Kyberterorismus jako hrozba v průmyslu komerční bezpečnosti

Cyberterrorism as a threat in the comercial security industry

Tereza Benešovská

Bakalářská práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Tereza BENEŠOVSKÁ**
Osobní číslo:	**A08114**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Kyberterorismus jako hrozba v průmyslu komerční bezpečnosti**

Zásady pro vypracování:

1. **Stanovte konkrétní hrozby kyberterterorismu pro podniky průmyslu komerční bezpečnosti a navrhněte způsob účinné ochrany.**
2. **Proveďte analýzu hrozeb pro podniky PKB.**
3. **Zhodnoťte současný stav v České republice.**
4. **Popište řešení funkční ochrany z taktického hlediska.**
5. **Doporučte nejúčinnější technická řešení a konfigurujte použitelný materiál k ochraně.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín : Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.**
3. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.**
4. **JIROVSKÝ, Václav. Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha : Grada, 2007. 284 s. ISBN 978-80-247-1561-2.**
5. **VERTON, Dan. Black Ice : Neviditelná hrozba kyberterorizmu. Gliwice,Polsko : HELION S.A., 2004. 278 s. ISBN 83-7361-564-4.**
6. **LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vyd. 2. Zlín : Univerzita Tomáše Bati ve Zlíně, 2006. 101 s. ISBN 80-7318-432-X.**
7. **ZEMAN , Petr. Česká bezpečnostní terminologie : Výklad základních pojmů. Brno : Masarykova univerzita-Vydavatelství, 2003. 186 s. ISBN 80-210-3037-2.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá problematikou kyberterorismu. Je zde popsána jak jeho obecná podstata tak i metody, které kyberteroristé používají ke svému nekalému jednání v kyberprostoru. Dále je zhodnocen současný stav v ČR a popsána legislativa s tímto problémem související. Výsledkem je analýza možných útoků a následný návrh opatření ke zvýšení bezpečnosti před hrozbou kyberterorismu.

Klíčová slova: kyberterorismus, metody kyberteroristů, kyberprostor, kybernetická bezpečnost, softwarová ochrana

ABSTRACT

This thesis deals with the issue of cyberterorrism. It shows its very essence as well as the methods, which cyberterrorists use to operate in the cyberspace. The current state in the Czech Republic is evaluated and the legislature considering the problem is described in the text. The result is an analysis of possible attacks and subsequent proposal of moves to intensify the security against the threat of the cyberterrorism.

Keywords: cyberterrorism, cyberterrorist methods, cyberspace, cyber security, software protection

Děkuji vedoucímu své bakalářské práce JUDr. Vladimíru Lauckému za cenné a ochotně poskytnuté rady, připomínky a metodické vedení práce. A v neposlední řadě mým rodičům za jejich trpělivost po celou dobu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Informační a komunikační technologie (ICT) nesou se svým rozvojem i negativní stránku. Stávají se nezbytnou součástí života mnoha jedinců i společnosti a tím se zvyšuje četnost a dopady jejich zneužití. Vynalézavost kriminálníků vzrůstá nezadržitelně spolu s tempem technologického pokroku.

Teroristé využívají stále nové metody, prostředky a techniky. V souvislosti s využitím ICT vznikl kybernetický terorismus, čili kyberterorismus. Tento fenomén má celosvětový charakter. Scénář, kdy dojde k napadení rozsáhlé komunikační sítě a narušení jejich funkcí je dnes možný a proveditelný během několika minut.

Kyberterorismus by mohl být jedním ze špatně pochopených a vyložených pojmů. Zeptáme-li se 10 lidí co kyberterorismus je, dostaneme nejméně třetinu různých odpovědí. Když by těchto 10 lidí bylo bezpečnostními počítačovými experty, jejichž úkolem je vytvářet formy ochrany proti kyberterorismu, mohl by se rozdíl těchto odpovědí považovat za znepokojující. Když těchto 10 lidí bude představovat různé nevládní i vládní bezpečnostní agentury, je to vážný problém.

Musíme si uvědomit, že kyberterorismus může mít samozřejmě i formu tradičního teroristického útoku, jelikož Internet, komunikační služby a zdroje energie je možné napadnout i fyzicky. Bomba, ať už chemická, biologická či vyrobená z umělého hnojiva, která zabrání vstupu do důležitých zařízení na výrobu elektrické energie či ovládání Internetu, může vyvolat stejné popření efektu této služby stejně jako útok vedený přes počítač s využitím virů a červů. Fyzická likvidace budovy, jejíž každodenní provoz závisí na počítačích, má kybernetické důsledky.

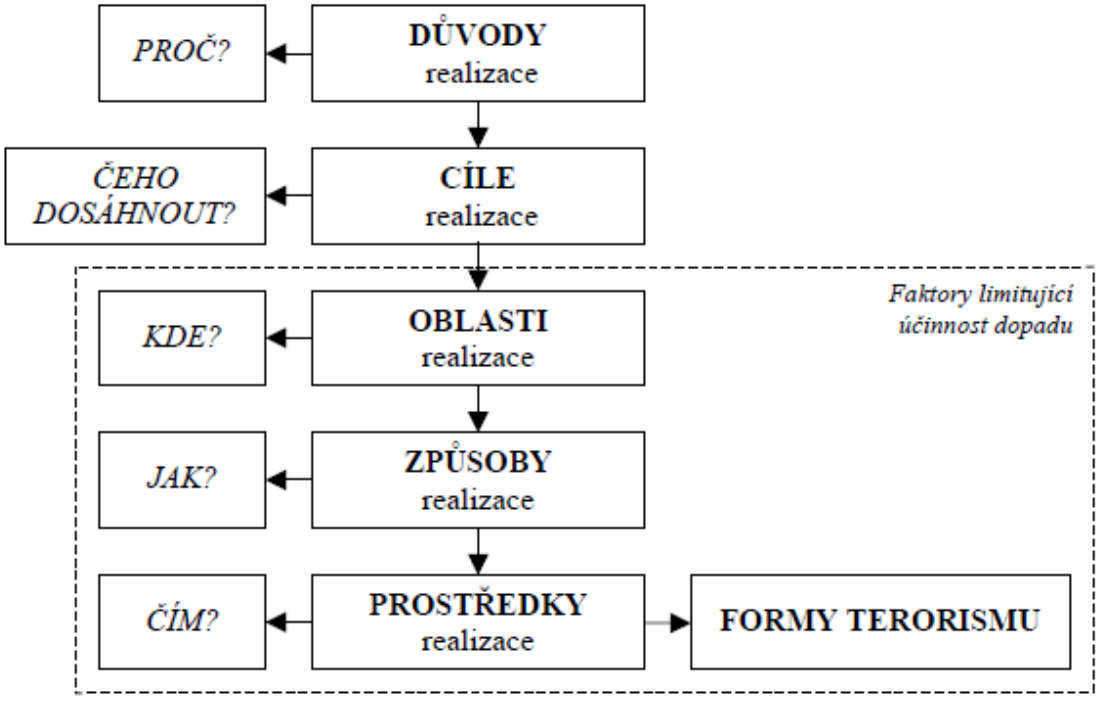
Cílem této práce je seznámit čtenáře se vznikající hrozbou kyberterorismu a zvýšit tak jeho povědomí o této nově vznikající formě terorismu. Část práce se zabývá definicí a podstatou kyberterorismu, popisem jednotlivých forem a metod. V další části jsou představeny jednotlivé hrozby související s tímto tématem. Konec práce je věnován návrhu nejúčinnějšího technického řešení k ochraně.

I. TEORETICKÁ ČÁST

1 PROCES REALIZACE KYBERTERORISTICKÝCH AKCÍ

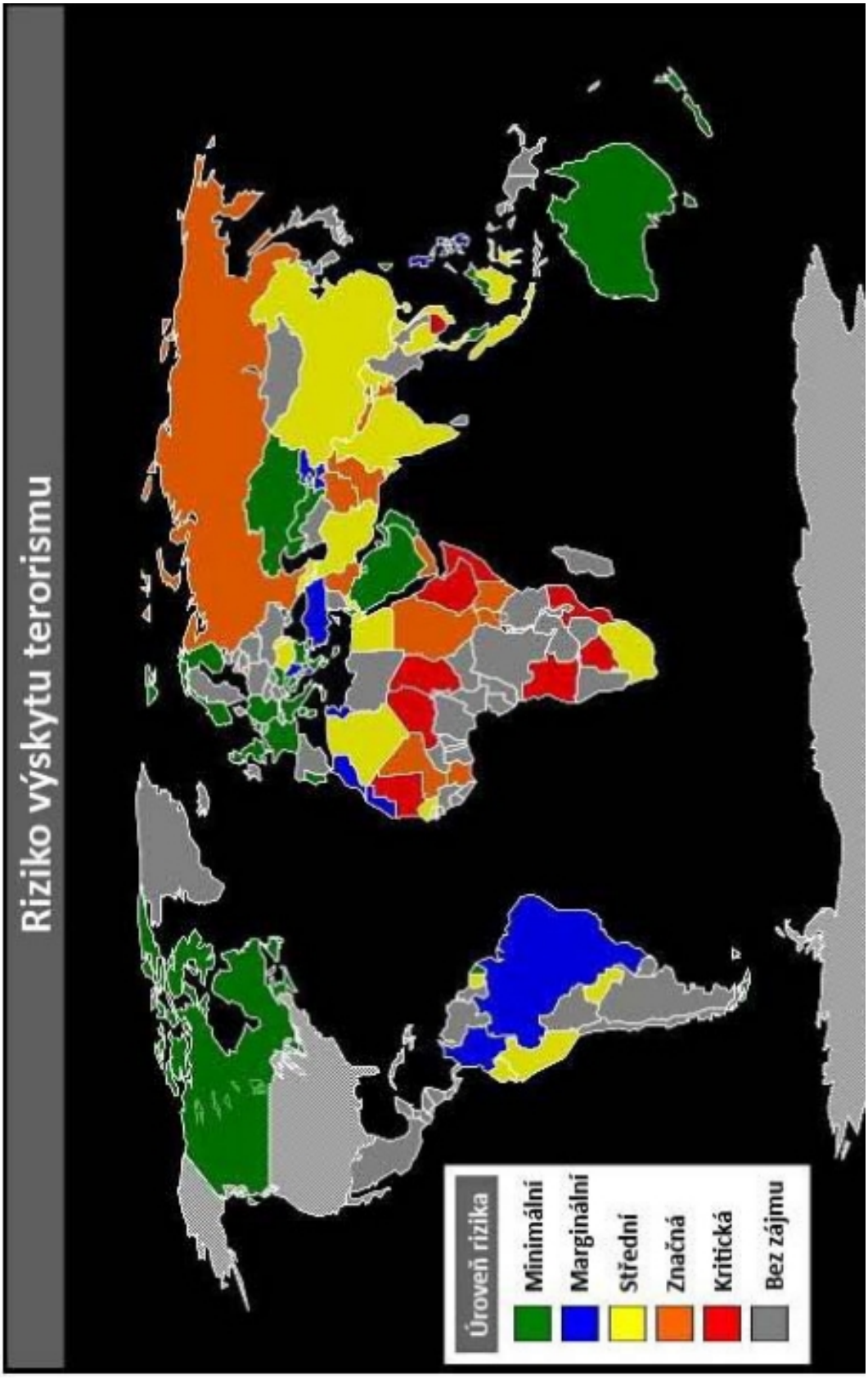
Terorismus je většinou prováděn za konkrétním účelem, který lze označit jako důvod k jeho realizaci. U kyberterorismu je to celkem sporné, jelikož je občas prováděn z nudy nebo pro zábavu a účel v tom případě postrádá. Zprvu byly teroristické akce motivovány spíše ideologicky, avšak s postupem času tento motiv vystřídal a postupně se začal upevňovat terorismus náboženský a nacionalistický. Důsledkem tohoto vývoje je změna teroristických cílů, metod a prostředků.

Teroristický čin, a to i kyberteroristický, je soustředěn na 3 základní faktory – oblast, způsob a prostředky realizace. Při jejich optimální kombinaci, následky realizovaného útoku dosahují vyšší úrovně smrtících a ničivých dopadů. Proces realizace teroristické akce schematicky vyjadřuje obrázek č. 1.



Obrázek 1: Schéma procesu realizace kyberteroristických akcí. [1]

Obrázek na následující straně znázorňuje některé oblasti s nejvyšším rizikem výskytu terorismu a nepřátelských akcí v kyberprostoru i mimo něj.



Obrázek 2: Riziko výskytu terorismu. [19]

2 FORMY TERORISMU

Z dlouhodobého trendu realizace teroristických útoků došlo k celkovému snížení počtu útoků, avšak při současném nárůstu celkového počtu obětí. [1] Také rozsah materiálních škod se podstatně zvýšil. Tento nárůst bývá spojován s nárůstem počtu využívaných forem. Pro snadnější klasifikaci používaných forem je možné provést jejich členění do dvou skupin:

- letální formy,
- neletální formy.

2.1 Letální formy terorismu

Tyto formy terorismu představují využití základních prostředků realizace násilí. Skupinu letálních forem terorismu je možné ještě podrobněji rozčlenit na dvě podskupiny - konvenční a nekonvenční terorismus. Podskupiny se liší použitými prostředky. Do podskupiny **konvenčního terorismu** můžeme zařadit útoky využívající:

- sečné a bodné zbraně,
- střelné zbraně,
- hořlavé látky,
- výbušné zbraně.

Podskupinu letálních **nekonvenčních forem terorismu** představuje především zneužití jednotlivých typů zbraní hromadného ničení, v plné či částečné podobě. Reálnou hrozbu představuje zneužití:

- chemických zbraní,
- zbraní založených na biologickém účinku,
- jaderných zbraní,
- radiologických zbraní,
- termických zbraní.

2.2 Neletální formy terorismu

Útoky, při kterých jsou využívány moderní nástroje, resp. staré, ale novým způsobem v kombinaci s letálními prostředky. Neletální formy terorismu lze rovněž označit jako moderní či sofistikovaný terorismus. Dle používaných prostředků (forem), které jsou při vlastním teroristickém aktu použity, je možno tuto skupinu rozdělit do dvou podskupin. První podskupina představuje terorismus realizovaný běžnými prostředky (unarmed terrorism) a druhá podskupina představuje nekonvenční terorismus.

Terorismus realizovaný běžnými prostředky (unarmed terrorism) – tato podskupina představuje oblast teroristických aktivit, při kterých jsou prostředky každodenního života použity novým způsobem, a to jako zbraň či donucovací prostředek. Zde je možno zařadit zneužití:

- **Dopravních prostředků** jako je automobil, vlak, loď či letadlo. Historie ukazuje, že každý z těchto prostředků byl již použit. Jako příklad zneužití dopravních prostředků při teroristickém útoku lze uvést únosy civilních dopravních letounů, které byly použity 11. září 2001 v New Yorku a Washingtonu ve smyslu řízené střely s lidským naváděním na cíl. Ztráty na lidských životech představovaly téměř 3 000 obětí. Teroristická skupina Al-Kájda v čele s Usámou bin Ládinem je považována za viníka této akce.
- **Výpočetní techniky a Internetu** jako prostředku pro uskutečnění teroristického útoku, označována jako tzv. kyberterorismus. Obdobně jako klasický konvenční terorismus je i kyberterorismus předem plánovaná činnost. Vzhledem k rychlému šíření komunikačních a výpočetních systémů po celém světě, představuje kyberterorismus jedno z velkých nebezpečí 21. století.
- **Mediální terorismus**, někdy také označován jako psychologický terorismus. Jedná se o plánované zneužívání hromadných sdělovacích prostředků a dalších psychologických prostředků v době míru, za účelem ovlivnění názorů, emocí, postojů, chování jednotlivců či cílových skupin populace tak, aby přímo nebo svými důsledky ohrožovaly bezpečnost a ústavní principy státu. Pro moderní vedení propagandy je typické zejména využití široké palety různých masových médií, např. plakátů, filmů, televizních programů, inzerátů, fotografických snímků, novinářských tiskových forem, ale také počítačové techniky. [1]

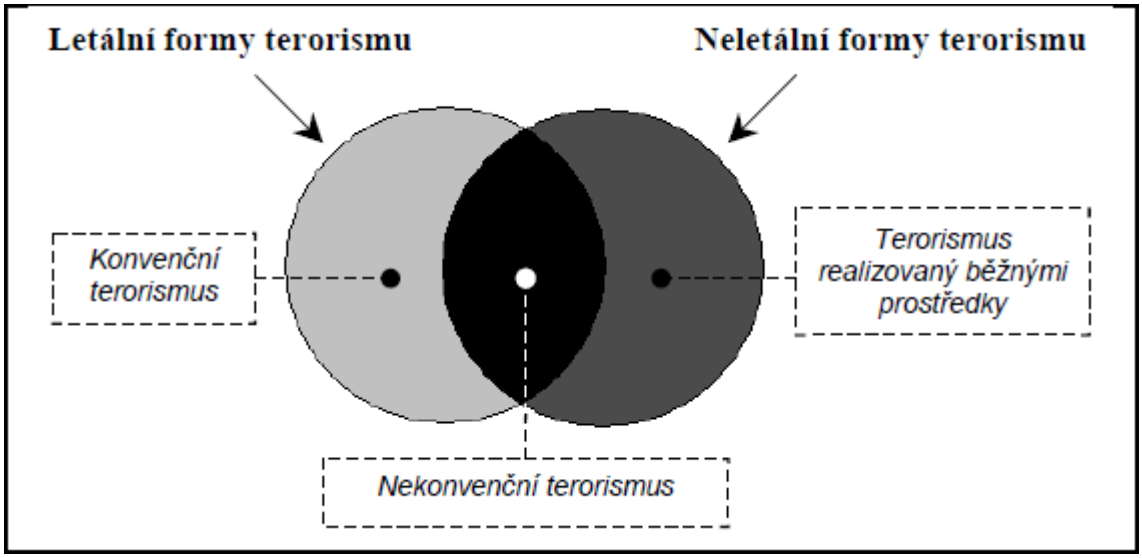
Nekonvenční terorismus

Lze zde zařadit zbraně využívající principy:

- akustiky,
- optiky,
- elektromagnetického pulsu.

Při jejich použití je hlavním efektem vyřazení protivníka na určitou dobu z boje, a to bez přímého ohrožení života. Současně ovšem může dojít i k vyvolání psychického účinku. EMP (elektromagnetického pulz) může být smrtelný pro osoby s kardiostimulátory. Díky tomu, že se jedná o zbraňové prostředky, které jsou neustále podrobovány vývoji, nejsou zatím příliš rozšířeny.

Na obrázku č. 3 je graficky vyjádřen vztah letálních a neletálních forem terorismu.



Obrázek 3: Schéma vztahu letálních a neletálních forem terorismu. [1]

3 KYBERTERORISMUS

Vznik Internetu sebou nese existenci tzv. „informační společnosti“. Tento pojem můžeme definovat jako společnost založenou na intenzivním využívání informačních a komunikačních technologií. Vytváření, šíření a manipulaci s informacemi považuje tato společnost za určující část svých ekonomických, kulturních a společenských aktiv.

Informační společnost se pohybuje v tzv. kyberprostoru, který byl definován Williamem Gibsonem takto: „*Konsensuální halucinace každý den zakoušená miliardami oprávněných operátorů všech národů, dětmi, které se učí základy matematiky. Grafická reprezentace dat abstrahovaných z bank všech počítačů lidského systému. Nedomyslitelná komplexnost. Linie světla seřazené v ne-prostoru mysli, shluky a souhvězdí dat.*“. [2]

Dnes pod pojmem kyberprostor bývá označován svět virtuální reality, v němž se odehrávají různé reálné věci – např. telefonické hovory, e-mailová komunikace a podobně.

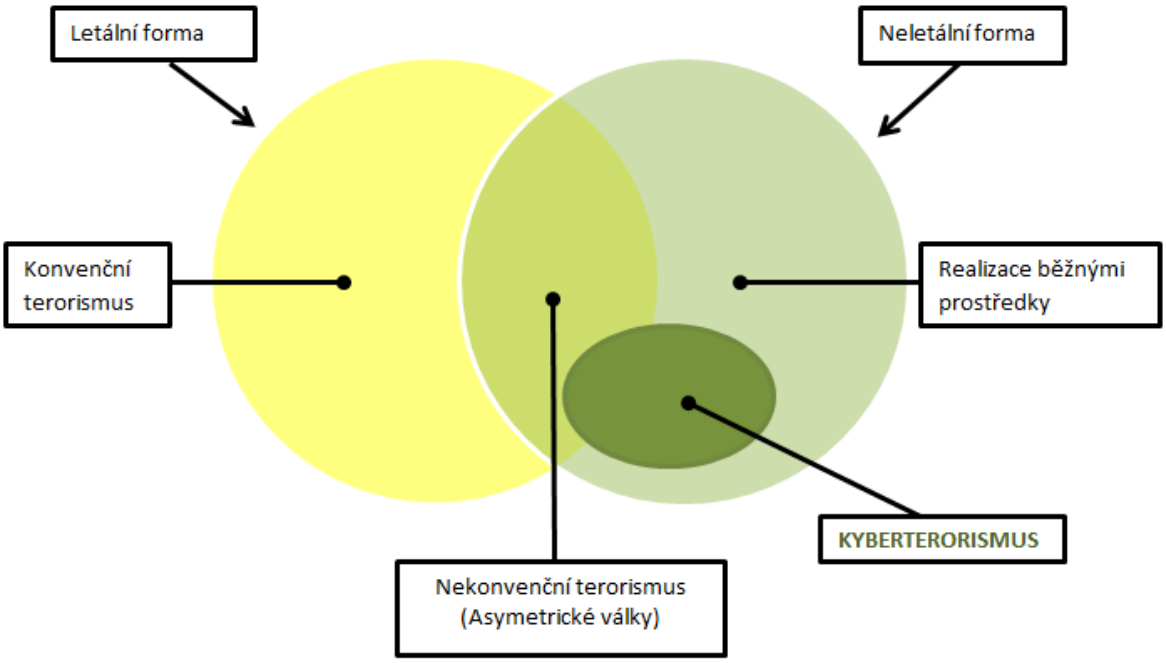
Kyberprostor byl uměle vytvořen, ale stal se neoddělitelnou součástí života společnosti a promítl se do všech jejích součástí. Prioritní dopady:

- závislost na kyberprostoru,
- kybernetická kriminalita,
- používání a zneužívání informace v kyberprostoru,
- kybernetický terorismus a kybernetické války.

Vlastnosti kyberprostoru:

- je globální,
- je decentralizovaný,
- je otevřený,
- obsahuje množství informací,
- je řízen pouze uživateli,
- je interaktivní,
- je závislý na infrastruktuře. [3]

Kyberprostor čelí určitým hrozbám. Jednou z nich je kyberterorismus, který lze začlenit do neletální formy teroristické činnosti realizovanou skrze služby, které podporuje a sdílí daná komunikační či informační síť. Sekundárním důsledkem kyberútoku může být i fyzická likvidace konkrétního objektu nebo systému, což může vést i ke ztrátám na lidských životech, a proto lze neletální formu považovat za vnější skořápku. Je ovšem zřejmé, že se většinou nejedná o primární cíl takového útoku. Začlenění pojmu kyberterorismu do množiny terorismu je graficky znázorněno na obrázku č. 4.

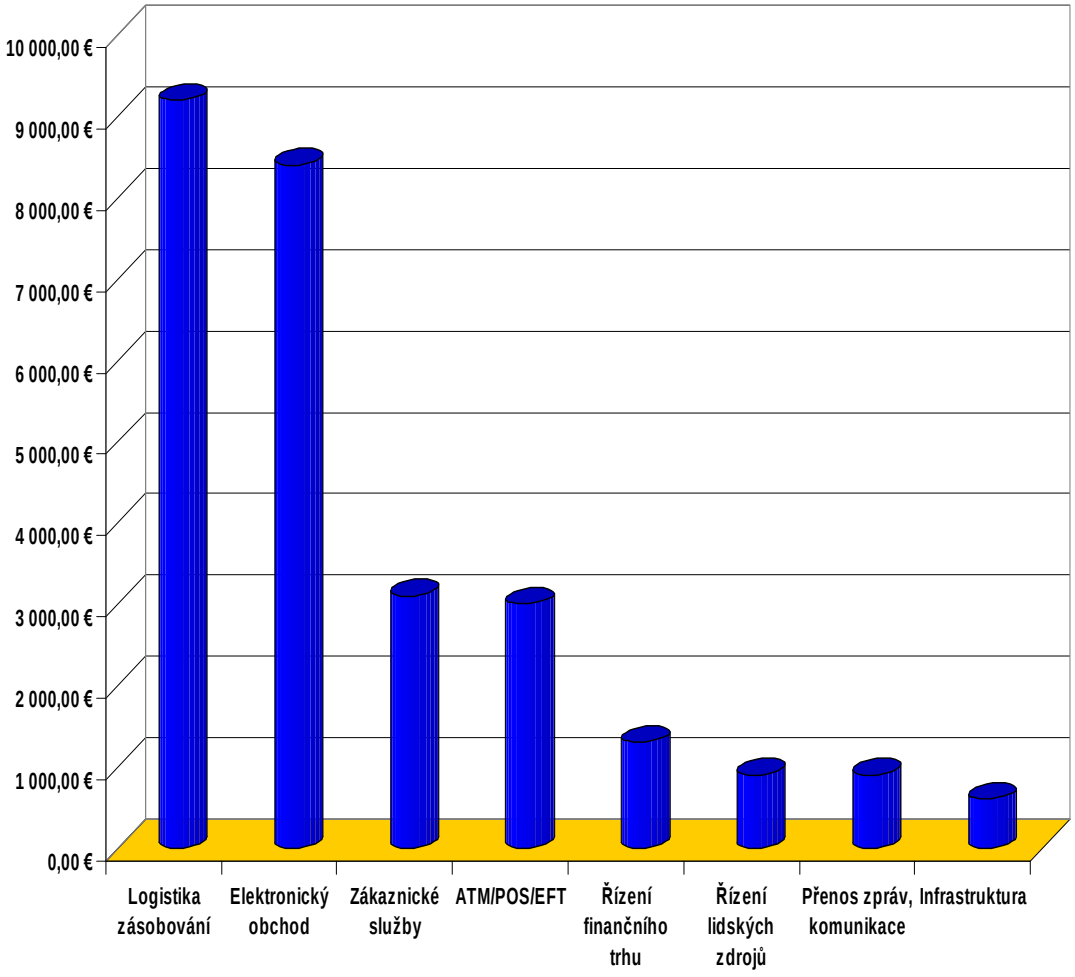


Obrázek 4: Schéma začlenění pojmu kyberterorismu do množiny terorismu. [4]

Oficiální definice kyberterorismu vyřčená D. E. Denningem zní: „*Kyberterorismus je konvergencí terorismu a kyberprostoru obecně chápaný jako nezákonný útok nebo nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným v případě, že útok je konán za účelem zastrašit nebo donutit vládu, nebo obyvatele k podporování sociálních nebo politických cílů.*“. [4]

Definice je bohužel poněkud zavádějící, protože akty kyberterorismu chápe jako útoky směřované proti kritické infrastruktuře, jejichž cílem je získání informační nadvlády. Častěji jsou na Internetu zaznamenány útoky narušující funkci určité služby nebo její součásti, aniž by útok byl veden proti konkrétní společnosti nebo vládě s konkrétním účelem.

Scénáře kybernetických útoků jsou často předmětem kritiky, a to z důvodu uvádění enormní výše škod. Je samozřejmě možné, že některé scénáře jsou poněkud nadsazené, ale škody způsobené výpadky informačních systémů mohou dosahovat opravdu značných rozměrů. Samozřejmě je nutné brát v úvahu fakt, že spousta informačních systémů je závislá na jiných a tudíž může být velmi obtížné definovat globální dopad jejich výpadku. Následující obrázek znázorňuje odhadované ztráty způsobené jednou minutou výpadku informačního systému. Jsou děleny podle typických segmentů trhu. Vyřazení serverů protivníka bývá často cílem kyberteroristického útoku. [2]



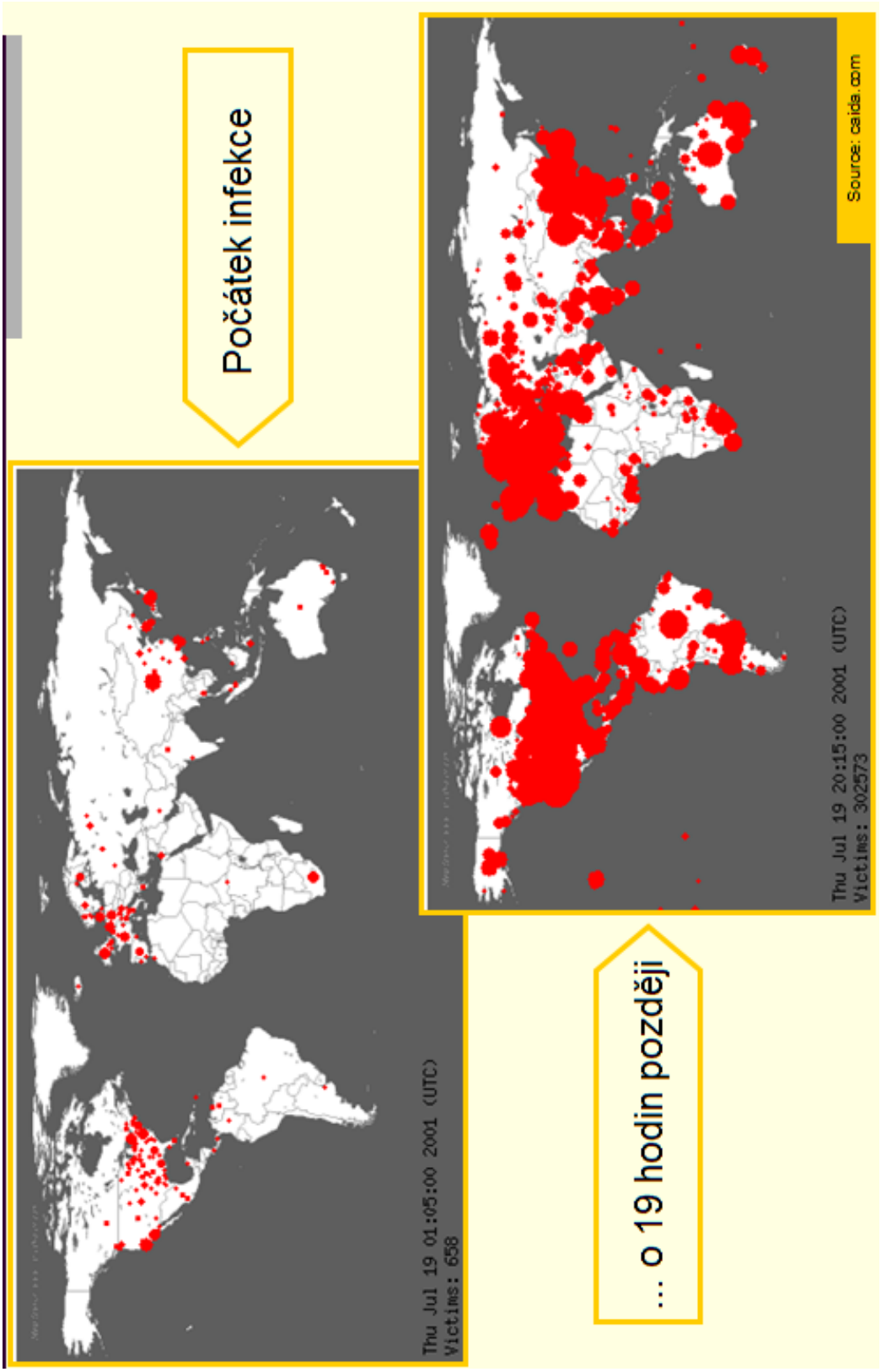
Graf 1: Ztráty za jednu minutu výpadku systému. [4]

Mnoho aktiv vyžaduje vysokou dostupnost systému, zpravidla bez přerušení v tzv. režimu 24x7. Není jednoduché dosáhnout takového stavu, avšak společnosti tuto spolehlivou službu vyžadují zejména ze tří hlavních důvodů:

- **Globalizace obchodu a podnikatelských aktiv** – firmy si otvírají své zahraniční kanceláře a z obchodních důvodů chtějí udržet systém centralizovaný. To znamená, že databáze a aplikace centrálního systému musí být kdykoli k dispozici.
- **Tlak konkurence.**
- **Ztráty při výpadku systému** – je zřejmé, že firma bude automaticky přicházet o značné příjmy každou minutu po dobu výpadku jejího systému, když nebude disponovat systémem poskytujícím služby v režimu 24x7.

Ekonomické dopady kyberterorismu se mohou vyšplhat k obrovským hodnotám. Například vyčíslení škod po viru **Code Red**, který ohrožoval v červenci 2001 americké servery, se podle studie nevládní výzkumné organizace „Computer Economics“ v roce 2001 vyšplhalo až k hodnotě 2,6 miliardy dolarů. [19]

Následující obrázek znázorňuje průběh virové nákazy v kyberprostoru. Šlo o šíření viru **Code Red** během 19 hodin od jeho prvního zjištění. Rychlost šíření je téměř blesková. Šířil se především kvůli chybě na softwarovém webovém serveru Microsoftu. 18. června 2001 zveřejnil Microsoft bezpečnostní bulletin a provedl opravu. Zveřejněním problému (chyby rejstříku v aplikačním rozhraní ISAPI) ukázal protivníkům skulinu, jak proniknout do serverů. Servery, jež nebyly opraveny a tím ochráněny před napadením, byly zranitelné. Obrana tedy byla možná.



Obrázek 5: Průběh virové nákazy v kyberprostoru. [4]

3.1 Teroristické aktivity vůči informačním technologiím

Při pokusu o kategorizaci možných útoků proti informačním technologiím (IT) protistrany dojdeme k následujícím třem základním skupinám:

- **Přímý útok na lokální technologii** - druh útoku je závislý na lokalitě a na významu umístěné technologie.
- **Souběžný útok** - nejnebezpečnější varianta útoku, při které dochází k několika paralelním útokům na konkrétní oblasti či cíle na různých úrovních. V této fázi je kyberútok pouze přípravou pro napadení útočníka nebo podporou pro jeho dezorientaci a likvidaci.
- **Zneužití technologie k řízení teroristické organizace** - Globální charakter informatického a telekomunikačního prostředí umožňuje předávání informací a koordinaci teroristických skupin a aktivit po celém světě. Zde typicky patří např. využití steganografie, spočívající ve skrytí textu do obrázků, pro předávání úkolů a reportů mezi jednotlivými členy skupiny. [2]

3.2 Taxonomie útočníků podle motivace

Motivace útočníků (kyberteroristů) je rozhodně různorodá - od finančního zisku přes slávu, publicitu, zábavu a nudu až po pomstu konkrétní společnosti nebo skupině lidí. Zajisté nejde zcela detailně všechny kyberteroristy zařadit do nějaké skupiny, ale je možné motivačně a typově dané útočníky rozdělit do 10 různých skupin.

3.2.1 Internetový exhibicionismus

Jiným slovem výstřednost, je prvním společným motivačním faktorem, kdy v rámci své skupiny tzv. odborníků mají útočníci touhu být uznáváni.

Script Kiddies

- Nejnižší stupeň hackerského žebříčku, často označován jako tzv. lamer (trapný snaživec).
- Většinou spouští hackerské programy jiných, a to i bez porozumění jejich funkci.

Hacker-začátečník

- Začátečník v oblasti IT, využívající volně dostupných programových nástrojů z Internetu.
- Mezistupeň mezi hackerem – profesionálem a běžným uživatelem.
- Zcela nepokrytě „rozšiřuje“ malware (software nebo kód programu, navržený tak, aby poškodil nebo získal tajný přístup k informacím bez vědomí majitele) do počítačů a tím přímo nebo nepřímo podporuje činnost hackera profesionála.
- Jeho motivací je vzrušení, uznání a sláva v rámci „hackerské“ komunity.
- Neexistují u něj typizované cíle útoků, protože se snaží útočit na cokoli bez ohledu na smysluplnost napadení.

Hacker-profesionál

- Znalec IT, preferující myšlenku hackerství mluvící o svobodném přístupu a sdílení všech informací.
- Jeho motivací je tzv. internetový exhibicionismus.
- Spolupodílnictví -nechce nést přímou vinu za útok a z toho důvodu nechává šířit své programové skripty pomocí jiných uživatelů v počítačové síti popř. skrze hackera-začátečníka.

3.2.2 Pomsta

Další možnou motivací v kyberprostoru je realizace pomsty, jež je vedena proti konkrétní firmě, organizované skupině či zájmové skupině lidí. Zpravidla se jedná o skupiny zkušených lidí nebo IT odborníků.

Virový tvůrce

- Odborník IT, většinou programátor s hlubokými znalostmi bezpečnosti IT a počítačových sítí.
- Motivací je většinou pomsta vůči konkrétní skupině či organizaci nebo společnosti, snaha dokázat světu svou „dokonalost“, překonávání intelektuálních výzev ale někdy i zábava aby se mohli dívat jak svět „hoří“.

- Cílem jeho útoku jsou počítačové systémy a počítačové sítě (útočí prostě na cokoli).

Vnitřní nepřítel

- Nejzákeřnější forma útočníka, nejčastěji představována „zrazeným“ zaměstnancem firmy či organizace.
- Zneužívá svých pravomocí k odplatě vůči organizaci či společnosti.
- IT odborník nebo administrátor výpočetních systémů.
- Velmi dobře využívá maskovaného útoku pomocí malware vedoucí často k likvidaci či vysokým finančním ztrátám pro cílovou společnost.

3.2.3 Zisk

Snaha o finanční zisk, popř. finanční ztrátu pro cílový objekt může být brána jako další velká motivace pro kyberútočníky. Pokusy o odposlechy přihlašovacích údajů do jednotlivých systémů organizací a firem jsou dnes popsány v desítkách variant.

Informační válečník

- Profesionál zabývající se primárně ochranou IT systémů před narušiteli.
- Hluboké znalosti, speciální trénink, díky čemu se stává velmi těžkým protivníkem a ideálním útočníkem.
- Motivace buď ve vlastenectví nebo sounáležitost s náboženskou, sociální či jinou entitou a také i zábava.
- Extrémní motivací může být i snaha o finanční zisk či snaha o finanční likvidaci protivníka.
- Útoky vedeny za účelem destabilizace a poškození integrity dat či nabourání do informačních systémů.
- K dosažení cíle využívá své schopnosti z oblasti bezpečnosti informačních systémů.

Zloděj

- Průměrná znalost IT.
- Zkušenostmi se mění jeho znalost IT, zdokonaluje se až na úroveň profesionálního kriminálníka.

- Motivací je nenasytnost po finančním zisku bez zbytečné slávy a publicity.
- Typický druh útoku je zisk přihlašovacích údajů (phishing) do informačních systémů svých obětí přes podvrženou stránku.

Profesionální kriminálník

- Znalosti z oblasti IT plně využívá k páchání svých protizákonných aktivit, může být i najímán.
- Jeho jediným cílem jsou peníze nebo finanční prospěch.
- Popularita je pro jeho aktivity rizikem.

3.2.4 Publicita a sláva

Poslední možnou motivací k útokům je snaha o publicitu a slávu, mnohdy související s labilní psychikou daného jedince, popř. s traumaty, která zažil.

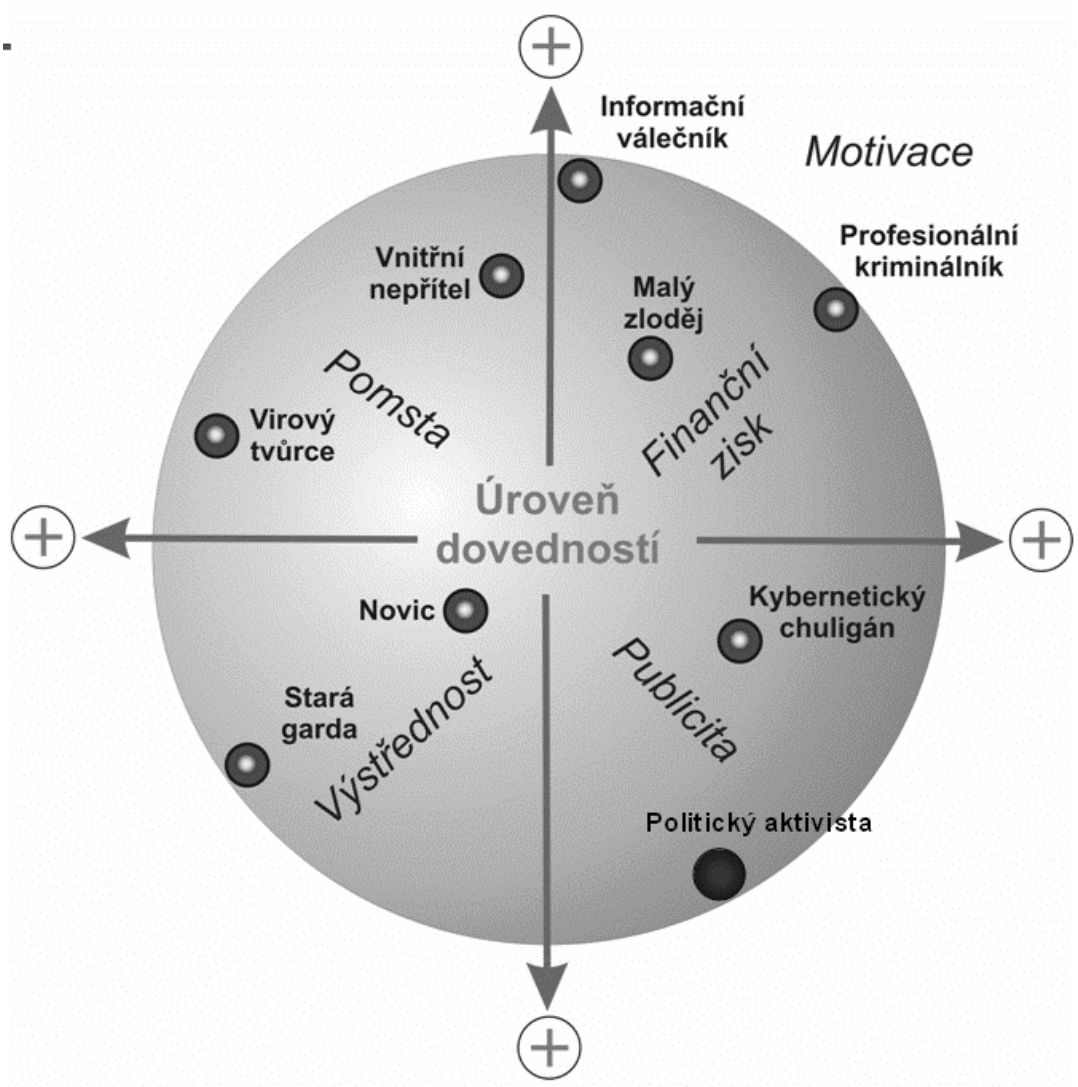
Kybernetický chuligán

- Vyšší znalosti IT, často programující vlastní skripty.
- Vybírá si cíle tak, aby upoutal pozornost médií, proto často útočí na státní nebo polostátní organizace.
- K jeho typickým útokům patří defacement webových stránek (záměna webu za svou verzi), krádeže a zneužití platebních karet, personálních údajů a telekomunikační podvody.

Politický aktivista

- Po informačním válečníkovi druhy nejhorší druh útočníka.
- Znalec IT, jehož snahou je skrze kyberprostor reagovat na politické dění.
- Motivací je mu aktuální politické dění na úrovni národní nebo mezinárodní politiky.
- K dosažení svých cílů využívá v útoku plně svých znalostí - od propagandistického defacementu po přímé napadení a likvidaci informačních systémů.

Členění dle motivace lze považovat za obecnou typizaci útočníků, neboť v běžném životě některé druhy útočníků splývají a jiné se mohou dále detailněji členit. Na následujícím obrázku je možné vidět skupiny v přehledném schématu.



Obrázek 6: Graf klasifikace typů kyber-útočníků. [8]

Kybernetické útoky nejsou ničím novým. Mění se však motivace, která se za nimi skrývá. V budoucnu se nebudeme setkávat s kybernetickými chuligány, jako spíše s vnitřním nepřítelem, autorem virů, profesionálním kriminálníkem či informačním válečníkem.

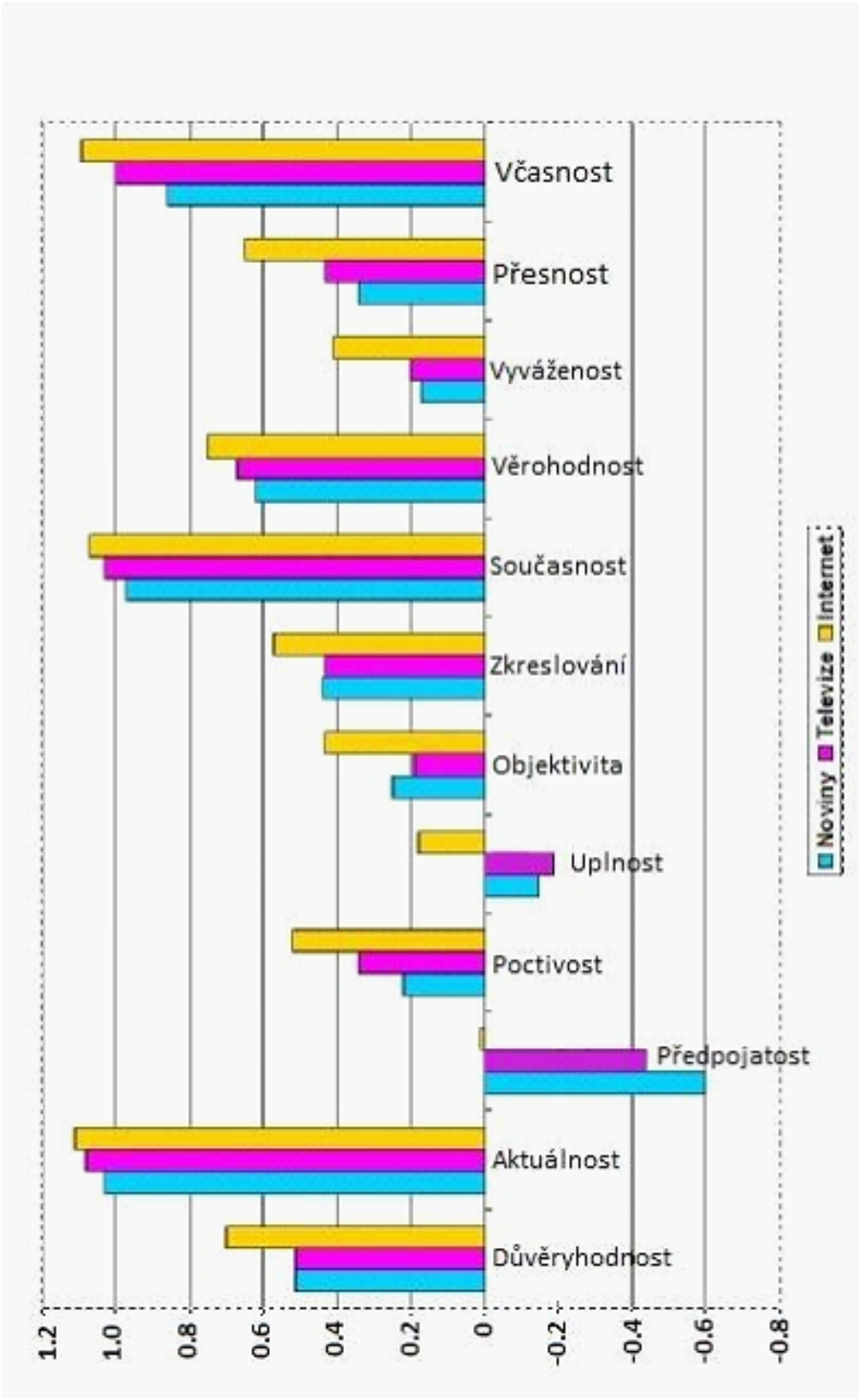
4 NEPŘÍMÝ KYBERTERORISMUS

Existence tzv. nepřímého kyberterorismu byla donedávna opomíjena, a to i přesto, že jeho latentní chování je mnohem nebezpečnější než některé kybernetické útoky. Do této skupiny lze dle Václava Jirovského zařadit terorismus spojený s IT bez přímého vztahu k existující IT infrastruktuře a je příznačně svázán s vývojem „informačního věku“, informatikou a telekomunikacemi. Obecně je založen na využití pocitu svobody, který je podporován vnímáním volnosti na Internetu a sítě IT používá jako nástroj. Patří zde tři typy „terorismu“ související s informačními technologiemi – mediální terorismus, procesní terorismus a tzv. IT governance.

4.1 Mediální terorismus

Hlavní roli zde hrají masová média, mezi něž patří i Internet. Pojem mediální terorismus se objevil v souvislosti s metodami vedení psychologické války a mediálních manipulací. Graf č. 2 dokazuje skutečnost, že důvěra v elektronická média je daleko vyšší než důvěra v média běžné – noviny, televize nebo rozhlas, a to ve všech oblastech. Uvedený graf byl zpracován pro americký kontinent, avšak rozložení jednotlivých skupin se nebude v Evropě příliš lišit.

Pojem mediální terorismus se také často objevuje v souvislosti se sociálními sítěmi typu facebook, twitter atd. Tyto sítě poskytují nástroje pro své členy na organizování akcí, vytváření skupin, které podporují prakticky cokoli, a jednoduchý způsob jak komunikovat s někým na vzdáleném místě. Bohužel stejně jako všechny užitečné věci používané pro špatnosti, můžou se i sociální sítě stát nebezpečnou silou.



Graf 2: Důvěra občanů v různé typy médií. [4]

Mezi základní metody zneužití kyberprostoru pro mediální terorismus patří:

- **Vydávání internetových novin a časopisů**, které významnou část svého obsahu přebírají od svých „korektnějších“ internetových kolegů. Výběrem zpráv a vlastními příspěvky směřují ke změně názorů svých čtenářů ve svůj prospěch.
- **Kybertronika** - zneužívání podprahového vnímání. Do souborů reklamních banerů, na webech nebo prezentacích je zakomponován obrázek s požadovanou zprávou. Obrázek se zjeví pouze na nepatrný zlomek sekundy nebo zakomponován jako nevýrazný vzor do podkladové grafiky.
- **Hacktivismus** - provozování aktivistických stránek a serverů s touto tématikou.
- **Aktivistický spam** můžeme v některých případech zařadit do metod mediálního terorismu, neboť pro rozšíření zprávy je použito veřejné médium. Často jej zasílají různé aktivistické skupiny (náboženské, ekologické apod.) za účelem získat podporu pro svůj program.

Typickým příkladem takového terorismu je případ z konce roku 2001, kdy se objevila zpráva o tom, že FBI implantuje do počítačů sledovací program s názvem „Magic Lantern“ (tzv. Kouzelnou Lampu), a že nutí antivirové společnosti, aby jej nezařazovaly do svých detekčních zařízení. Tím se zvedla obrovská vlna protestů obyvatel a ochránců autorských práv. Později však vyplynulo, že se jednalo o fámu, která se nečekaně nafoukla, a že FBI takový software niky nenavrhla.

4.2 Procesní terorismus

Základem procesního terorismu je zneužití zákonných ustanovení nebo pravidel a soudní moci k vyvolání často až absurdního soudního řízení, jenž vede k omezení bezpečnostních prvků států pod rouškou odstraňování nezákonností. Často úzce souvisí s mediálním terorismem, protože mnohdy je spojen se společenskými aférami nebo kampaněmi. Pokud jsou k dispozici prostředky, je možné pro takovou kampaň najmout specializovanou firmu, která je schopna uspořádat demonstrace, připravit mediální podklady apod. Aktéry jsou většinou nevládní organizace a spolky, které spatřují v takovém konání zejména možnost získání mediální pozornosti. [2]

4.3 IT governance

Se stále zvyšující se závislostí na informačních technologiích vzrůstá tedy i vliv těch, kteří tyto technologie spravují a ovládají, na jim nadřízenou exekutivu. Postupný vznik „IT governance“, čímž je označován stav, kdy fakticky dochází k nenásilné, ale výrazné dominanci firemních složek, odpovědných za správu a provoz informačních technologií, vede k nenápadnému ovlivňování rozhodnutí exekutivy. Požadavky, záměry a strategie IT součásti instituce začínají ovlivňovat i její původní zaměření. Firma se technologizuje, důraz na bezporuchový a vysoký výkon výpočetního systému se stává prvotním zájmem vedení firmy a i nesmyslné nebo nepodstatné požadavky útvarů IT jsou plněny. A to zejména tehdy, když je vhodně vytvořena situace „ohrožení“ důležité dodávky nebo nějaké podstatné funkce firmy. [2]

5 ANALÝZA HROZEB PRO PODNIKY PKB

5.1 Analýza bezpečnostních hrozeb a rizik jako součást bezpečnostní politiky podniku

Kvalifikovaný management podniku mezi prvními akty řízení při jeho vzniku stanoví svou bezpečnostní politiku. Jde o soubor organizačně řídících opatření, norem a pravidel chování, jejichž cílem je zajistit bezpečnost podniku nebo organizace. Bezpečnost podniku můžeme dělit takto:

- **Obecnou** – tím rozumíme zejména ochranu veřejného pořádku v objektu, zajištění přístrojů a zařízení, zásob a ostatních prostředků podnikání.
- **Speciální** – zde patří použití technických prostředků k ochraně majetku a osob (CCTV,PZS,EPS, EKV apod.).
- **Zvláštní** – tato bezpečnost zahrnuje ochranu dat a zajištění informačních a telekomunikačních sítí, ochrana know-how podniku, ochrana utajovaných informací a podobně.

Dokument „Bezpečnostní politiky podniku“ se po zpracování stává zastřešující normou bezpečnosti organizace. Při vzniku mimořádných událostí musí být tento dokument okamžitě k dispozici.

Analýza bezpečnostních hrozeb a rizik a její výstupy jsou součásti bezpečnostní politiky podniku.

5.2 Obecný postup analýzy hrozeb a rizik

Analýza hrozeb a rizik je počátečním, východiskovým krokem před začátkem projektování jakéhokoli bezpečnostního systému. Je to proces, ve kterém se podrobně identifikují hrozby, určuje se jejich velikost a zkoumá se jejich vliv na bezpečnost posuzovaného subjektu. Velikost rizika se vyhodnocuje s cílem současně stanovit hodnoty pro:

- pravděpodobnost, že se ohrožení projeví,
- následek, který vznikne, když se ohrožení projeví.

Obsah analýzy rizik je následující:

- Analýza bezpečnostního prostředí a identifikace hrozeb vyskytujících se v bezpečnostním prostředí.
- Kvantifikaci hrozeb, spočívající v jejich ohodnocení.
- Kvantifikaci možných důsledků působení hrozby.
- Ohodnocení rizika, které zahrnuje přiřazení číselné nebo jiné hodnoty, umožňující stanovit jeho závažnost.

Zvažování nejhorší varianty realizace hrozby při analýze hrozeb a rizik je nezbytné. Výsledky této analýzy napomáhají k určení priorit v procesu zvládání rizik a při realizaci opatření k jejich snížení nebo zamezení. Cílem je ochrana hodnot, které jsou z hlediska referenčního objektu vnímání jako značná újma.

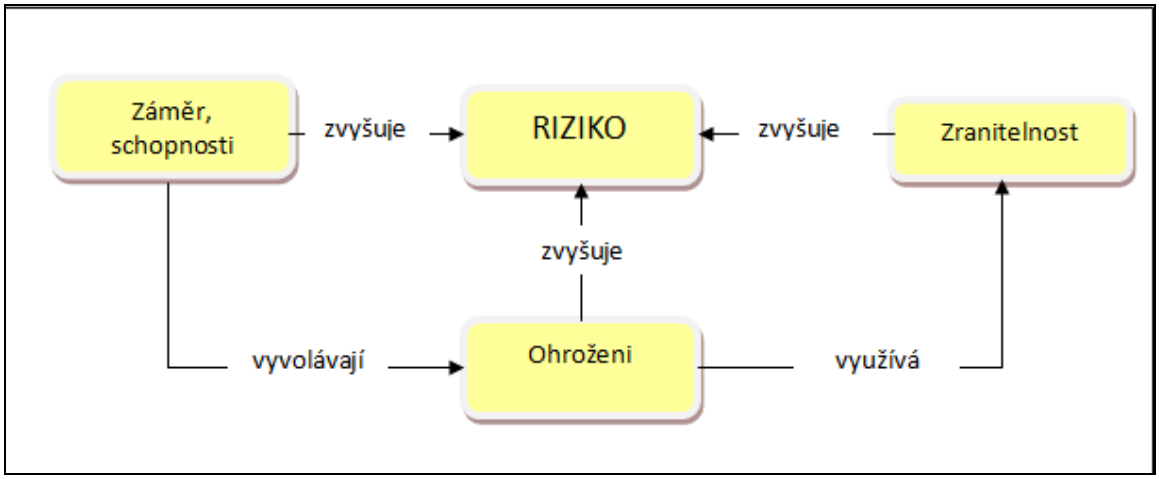
5.3 Hrozba a riziko v bezpečnostní terminologii ve vztahu k informačním systémům

Pod označením **hrozba,** můžeme chápat cokoliv, co nějakým způsobem může vést k nežádoucí změně informace, chování systému nebo k ovlivnění jeho parametrů. Zde je možno zahrnout osoby, prostředky, události nebo i myšlenky, které představují nějaké potencionální narušení důvěrnosti, integrity, dostupnosti nebo legálnosti použití systému. Útok je faktickou realizací hrozby. Ochranou pak rozumíme veškeré fyzické mechanismy, definované politiky nebo procesy, které mají sloužit k ochraně systému nebo obecně majetku před hrozbou nebo útokem. Každá ochrana se však vyznačuje zranitelností, což jsou většinou slabá místa ochrany nebo její úplná absence. [2]

Velmi důležitým pojmem je již zmíněné **riziko,** jehož míru můžeme vztáhnout k hodnotě chráněného majetku v případě, že dojde k úspěšnému útoku ve zranitelném místě systému. Riziko bude vysoké, když hodnota chráněného majetku je vysoká a existuje velká pravděpodobnost úspěšného útoku. Naopak, riziko bude malé, pokud hodnota chráněného majetku bude nízká nebo bude malá pravděpodobnost úspěšného útoku. [2]

Odlišnost fenoménů hrozby a rizika můžeme dle Petra Zemana shrnout do lapidární formulace:

„Hrozeb se obáváme, rizika z nich plynoucí jednak poměřujeme, jednak je podstupujeme.“.[25]



Obrázek 7: Vztah činitelů rizika. [26]

5.4 Kategorizace kyberteroristických hrozeb

Nelze říct, že v současné době existuje nějaké univerzální rozčlenění hrozeb, neboť jejich význam a existence se mění podle prostředí, ve kterém ohrožený proces probíhá a navíc se celkově dynamicky vyvíjí, takže je možné, že na něco stejně zapomeneme. Abychom byli schopni popsat roli bezpečnostních prvků systému v počítačové síti a také veškeré entity s hrozbou spojené, můžeme shrnout některé rysy hrozeb do tří velkých skupin – základní hrozby, aktivační hrozby a podkladové hrozby.

5.4.1 Základní hrozby

Lze rozeznat čtyři skupiny základních hrozeb, které odrážejí čtyři hlediska bezpečnosti informačních systémů:

- **Únik informace** - případ, kdy informace důvěrného charakteru je prozrazena neautorizovaným subjektem nebo je jím odhalena. Takový únik informace může vést k přímým útokům se značným dopadem.
- **Narušení integrity** - porušení konzistence dat, kdy může dojít k vytvoření nových dat, změně či k vymazání stávajících dat neautorizovaným subjektem.

- **Potlačení služby** - úmyslné bránění přístupu legitimnímu subjektu k informacím nebo jiným systémovým zdrojům. Příkladem jsou známé útoky DOS, často i DDOS, kdy úmyslné vytvoření vysoké zátěže nelegitimními žádostmi vede k neúspěšným pokusům o přístup legitimních subjektů.
- **Nelegitimní použití** - zdroj je používán neautorizovaným subjektem nebo neadekvátním způsobem. Příkladem je průnik do systému a používání placených služeb, aniž by došlo k opravdovému vyúčtování a zaplacení služby.

5.4.2 Aktivační hrozby

Realizace aktivačních hrozeb vede k bezprostřednímu vytvoření základní hrozby, tím i k přímému ohrožení bezpečnostních parametrů systému. Odtud také plyne jejich název, protože aktivují základní hrozby. Rozdělení je následující:

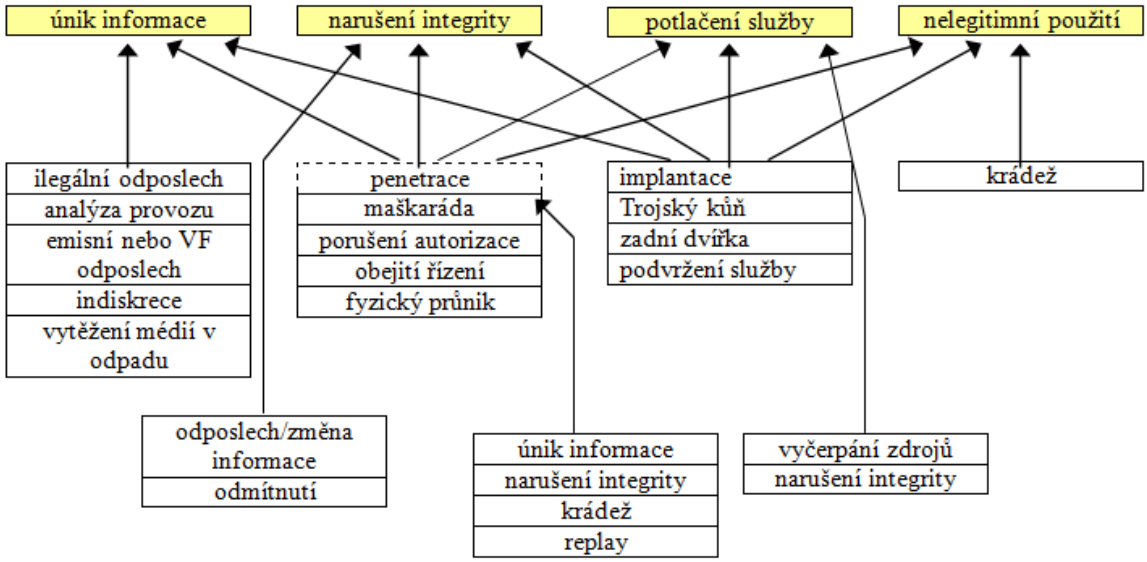
- Penetrační hrozby:
    - **Maškaráda** - stav, kdy se jedna entita (osoba nebo systém) představuje jako jiná entita. Jde o jeden z nejběžnějších způsobů narušení bezpečnostního perimetru systému. Např. neautorizovaná entita „přesvědčí“ příslušný ochranný systém o tom, že je odpovídající autorizovaná entita a tím využívá všech práv a privilegií oné fiktivní autorizované entity.
    - **Obejití řízení** - zde útočník využije systémové nebo bezpečnostní slabiny k získání neautorizovaných práv a privilegií.
    - **Narušení autorizace -** jedná se o zneužití autorizovaného přístupu ke zdroji pro neautorizované účely. Útok musí být veden zevnitř systému uživatelem, který má k němu přístup. Nejedná se ani tak o selhání systémové jako o selhání personální.
    - **Sociální inženýrství** - ovlivňování a přesvědčování lidí s cílem oklamat je tak, aby uvěřili, že sociotechnik je osoba s totožností, kterou předstírá.
- Implantační hrozby:
    - **Trojský kůň** - jedná se o software obsahující část kódu, který po spuštění ohrozí bezpečnost uživatele.

- **Zadní vrátka** – případ, kdy je do systému zabudována vlastnost nebo vložena součást, která při jisté konstelaci vstupních dat umožní obejít bezpečnostní mechanismy.

Když implantovaná součást software ležela v systému již dostatečně dlouho a případný „implantátor“ je mimo podezření nebo dosah, jsou implantační hrozby probouzeny autory až po nějaké době.

5.4.3 Podkladové hrozby

Analyzujeme-li základní a aktivační hrozby v nějakém systémovém prostředí, můžeme určit některé hrozby, které mohou vést ke vzniku i několika základních hrozeb. Např. uvažujeme-li o úniku informací jako o základní hrozbě, pak najdeme několik hrozeb, které mohou vést k úniku informace – tajný odposlech, indiskrece zaměstnance nebo analýza komunikačního provozu. Hrozbám, které jsou tedy podkladem pro uskutečnění až několika základních hrozeb říkáme podkladové hrozby. Vztah mezi základními hrozbami a podkladovými hrozbami je znázorněn na obrázku č. 8.



Obrázek 8: Vztah základních a podkladových hrozeb. [2]

5.5 Prognóza hrozeb do roku 2017

Celkový pohled na hrozby ICT znázorňuje graf č. 3. Tento graf vytvořila v roce 2006 firma Gartner, poskytující analytické a srovnávací studie v oblasti nových technologií, produktů a jejich dopadů, včetně bezpečnostních. Při detailním zkoumání grafu je nutné si uvědomit, že většina hrozeb již plně propukla.

Na ose y je vyjádřena míra výskytu dané hrozby, na ose x pak její vyspělost. To znamená, že v levé části osy x najdeme zcela nové hrozby, které se teprve začínají objevovat nebo se o nich začíná diskutovat, v pravé části pak hrozby, které se staly součástí každodenního života.

Je možné říci, že hrozba ve svém historickém vývoji prochází grafem postupně z leva doprava. Zprvu se objevuje s nějakou novou technologií, aby se za nějakou dobu ustálila a stala se stálou, vyspělou hrozbou, které je nutné věnovat neustále pozornost. Je ale také možné, že nějaké hrozby se mohou v polovině grafu ztratit (neprojdou všemi oblastmi).

Křivka grafu je rozdělena do pěti základních oblastí:

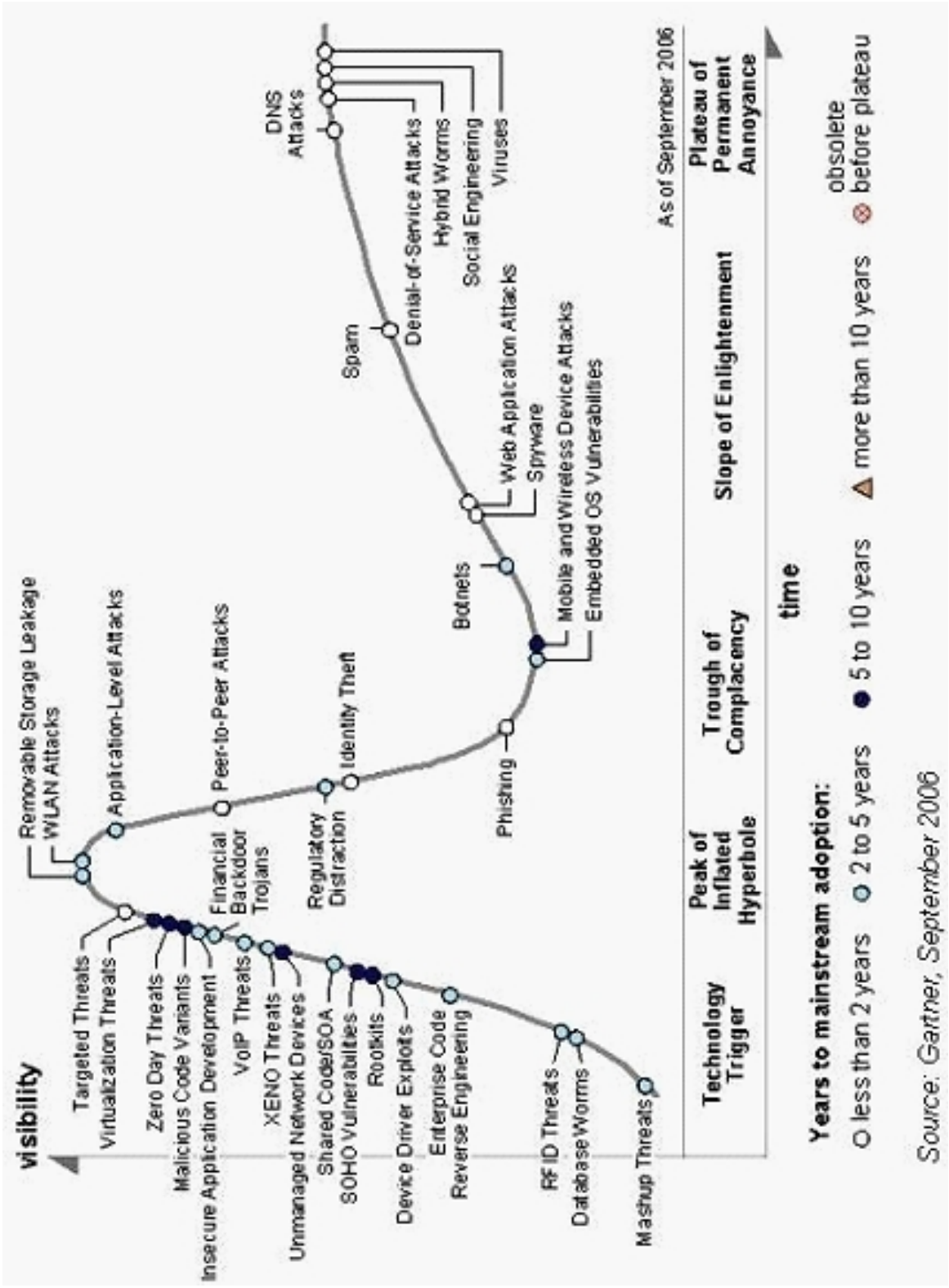
1) **Oblast nových technologických hrozeb** (Technology Trigger) - zde patří zcela nové hrozby, které se objevují s novými technologiemi. Jedná se o novinky na trhu nebo ve sledované oblasti.

2) **Vrchol zvýšeného zájmu** (Peak of Inflated Hyperbole) - zde je možno zařadit hrozby, o kterých se hovoří a je jim věnována velká pozornost. Velké úsilí je směřováno na ochranu.

3) **Oblast ztráty zájmu** (Trough of Irrelevance) - hrozby, o kterých se přestává mluvit, svůj vrchol mají už za sebou. Původní předpoklady se nestaly skutečností.

4) **Oblast renesance** (Slope of Enlightenment) – technologie a hrozba se postupně stává realitou, začíná se vyskytovat ve velké míře.

5) **Oblast trvalých potíží (**Plateau of Permanent Annoyance) – hrozba se běžně projevuje, její masová rozšířenost způsobuje závažné problémy. [31]



Graf 3: Pohled na hrozby v Hype Cycle diagramu z roku 2006. [28]

Název hrozby	Popis
Nespokojení zaměstnanci (insiders)	Nespokojení zaměstnanci přestavují velké riziko z důvodu znalostí chodu firmy a její bezpečnostní nedostatky. Může tedy napadnout firmu v tom nejslabším místě a s největšími dopady na firmu.
Fyzický útok proti informační infrastruktuře (Physical Attack)	Fyzické napadení informačního systému a jeho případná destrukce, znamená pro firmu absolutní kolaps.
Špionáž (Spying)	Špionáž ohrožuje firemní know-how a interní informace, tím může překazit zájmy firmy.
Krádež identity, e-identity (Identity Theft)	Krádeží identity rozumíme krádež osobních informací za účelem spáchání trestné činnosti.
Sociální inženýrství (Social Engineering)	Metoda, způsob manipulace s lidmi za účelem získání určité informace nebo provedení akce. Pouhým lidským faktorem jsou prolomena bezpečnostní, organizační a technologická opatření.
Spyware	Programy, jež skrytě monitorují chování uživatele a svá zjištění zasílají subjektu, který program vytvořil, popřípadě umístil.
Cílené hrozby (Target Threats)	Kybernetické útoky s finanční, politickou či jinou motivací vedené proti konkrétní firmě, i celému oboru (průmyslu).
Viry (Viruses)	Parazitující soubor, který je schopen napadnout programy a systémové oblasti a následně je pozměnit. Může se i dále rozšiřovat, nebo provést destrukci operačního systému.
DOS útoky (Denial of Service Attacks)	Potlačení služby. Hlavní funkcí útoku není proniknutí do systému, ale spíše degradace jeho činnosti a následné znemožnění jeho používání.
DNS útoky (DNS Attacks)	Útoky na jmenné doménové servery. Překlad jmen na podvržené adresy a tím změněná místa určení zpráv. Nejenom že způsobí zmatek v příslušné doméně, ale může sloužit i k získání jinak nedosažitelných datových toků.
Hybridní červi (Hybrid Worms)	Komplexní programy, samo spustitelné, analyzují slabá místa softwaru.

„Peer to peer“ útoky **(Peer to peer Attacks)**	Peer to peer prostředí umožňuje přenos virů. Například Instant messaging (IM).
Phishing	„Rybaření“. Technika používaná k získávání citlivých údajů od oběti útoku. Příkladem je rozesílání emailu od banky se žádostí zadání údajů na odkazovanou stránku.
Spam	Nevyžádaná elektronická pošta. K jeho šíření se mnohdy používají botnety.
Útoky na webové aplikace **(Web Application Attacks)**	Soubor útoků na webové aplikace, zneužívající slabá místa webu. Není vyloučena jejich změna (defacement).
Útoky na aplikační úrovni **(Application Level Attacks)**	Aplikace vyvinuté a provozované bez webového rozhraní.
Botnety (Bootnets)	Softwaroví roboti, pracující v autonomním režimu mimo kontrolu napadeného prostředí.
Databázoví červi **(Database Worms)**	Samo šířící, zaměření na systém řízení relační databáze. V krátkém čase jsou schopni zničit velké množství dat.
Finanční trojští koně **(Financial Trojans Backdoor)**	Škodlivý software typu trojského koně, speciálně určený pro finanční podvody.
Nezabezpečený aplikační vývoj **(Insecure Application Development)**	Umožní útočníkovi detekovat a zneužít slabá místa softwaru.
Zranitelnost rozšířených operačních systémů **(Embedded OS Vulnerabilities)**	Operační systémy jsou přenášeny do prostředí koncových zařízení (bankomaty, procesní kontrolery), kde byly v minulosti jiné operační systémy. Cílem je zajištění kompatibility. Problém je, že koncová zařízení jsou slaběji chráněna proti hrozbám.
Hrozby regulatorních, auditorských společností **(Regulatory Distraction)**	Auditorské společnosti mnohdy požadují po instituci množství kritických informací. Jejich zneužití by instituci přineslo velké ztráty.
Úniky dat z přenositelných médií **(Removable Storage Leakage)**	Přenositelná média umožňují přenos dat i mimo organizaci. I v případě, kdy je přenos autorizován, může být médium odcizeno.
Hrozby RFID	Útoky proti soukromí a majetku. Změna identity osob a zboží. Mohou být spojeny s útoky na vyhodnocovací

(RFID Threats)	systém pomocí virů.
Útoky na bezdrátové sítě **(WLAN Attacks)**	Pokud je komunikace přes bezdrátovou síť organizace nechráněná, může přes ni dojít k úniku mnoha citlivých informací.
Hrozby VoIP **(VoIP Threats)**	Termín pro IP a internetovou telefonii. Hlasové služby mohou ohrozit útoky typu DOS, DNS nebo technologická zranitelnost.
Outsourcing v zahraničí **(XENO Threats)**	Jde zpravidla o outsourcing datových center, kde hrozí manipulace nebo únik dat.
Reverzní inženýrství firemních zdrojových kódů **(Enterprise Code Reverse Engineering)**	Předmětem je analýza zdrojových kódů podnikových aplikací za účelem zjištění zranitelnosti, know-how a následného odcizení.
Hrozby webu 2. generace **(Mashup Threats)**	Tyto weby umožňují směšování obsahů různých webových stránek pomocí aktivního skriptování na straně prohlížeče.
Rootkity **(Rootkits)**	Programy, které útočníkovi umožňují skrýt svou nekalou činnost. Slouží k maskování změn v registrech, procesech, popř. k maskování zvýšené síťové aktivity.
Nespravovaná koncová zařízení **(Unmanaged Network Device)**	Zařízení, která jsou připojena do sítě instituce, ale nejsou registrována a nijak řízena. (tiskárny, kopírky apod.)
Virtualizační hrozby **(Virtualization Threats)**	Zranitelnost operačních systémů, využívající virtualizační technologie, virtuální manažery.
Hrozby „nechráněného“ dne **(Zero Day Threats)**	Útoky prováděné ještě předtím, než je dodána nová verze softwaru odstraňujícího nedostatky.
Útoky na mobilní a bezdrátová zařízení **(Mobile and Wireless Device Attacks)**	Viry mohou napadnout jak mobilní telefon, tak i bezdrátová zařízení. Taktéž mohou být tato zařízení odcizena spolu s citlivými daty v nich.
Generátory zákeřných kódů **(Malicious Code Software)**	Jde o generátory škodlivých kódů (virů, červů apod.). Velké množství kódů je rychle generováno v nejrůznějších variantách. Některé antivirové ochrany mohou být prolomeny, když včas nezareagují na nově vzniklou hrozbu.

Tabulka 1: Popis hrozeb z grafu č. 3. [31]

Většina hrozeb je již aktuálních a zcela běžně se s nimi setkáváme. S výhledem do budoucna je možné počítat například se zneužitím nanotechnologií. Z následující tabulky je možné vyčíst dopad jednotlivých hrozeb.

Dopad	**Aktuální hrozby**		
Transformovatelný			Rootkity
Vysoký	Krádeže identity Sociální inženýrství Spyware Cílené hrozby Viry	Útoky na aplikační úrovni Bootnety Databázoví červy Nezabezpečený aplikační vývoj Špionáž	Nezpracovaná koncová zařízeni Virtualizační hrozby Hrozby "nechráněného dne" Fyzický útok proti informační infrastruktuře Nespokojení zaměstnanci
Střední	DoS útoky DNS útoky Hybridní červi "Peer to peer" útoky Phishing Spam Útoky na webové aplikace	Zneužití ovladačů koncových zařízení Zranitelnost rozšířených OS Únik dat z přenositelných médií Hrozby RFID Sdílený kód/SOA Hrozby VoIP Útoky na bezdrátové sítě (WLAN) Outsourcing v zahraničí	Útoky na mobilní a bezdrátová zařízení
Nízký		Rezervní inženýrství firemních zdrojových kódů Hrozby webu 2. gnerace	Generátory zákeřných kódů Zneužití malých kancelářských nebo domácích aplikací

Tabulka 2: Aktuální hrozby a jejich dopad. [31]

6 SOUČASNÝ STAV V ČR

Řada uživatelů počítačů a Internetu, včetně firem a orgánů státní správy, a to nejen v ČR, si neuvědomuje rozsah nebezpečí kybernetické kriminality a ještě méně kyberterorismu. Přitom se už dnes běžně setkáváme s mediálním či procesním terorismem. Setkáme se také s viry, červy či útoky DOS, což jsou jevy, se kterými si dokážeme poradit. Problém ovšem spočívá v nově vznikajících hrozbách, což jsou v 21. století útoky na SCADA systémy.

Problémem je také legislativa, která se ve státech Evropské unie liší. Je to dáno i tím, že současné zákonodárství staví na staletých základech, tradicích. Snažíme se o modifikaci zákonů, postihovat něco co existuje chvíli, a tudíž to neumíme.

6.1 Role odboru kybernetických hrozeb k ochraně českého kybernetického prostoru

Tento orgán byl založen vládním usnesením č. 205 z 15. 3. 2010, ve kterém jsou definovány i základní úkoly odboru. Dále jsou úkoly rozvedeny ve vládním usnesení č. 380 z 24. 5. 2010. Vzhledem k prozatím krátkému působení je odbor kybernetické bezpečnosti ve fázi formování, ale je nepochybné, že bude hrát důležitou roli v informační bezpečnosti na národní i mezinárodní úrovni.

6.1.1 Přijetí zásadních vládních usnesení

6.1.1.1 Vládní usnesení č. 205 z 15. 3. 2010

Ministerstvo vnitra je ustanoveno gestorem problematiky kybernetické bezpečnosti a také národní autoritou pro oblast kybernetické bezpečnosti s těmito úkoly:

- Koordinovat činnost ostatních státních institucí v oblasti zajišťování kybernetické bezpečnosti.
- Koordinovat zastupování České republiky v otázkách kybernetické bezpečnosti na mezinárodních fórech, včetně účasti státních orgánů na činnosti příslušných mezinárodních organizací.
- Předložit vládě ke schválení statut meziresortní koordinační rady pro kybernetickou bezpečnost.

- Předložit vládě strategii pro oblast kybernetické bezpečnosti.
- Zahájit zajišťování provozu vládního pracoviště CSIRT. [5]

6.1.1.2 Vládní usnesení č. 380 z 24. 5. 2010

Koordinační meziresortní rada pro oblast kybernetické bezpečnosti podporuje výkon gesční a koordinační role MV ČR v oblasti kybernetické bezpečnosti vyžadující součinnost státních institucí a v této oblasti plní mimo jiné tyto úkoly:

- Koordinuje činnost státních institucí v oblasti kybernetické bezpečnosti.
- Koordinuje státní instituce při plnění úkolů vyplývajících z členství ČR v mezinárodních organizacích.
- Vytváří podmínky pro hladké fungování spolupráce mezi členy rady.
- Řeší aktuální otázky a předkládá odborné návrhy a doporučení ministru vnitra a jeho prostřednictvím vládě.
- Sleduje plnění závěrů z jednání rady jejími členy.
- Spolupracuje s externími odbornými subjekty a využívá jejich výstupů v zájmu zajišťování kybernetické bezpečnosti ČR.
- Zřízení rady a výkon její činnosti nezbavuje státní instituce zodpovědnosti kybernetickou bezpečnost v rámci kompetencí. [5]

Složení koordinační meziresortní rady pro oblast kybernetické bezpečnosti:

- Předseda – ministr vnitra.
- Výkonný místopředseda – náměstek ministra vnitra pro vnitřní bezpečnost.
- Tajemník rady – ředitel odboru kybernetické bezpečnosti.
- Členové:
    - Policie ČR,
    - Ministerstvo obrany,
    - Ministerstvo zahraničních věcí,
    - Ministerstvo financí,

- Ministerstvo průmyslu a obchodu,
- Ministerstvo dopravy,
- Národní bezpečnostní úřad,
- Česká národní banka,
- Úřad pro zahraniční styky a informace,
- Bezpečnostní informační služba,
- Vojenské zpravodajství,
- Český telekomunikační úřad.

Pro specifické úkoly zřizuje Koordinační rada v případě potřeby pracovní skupiny, do kterých může přizvat externí odborné subjekty.

6.1.2 Cíle odboru kybernetické bezpečnosti

- Vybudovat sebe sama (vytvořit organizační strukturu, najít prostory, zajistit financování, obsazení, vybavení).
- Zajistit plnění úkolů vyplývajících z vládního usnesení 205.
- Zapojit se aktivně do cvičení kybernetické obrany.
- Iniciovat zefektivnění programů počítačového vzdělání na všech stupních škol.
- Vybudovat pracoviště CSIRT/CERT na základě převzetí zkušeností modelového pracoviště CSIRT.CZ.

Aby nebyl cíl ztracen z dohledu, je zapotřebí využít tuzemských i zahraničních zkušeností. Trvalý přísun výsledků výzkumných projektů z akademické sféry nesmí být opomíjen stejně jako nabízení pomocných rukou. Maximum potenciálu je zapotřebí využít i u odborníků v různých oborech:

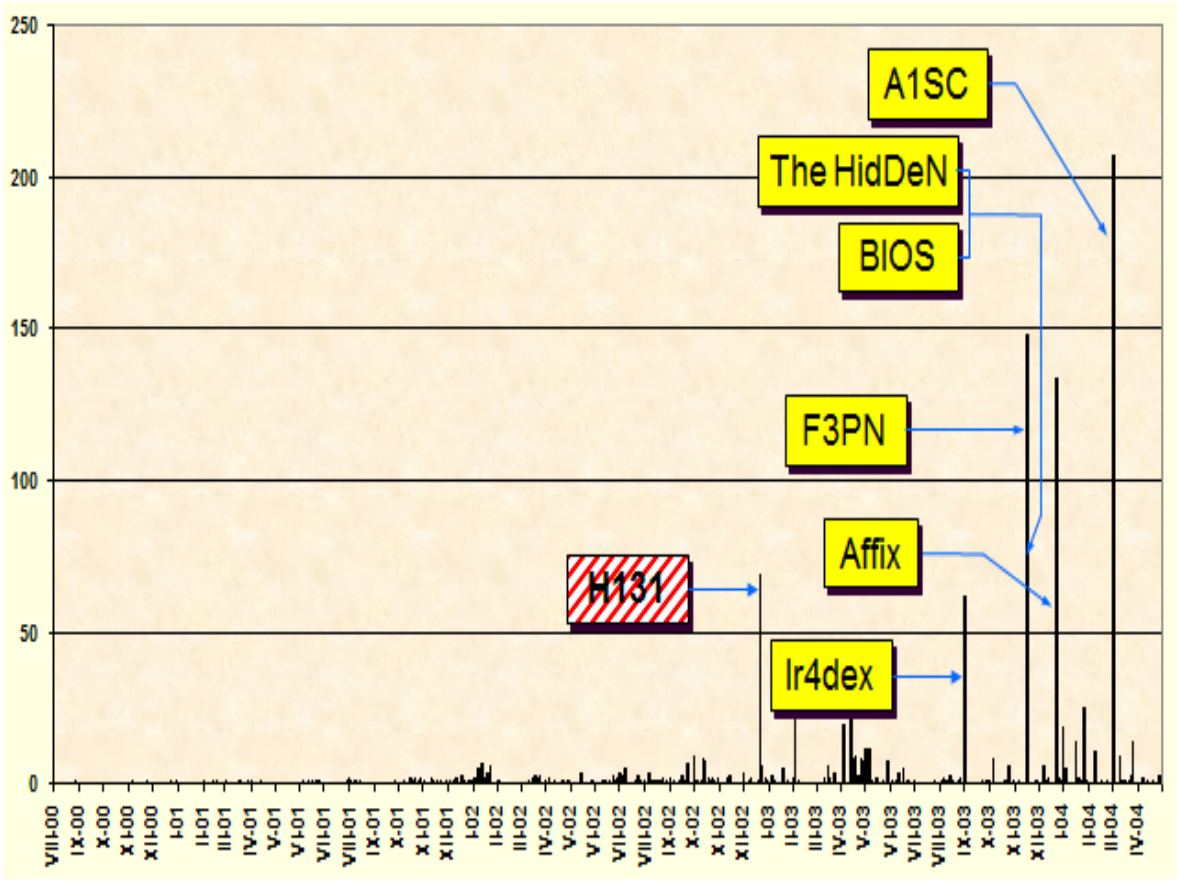
- ICT specialisté,
- právníci,
- psychologové,
- pedagogové,

- sociologové,
- ostatní.

Bez důvěryhodné spolupráce všech zapojených subjektů, ať už je to veřejný nebo soukromý sektor, k cíli nelze dojít. Výměna informací mezi těmito dvěma sektory je velice důležitá. A. Špidla, ředitel odboru kybernetické bezpečnosti MV ČR, uvedl na konferenci Cyter 2010 konané v Praze, že si uvědomuje význam spolupráce s veřejnou sférou, soukromým sektorem i akademickou sférou a proto ji vítá. Otázkou je jestli se tak uskuteční a spolupráce se bude dále rozvíjet.

6.2 Základní charakteristika současného kybernetického ohrožení České republiky

Česká republika nepatří mezi země, kterým by se kybernetické ohrožení, včetně politicky motivovaných incidentů vyhýbalo. Doména.cz byla v minulosti vystavena řadě útoků, respektive výhrůžek takovými útoky (např. v souvislosti s konáním summitu Mezinárodního měnového fondu a Světové banky v roce 2000 a summitu Severoatlantické aliance v roce 2002).



Graf 4: Útoky v doméně.cz. [4]

Současná úroveň ohrožení České republiky ze strany kyberterorismu je následující:

- Informační technologie jsou stále ve větší míře využívány pachateli celého spektra trestné činnosti. Výskyt a počet kybernetických incidentů bude v České republice narůstat.
- Klesá počet incidentů motivovaných snahou o medializaci (např. defacement). Předpokládá se, že roste počet skrytých incidentů.
- Přibývá pachatelů (expertů), kteří zneužívají své znalosti za úplatu.
- Je zaznamenáván rostoucí výskyt nežádoucích materiálů.

Kybernetickou bezpečnost v České republice hlídá od začátku letošního roku správce české národní domény CZ.NIC. Od ledna 2011 převzal agendu národního bezpečnostního týmu CSIRT.CZ (Computer Security Incident Response Team), kterou doposud provozovalo sdružení CESNET. Sdružení CZ.NIC se především zabývá provozováním registru doménových jmen.cz.

7 USÁMA BIN LÁDIN

Považuji za důležité, zmínit se ve své práci o zprávě, která nepochybně obletěla celý svět. Myslím tím informaci podle které je vůdce teroristické skupiny Al-Kájda Usáma bin Ládin mrtev. V pondělí 2. 5. 2001 to oznámil v přímém přenosu na CNN americký prezident Barack Obama. Identita Usámy bin Ládina byla potvrzena pomocí faciálních rozpoznávacích technik, které identitu vyhodnotí na základě tvarů a rysů obličeje. Dále byla potvrzena i pitvou. Usámu bin Ládina zabilo zvláštní komando amerických sil při cílené operaci v odlehlé horské oblasti v Pákistánu. Akce byla plánována již delší dobu. Zahynul v domě, kde s ním byli další příslušníci rodiny.

Obrázek 9: Místo útoku na Usámu bin Ládina. [33]

V důsledku této události, USA uvedlo do pohotovosti svá velvyslanectví a varovaly Američany před možnými odvetnými útoky Al-Kájdy. Islámští radikálové již odvetou pohrozili.

Saudský Arab Usáma bin Ládin pocházel z bohaté rodiny. Založil a také financoval činnost Al-Kájdy. Stál za řadou útoků, a to především za útokem na New York a Washington 11. září 2001. Americké síly po něm pátraly od roku 2001. Dařilo se mu dlouhou dobu skrývat. Občas se objevil i na videozáznamu s různými prohlášeními.

Obrázek 10: Usáma bin Ládin. [33]

Zabití Usámy bin Ládina představuje významné vítězství nad mezinárodním terorismem, avšak je to jen milník v pokračujícím boji, jehož konec je v nedohlednu. Dosažený úspěch spočívá v jeho symbolickém významu. Byl ikonou a ztělesněním schopnosti udeřit proti USA a Západu. Jakkoli byla jeho smrt vítána, neměla by být v žádném případě ztotožňována se zánikem terorismu.

PRAKTICKÁ ČÁST

8 PODOBY KYBERTERORISTICKÉHO ÚTOKU

Při výčtu útoků a jejich možných variant v budoucnu se mnohdy zapomíná na fakt, že informační sítě lze použít nejen jako cíl, ale také jako prostředek. V první řadě může jít o nástroj ke komunikaci. Díky použitým technologiím mohou spolu kyberteroristé rychleji komunikovat nebo pružně reagovat. Stejně tak může být kyberprostor jen prostředkem pro provedení útoku v reálném světě. Je proto důležité nepochybovat o úsilí, schopnostech a představivosti teroristů používat informační technologie pro organizaci většiny operací, ke komunikaci s množstvím dalších buněk, k přípravě a ke kontrole průběhu svých násilných akcí.

Dle mého názoru většina lidí považuje např. Al-Kájdu za bezduchou hordu. V každém případě je to organizace, která má mnoho různých tváří a podporuje rozvoj high-tech (vyspělá technologie) schopností svých vůdců a společníků.

Kybernetické hrozby, kterým nás vystavují teroristické organizace jako je i Al-Kájda, nezávisí pouze na vůli jejich členů a vůdců přijmout nové kybernetické taktiky boje. Už nyní můžeme podle Dana Vertona na Internetu nalézt řadu aliancí hackerů a internetových aktivistů („hacktivisti“), kteří vyjádřili svou ochotu zapojit se do „kyberdžihádu“, neboli elektronické svaté války, proti západu, zejména proti Izraeli a USA.

Obrázek 11: Informační věk v Al-Kájdě. [3]

Je důležité zmínit významný aspekt kybernetického útoku, a to jeho asymetrii. To znamená, že několik málo specialistů může s relativně malými náklady poškodit hospodářství technicky vyspělého státu natolik, že jeho obnova může trvat roky. To, že kyberteroristický útok může zasáhnout na několika místech světa naráz a zapříčinit tak značné dopady na reálný svět, činí scénář takového útoku přitažlivý nejen pro teroristické skupiny, zločinné státy ale i pro osamocené jedince. Provázanost informačních systémů moderní společnosti je tak vysoká, že bez ochrany kyberprostoru ztrácí efekt ostatní bezpečnostní strategie.

V následující části práce se budu snažit o výčet útoků, které se již staly nebo by se stát mohly a mohly by ohrozit PKB. Výběr není zcela vyčerpávající, a to z toho důvodu, že v dnešní době moderních informačních technologií ve spojení s jinými technologiemi a nástroji je možné téměř cokoli.

8.1 Defacement

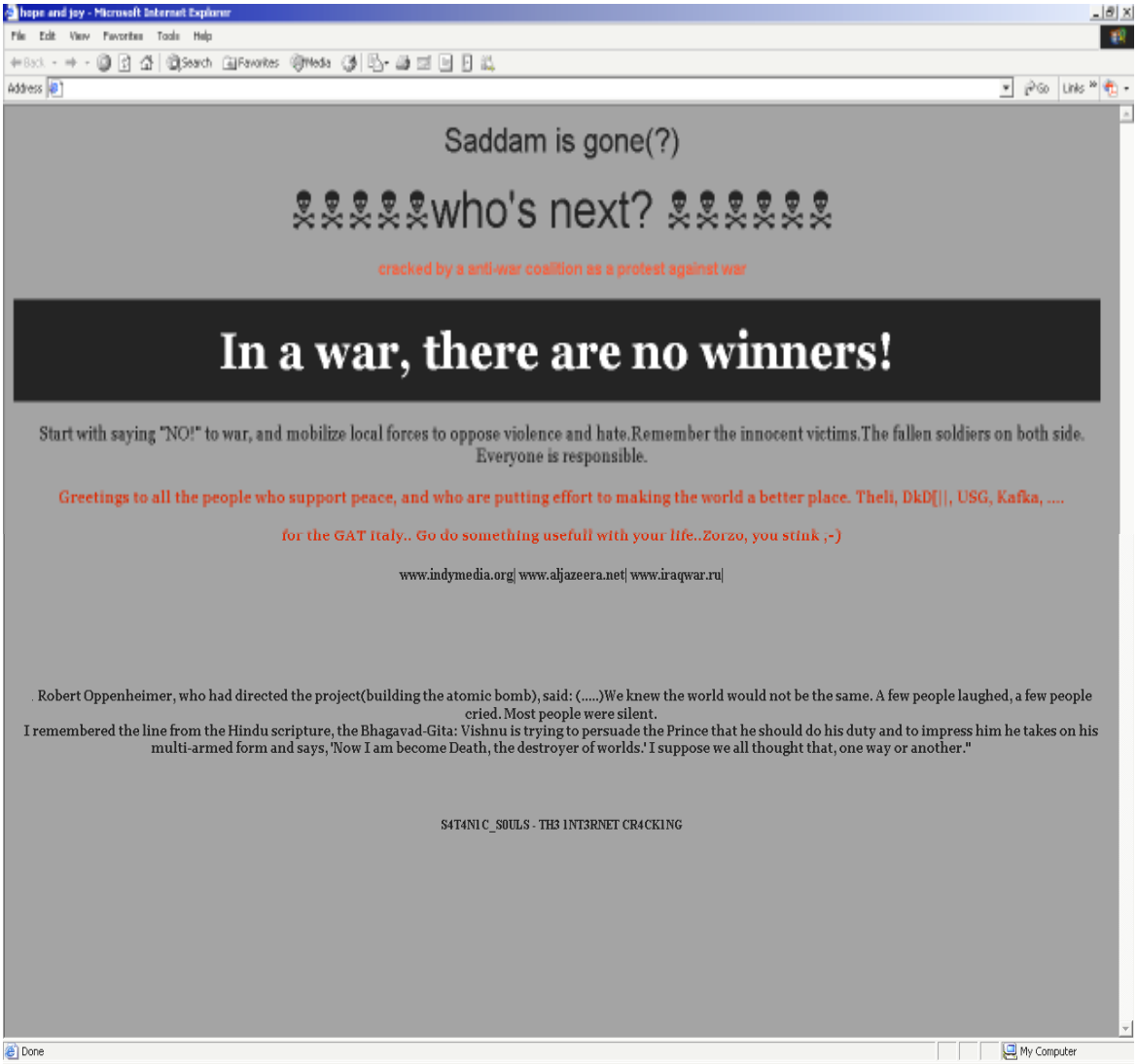
Nepřátelská změna obsahu webových stránek. Tato změna může být nápadná a např. zesměšňovat protivníka, prezentovat útočníkovu ideologii nebo jinak psychologicky působit. Může to být i změna nepatrná, která změní jen některé údaje na webových stránkách a takový defacement bude sloužit k získání důvěrných informací nebo ke zmatení protistrany.

Defacement protivníkova serveru, používaný často kyberteroristickými skupinami může mít nejrůznější formy, např.:

- Získat prostředky nebo informace pro další operace skupiny umožní náhrada přihlašovací stránky vedoucí ke krádeži přihlašovacích údajů uživatelů.
- Změny na stránkách významných organizací nebo firem mohou vést ke snížení jejich autority. Stránka může být nahrazena výsměšným textem nebo obrázkem, ale lze říct, že často spočívají v nepatrné úpravě, které si pravidelný návštěvník nemůže všimnout. Může jít např. o změnu akčních cen nebo o drobnou úpravu názvu firmy.

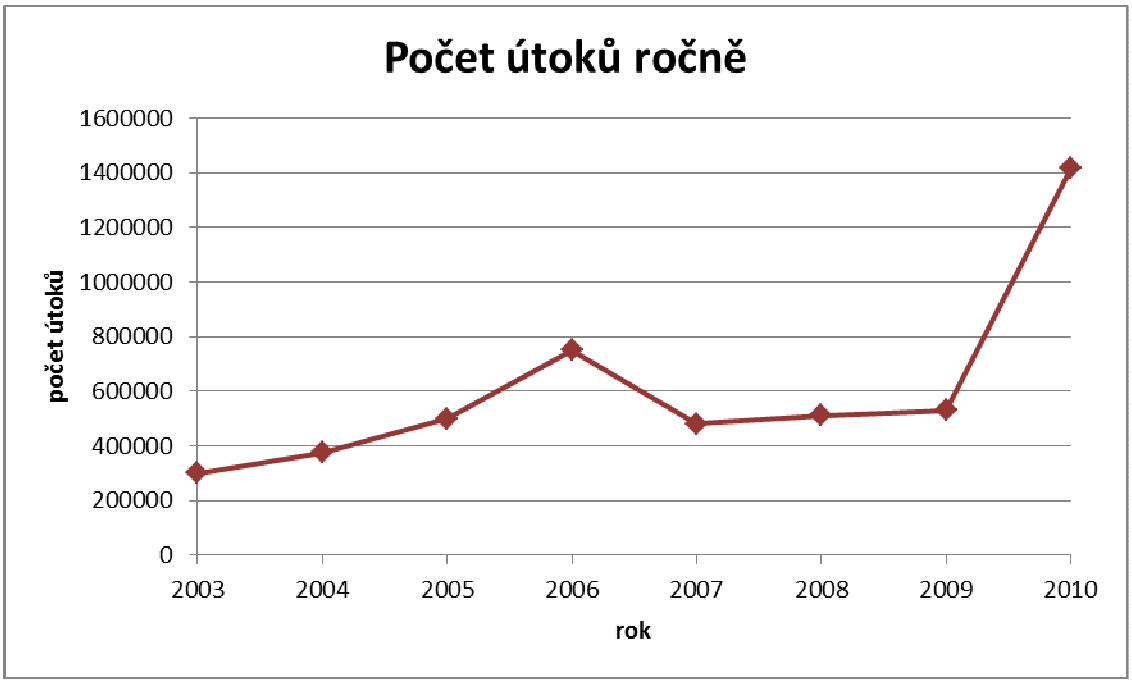
Útoky tohoto typu jsou nejnebezpečnější v případě, kdy podvržená stránka má stejný nebo téměř stejný vzhled jako původní stránka.

Obrázek 12: Defacement stránky agentury CIA provedený švédskými hackery 19. září 1996. [4]



Obrázek 13: Defacement použitý v souvislosti s válkou v Iráku. [4]

Počet útoků tohoto typu zatím neustále stoupá, což je znázorněno v grafu č. 5. V roce 2010 je tato hodnota na rekordním čísle, a to 1 419 203 webových defacementů za rok.



Graf 5: Počet defacementů ročně. [32]

8.1.1 Boj s problémem

V praxi PKB tento druh útoku nesmí být opomíjen a musí se mu věnovat pozornost. Mohou nastat situace, kdy podnik komerční bezpečnosti bude nucen chránit dobré jméno a čest podniku, na jehož ochraně se zavázal. Taktéž může nastat situace, kdy se terčem útoku stane i on sám.

Abychom byli schopni bránit web proti tomuto útoku, je nutné zabezpečit (uzavřít) všechny porty a zranitelné služby systému. Důležité je také verzování a aktuálnost softwaru, protože značná část útoků je podle statistik vedena proti neaktuálním verzím operačních systémů. K ochraně nám tedy poslouží periodické provádění penetračních testů za účelem odhalení a zabezpečení případných slabin.

Další krokem k bezpečnému webu firmy je zajištění spolupráce mezi vývojářem a správcem serveru, jelikož oba žijí ve dvou odlišných světech. A pokud něco nefunguje správně, jejich odpovědí je, že problém je s největší pravděpodobností na druhé straně.

8.2 Fyzické napadení

Velmi často opomíjenou problematikou z hlediska bezpečnosti IT sytému je jeho fyzická bezpečnost. Neautorizovaný přístup do prostor vyhrazených jen pro oprávněné může znamenat velký problém. Cíl útoku může být například umístění odposlechového zařízení, kopírování a krádež informací. Kompletní fyzická likvidace počítačového systému nebo jeho odcizení není vyloučeno.

Ve firmách jsou hesla do systému běžná, mnohdy mají předem definovanou složitost a také interval jejich změn. Proto se může jevit tento typ zabezpečení pro někoho dostačující a bezpečný. Avšak to nemusí být pravda při nedostatečném fyzickém zabezpečení.

Pro představu si vymyslíme situaci. Máme modelovou společnost, která neřeší fyzické zabezpečení osobních počítačů, serverů a diskových polí pro zálohování dat. Firma pracuje s citlivými daty. Zaměstnanec nasazený teroristickou organizací jako „šťenice“ může počkat až ostatní kolegové odejdou. Nepozorovaně a hlavně bez problémů se pak dostat do místnosti, kde jsou uloženy zálohy dat. Ty pak vytáhnout a dát do příruční tašky. Tu samou činnost může zopakovat i v serverovně. Data následně využije pro svou potřebu. Neřešíme zde možnost šifrování dat, nebo dalších ochranných prvků.

8.2.1 Boj s problémem

Omezení přístupu do místností a míst obsahujících prvky IT infrastruktury je prvním krokem k fyzickému zabezpečení PC systémů. Také je možno uvažovat použití zvláštních klíčů místo univerzálních.

Ochrana serveroven a datových úložišť:

- Jejich uzamčení, definování oprávněných a kvalifikovaných osob s přístupem do nich.
- Serverové rozvaděče by měly být uzamykatelné. Klíče budou mít na starosti jen správci hardwarových částí serverů.
- Naprostá separace datových záloh do jiné budovy. Přístup k nim budou mít jiné osoby.
- Využití CCTV pro dozor.

Ochrana osobního počítače:

- Uzamčení počítačové skříně pomocí zámku.
- Umístění počítačové skříně do uzamykatelného oddílu.
- Pokročilé metody autentizace:
    - využití čipových karet,
    - bezpečnostní tokeny,
    - biometrické metody – scany otisků prstů, scany sítnice, scany dlaní, DNA autentizace,
    - analýza chování uživatele,
    - kombinace jednotlivých metod.

8.3 Teror ve vzduchu

S vývojem informačních technologií se zdá být z hlediska kyberterorismu nejvíce ohrožena letecká doprava. Jak jsme v minulosti mohli slyšet v masmédiích, nebudou se některé aerolinky zabývat hledáním manikůrních nůžek, pilníků a podobně. Zato budou více pozornosti věnovat jiným, závažnějším problémům souvisejícím s ochranou přepravy. Měli zde možná na mysli ochranu proti možnému kyberterorismu.

Nebezpečnost nezabezpečení bezdrátových sítí ukazuje případ v roce 2001, kdy se jeden z manažerů American Airlines pokusil upozornit na slabinu, kterou je třeba řešit. American Aerlines byla jednou z prvních aerolinek, která začala instalovat nové technologie jako roving agent nebo curbside check-in systems s cílem vycházet zákazníkovi vstříc. Tento systém umožňuje pracovníkům aerolinií odbavovat pasažéry letů kdekoli v prostorách terminálu, dokonce i venku na ulicích, a tím pomáhat pasažérům vyhnout se dlouhým frontám. Tyto systémy však nepoužívají žádný způsob zabezpečení a navíc jsou napojené na systémy odbavování zavazadel, rezervací letenek, letecké databáze a celou řadu informačních systémů obsahujících citlivé údaje. Teroristům by pak stačilo použít program nazývaný sniffer, který by mohl sbírat citlivé údaje, jako jsou uživatelská jména a hesla, přímo ze vzduchu. Tyto informace by mohl využít k přístupu do kontrolních systémů leteckých společností. Poté by bylo možné poslat zavazadlo bez cestujícího, nabourat se do

systému letenek a změnit údaje o cestujícím, a tak proniknout na palubu letadla aniž by si ho někdo z personálu všiml.

Bezdrátové sítě velmi často pokrývají větší prostor než je potřeba, a proto může útok přijít i z větší vzdálenosti. Připojením do nezabezpečené sítě podniku nebo organizace, získá útočník přístup ke všem vnitřním podnikovým serverům a síťovým zařízením. Z toho samozřejmě plyne i možný únik citlivých informací. Proto je nutné zacházet s interní bezdrátovou sítí jako by byla veřejně přístupná a nepředpokládat, že provoz bude soukromý a bezpečný.

Dalším rizikem může být bezdrátový přenos dat ze střeženého objektu na PCO.

8.3.1 Boj s problémem

Jako účinné opatření bych doporučila použít šifrování WPA II. Důležité je samozřejmě i umístění přístupových bodů, které volíme podle typu objektu. Jestli by se jednalo např. o uzavřenou firemní budovu, je lepší volit umístění spíše ke středu budovy než poblíž oken. Pokrytí pak naplánovat tak, aby sahalo k oknům, ne za ně. Dalším krokem jsou preventivní prohlídky ve smyslu kontroly, abychom zjistili, zda se neobjevují neschválené přístupové body. Postačí nám k tomu nástroj jako NetStumbler. Také překontrolujeme sílu signálu vně objektu, protože i jeho malý únik může vést k narušení bezpečnosti.

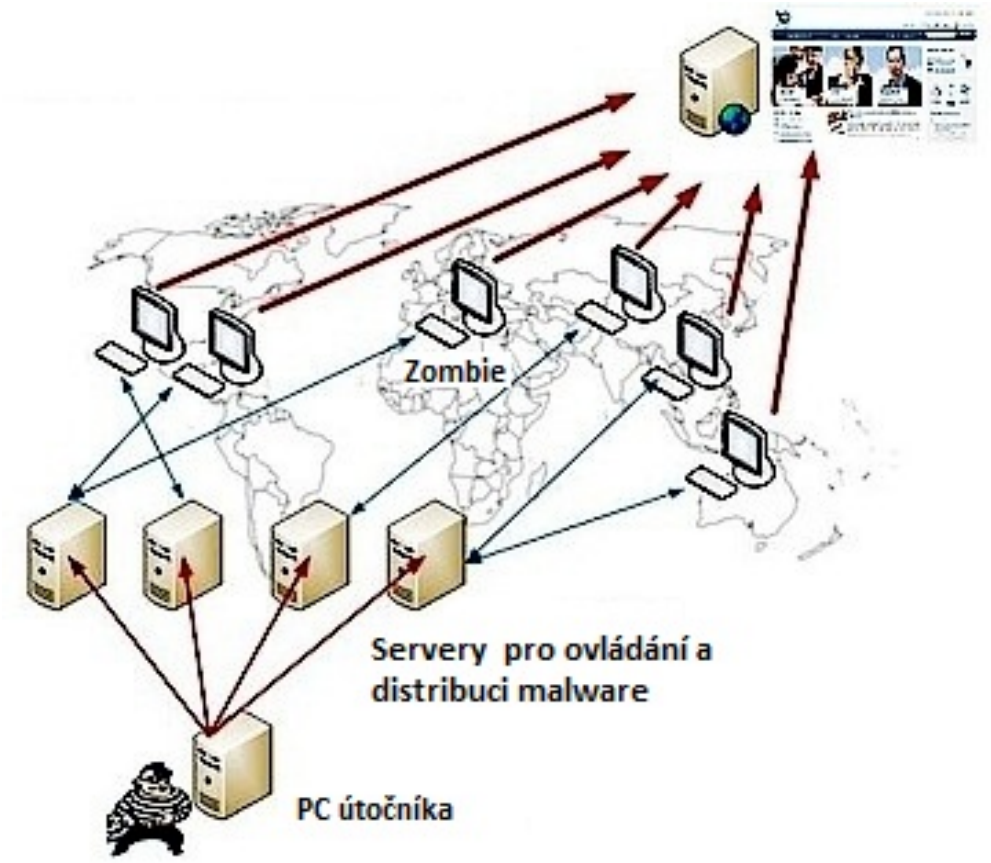
Je důležité si uvědomit, že někdo s dostatkem času, odhodlání a prostředků se dovnitř stejně nakonec dostane.

Při riziku odposlouchávání dat přenášených z chráněného objektu na PCO, je nejlepším řešením přenos přes radiový kanál, kde je více pásem a můžeme provést modulaci a šifrování dat.

8.4 Spuštění útoku typu DOS

DOS je zkratka spojení „Denial of Service“, v překladu to znamená odmítnutí služby. Je to typ útoku, který má za cíl ochromení provozu serveru nebo systému zaplavením množstvím náhodných dat. Příkladem může být útok, při kterém útočník pomocí programu náhodně generuje nesmyslná data, která jsou následně posílána na cílový server. Těmito přicházejícími daty je pak server zahlcen a není schopen reagovat na požadavky oprávněných uživatelů. V horším případě může dojít k úplnému zhroucení.

Jenou z variant DOS útoku je DDOS útok, tzv. distribuovaný útok, vedený ne z jednoho počítače, ale souběžně z velkého počtu stanic. V praxi to znamená, že stanice byly předtím kompromitovány a jsou pod kontrolou útočníků. Ti však u nich fyzicky v danou chvíli nesedí, nýbrž je na nich útočníkem nainstalován nějaký program (tzv. zombie), ten se příkazem aktivuje a oběť zasype přívalem dat. Protože útok pochází od mnoha stanic rozmístěných po celé síti, je jednoduché vypátrání útočníka nemožné.



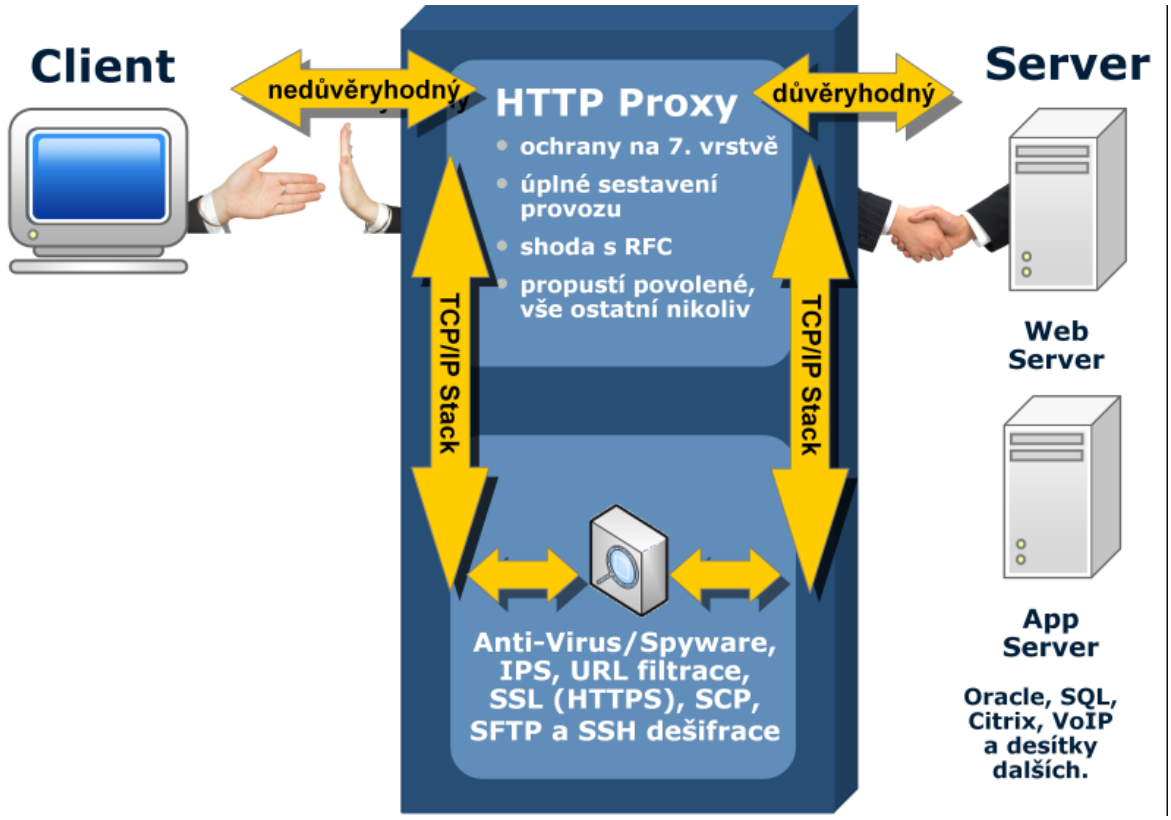
Obrázek 14: Princip útoku DDOS. [20]

DOS útok by se stal pro podniky PKB značnou újmou. Ztráty jsou způsobeny nedostupností systému, ztrátou tržeb, nutností analyzovat a hlavně napravit vzniklý problém. Narušit činnost sítě je mnohdy jednodušší než do ní vniknout.

8.4.1 Boj s problémem

Jako účinnou ochranu proti hrozbě DOS, doporučuji použít bezpečnostní řešení od McAfee. Konkrétně se jedná o produkt Enterprise Firewall (Sidewinder®), využívající

integrované geolokace, kdy můžeme omezit přístup na server jen pro určité uživatele (např. přistupující jen z ČR). Další vazba může být např. na globální reputační systém TrustedSource™, jenž analyzuje chování miliónů počítačů připojených k Internetu. Když je počítač jednoznačně infikován, je uživatelům těchto stanic přístup ke službě zamítnut.



Obrázek 15: Princip bezpečnostního řešení. [21]

8.5 Útok pomocí EMP

Zbraně s elektromagnetickým pulzem (EMP) – tzv. e-bomby, představují další významnou hrozbu. Tyto zbraně lze označit za dokonale asymetrické teroristické zbraně. Je zřejmé, že dnešní způsob života závisí na fungování moderní elektronické společnosti, a proto paralýza, která by postihla elektronické počítačové systémy, komunikační sítě a dopravní systémy by neznamenala jen menší nepohodlí.

V okamžiku výbuchu takovéto bomby začnou v jejím okruhu vznikat stlačené elektromagnetické vlny, které vysílají elektromagnetický pulz podobný tomu, který způsobuje jaderné bomba, pouze bez ničivého fyzického dopadu na budovy a lidi. Tento

pulz má ionizující efekt, který se jako rádiové vlny šíří po okolí, a následně ničí elektrické obvody, které se nacházejí uvnitř napadené zóny. [6]

V roce 1870 vynalezl EMP technologii Heinrich Hertz. Aby e-bombu teroristé vytvořili, potřebují jen základní inženýrské vybavení a základní technické znalosti. Výhodou (nevýhodou) EMP zbraní je jejich dobrá přenositelnost a působnost na velkou vzdálenost. Útočník vybavený několika kufříkovými e-bombami si dokáže velmi dobře naplánovat jejich rozmístění tak, aby zasáhli co největší oblast.

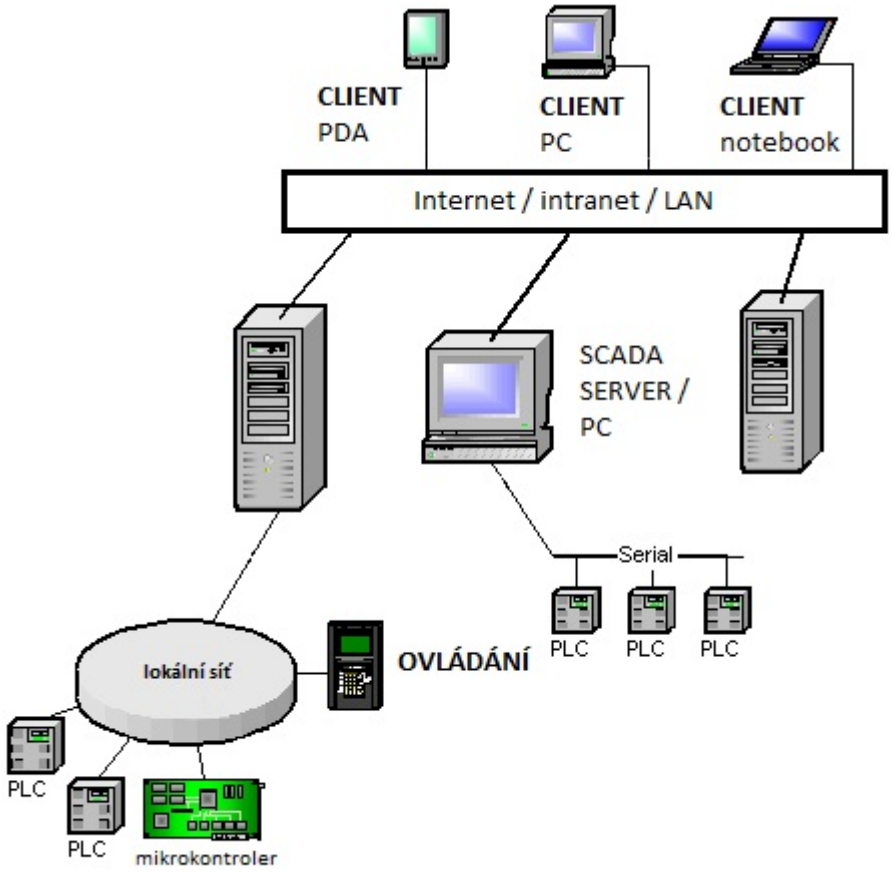
8.5.1 Boj s problémem

Proti většině zbraní se časem najde protizbraň, a EMP není výjimkou, ale naprosto spolehlivá ochrana proti němu je téměř nemožná. EMP lze částečně „odstínit“, nebo spojit všechna zařízení vodiči, čímž budou převedena na stejný potenciál, popřípadě uzavření nejdůležitějších prvků do kovových klecí, tzv. Faradayova klec (prakticky ale není možné do ní zavřít všechny počítače). V serverovně je nutné chránit i zdroj napájení UPS a také klimatizaci. Část zařízení takto ale chránit nelze, protože bychom tím zamezili jejich normálnímu fungování (radary, řízené střely).

8.6 Útoky na SCADA systémy

Novým trendem je přes Internet zpřístupňovat klíčové systémy „velení a kontroly“. Je to z důvodu zjednodušení jejich užívání a ovládání. Tyto systémy nazýváme „SCADA systémy“. Mohou ovládat tok elektřiny a zemního plynu i kontrolní systémy dálniční a železniční dopravy. Také kontrolují provoz dalších průmyslových provozů, např. chemiček, čistíren vod a vodáren. Většinou zabezpečují chod kritické infrastruktury, a to vše v reálném čase. Všichni jsme zvyklí považovat základní služby za samozřejmost a málo kdo z nás si uvědomuje jejich závislost na počítačích a Internetu.

Jako první známý červ, který se soustředil na SCADA systémy, byl počítačový červ **Stuxnet**, který dokázal přeprogramovat PLC (programovatelné logické automaty) a své změny skrýt. Byl šířen jako hrozba „nechráněného dne“, prostřednictvím zranitelnosti operačních systémů. Tedy takových, na které přišel útočník dřív než výrobce softwaru. Pravděpodobný cíl útoku byla jaderná elektrárna Búšehr, či závod na obohacování uranu v Natanzu. Obě lokality jsou v Íránu.



Obrázek 16: SCADA systém. [13]

Útok na tyto systémy by pravděpodobně vyvolal katastrofické následky. Faktory rizika:

- komunikace,
- „kybernetická válka“, pro kterou jsou SCADA systémy perfektním hřištěm,
- historický nedostatek zájmu o bezpečnostní otázky v rámci sítí SCADA,
- představa, že SCADA sítě jsou bezpečné, protože jsou fyzicky nebo logicky izolovány.

Nové polohy SCADA systémů jsou centrální. Mají na starosti distribuci stále více informací v reálném čase z více částí světa pro více uživatelů a více systémů.

8.6.1 Boj s problémem

Komunikace se systémy SCADA podle mě představuje největší bezpečnostní riziko. Cílem zabezpečení komunikace bude:

- autentizace a integrita zpráv,
- nízké nároky na čas a systémové zdroje,
- kompatibilita.

Chceme-li reagovat na hrozby pro systémy SCADA, doporučuji použít řešení od společnosti Radware s DefensePro. Toto zabezpečení nabízí komplexní ochranu pro komunikační protokol SCADA. Tato ochrana je založena na několika modulech, které lze rozdělit do dvou částí – specifické ochrany a druhové ochrany.

Specifická ochrana

Mimo standartního zabezpečení na úrovni TCP/IP nabízí Radware i speciální formu, kde jsou zohledněny i další komunikační protokoly, včetně:

- ICCP – protokol, který poskytuje generické „bloky shody“ pro ovládání zařízení, programového řízení, hlášení událostí a další.
- MODBUS – sériový komunikační protokol použitý pro PLC.
- DNP3 – sada protokolů pro zpracování automatizace.

Druhová ochrana

Komunikace SCADA je založena na protokolu TCP/IP, a jako takový je předmětem mnoha typů útoků, proti kterým ho DefensePro chrání:

- Síťové povodně – DOS a „prostoje“ na určité služby.
- Síťové skenování.
- TCP/IP anomálie.

DefensePro řeší tyto útoky pomocí několika ochranných modulů: podpisová ochrana, prevence šíření škodlivého kódu, DOS ochrana.

9 ŘEŠENÍ FUNKČNÍ OCHRANY

Spoléhat na myšlenku: „Nám kyberterorismus přece nehrozí a nemůže se nám to stát“, je hloupost. Komplexním přístupem k řešení otázek bezpečnosti se proti této hrozbě můžeme alespoň bránit. Řešení ochrany před touto hrozbou musí nabídnout bezpečnost a ochranu sítě sestávající z monitoringu, automatické analýzy a vyhodnocení provozu, varování a konečné řešení incidentů, evidence a dokumentace. V této části jsou uvedena základní opatření v oblasti zabezpečení informačních systémů, které by měla organizace PKB a také i jakákoli jiná dodržovat a použít ke své ochraně a prevenci před možným kyberteroristickým útokem.

9.1 Softwarová ochrana

9.1.1 Firewall

Instalací brány firewall zabráníme neoprávněnému vzdálenému přístupu k síti z Internetu. Je to vlastně hradba, která odděluje vnitřní informační systém organizace od vnějšího „nebezpečného“ prostředí. Firewall umožňuje:

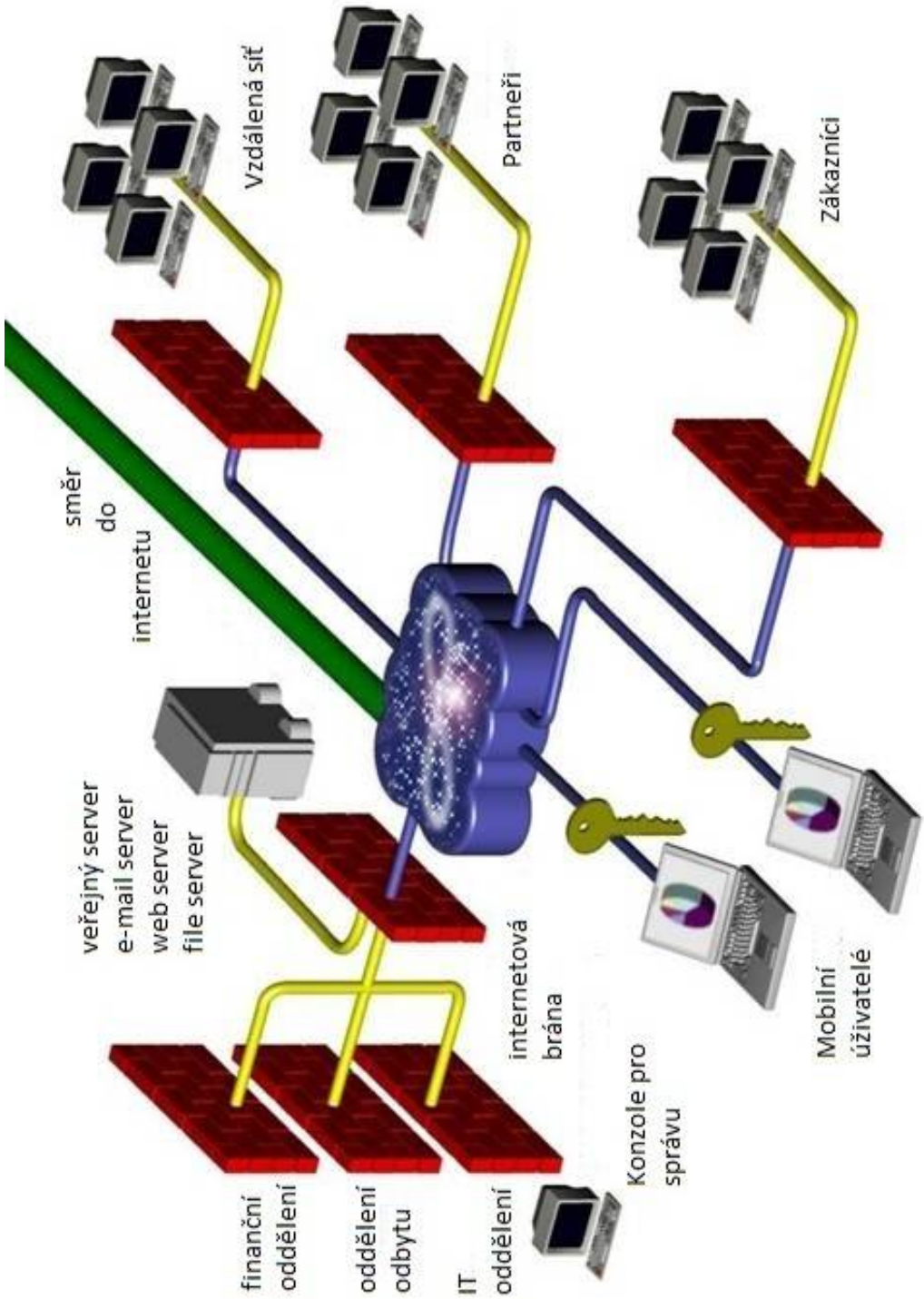
- řízení datových toků mezi vnitřním a vnějším prostředím,
- filtrovat požadavky na připojení,
- filtrovat některé přímé útoky typu DOS a záplavové pingy.

Základní dělení firewallu:

- softwarové – většinou součástí operačního systému,
- hardwarové – mají většinou zároveň funkci routeru (směřovače) a switche (přepínače).

Je důležité si uvědomit, že firewall nám neposkytuje celkovou ochranu, ale je pouze jednou ze součástí ochrany.

Pro zvýšení zabezpečení je vhodné použít firewall samostatně ve všech podsítích a následně jeden sdružený firewall před vstupem do Internetu, jak je znázorněno na následujícím obrázku č. 17.



Obrázek 17: Firewall. [14]

9.1.2 Bezpečnostní monitoring sítí – IDS/IPS

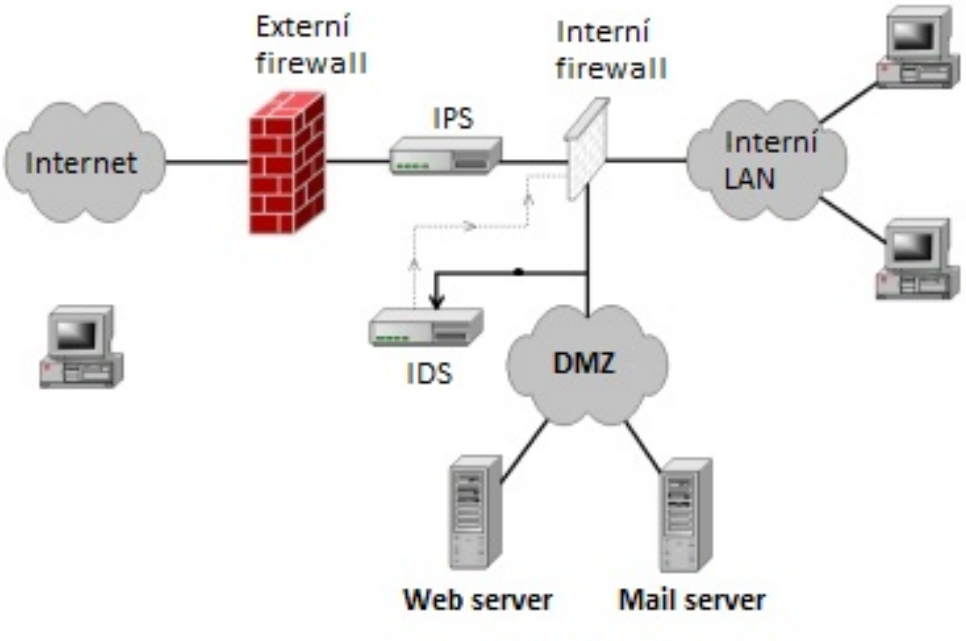
Jedná se o systémy detekce a prevence narušení a lze je využít jako druhou obrannou linii za firewally, aby chránily aplikace komunikující uvnitř chráněné sítě. Tedy za otevřenými porty firewallu.

IDS

- Sleduje datové toky, ve kterých hledá pokusy o útok na konkrétní aplikace.
- Pasivní zařízení - pouze sleduje a nijak nezasahuje do provozu sítě.
- Informace o útocích poskytuje formou statistik a alertů.

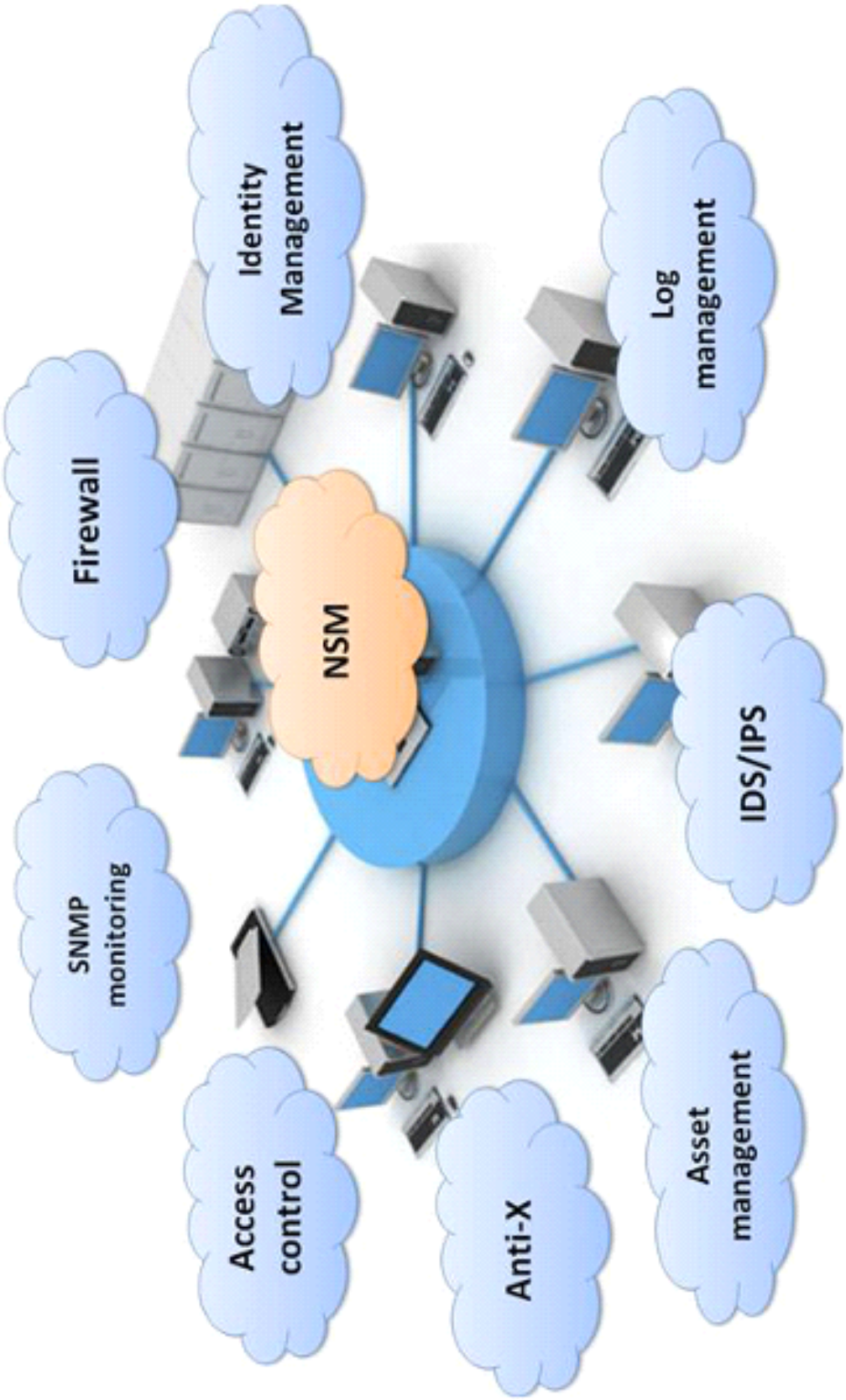
IPS

- Detekuje útoky jako IDS, navíc je schopno útoku i zabránit.



Obrázek 18: Příklad využití IDS a IPS. [29]

Dílčí problémy z oblasti bezpečnosti řeší ve stávajících firemních prostředí např. firewally, antiviry, IDS/IPS, SNMP dohled a podobně. Bezpečnostní monitoring sítě (NSM) jako prostředek ochrany funguje v podobě odhalení infikovaných počítačů, porušování bezpečnostní politiky a také má za následek větší ukázněnost uživatelů dané sítě.



Obrázek 19: Bezpečnostní monitoring sítě. [29]

Vysvětlení pojmů z obrázku č. 19

Identity management

- Management centrální správy uživatelských účtů.

Log management

- Definice toho co potřebujeme protokolovat, jakým způsobem uchovávat a jak dlouho takové informace uchovávat.
- Tvoření velkého objemu dat může být problém, proto je důležité vymyslet strategie pro zvládnutí takových objemů dat.

Asset management

- Systémy pro řízení a správu zdrojů organizace, jinak řečeno softwarový a hardwarový management.

Anti-X

- Např: antivir, antispam, anti spyware.
- Obecně programy, které blokují, odhalují, odstraňují viry, spam nebo spyware.

Access control

- Kontrola přístupu.

SNMP monitoring

- Protokol sloužící pro monitorování a správu sítí.

9.1.3 Aktualizace softwaru

Při stahování a instalování nejnovějších aktualizací používaného softwaru, jsme napřed před útočníky. Je známo, že k mnoha virovým útokům dochází mnohdy zbytečně. Často existují aktualizace, které by potížím zabránily. Udržování aktuálních verzí všech systémů je v praxi problematické, a to z důvodu otázky ceny.

9.1.4 Antivirový software

Virové infekci počítače zabráníme instalací antivirového softwaru a jeho pravidelnými aktualizacemi. Viry jsou pro počítače škodlivé a mají různé chování. Odstraňují, mění

soubory, spotřebovávají prostředky počítače nebo umožní externím uživatelům přístup k našim souborům. Jejich odstranění může být časově velmi náročné a jejich rozšíření do počítačů např. zákazníků, může přinést komplikace v podobě ztráty důvěryhodnosti.

Opatření, které mohou snížit riziko nakažení viry:

- zakoupení a instalace antivirového softwaru a udržení jeho aktuálnosti,
- neotevírat podezřelé soubory,
- používat funkce zabezpečení aplikací,
- inteligentní chování uživatele:
    - neotvírat přílohy emailů od neznámých uživatelů,
    - nepřistupovat na webové stránky, na které odkazuje neznámy email,
    - nereagovat na email od banky (případně ho ověřit jinou cestou).

Doporučení

Na trhu jsou dostupné produkty od mnoha společností. Poskytují různé stupně ochrany stanic a serverů. K dostání jsou placené i neplacené varianty. Mezi 10 nejlépe hodnocených patří:

- ESET (NOD32),
- BitDefender,
- Symantec Norton,
- Kapersky,
- AVG,
- Microsoft,
- AVIRA,
- Panda,
- Trust Port,
- McAffe.

Doba reakce na novou hrozbu bývá v rozpětí desítek minut až dnů, např. u Kapersky je aktualizace virových databází prováděna každou hodinu.

9.1.5 Autentizace a autorizace

Autentizace slouží k jednoznačnému určení uživatele, který k danému systému přistupuje. Jejím cílem je zajištění toho, že systém ví, s kým komunikuje. Jestli chceme bezpečný systém tak by měl podporovat autentizaci uživatele. Základem je databázový server, kde jsou vytvořeni uživatelé s přidělenými hesly, která v zájmu bezpečnosti musí být šifrovaná. Možnosti autentizace:

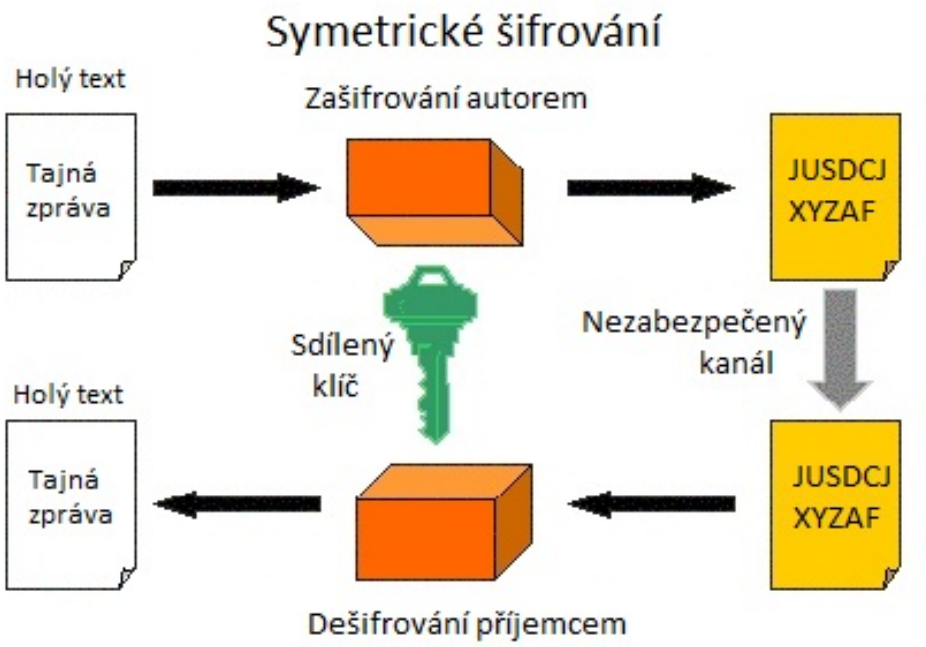
- **hesla**
    - Aby bylo heslo silné, jeho minimální délka je 15 znaků, obsahuje kombinaci velkých a malých písmen, číslic a symbolů, a v pravidelných intervalech se mění. Vytváříme taková hesla, která si lze zapamatovat. Podvody v podobě sociálního inženýrství mohou uživatele přesvědčit k prozrazení svého hesla.
    - Expirace hesel: např. 30 dní je heslo platné, po uplynutí doby platnosti je uživatel nucen si heslo změnit.
- **tokeny, magnetické nebo čipové karty**
    - Tyto systémy informace nezpracovávají, pouze je ukládají a na druhé straně vyžadují ověřující subjekt v podobě čtecího zařízení. Velké riziko u tohoto způsobu autentizace tu představuje krádež nebo poškození.
- **biometrika**
    - Uživatel má vlastnosti, které lze prověřit – otisk prstu, struktura oční duhovky nebo tvar hlavy. Dále to můžou být vlastnosti v podobě jeho hlasu, způsobu podpisu nebo jeho chůze.

Pod pojmem **autorizace** rozumíme proces ověření oprávnění uživatele, který vstupuje do informačního sytému. Ve většině případů navazuje na proces autentizace. Podstatou autorizace je ověření, zda daný uživatel má oprávnění provést příslušnou akci. Např. jestli může vložit nový záznam do seznamu zaměstnanců a podobně. V praxi v návaznosti na zvolenou strategii můžeme oprávnění rozdělit mezi více subjektů, např. administrátor, správce a běžný uživatel

9.1.6 Šifrování

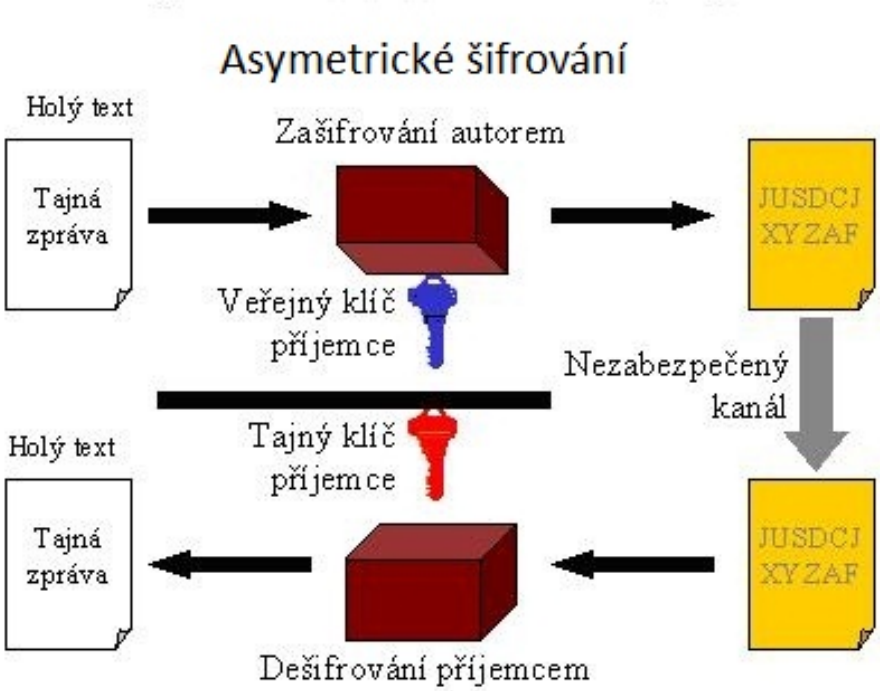
Data jsou cenné informace, a jejich zneužití neoprávněnou osobou by mohlo mít značný dopad. Šifrování dat nám umožní skrýt jejich obsah. Při samotném šifrování lze využít funkce operačních systémů nebo speciální software. Základní dělení šifrovacích algoritmů je následující:

- **symetrické šifry**
    - Systémy se soukromým klíčem,
    - k šifrování a dešifrování jediný klíč,
    - nízká výpočetní náročnost,
    - FISH,DES, 3DES, IDEA.



Obrázek 20: Princip symetrického šifrování. [31]

- **asymetrické šifry**
    - Systémy s veřejným klíčem,
    - dva klíče, jeden veřejný (všem) a soukromý (ten kdo odšifruje data),
    - RSA, DSA (digitální podpis),El-Gamal.

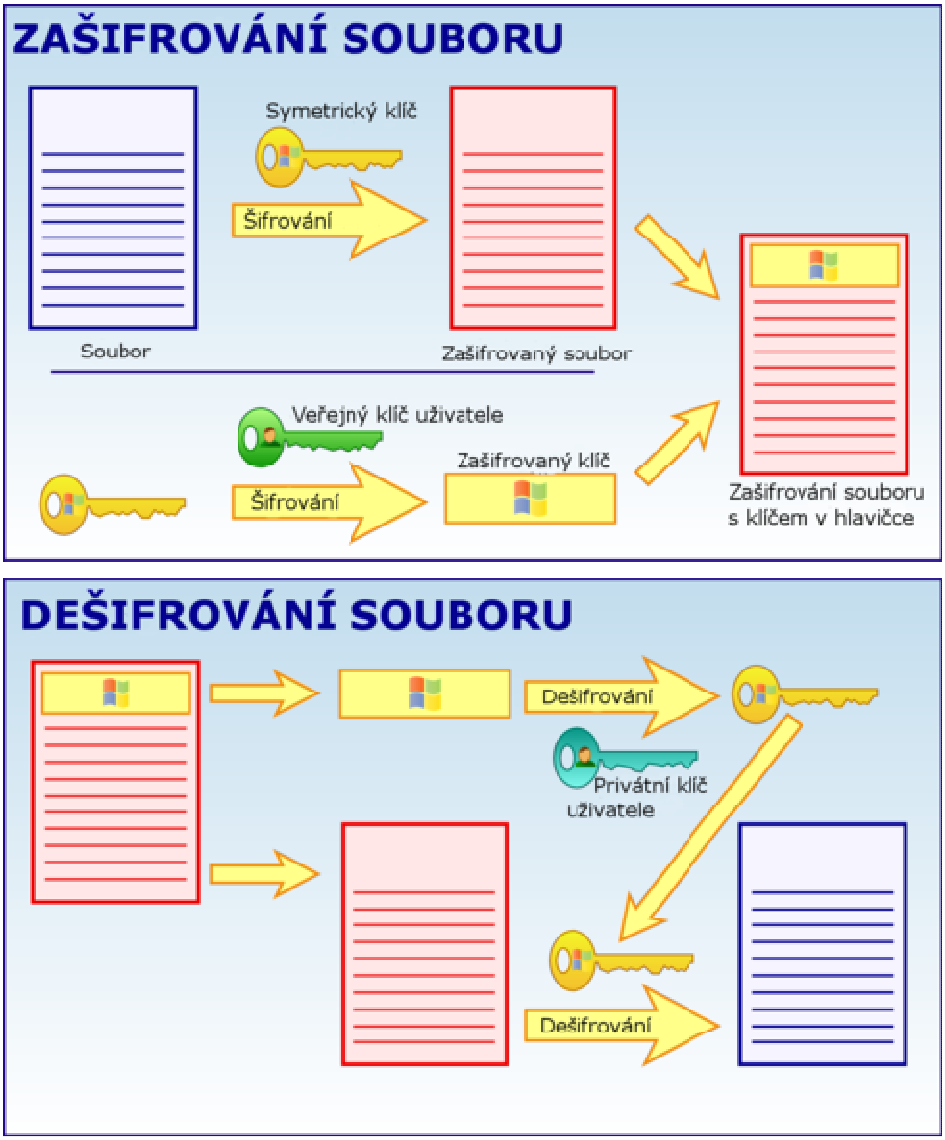


Obrázek 21: Princip asymetrického šifrování. [31]

Lze nasadit např. systémy:

EFS

- Funkce systému Windows,
- umožňuje uložit informace na pevném disku v šifrovaném formátu na úrovni.



Obrázek 22: Operační schéma EFS. [30]

Bitlocker

- Vylepšený nástroj pro systém Windows 7,
- výhoda šifrování celého disku, oproti EFS šifrování obsahu souborů spočívá v tom, že pro nepovolané není přístupná ani struktura disku, celý disk pak vypadá jako kopa náhodných dat,
- používá AES – 128, AES – 256,
- podporuje i šifrování RAID – 0, 1, 5.

9.1.7 Zálohování a obnova

Informace jsou nejdůležitější částí informačního sytému. Dnes se povětšinou data uchovávají v elektronické podobě. Pravidelné zálohování je jednou z hlavních zásad jejich zabezpečení. Také je nezbytné provádět pravidelně jejich zkušební obnovení, což může být někdy problém, a to při nesprávném postupu zálohování. Je potřeba mít na paměti i záložní kopii, která by měla být uložena mimo budovu. Další možností je provádění zálohy na jiný vzdálený server.

Doporučení

Možnosti datových úložišť pro zálohování:

- **Přenosná média** (cd, dvd, flash disk): Nejprimitivnější způsob zálohování dat. Výhodou je nejnižší cena. Nevýhodou pak možnost odcizení, popř. ztráty.
- **Pevný disk interní**: Poskytuje prostor pro zálohování systému a důležitých dat. Výhodou tohoto druhu je nízká cena, nevýhodou je nemožnost rozšířeného zabezpečení uložených dat a fakt, že zálohovaná data jsou uložena na disku staticky umístěném v PC.
- **Pevný disk externí**: Odstraňuje nevýhodu statického umístění interního disku. Disk je možno připojit pouze ve chvíli zálohy a poté umístit odděleně na zabezpečené místo. Cenově je srovnatelný s předešlým typem.
- **Server:** Zálohovací server se sloty pro pevný disk. Výhodou je možnost zálohování dat přes síťové LAN rozhraní, větší zálohovací kapacita (v závislosti na počtu a velikosti použitých pevných disků), další možností je multiplikace dat, tzv. zrcadlení, které chrání data před vícenásobným selháním systému (RAID pole). Cenově však nejnáročnější varianta.
- **SAN systémy:** Vysokorychlostní síť, obvykle komunikuje se serverem prostřednictvím optického kabelu. Síť je tvořena množstvím vzájemně propojených úložných prostorů.
    - Výhody: Snadná správa, otevřená řešení, vysoká úložná kapacita.
    - Nevýhody: Vyšší pořizovací náklady.
- **NAS systémy:** Speciální servery pro připojení úložných zařízení k síti.

- Výhody: Nízké náklady na pořízení, jednoduchá implementace.
- Nevýhody: Obtížnost rozšíření.

9.1.8 Zabezpečení bezdrátové sítě

Připojit se k bezdrátové síti je možné bez kabelů, a proto je její nastavení rychlé a pružné. V porovnání s kabelovými sítěmi jsou bezdrátové sítě více ohroženy. Volně dostupné nástroje umožnují hledat nezabezpečené sítě. Kdokoli v dosahu může síť „poslouchat“.

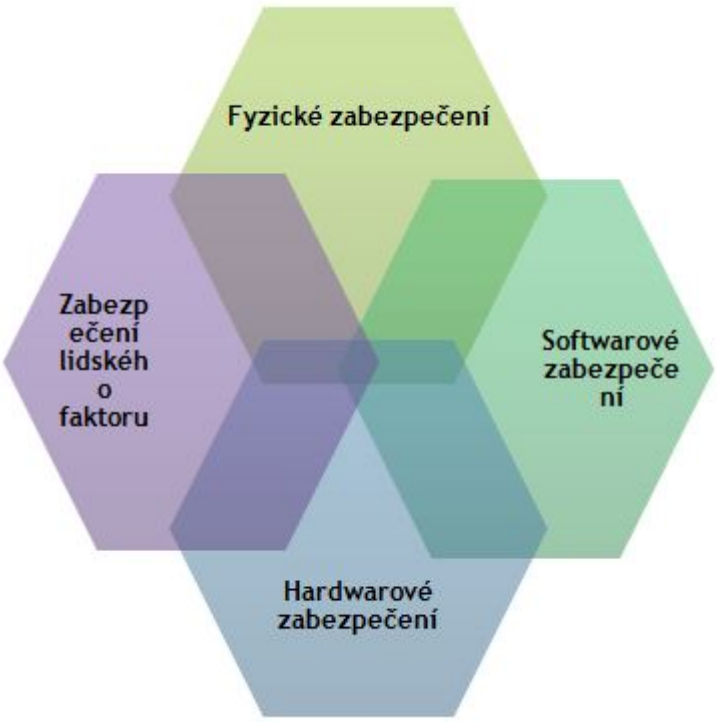
Doporučení

Cílem je nastavit síť co nejbezpečněji:

- použít šifrování WPA II k zabránění odposlechu,
- umístění přístupových bodů podle typu budovy,
- omezit možnost uživatelů nastavení sítě,
- použít filtrování adres MAC,
- preventivní kontroly sítě.

9.2 Hardwarová a ostatní ochrana

9.2.1 Fyzické zabezpečení



Obrázek 23: Schéma víceúrovňového zabezpečení IT systému. [11]

Ne všechny potíže s IT musí být způsobeny útočníky z prostředí Internetu. K vytvoření bezpečného prostředí je teda nutné brát ohled i na jejich fyzické zabezpečení, tedy zabránění přístupu neoprávněným osobám.

Možný postup vytvoření fyzického zabezpečení:

- vytvoření bezpečné oblasti kolem pracovní plochy (např. zdi, bezpečnostní dveře, PZS, bezpečnostní přepážky, trezory, aj.),
- návštěvníci procházejí identifikační zónou, a vše je zaznamenáno,
- umístění přídavných bariér kdekoli je to možné, kvůli omezení přístupu do důležitých míst,
- sledování kdo, kam, kdy, jak,
- pravidelné testy PZS,

- pravidelná i náhodná kontrola,
- školení zaměstnanců.

9.2.2 Záložní zdroje

Záložní zdroj využijeme v případě, že potřebujeme ochránit počítač před výpadkem elektrické sítě, při kterém by potencionálně mohlo dojít ke ztrátě neuložených dat, ztrátě příjmů apod.

Princip záložního zdroje spočívá v použití olověných akumulátorů jako náhradních zdrojů elektrické energie. V případě poklesu napětí v síti elektrického rozvodu dojde k přepnutí napájení a energie se začne čerpat z akumulátorů až do chvíle jejich vybití nebo opětovné dodávky elektrické energie ze sítě. Takto chráněný počítač je tedy v případě výpadku možno řádně vypnout s ukončením všech aplikací, uložením rozpracovaných dat a se správnými konfiguračními nastaveními počítače.

Nejdůležitějším faktorem záložních zdrojů je velikost akumulátorů - kapacita, kterou je možno v případě výpadku využít a maximální zatížení záložního zdroje. Dnes se u záložních zdrojů pro osobní počítače setkáváme s kapacitou až 750VA při zatížení 480W. Tato kapacita umožňuje při maximálním zatížení až 7 minut záložního provozu. Baterie jsou povětšinou bezúdržbové a měnitelné za provozu. Pro využití v serverovnách lze využít záložní zdroje s kapacitou až 80 000VA.

Dalšími možnostmi dnes komerčně dostupných záložních zdrojů jsou přepěťové ochrany připojených zařízení včetně telefonní a DSL linky, komunikace s PC přes rozhraní USB, vypnutí PC v případě přechodu do záložního režimu, světelná a zvuková signalizace stavu záložního zdroje a další.

Doporučení

Cenová dostupnost je odvozena od typu zařízení a samozřejmě kapacity. Záložní zdroje pro PC se pohybují od 2000Kč do 5000Kč. Záložní zdroje pro servery pak od 10 000Kč.

Další, rozšiřující možností je pak připojení záložního agregátu - elektrocentrály v případě rozsáhlého výpadku elektrické energie pro udržení provozu nezbytně nutných systémů. Jedná se o benzínové agregáty, které jsou schopny prakticky neomezeně dodávat výkon v řádu kW, dostačující k zajištění provozu PC, respektive serveru v případě dlouhodobého

výpadku elektrické sítě. Cena těchto zařízení je však již vyšší, v závislosti na jmenovitém výstupním výkonu, ceny začínají na 10 000Kč.

9.2.3 Režimová bezpečnost

Jedná se především o preventivní opatření. Základem je určit režimová opatření pro práci s informacemi, komunikačními a počítačovými systémy. Režimová opatření by měla stanovit v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a bezpečnostní způsobilosti následující:

- stupeň utajovaných informací,
- kdo má k utajovaným informacím přístup a jaká jsou jejich oprávnění,
- postupy a manipulaci s utajovanými informacemi,
- stanovit režim pohybu zaměstnanců ve firmě,
- návštěvní řád.

ZÁVĚR

Možným a pravděpodobným rysem kyberterorismu v budoucnu je jeho rozsáhlost a brutalita. Jeho hlavním cílem už nemusí být degradace daného systému, ale znásobení účinků tradičního fyzického teroristického útoku, a to např. vyvolat paniku, strach a zmatek v celé populaci.

S rostoucí složitostí ICT je boj proti kyberterorismu velmi složitý. I přes veškerou snahu budou kyberteroristé vždy o krok napřed. Složitost a promyšlenost útoků stálé stoupá, a proto musíme brát v úvahu budoucí taktiky nebo cíle kyberteroristů a všímat si drobných změn v jejich jednání. Musíme se ponaučit z minulosti, kdy mnozí experti považovali za nemožné využít dopravní letouny jako zbraň. Je tedy nutné brát v úvahu každý možný i nemožný scénář kyberteroristického útoku, a to i ve spojení s fyzickým.

K řešení tohoto problému lze přistupovat z mnoha směrů. Je nezbytná spolupráce na úrovni vládního i soukromého sektoru, ve smyslu sdílení informací mezi sebou. Neustálé vzdělávání společnosti v oblastech informační bezpečnosti, kryptografii, ochraně dat a dalších oborech je nezbytné. Připravenost na tento typ útoku je jedním z hlavních pilířů obrany.

Avšak úplná ochrana před kyberterorismem není dle mého názoru možná. Pokud chce útočník někam proniknout, nakonec se tam zcela jistě dostane. Nejdůležitější součástí útoku je sama osoba útočníka. Jsou to jeho nabyté vědomosti, znalosti a dovednosti, které určují úspěšnost útoku.

CONCLUSION

The possible and probable attribute of cyberterrorism in the future is its expansiveness and brutality. Its main goal is no longer a system degradation, but to intensify the effects of traditional, physical terrorist´s attack, e.g. cause panic, fear and confusion among the population.

With growing potential of ICT is the fight against cyberterrorism very difficult. Despite all the effort, cyberterrorists will always be one step ahead. The complexity and premeditation of the attacks is growing up and therefore we have to consider future tactics or the cyberterrorist´s targets and notice slight changes in their behaviour. The necessity to learn from the past, where many experts thought the use of an airplane as a weapon is impossible, is essential. It is necessary to consider every possible scenario of a cyberterrorists attack even in a connection with a physical one.

There are many ways how to approach the problem. The cooperation between the government and private sectors is essential, especially in the sense of sharing information. Insistent education of the society in the field of informational security, cryptography, data security and other fields is fundamental. Being prepared is one of the main pillars in the fight against that kind of attacks.

Nevertheless in my opinion a full protection against cyberterrorism is not possible. When the attacker wants to get somewhere he will find a way. The most important part of the attack is the person of the attacker itself, his knowledge and skills are the abilities that determine the success of the attack.

SEZNAM POUŽITÉ LITERATURY

[1] FOLTIN, Pavel; ŘEHÁK, David. *Důvody realizace a formy terorismu. Strategie a obrana* [online]. 2005, č. 1, [cit. 2010-11-18]. Dostupný z WWW: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2005/1-2005/duvody-realizace-a-formy-terorismu.html>.

[2] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007. 284 s. ISBN 978-80-247-1561-2.

[3] JIROVSKÝ, Václav. *Společnost ve virtuálním světě*. Konference *CYTER* [online]. 2010, č. 01, [cit. 2011-03-20]. Dostupný z Internetu pro registrované účastníky: <https://cythres.fd.cvut.cz/cyter2010/cs/presentation.php>.

[4] JIROVSKÝ, Václav. Kyberterorismus. *Personalis* [online]. 2006, [cit. 2011-03-20]. Dostupný z WWW: <www.as4u.cz/filemanager/files/file.php?file=3990 >.

[5] ŠPIDLA, Aleš. *Role odboru kybernetické bezpečnosti v ochraně českého kybernetického prostoru*. Konference *CYTER* [online]. 2010, [cit. 2011-03-20]. Dostupný z Internetu pro registrované účastníky: <https://cythres.fd.cvut.cz/cyter2010/cs/presentation.php>.

[6] VERTON, Dan. Black Ice : Neviditelná hrozba kyberterorizmu. [s.l.] : Helion , 2004. 278 s. ISBN 83-7361-565-2.

[7] DUNNIGAN, James F. Bojiště zítřka: Jak čelit globálnímu nebezpečí kyberterorizmu. Vyd. 1. Praha: Baronet, 2004. 356 s. ISBN 80-7214-642-4. [kniha]

[8] JANOUŠEK, Michal. Kyberterorismus: Terorismus informační společnosti. Strategie a obrana [online]. 2006, č. 2, [cit. 2010-11-18]. Dostupný z WWW: <http://www.defenceandstrategy.eu/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html>.

[9] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[10] Základní definice, vztahující se k tématu kybernetické bezpečnosti [online]. Praha: Grada Publishing a.s, 2009 [cit. 2011-03-28]. Dostupné z WWW: <www.mvcr.cz/soubor/cyber-vyzkum-studie-pojmy-pdf.aspx >.

[11] MALANÍK, David. Význam fyzického zabezpečení IT systémů.[online]. 2010, [cit. 2011-04-09]. Dostupný z WWW: <http://www.securityrevue.com/article/2010/09/vyznam-fyzickeho-zabezpeceni-it-systemu/>.

[12] Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?. [online]. 6. 1. 2011, [cit. 2011-04-09]. Dostupný z WWW: <http://www.zone-h.org/news/id/4737>.

[13] SCADA software for industrial control systems and building automation.. *Ss* [online]. 2008, ss, [cit. 2011-04-09]. Dostupný z WWW: <http://broadwin.com/SCADA.htm>.

[14] FSE Computing [online]. 2008, ss, [cit. 2011-04-09]. Dostupný z WWW: <http://www.fsecomputing.co.uk/fsec_firewalls.html>.

[15] Kyberterorismus II.. *Vírusy.sk* [online]. 2003, [cit. 2011-04-09]. Dostupný z WWW: <http://www.virusy.sk/clanok.ltc?ID=403>.

[16] Kyberterorismus I.. *Vírusy.sk* [online]. 2003, [cit. 2011-04-09]. Dostupný z WWW: <http://www.virusy.sk/clanok.ltc?ID=402>.

[17] Kyberterorismus III.. *Vírusy.sk* [online]. 2003, [cit. 2011-04-09]. Dostupný z WWW: <http://www.virusy.sk/clanok.ltc?ID=40a>.

[18] HOCH, Karel . Datová bezpečnost v praxi. Zlín, 2006. 75 s. Bakalářská práce. Univerzita Tomáše Bati, fakulta technologická.

[19] JIROVSKÝ, Václav. *Kybernalita* [online]. 2005 [cit. 2011-04-09]. Dostupný z WWW: <http://www.studentsummit.cz/data/129130369BGR_ECOSOC_Kybernalita.pdf>.

[20] WALLETZKÁ, Lenka . Jak účinně čelit DDoS útokům. *Comguard* [online]. 2010, [cit. 2011-04-09]. Dostupný z WWW: <http://www.comguard.cz/novinky/komentar-jak-ucinne-celit-ddos-utokum/>.

[21] Globální bezpečnostní platforma pro aplikační kontrolu. [online]. 2009, [cit. 2011-04-09]. Dostupný z WWW: <http://www.comguard.cz/produkty/mcafee-network-defense/mcafee-firewall-enterprise-edition-sidewinder/>.

[22] LAUCKÝ, Vladimír. Speciální bezpečnostní technologie. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. 223 s. ISBN 978-80-7318-762-0.

[23] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010. 81 s. ISBN 978-80-7318-889-4.

[24] LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007. 123 s. ISBN 978-80-7318-631-9.

[25] LAUCKÝ, Vladimír. Řízení technologických procesů v průmyslu komerční bezpečnosti. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006. 101 s. ISBN 80-7318-432-X.

[26] ZEMAN, Petr. Česká bezpečnostní terminologie: Výklad základních pojmů. Brno: Masarykova univerzita-Vydavatelství, 2003. 186 s. ISBN 80-210-3037-2.

[27] Metody analýzy a predikce bezpečnostních hrozeb a rizik: [online] sborník z odborného semináře / Vlastimil Galatík, Petr Hlaváček, Karel Zetocha. 1. vyd. Brno: Univerzita obrany, 2009, [cit. 2011-04-09]. Dostupný z WWW: <http://www.defenceandstrategy.eu/cs/informacni-servis/metody-analyzy-a-predikce-bezpecnostnich-hrozeb-a-rizik.html>

[28] FISCHER, Hans. Reifegrad der Cyber Kriminalität. - [online]. 26. 09. 2006, [cit. 2011-05-04]. Dostupný z WWW: <http://www.rolotec.ch/blog/archives/sicherheit/>. MINAŘÍK, Pavel. AdvaICT - Bezpečnostní monitoring sítí - IDS/IPS nové generace. *ICT Security* [online]. 2010, [cit. 2011-05-04]. Dostupný z WWW: <http://ictsecurity.cz/sk/10/06/2-ids-ips-monitoring/advaict-bezpecnostni-monitoring-siti-ids/ips-nove-generace.html>.

[29] Encrypting File System. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 9. 9. 2010, last modified on 9. 9. 2010 [cit. 2011-05-04]. Dostupné z WWW: <http://cs.wikipedia.org/wiki/Encrypting_File_System>.

[30] ŠUMOVÁ, Věra. Elektronický podpis [online]. 2001 [cit. 2011-05-04]. Elektronický podpis. Dostupné z WWW: <http://sandbox.cz/~varvara/El_podpis/index.html>.

[31] GROSS, Stanislav. Historie, vývoj a kybernetické hrozby spojené s kybernetickou kriminalitou. In *Bezpečné slovensko a európská únia : Zborník príspevkov z 2. Medzinárodnej vedeckej koferencie*. Slovensko: Vysoká škola bezpečnostnostného manažerstva v Košiciach, 2008. s. 360. ISBN 978-80-89282-289.

[32] ALMEIDA, Marcelo. *Zone-h* [online]. 2011 [cit. 2011-05-05]. Defacements Statistics 2010: Almost 1,5 million websites defaced, what's happening?. Dostupné z WWW: <http://www.zone-h.org/news/id/4737>.

[33] Američané zabili Usámu bin Ládina. *Novinky.cz* [online]. 2011, [cit. 2011-05-06]. Dostupný z WWW: <http://www.novinky.cz/zahranicni/blizky-a-stredni-vychod/232217-americane-zabili-usamu-bin-ladina.html?ref=zpravy-dne>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

CCTV	Closed Circuit Television - Uzavřený kamerový systém.
CERT	Computer Emergency Response Team.
CESNET	Sdružení založené vysokými školami a Akademií věd České republiky.
CIA	Central Intelligence Agency - Zpravodajská služba USA.
CNN	Cable News Network - Americká kabelová televize.
CSIRT	Computer Security Incident Response Team - Bezpečnostní tým pro koordinaci řešení bezpečnostních incidentů v počítačových sítích v České republice.
ČR	Česká republika.
DDOS	Distributed Denial of Service - Distribuovaný DOS útok.
DNA	Deoxyribonukleová kyselina – Nositelka genetické informace.
DNP3	Distributed Network Protokol - komunikační protokol pro SCADA.
DNS	Domain Name Systém - Systém doménových jmen.
DOS	Denial of Service - Odmítnutí služby.
DSA	Digital Signature Algorithm - Standart pro digitální podpis v USA.
DSL	Digital Subscribe Line - Digitálně připojená linka.
EFS	Encrypting File System - Šifrovaný systém souborů.
EKV	Elektronická kontrola vstupu.
EMP	Elektromagnetický pulz.
EPS	Elektronická požární signalizace.
FBI	Federal Bureau of Ivestigation - Federální úřad pro vyšetřování.
ICCP	Inter-Control Centre Communications Protokol - komunikační protokol pro SCADA.
ICT	Information and Communication Technologies - Informační a komunikační technologie.

IM	Instatnt Messaging - Internetová služba.
IS	Informační systém.
ISAPI	Internet Server Application Program Interface - množina funkcí ve
IT	Informační technologie.
LAN	Local Area Network - Místní počítačová síť.
MAC	Medis Access Control - Identifikátor síťového zařízení.
MV	Ministerstvo vnitra.
NAS	Network - Attached Storage - Úložiště dat připojitelné pomocí LAN/WAN.
OS	Operační systém.
PC	Personal Computer - Osobní počítač.
PCO	Pult centralizované ochrany.
PKB	Průmysl komerční bezpečnosti.
PLC	Programmable logic controller - Programovatelný logický automat.
PZS	Poplachový zabezpečovací systém.
RAID	Redundant Array of Inexpensive/Independent Disk - Vícenásobné diskové pole nezávislých disků.
RFID	Radio Frequency Identification - Identifikace na rádiové frekvenci.
RSA	Iniciály autorů Rivest, Shamir, Adleman.
SAN	Storage Area Network - Úložiště dat.
SBS	Soukromé bezpečnostní služby.
SCADA	Supervisory control and data acquistion - Nadřazené ovládání a sběr dat.
SOA	Service Oriented Architecture - Servisně orientovaná architektura.
TCP/IP	Transmission Control Protocol / Internet Protocol - komunikační protokol pro SCADA.
UPS	Uninterruptible power supply – Nepřerušitelný zdroj napájení.

URL	Unique Resource Locator - Jednoznačné určení zdroje.
USA	United States of America - Spojené státy americké.
USB	Universal Serial Bus - Univerzální sériová sběrnice.
VoIP	Voice over Internet Protocol - technologie umožňující přenos hlasu.
WLAN	Wireless Local Area Network - Rozlehlá počítačová síť.
WPA	Wi-Fi Protected Access - Typ zabezpečení bezdrátové sítě.

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ