přijímají bezpečnostní předpisy Rady
- Směrnice Evropského parlamentu a Rady 2002/19/ES ze dne 7. března 2002 o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice)
- Směrnice Evropského parlamentu a Rady 2002/20/ES ze dne 7. března 2002 o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice)

- Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice)
- Směrnice Evropského parlamentu a Rady 2002/22/ES ze dne 7. března 2002 o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě)
- Směrnice Komise 2002/77/ES ze dne 16. září 2002 o hospodářské soutěži na trzích sítí a služeb elektronických komunikací
- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu)
- Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu
- Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele
- Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES
- Směrnice Evropského parlamentu a Rady 2009/136/ES ze dne 25. listopadu 2009 , kterou se mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací, směrnice 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací a nařízení (ES) č. 2006/2004 o spolupráci mezi vnitrostátními orgány příslušnými pro vymáhání dodržování zákonů na ochranu zájmů spotřebitele

- Směrnice Evropského parlamentu a Rady 2009/140/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, směrnice 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení a směrnice 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací
- Směrnice Evropského Parlamentu a Rady 98/34/ES ze dne 22. června 1998 o postupu při poskytování informací v oblasti norem a technických předpisů
- Návrh směrnice Evropského parlamentu a Rady o útocích proti informačním systémům a zrušení rámcového rozhodnutí Rady 2005/222/SVV
- Nařízení Evropského parlamentu a Rady (ES) č. 1007/2008 ze dne 24. září 2008 , kterým se mění nařízení (ES) č. 460/2004 o zřízení Evropské agentury pro bezpečnost sítí a informací, pokud jde o období její činnosti
- Nařízení Evropského parlamentu a Rady (ES) č. 1049/2001 ze dne 30. května 2001 o přístupu veřejnosti k dokumentům Evropského parlamentu, Rady a Komise
- Nařízení Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů
- Nařízení Evropského parlamentu a Rady (ES) č. 1073/1999 ze dne 25. května 1999 o vyšetřování prováděném Evropským úřadem pro boj proti podvodům (OLAF)
- Rozhodnutí Komise ze dne 29. července 2002, kterým se zřizuje skupina evropských regulačních orgánů pro sítě a služby elektronických komunikací
- Rozhodnutí Rady 92/242/EHS ze dne 31. března 1992, o bezpečnosti informačních systémů
- Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005, o útocích proti informačním systémům
- Rámcové rozhodnutí Rady 2002/465/JHA ze dne 13. července 2002 o společných vyšetřovacích týmech
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2006) 688 ze dne 15. listopadu 2006, boj proti

spamu a špionážnímu („spyware“) a škodlivému softwaru („malicious software“)

- Sdělení Komise Evropskému parlamentu, Radě a Evropskému výboru regionů KOM(2007) 267 ze dne 22. května 2007, k obecné politice v boji proti počítačové kriminalitě
- Závěry Rady 2009/C 62/05 ze dne 27. listopadu 2008, o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti
- Sdělení Komise Evropskému parlamentu, Radě, Hospodářskému a sociálnímu výboru a výboru regionů KOM(2009) 149 ze dne 30. března 2009, o ochraně kritické informační infrastruktury
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2008) 199 - Příprava digitální budoucnosti Evropy - i2010 – přezkum v polovině období
- Sdělení komise Evropskému parlamentu a Radě Evropské agentury KOM(2008) 135 – cesta vpřed
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2004) 0028 o nevyžádaných obchodních sděleních neboli „spamu“
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2004) 61: „Propojování Evropy vysokou rychlostí: současný vývoj v sektoru elektronických komunikací“
- Sdělení Komise KOM(2002) 718: Operační rámec evropských regulačních úřadů
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2001) 298: Bezpečnost sítí a informací – návrh evropského postoje
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2000) 890 o vytvoření bezpečnější informační společnosti zdokonalením bezpečnosti informační infrastruktury a bojem proti počítačovým trestným činům

- Sdělení Komise Radě, Evropskému parlamentu, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2006) 251 – Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“
- Sdělení komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů KOM(2009) 149 o ochraně kritické informační infrastruktury - „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“
- Strategie Evropa 2020: Digitální agenda pro Evropu
- Akční plán Evropské unie pro boj s terorismem
- Strategie Evropské unie pro boj s radikalizací a rekrutováním
- Zelená kniha o detekčních technologiích při práci donucovacích, celních a jiných bezpečnostních orgánů 13183/2006, ze dne 25. září 2006
- Rezoluce Evropské rady 2003/C 48/01 o evropském postoji vůči kultuře bezpečnosti sítí a informací
- Rezoluce Evropské rady 2002/C 43/02 o společném postoji a specifických činnostech v oblasti bezpečnosti sítí a informací

Dokumenty RE, OECD, OBSE, NATO, G8:

- Úmluva Rady Evropy č. 185 o kyberkriminalitě
- Dodatkový protokol č. 189 k Úmluvě o kyberkriminalitě, o kriminalizaci činů rasistické a xenofobní povahy
- Doporučení Rady ministrů RE č. 13 z roku 1995, týkající se problému trestního práva procesního,
  spojeného s informačními technologiemi.
- Doporučení Rady ministrů RE č. 5 z roku 1999, týkající se ochrany soukromí na Internetu
- OECD”Přehled: Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti”
- „Antispamová příručka OECD“
- Rozhodnutí Rady ministrů OBSE č. 3/2004 ”O boji proti používání Internetu pro účely terorismu” ze dne 7. prosince 2004

- EAPC(CCPC)D(2006)0002 ze dne 2. února 2006: ”Civilní nouzové plánování: Následky, související s kybernetickými útoky a informačními zbraněmi na kritickou civilní komunikační infrastrukturu a služby; Civilní nouzové plánování: Následky ustavení Týmu pro civilní počítačové bezpečnostní incidenty”
- Akční plánu zemí G8 pro potírání ”high-tech” zločinu

Právně nezávazné, avšak mezinárodně uznávané normy:

- ČSN ISO/IEC 17799 – soubor - Informační technologie – Bezpečnostní techniky - Soubor postupů pro management bezpečnosti informací.
- ČSN ISO/IEC 15408 – soubor Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT.
- ČSN ISO/IEC 14598 – soubor Informační technologie – Hodnocení softwarového produktu.
- ČSN ISO/IEC 12207 Informační technologie – Procesy v životním cyklu softwaru.
- ČSN ISO/IEC 10181 – soubor Informační technologie – Propojení.
- ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky - Informační bezpečnost.