Univerzita Pardubice
Fakulta ekonomicko-správní

Analýza zranitelnosti prvků kritické infrastruktury - informační a komunikační systémy

Pavla Břichnáčová

Bakalářská práce
2012

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavla Břichnáčová**
Osobní číslo:	**E08565**
Studijní program:	**B6208 Ekonomika a management**
Studijní obor:	**Management ochrany podniku a společnosti**
Název tématu:	**Analýza zranitelnosti prvků kritické infrastruktury - komunikační a informační systémy**
Zadávající katedra:	**Ústav ekonomiky a managementu**

Zásady pro vypracování:

1. Charakteristika komunikačních a informačních systémů
2. Bezpečnost komunikačních a informačních systémů
3. Analýza komunikačních a informačních systémů ve vybrané společnosti
4. Formulace závěrů, návrhy a doporučení

Rozsah grafických prací: -

Rozsah pracovní zprávy: cca 30 stran

Forma zpracování bakalářské práce: tištěná/elektronická

Seznam odborné literatury:

MOZGA, Jaroslav, VÍTEK, Miloš, KOVÁŘÍK, František. Kritická infrastruktura společnosti. 1. vyd. Hradec Králové : Gaudeamus, 2008. 155 s. ISBN 978-80-7041-299-2.

NORTHCUTT, Stephen. Bezpečnost sítí : velká kniha. Vyd. 1. Brno : CP Books, 2005. 589 s. ISBN 80-251-0697-7.

PUŽMANOVÁ, Rita. Bezpečnost bezdrátvé komunikace. Vyd. 1. Praha : Computer Press, 2005. 184 s. ISBN 80-251-0791-4.

ŘÍHA, J. Typological Features of The Critical Infrastructure . The Science for Population Protection [online]. 2009, 1, [cit. 2011-06-28]. Dostupný z WWW: www.population-protection.eu/attachments/033_vol1n1_riha.pdf. ISSN 1803-635X.

ŠENOVSKÝ, Michail, ADAMEC, Vilém, ŠENOVSKÝ, Pavel. Ochrana kritické infrastruktury. 1. vyd. Ostrava : SPBI, 2007.141 s. ISBN 978-80-7385-025-8.

Vedoucí bakalářské práce: **Ing. Ondřej Svoboda**
Ústav ekonomiky a managementu

Datum zadání bakalářské práce: **21. září 2011**

Termín odevzdání bakalářské práce: **30. dubna 2012**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Marcela Kožená, Ph.D.
vedoucí ústavu

V Pardubicích dne 21. září 2011

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využil/a, jsou uvedeny v seznamu použité literatury.

Byla jsem seznámena s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 30. 4. 2012 Pavla Břichnáčová

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce Ing. Ondřeji Svobodovi za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Práce se zabývá zranitelností informačních a komunikačních systémů, což je jeden z prvků kritické infrastruktury. V první části jsou uvedeny základní pojmy týkající se kritické infrastruktury. V druhé kapitole je blíže charakterizován problém zranitelnosti komunikačních a informačních technologií. Třetí část je zaměřena na analýzu možných problémů v oblasti komunikačních a informačních technologií a v neposlední části se zabývá zranitelností informačních a komunikačních systémů ve společnosti eBRÁNA, s. r. o.

KLÍČOVÁ SLOVA

Kritická infrastruktura, informační a komunikační systémy, zranitelnost, infrastruktura, ochrana kritické infrastruktury

TITLE

Analysis of the vulnerability of critical infrastructure elements: Information and communication technology

ANNOTATION

The bachelor thesis deals with vulnerability of information and communication systems which is an element of the critical infrastructure. In the first part there are given basic information about critical infrastructure. In the sekond part is closer characterized problem of vulnerability of communication and information technologies. The third part is focused on analysis of potential problems in the area of communication and information technology and in the last part deals with vulnerability of information and communication systems in the company eBRÁNA, s. r. o.

KEYWORDS

Critical infrastructure, information and communication systems, vulnerability, infrastructure, protection of critical infrastructure

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

ACL	ACCESS CONTROL LIST
B2B	BUSINESS TO BUSINESS
B2C	BUSINESS TO COMPANY
BOZP	BEZPEČNOST OCHRANY ZDRAVÍ PŘI PRÁCI
CCA	CAUSES AND CONSEQUENCES ANALYSIS
ČR	ČESKÁ REPUBLIKA
DSL	DIGITAL SUBSCRIBER LINE
ETA	EVENT TREE ANALYSIS
FTA	FAULT TREE ANALYSIS
GiB	GIBIBYTE
GNU	GNU'S NOT UNIX
HAZOP	HAZARD OPERATION PROCESS
HRA	HUMAN RELIABILITY ANALYSIS
ICT	INFORMATION AND COMMUNICATION TECHNOLOGY
IDS	INTRUSION DETECTION SYSTÉM
IIS	INTERNET INFORMATION SERVICES
IP	INTERNETOVÝ PROTOKOL
IT	INFORMAČNÍ TECHNOLOGIE
LDAP	LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL
NDA	NON-DISCLOSURE AGREEMENT
NKBT	NÁRODNÍ KONTAKTNÍ BOD PRO TERORISMUS
OECD	ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT
OM	OBCHODNÍ MANAGAMENT
OS	OPERAČNÍ SYSTÉM
PHA	PREMINARY HAZARD ANALYSIS
PSA	PROBABILISTIC SAFETY MANAGAMENT
SW	SOFTWARE
TCP	TRANSMISSION CONTROL PROTOCOL

THC	THE HACKER'S CHOICE
UDP	USER DATAGRAM PROTOCOL
URL	UNIFORM RESOURCE LOCATOR
VPN	VIRTUAL PRIVATE NETWORK
WWW	WORLD WIDE WEB

ÚVOD

Už od nepaměti je společnost závislá na dobře fungující kritické infrastruktuře. V historii byla známa důležitost infrastruktury, a proto byla ochraňována vojenskou silou. Vybudováním ochrany se vládci pojistili proti rozpadu jejich říše. V dnešní době se význam ochrany kritické infrastruktury prohloubil především díky rostoucí závislosti společnosti na technologiích a současně i s růstem pravděpodobnosti teroristických útoků.

Společnost je závislá na dobře fungující infrastruktuře, zejména technologické (dodávka vody a potravin, dodávky elektřiny a tepla, dodávky pohonných hmot, komunikace, apod.). Ztráta nebo oslabení technické infrastruktury by měla za následek snížení kvality lidského života a neblahé dopady na základní lidské potřeby. Dnes si společnost neumí představit svět bez moderních technologií, které používá v běžném životě takřka denně. Každý den používá mobilní telefony, počítače, Internet, a to nejen v pracovním životě, ale i v životě soukromém. Technologii používá jako komunikační prostředky, jako informační kanál, anebo také jako ochranu svých osobních údajů.

Moderní technologie se vyvíjí geometrickou řadou a pokrok nejde nijak zastavit. Stejně jako hrozba útoku se díky novým znalostem a zkušenostem neustále rozrůstá a dochází k napadení internetových portálů, ale i počítačových sítí a soukromých dat. Jde o věčný boj mezi „dobrem a zlem“, kdy útočníci testují své znalosti a možnosti a na straně druhé napadený hledá nejlepší a nejrentabilnější možnost, jak útokům bránit. S vývojem nových technologií už není naším nepřítelem nevzdělanost, ale nepozornost.

V první kapitole této práce budou vymezeny základní pojmy problematiky kritické infrastruktury a další definice, které zjednoduší orientování v ostatních kapitolách.

Druhá kapitola bude orientována na téma komunikační a informační systémy, slabá místa a jejich ochranu. Dále se bude věnovat problematice kritické infrastruktury komunikačních a informačních systémů na území České republiky.

Čtvrtá kapitola pojednává o analýzách používaných k odhalení rizika. Dále zde budou uvedeny některé metody analyzování rizika.

V poslední kapitole bude analyzována hrozba zranitelnosti informačních a komunikačních systémů u konkrétních subjektů. Poté bude následovat rozbor a návrh ochranných opatření proti napadení a ztrátě citlivých dat.

Hlavními cíli této práce jsou:

1. **Vymezení pojmů kritické infrastruktury a objasnění problematiky informačních a komunikačních technologií.**
2. **Analýza zranitelnosti informačních a komunikačních systémů a návrh vhodných opatření.**

1. KRITICKÁ INFRASTRUKTURA

V následujících kapitolách se budeme věnovat vymezením a popsáním pojmů, které jsou úzce spjaty s kritickou infrastrukturou. S těmito pojmy bude spojen i zbytek bakalářské práce.

1.1. Infrastruktura

Pojem infrastruktura vznikl v 19. století ve Francii a během první poloviny 20. století primárně označoval vojenská zařízení. Pojmem infrastruktura jsou vymezena všechna základní zařízení dlouhodobého užívání personálního, materiálního a institucionálního druhu sloužící k zaručení fungování dělby úkolů v národním hospodářství [12].

Existuje velmi úzká vazba mezi člověkem a infrastrukturou, protože člověk potřebuje infrastrukturu, poněvadž bez jejich služeb by se výrazně zhoršila úroveň a kvalita žití, a infrastruktura potřebuje člověka, jelikož bez jeho přičinění by nevznikla, nevyvíjela se, nebyla by udržitelná a neustále by selhávala. Lidský faktor je tedy řídícím a kontrolním prvkem každé infrastruktury [6].

Infrastruktura se dělí na veřejnou a kritickou.

1.2. Veřejná infrastruktura

Veřejnou infrastrukturou se rozumí (dle stavebního zákona) pozemky stavby a zařízení, a to [14]:

1. Dopravní infrastruktura, například stavby pozemních komunikací, drah, vodních cest, letišť a s nimi souvisejících zařízení;
2. Technická infrastruktura, kterou jsou vedení a stavby a s nimi provozně související zařízení technického vybavení, například vodovody, vodojemy, kanalizace, čistírny odpadních vod, stavby a zařízení pro nakládání s odpady, trafostanice, energetické vedení, komunikační vedení veřejné komunikační sítě a elektronické komunikační zařízení veřejné komunikační sítě, produktovou;
3. Občanská vybavení, kterými jsou stavby, zařízení a pozemky sloužící například pro vzdělávání a výchovu, sociální služby a péči o rodiny, zdravotní služby, kulturu, veřejnou správu, ochranu obyvatelstva;
4. Veřejné prostranství, zřizované nebo užívané ve veřejném zájmu.

1.3. Kritická infrastruktura

Kritickou infrastrukturou se rozumí vzájemně propojené sítě či systémy obsahující identifikovatelná odvětví a instituce (včetně lidí a postupů) poskytující spolehlivý tok produktů a služeb nezbytných pro obranu a ekonomickou bezpečnost, která se chápe jako schopnost státu konkurovat na globálních trzích, zatímco se udržují na přijatelné úrovni reálné příjmy obyvatel a fungování veřejné správy na všech úrovních společnosti. K ekonomické bezpečnosti se připojuje i bezpečnost fyzická týkající se ochrany fyzických aktiv před škodami v důsledku působení fyzických sil a bezpečnost kybernetická zabývající se především ochranou před poruchami nebo neautorizovanými přístupy do počítačové sítě. A jednotlivé položky infrastruktury se mohou dělit na typické procesy, jako jsou distribuce, skladování, platby, recyklace, přenos dat, doprava apod [6].

1.3.1. Objekty a subjekty kritické infrastruktury

Objekty kritické infrastruktury jsou vybrané stavby a zařízení veřejné infrastruktury a další prvky, které vlastní nebo provozují subjekty kritické infrastruktury. Subjekty kritické infrastruktury jsou vlastníci a provozovatelé výrobních a nevýrobních systémů vytvářející produkty nebo poskytující služby kritické infrastruktury [9].

1.4. Ochrana kritické infrastruktury

Význam slova ochrana je prevence či obrana. V kritické infrastruktuře pojem ochrana svádí dohromady nespočet strategií, plánů a procedur zabývajících se prevencí, připravenosti a odezvou a obnovou.

Ochrana kritické infrastruktury vyžaduje aktivní část vlastníků a operátorů, regulátora, profesních asociací a institucí ochrany obyvatel. Pro tuto spolupráci by měly platit tyto zásady [6]:

- Ochrana by se měla soustředit na minimalizaci zdravotních a bezpečnostních rizik pro veřejnost a měla by napomoci kontinuitě podnikání a kontinuitě služeb veřejné správy.
- Ochrana by měla vycházet z analýzy vzájemných závislostí a analýzy zranitelnosti vůči všem typům hrozeb a nebezpečí.
- Měly by se využívat vhodné postupy a techniky řízení rizik pro určení úrovně tzv. bezpečné ochrany (ochranné bezpečnosti) a pro nastavení priorit alokace zdrojů.

- Odpovědnost za řízení rizik infrastruktury primárně leží na vlastnících a operátorech.
- Ochrana vyžaduje konzistentní a kooperativní partnerství mezi vlastníky a operátory kritické infrastruktury a veřejnou správou.
- Pro lepší řízení rizik se předpokládá sdílení informací o hrozbách a zranitelnostech mezi veřejnou správou a vlastníky a operátory.
- Vzhledem k tomu, že většina kritické infrastruktury je v rukou soukromých vlastníků, měla by veřejná správa specifikovat požadavky na její ochranu na základě vlastní analýzy potenciálních dopadů nefunkčnosti kritické infrastruktury na obyvatele. Veřejná správa ale musí mít strategické záměry a strategické cíle.
- Kritická infrastruktura je vhodným východiskem pro strukturování ochrany do tří vrstev:
  - Vrstva fyzická – systém řízení bezpečnosti vlastníka/operátora
  - Vrstva provozní – lidský faktor a organizační kultura
  - Vrstva strategická – veřejná správa se zabývá dopady na obyvatele – *social impal assessment*, vlastník analyzuje možnosti plánování životního cyklu aktiv

1.5. Prvky kritické infrastruktury

Pro kritickou infrastrukturu je definováno devět oblastí kritické infrastruktury. Jsou to energetika, vodní hospodářství, komunikační a informační systémy, nouzové služby, zdravotní péče, potravinářství a zemědělství, bankovnictví a finanční sektor, veřejná správa a doprava.

Prosté seznamy kritické infrastruktury v současné době dominují ve většině národních strategií bezpečnostního rizika a vzájemně nepředstavují podstatné rozdíly. Aktéři v této oblasti se snaží výběr objektů kritické infrastruktury opřít o soubor kritérií a tím zdůvodnit potřebnou ochranu ekonomicky, společensky a politicky [9].

1.5.1. Energetika

Pro rozvoj technické infrastruktury je nezbytná energie. Z tohoto důvodu je nezbytné pro rozvoj každé země zajistit systémy pro trvale udržitelné dodávky energie [7].

Bez energetiky bychom si jen stěží představili každodenní chod běžného života. Proto je to bezesporu jeden z nejcitlivějších a nejdůležitějších prvků kritické infrastruktury.

Energetika spadá pod Ministerstvo průmyslu a obchodu, a to se také stará o krizový plán. Do této oblasti spadají tyto podoblasti [7]:

→ Elektřina,

→ plyn,

→ tepelná energie,

→ ropa a ropné produkty.

1.5.2. Vodní hospodářství

Voda je také nedílnou součástí každodenního života. Vodu potřebují nejenom lidé, ale i živočichové a rostliny. Je nezbytné ochraňovat zásoby pitné vody před možným útokem.

Vodní hospodářství spadá v České republice pod Ministerstvo zemědělství, a to má také na starosti koncepci zabezpečení obyvatelstva pitnou vodou za krizových situací.

1.5.3. Komunikační a informační systémy

Komunikační a informační systémy se promítají v každodenní činnosti běžného života. Riziko napadení právě informačních systémů je opravdu vysoké vzhledem k pokroku moderní technologie. Potencionálních útočníků na informační a komunikační systémy je nesčetně mnoho, protože možnost napadení je prakticky nejvyšší.

1.5.4. Nouzové služby

Nouzové služby slouží pro odhalování hrozícího nebezpečí, kriminality a udržování bezpečnosti.

Patří sem [4]:

- Hasičský záchranný sbor ČR a příslušné jednotky požární ochrany,
- Policie ČR (vnitřní bezpečnost a veřejný pořádek),
- Armáda ČR (zabezpečení obrany),
- Radiační monitorování vč. Podkladů pro rozhodování o opatřeních vedoucích ke snížení nebo odvrácení ozáření,
- Předpovědní, varovná a hlásná služba.

1.5.5. Zdravotní péče

Zdravotní péči zastřešuje Ministerstvo zdravotnictví České republiky. Do této oblasti se zahrnují [4]:

- Přednemocniční neodkladná péče,
- Nemocniční péče,
- Ochrana veřejného zdraví,
- Výroba, skladování a distribuce léčiv a zdravotnických prostředků.

1.5.6. Potravinářství a zemědělství

Zásobování potravin je opět jeden z důležitých prvků kritické infrastruktury. Potraviny patří mezi životně důležité potřeby, stejně jako voda. Do potravin se řadí nápoje a jídlo.

1.5.7. Bankovní a finanční sektor

Na bankovním a finančním sektoru jsou denně závislé tisícovky lidí, protože denně dochází ke směně zboží a služeb za peníze. Hlavním orgánem spravujícím peníze na území České republiky je Česká národní banka.

1.5.8. Veřejná správa

Do oblastí veřejné správy spadá [21]:

- Právo a zákony,
- Práce a sociální věci,
- Obchod – průmysl,
- Finance,
- Vnitro,
- Obrana a bezpečnost,
- Zahraničí,
- Doprava,
- Školství,
- Kultura,
- Životní prostředí,

- Zemědělství,
- Místní rozvoj,
- Zdraví,
- Informatika.

1.5.9. Doprava

Při osobní a nákladní silniční dopravě, jakož i dopravě železniční, mohou být postiženi jak cestující, tak i obyvatelstvo podél přepravních koridorů haváriemi dopravních prostředků, zvláště těch, které převážejí nebezpečné látky (munici, jedy, hořlaviny, radioaktivní látky apod.). V letecké dopravě může navíc dojít ke katastrofám mimo letiště s možným vznikem velkých lidských ztrát jak mezi cestujícími, tak i obyvateli, které vyžadují provedení záchranných prací spojených s vyhledáváním postižených [12].

2. INFORMAČNÍ A KOMUNIKAČNÍ SYSTÉMY

Tato kapitola se bude zabývat problematikou vymezení a zranitelnosti informačních a komunikačních systémů.

2.1. Informační systémy

Informační systém zabezpečuje sběr, přenos, zpracování a uchování dat za pomoci lidí, technologických prostředků a metod. Účelem je tvorba prezentace informací pro potřeby uživatelů.

Informační systém nemusí mít nutně formu elektronickou, ale i také například papírovou. Jsou to různé kartotéky, telefonní seznam, nebo také účetnictví.

2.2. Komunikační systémy

Komunikačními systémy jsou cesty, jak lze komunikovat mezi dvěma subjekty. Ať už se jedná o telefonické spojení, mohou to být i chatovací místnosti, softwarové programy nebo také pošta.

2.3. Specifika kybernetické infrastruktury

Evropská unie zpracovala v roce 2002 akční plán na ochranu kybernetické infrastruktury. Rada Evropy připravila mezinárodní dohodu (konvenci) o kybernetických zločinech, do kterých patří zločiny proti důvěrnosti, integritě a dosažitelnosti počítačových dat a systémů, které se dále dělí na [7]:

- Nezákonný přístup,
- Nezákonné odposlouchávání,
- Narušování dat,
- Narušování systémů,
- Zneužití prostředků,
- Zločiny se vztahem k počítači, které jsou děleny na počítačové padělání a počítačový podvod,
- Zločiny se vztahem k obsahu počítače, což je především dětská pornografie,
- Zločiny se vztahem k autorským nebo obdobným právům.

2.4. Útočníci

Na počítačový systém může (a s velkou pravděpodobností to dříve či později udělá) zaútočit člověk se zlými úmysly. Taková osoba se označuje útočník.

Útočníci se mohou dělit podle nebezpečnosti útoků, kterých jsou schopni. Ne každý je schopen provést sofistikovaný útok, velká část útočníků se omezí na využití dostupných nástrojů na Internetu, další skupina zase jen zkouší, čeho je schopna [3].

2.4.1. Amatéři

Jedná se o nejméně nebezpečné útočníky. Většinou jen zkouší, zda dokáží využít nějakou na Internetu popsanou bezpečnostní díru. Často se omezí na spuštění dostupných nástrojů, kontrolují otevřenost portů, běžící služby apod. Motivací k útoku je tedy víceméně zvědavost [3].

2.4.2. Hackeři

Hacker je někdo, kdo má velmi rozsáhlé znalosti systém, jeho fungování a bezpečnosti. Tyto své znalosti obvykle nepoužívá k ničení, napadání nebo jakékoliv destrukční činnosti, ale chyby odhalí a následně na ně upozorní, aby se jim mohli všichni ostatní vyvarovat [5].

2.4.3. Crackeři

Definic Crackera je více. Podle jedné z definic se jedná o člověka, který obchází protipirátské ochrany počítačových programů. Dokáže z nich získat sériové číslo, případně program upravit tak, aby zadání tohoto čísla (nebo jiný druh ochrany) nevyžadoval. Druhá definice říká, že je to osoba zneužívající bezpečnostní chyby objevené hackerem. Používá je ke svému obohacení, počítačovému terorismu nebo vydírání [3].

2.4.4. Profesionálové

Rekrutují z řad počítačových profesionálů, jsou vybaveni velmi dobrými znalostmi a dostatečnými prostředky, vybavením i časem. Jejich útoky patří mezi nejnebezpečnější, často se vymykají všem známým postupům. Zabezpečení proti těmto útokům je velmi nákladné a velmi složité. V běžné praxi na něj firmy většinou předem rezignují a doufají, že právě jejich systému se útok vyhne [3].

Skupiny těchto odborníků jsou různé [5]:

- Komerční společnosti, provádějící penetrační testy a bezpečnostní audit. Jejich úkolem je pokusit se dostat do systému a tím najít chyby, které pak pomohou vlastníkovi dat zacelit.
- „Nájemní zločinci“ – tím můžeme chápat nejrůznější profesionály, kteří své znalosti prodávají.
- Vládní agenti. Každá bezpečnostní složka každého státu zaměstnává i tým lidí, kteří jsou profesionály na počítačovou bezpečnost. O náplni jejich práce se však může jen dlouze spekulovat.

2.5. Výběr oběti

Nejjednodušším způsobem, jak útočník může najít svoji potencionální oběť, je najít si ji na Internetu. Například na Googlu je běžný uživatel Internetu schopen si najít jakékoliv informace a to o čemkoliv a o komkoliv.

To, co je za běžných okolností bráno jako přednost, může být za jiných okolností Achillovou patou. Google je výborný vyhledávač, na webu umí najít prakticky cokoliv. Řada lidí na webu bohužel nechává citlivé informace. Pro Google jsou to informace jako každé jiné, takže pokud je najde, uloží je do své databáze a zprostředkuje komukoliv, kdo si o ně umí říci [10].

Útočník si může na Internetu vyhledat například Windows servery s IIS 4.0, který obsahuje řadu bezpečnostních děr, a který je pro řadu útočníků velmi snadným cílem. Mohou se připojit vzdáleně k nějakému počítači, hledají špatně zabezpečená rozšíření programu FrontPage apod. Obdobným způsobem může útočník zjistit hesla do databází a dostat tak přístup k citlivým datům.

2.6. Sběr informací

K chirurgicky přesnému útoku je zapotřebí dostatek informací o subjektu, který chce útočník napadnout. Je to z toho důvodu, aby útok byl co nejvíc nenápadný. Hodí se vlastně všechny informace, které se týkají zabezpečení organizace (připojení k Internetu, způsob práce se vzdáleným připojením, zabezpečení intranetu/extraktu…apod.)

Z veřejně dostupných informací, lze sestavit podrobný bezpečnostní profil organizace. Co všechno lze zjistit je uvedeno v následující tabulce.

Tabulka 1: Oblasti zájmu útočníka a kritické informace o nich

Technologie	Informace
Internet	doménová jména
	síťové rozsahy
	konkrétní IP adresy počítačů přístupných zvenčí
	TCP A UDP služby, které na těchto systémech běží
	Architektura
	přístupová práva (ACL)
	Systémy pro detekci průniku (IDS)
	Informace o systémech (jména uživatelů a skupin,…)
Vzdálený přístup	Telefonní čísla
	Typ vzdáleného systému
	Způsob autentizace
	VPN a další protokoly
Extranet	Počáteční a koncový bod spojení
	Typ spojení
	Typ kontroly přístupu

Zdroj:upraveno podle [10]

2.7. Útoky na operační systémy

V této kapitole si vysvětlíme pojmy týkající se operačních systémů. Dále si představíme nejběžnější operační systémy a poukážeme na slabá místa. Způsobů, jak chránit operační systémy před napadením je velmi mnoho a proto si ukážeme nejzákladnější z nich.

Operační systém je základní programové vybavení počítače. Jedná se o základní software, ve kterém se uživateli pracuje jednodušeji a vytváří si v něm vlastní aplikace, soubory, ukládá data apod.

2.7.1. Windows

Počítače s operačními systémy Windows tvoří významnou část většiny soukromých i veřejných sítí.

2.7.1.1. Útoky na Windows

Díky svému rozšíření je operační systém Windows častým terčem útoků hackerů. Za začátek éry útoků na Windows by se dal považovat rok 1997, ve kterém hacker jménem Hobbit uveřejnil článek o základním síťovém protokolu Windows.

Popularita Windows je dvousečná zbraň. Na jednu stranu z ní plyne velký zájem vývojářů, výborná kompatibilita a široce dostupná podpora. Na druhou stranu se monokultura Windows čím dál častěji stává obětí hackerů, kteří mohou snadno vytvořit a v prakticky celosvětovém měřítku nasadit nebezpečné exploity. Microsoft je zkrátka jedna z nejznámějších firem, v kladném i záporném slova smyslu.

Útoky na Windows se dělí na tři části [10]:

- Útoky na dálku:
    - proprietární síťové protokoly (hádání hesel, odposlechnutí hesla,…)
    - síťové služby (přečtení paměti…)
- Útoky na blízko (krádež hecovaných hesel, lámání hesel…)

2.7.1.2. Zabezpečení

Systém Windows 7, který už se stává nejběžnějším operačním systémem, uživateli nabízí základní možnosti obrany a konfigurace bezpečnostních nastavení prostřednictvím Centra akcí.

Mají následující význam [2]:

- Ochrana proti spywaru a nežádoucímu softwaru,
- Antivirová ochrana,
- Windows update,
- Údržba.

Windows Defender je novinkou v operačním systému Windows Vista. Jedná se o detekci spywaru, jehož přehled je rovněž dostupný z centra akci i ve Windows 7. Ochrana před spywarem postupem času získala na důležitosti – spyware, který špehuje uživatelskou práci, dokáže útočníkovi prozradit například používaná hesla, čísla kreditních karet apod [2].

2.7.2. Linux

Druhým nejrozloženějším operačním systémem je bezesporu Linux. Vznik operačního systému GNU/Linux se datuje do roku 1991. Cílem projektu GNU bylo vytvoření svobodného operačního systému, tedy takového, který bude dostupný všem, a to včetně zdrojového kódu, a uživatel jej bude moci získat zdarma a nezávisle na jakékoliv společnosti nebo vůli konkrétní osoby. Linux je pouze jádro operačního systému. Zbylá část je tvořena projektem GNU, který existuje o něco déle [5].

2.7.2.1. Útoky na Unix

Většina útoků na unixové operační systémy má stejný cíl: získat práva superuživatele neboli roota. Unix byl navržen jako silný, spolehlivý víceuživatelský operační systém, který se s výhodou spoléhá na malé, vzájemně snadno propojitelné programy. Bezpečnost sice nebyla hlavním cílem návrhu, ale i tak má Unix řadu dobře implementovaných bezpečnostních omezení. Stejně jako u útoků na Windows je i zde dělení útoků na útoky na dálku a útoky na blízko [10].

2.7.2.2. Zabezpečení

Jsou zde tři způsoby snížení rizika napadení. Riziko je zvláštní kombinace aktiv, zranitelnosti a útočníků. Obrana proto může být kategorizována následovně těmito prostředky [1]:

- Snížení hodnoty aktiva pro útočníky,
- Snížení specifické zranitelnosti,
- Neutralizování nebo prevence útoků.

2.7.3. Mac OS

Lidé žijí v domnění, že pokud vlastní počítač značky Apple, nemusí se obávat útoku na jejich data. Bezpečnost dřívějších verzí Mac OS spočívala do jisté míry v tom, že toho příliš neuměly. V každém Macovi se nyní skrývá unixový operační systém, a to, kromě jiného, kvůli vysokému počtu funkcí.

Výhody Unixu samozřejmě nejsou úplně zadarmo. Společně s rychlostí, elegancí a funkcemi nového systému přišla také větší pravděpodobnost bezpečnostních chyb [10].

2.8. Útoky na síťová zařízení

Datům přenášeným po počítačové síti hrozí celá řada nebezpečí. Prakticky ihned po připojení počítače k síti musíme počítat s hrozícími nebezpečími. Na nejvyšší úrovni je lze rozdělit na nebezpečí, která hrozí přenášeným datům a nebezpečí, která hrozí připojeným počítačům [3].

2.8.1. Odposlech a modifikace dat

Počítačovou síť lze obecně považovat za takzvaný nezabezpečený kanál. Data, která prostřednictvím sítě odesíláme, mohou být s většími či menšími problémy odposlechnuta či dokonce modifikována. Nejjednodušší přístup k přenášeným datům mají samozřejmě správci.

Nemusí se jednat přímo o správce firemní sítě, data přenášená prostřednictvím Internetu může odposlechnout správce kteréhokoliv počítače, který data na své cestě využijí [3].

2.8.1.1. Ochrana proti odposlechu a odposlechu sítě

Klasickou obranou proti odposlechu sítě je rozdělení sítě, ať už fyzické (například pomocí přepínače) nebo logické (například pomocí softwarového firewallu nebo virtuální sítě). Různé způsoby rozdělení sítě mají různou spolehlivost. Asi nejbezpečnější je šifrování, které se může nasadit už na úrovni sítě nebo na úrovni aplikací. S dobře šifrovanými daty neudělá ani ten nejlepší program pro odposlech zhola nic [10].

2.8.2. Útoky na připojené počítače

Počítač připojený k počítačové síti se stává snadným terčem útočníků. Připojení jim totiž usnadňuje práci, nemusí kvůli útokům nikam chodit, mohou sedět na druhé straně světa a podobně. Běžný uživatel si možná myslí, že zrovna jeho počítač není pro hackery zajímavý. Na Internetu ale existují (a v praxi se používají) jednoduché programy, které procházejí zvolený prostor IP adres a „zkusmo“ útočí jednoduchými útoky na počítače, které jsou zrovna v daném prostoru připojeny, tedy odpovídají například na ping [3].

2.9. Útoky na web

Navzdory drobnému zpomalení ze začátku nového tisíciletí se World Wide Web neustále rozšiřuje a daleko překračuje i ty nejdivočejší představy většiny svých uživatelů. Starší systémy jsou nahrazovány novými, dynamickými a interaktivními webovými aplikacemi, které běží na webových serverech a využívají nekonečné pokladnice databázových serverů. Rostoucí dostupnost vysokorychlostního připojení otevřela dveře bohatým multimediálním aplikacím a díky zlepšení bezdrátových sítí už můžeme webové aplikace použít prakticky kdekoliv a kdykoliv [10].

2.9.1. Útoky na webové servery

Pojem „webové útoky“ neboli „web hacking“ přišel společně s nástupem Internetu a společně s Internetem se též měnil. Původně označoval útoky na samotný webový server a další přidružený software, nikoliv útoky na aplikační logiku. Tento rozdíl nemusí být vždy zjevný. Chyby v technologiích jsou obvykle dobře popsané, není je těžké najít a není je těžké zneužít – veřejně dostupnými nástroji a exploity vybavený hacker dokáže zranitelný server pokořit v řádu minut [10].

2.9.2. Útoky na webové aplikace

Typy útoků na webové aplikace se příliš neliší od útoků na webové servery. Hlavní rozdíl je v tom, že hacker tentokrát útočí na aplikaci napsanou na míru a nikoliv na „krabicový“ software. Z toho plyne, že útočník bude potřebovat více trpělivosti a zkušeností.

Vyhledávací stroje mají pod palcem obrovský počet webových stránek a dalších zdrojů. Šikovný útočník tyto informace může zneužít k anonymním útokům, hledání vhodných cílů nebo hledání citlivých informací. Vyhledávací stroje mají navíc pro útočníka jednu výraznou výhodu, jsou anonymní. Samy o sobě ale nebezpečné nejsou – nebezpečná je bezstarostnost uživatelů [10].

2.9.3. Obrana

Objem internetových obchodů se zvyšuje a útoky na webové aplikace jsou čím dál častější a nebezpečnější. Osvědčí se pravidelná aktualizace softwaru, svědomitá konfigurace a pečlivá kontrola uživatelského vstupu. Pokud by se každý vstup od uživatele považoval za potenciální útok na aplikaci, budeme mít při skutečném útoku velký náskok. Neměly by s poslední řadě ani podceňovat audity vlastních webových aplikací [10].

2.10. Útoky na vytáčené linky

Analogové vytáčené linky mohou ve světle kabelového Internetu a DSL modemů vypadat jako anachronismus, ale ve skutečnosti jsou v mnoha domácnostech i firmách poměrně rozšířené. Přes senzační zprávy o nabouraných webových stránkách jen zřídka pronikne zmínka o útocích na vytáčené připojení, které jsou přitom většinou jednodušší a mívají horší následky [10].

Postup může vypadat třeba takto [10]:

- Přípravy: Pro začátek útočník potřebuje především seznam telefonních čísel, která chce otestovat pomocí skeneru.
- Skenování telefonních čísel: Na skenování telefonních čísel je nejdůležitější vybrat si ten správný nástroj. Zde je výčet několika programů, které se používají:
    - ToneLoc
    - THC-Scan
    - PhoneSweep

- Skriptované útoky hrubou silou: Výsledky skenu telefonních čísel se rozdělí do tzv. domén. Výběr systémů, které se útočník rozhodne napadnout, záleží na velkém počtu proměnných – například kolik je ochoten utratit, jak velkou výpočetní kapacitu má k dispozici, jaké má připojení, jak moc dokáže odhadnout vzdálený systém a jak dobře umí skriptovat.
- Telefonní ústředny: Slabým místem některých sítí jsou telefonní ústředny, které lze spravovat na dálku přes telefonní linku. Dříve se pro správu používala konzole připojená přímo k telefonní ústředně, dnešní telefonní ústředny už je možno ovládat přes IP sítě. Díky tomuto vývoji se na možnost obyčejného vytáčeného připojení k ústředně zapomíná, a to je z bezpečnostního hlediska velká chyba. Dodavatel obvykle řekne, že vytáčené připojení je na ústředně potřeba kvůli vzdálené správě, firma modem připojí a pustí z hlavy. Mnohem bezpečnější by bylo, kdyby firma při poruše ústředny zavolala dodavateli, podle potřeby připojila modem a po skončení údržby jej zase odpojila.

2.10.1. Obrana telefonních linek

K ochraně telefonních linek poslouží seznam, podle kterého se může při zabezpečování telefonních linek postupovat [10]:

- Je vhodné udělat seznam všech telefonních linek.
- Veškerý vzdálený přístup vytáčenými linkami by se měl soustředit do jednoho bodu a vnitřní síť od tohoto bodu oddělit firewallem.
- Snažit se, aby důležité linky nebyly na očích – je vhodné je přečíslovat mimo firemní rozsah telefonních čísel a nezveřejňovat je. Všechny relevantní údaje je nutné chránit heslem.
- Je dobré, zajistit fyzickou bezpečnost svého telekomunikačního vybavení.
- Dobré je i pravidelně kontrolovat protokoly softwaru pro vytáčené připojení.
- U obchodních linek je vhodné cenzurovat veškeré síťové bannery, aby poskytovaly co nejméně konkrétních informací.
- U všech systémů dostupných na dálku by se měla vyžadovat dvousložková autentizace, při které se uživatel musí prokázat dvěma nezávislými důkazy identity.

- Je dobré používat autentizaci zpětným voláním. Při tomto způsobu autentizace server ihned po navázání spojení zavěsí a připojí se na předem dané číslo, na kterém se má nacházet klient.

2.10.2. Obrana proti útokům na telefonní ústřednu

Stejně jako u obyčejných vytáčených linek platí, že modem by měl být zapnutý jen v nutných případech. Dále by se měla využívat vhodná autentizace (přinejmenším autentizace s uživatelským jménem a heslem) a po určitém počtu neúspěšných pokusů by se měl systém odpojit nebo zablokovat účet [10].

2.11. Útoky na uživatele Internetu

Lidský faktor je ve světě Internetu nejcitlivější a nejzranitelnější místo v bezpečnostním řetězci. Je to proto, že, jak se říká, nikdo není neomylný.

Útoky na uživatele Internetu jsou dnes plnohodnotným odvětvím počítačového zločinu. Na nové a nic netušící uživatele Internetu dnes čeká celá řada pohrom, od malwaru neboli škodlivého softwaru (jehož autoři jsou často ve spojení se „skutečným“ podsvětím) přes nevyžádanou poštu až po tisíce reklamních systémů různého stupně legitimity [10].

2.11.1. Sociální inženýrství

Škodliví jednotlivci mohou využívat hlasové komunikátory přes techniku známou jako sociální inženýrství. Sociální inženýrství je prostředek, kterým neznámý člověk získá důvěru někoho uvnitř organizace. Tento člověk může přesvědčit zaměstnance, že je spojen s vyšším managamentem, technickou podporou, help deskem, atd. Jakmile je oběť přesvědčena, často se jí doporučuje změna uživatelského hesla účtu ve vnitřním systému jako obnova jejího starého hesla. Jiné útoky nabádají oběť, aby otevřela konkrétní e-mailové přílohy, spustila aplikaci nebo se připojila na určitou adresu URL. Bez ohledu na to, jaká to je aktivita, směřuje k otevření zadních dveří, které útočník může použít k získání přístupu k síti [11].

Největšími lidskými vlastnostmi, které bývají zneužity, jsou autorita, sympatie, vzájemnost, důslednost, společenský souhlas a vzácná příležitost.

2.11.2. Obrana proti sociálnímu inženýrství

Jediný způsob, jak se ochránit proti útokům sociálního inženýrství je naučit uživatele, jak reagovat a pracovat pouze hlasovou komunikací. Zde jsou některé pokyny [11]:

- Pokaždé zpochybnit ze strany opatrnosti, když se hlasová komunikace zdá zvláštní, není na místě, nebo je neočekávaná.
- Vždy požadovat prokázání totožnosti. To může být řidičský průkaz, nebo cokoliv, co se dá snadno ověřit.
- Požadovat autorizaci zpětného volání na všechny hlasové žádosti síťových oprav nebo aktivit.
- Třídit informace (uživatelská jména, hesla, IP adresy, manažerská jména, atd.) a jasně stanovit, které informace mohou být projednány nebo dokonce potvrzeny pomocí hlasové komunikace.
- Jestliže jsou požadovány privilegované informace po telefonu od člověka, který by měl vědět, že podávat konkrétní informace po telefonu je proti bezpečnostní politice společnosti, je potřeba se zeptat, proč je vyžadována tato informace a znova si ověřit identitu volajícího. Tento incident by měl být i ohlášen správci bezpečnosti sítě.
- Nikdy by se nemělo dávat nebo měnit heslo pouze na základě telefonního rozhovoru.
- Vždy je nutné bezpečně odstranit nebo zničit všechny kancelářské dokumentace, hlavně v papírové podobě nebo médium, které obsahuje informace o IT infrastruktuře nebo jeho bezpečnostního mechanismu.

2.12. Útoky v České republice

Pořádek v České republice zaopatřuje Policie ČR. Policie přijala různá opatření s účelem snížit bezpečnostní rizika a dosáhnout svého poslání.

Jedním z takovýchto opatření, bylo vytvoření Národního kontaktního bodu pro terorismus Útvaru pro odhalování organizovaného zločinu (dále jen NKBT), jako specializovaného centrálního komunikačního, informačního a analytického pracoviště Policie České republiky. Toto pracoviště se zabývá sběrem, vyhodnocováním, analýzou a zpracováním informací, zjištěných Policií České republiky, o teroristech a osobách důvodně podezřelých z napojení na

teroristické organizace. NKBT je propojeno se všemi útvary Policie České republiky a spolupracuje s ostatními bezpečnostními orgány u nás i v zahraničí. Pro potřeby nejširší policejní veřejnosti vytváří NKBT metodiky předcházení, odhalování a vyšetřování teroristické trestné činnosti a zpracovává situační a poziční dokumenty za svěřenou problematiku [20].

Hlavními cíly NKTB jsou [20]:

- Shromažďovat a vyhodnocovat informace se vztahem k terorismu;
- Předcházet a případně odstraňovat škodlivé následky teroristické trestné činnosti;
- Působit pro naše domácí i zahraniční partnery jako centrální bod v otázkách vzájemné spolupráce;
- Být důvěryhodným a diskrétním kontaktním bodem pro občany České republiky a umožnit jim spolupodílet se na prosazování práva a bezpečnosti;
- Monitorovat a vyhodnocovat hrozby plynoucí z terorismu.

3. ANALÝZA RIZIK

V této kapitole se blíže seznámíme s metodami, které pomůžou analyzovat a blíže určit problémy, na které je třeba se zaměřit. Analýza rizik je prvním a zcela zásadním krokem v komplexním zabezpečení prevence pohrom a přípravy schopnosti dopady pohrom zvládnout, anebo alespoň zmírnit. Obě zmíněné a provázené etapy řízení jsou neopominutelnými součástmi řízení bezpečnosti, nouzového a krizového plánování [7].

3.1. Zásady analýzy rizik a řízení rizik

Zásady analýzy rizik a řízení rizik jsou důležitou součástí. Je nezbytné, aby sběr dat byl přesný a nebyl zkreslený.

Zásady analýzy rizik a řízení rizik jsou [7]:

- Zajistit monitoring jevu, jehož rizika chceme určit. Jeho cílem je získat objektivní a spolehlivá data;
- Provést interpretaci dat věrohodnými a spolehlivými metodami na základě spolehlivých a věrohodných modelů;
- Určit charakteristiky jevu, tj. věrohodnou velikost jevu, kterou lze na dané úrovni věrohodnosti očekávat za stanovený časový interval, četnost jevu, podstatu či příčinu vzniku jevu, dynamiku rozvoje jevu, velikost dopadů jevu (schopnost ničit);
- Určit dopady jevu v daném místě pro veličinu „ohrožení“ a dle místních zranitelností stanovit rizika a jejich velikosti;
- Určit nepřijatelná rizika a snížit zranitelnosti, která jsou jejich příčinou, jestliže to je možné anebo alespoň připravit technická a organizační opatření na zmírnění dopadů jevu v případě výskytu.

3.2. Metody analyzování rizik

Pro řízení bezpečnosti a rizikovou analýzu se používají různé pomocné pracovní technické nástroje. Jejich typologie je značně rozmanitá a jednotná klasifikace obtížná. Některé z nich jsou obecnější a jiné naopak výrazně specializované na určitý obor; jsou ovlivněny pojmy a postupy v daném oboru [7].

3.2.1. Kontrolní seznam (Check List)

Kontrolní seznam je postup založený na systematické kontrole plnění předem stanovených podmínek a opatření. Seznamy kontrolních otázek (checklists) jsou zpravidla generovány na základě seznamu charakteristik sledovaného systému nebo činností, které souvisejí se systémem a potenciálními dopady, selháním prvků systému a vznikem škod. Jejich struktura se může měnit od jednoduchého seznamu až po složitý formulář, který umožňuje zahrnout různou relativní důležitost parametru (váhu) v rámci daného souboru [7].

3.2.2. Analýza ohrožení a provozuschopnosti – HAZOP (Hazard Operation Process)

HAZOP je postup založený na pravděpodobnostním hodnocení ohrožení a z nich plynoucích rizik. Jde o týmovou expertní multioborovou metodu. Hlavním cílem analýzy je identifikace scénářů potenciálního rizika. Experti pracují na společném zasedání formou brainstormingu. Soustřeďují se na posouzení rizika a provozní schopnosti systému (operability problems). Pracovním nástrojem jsou tabulkové pracovní výkazy a dohodnuté vodicí výrazy (guidewords). Identifikované neplánované nebo nepřijatelné dopady jsou formulovány v závěrečném doporučení, které směřuje ke zlepšení procesu [7].

3.2.3. Analýza stromu událostí – ETA (Event Tree Analysis)

Analýza stromu událostí je postup, který sleduje průběh procesu od iniciační události přes konstruování událostí vždy na základě dvou možností – příznivé a nepříznivé. Metoda ETA je graficko statistická metoda. Názorné zobrazení systémového stromu událostí představuje rozvětvený graf s dohodnutou symbolikou a popisem. Znázorňuje všechny události, které se v posuzovaném systému mohou vyskytnout. Podle toho jak počet událostí narůstá, výsledný graf se postupně rozvětvuje jako větve stromu. Metoda ETA je s úspěchem používána v různých průmyslových odvětvích pro posuzování spolehlivosti provozu výrobní technologie [12].

3.2.4. Analýza stromu poruch – FTA (Fault Tree Analysis)

Analýza stromu poruch je postup založený na systematickém zpětném rozboru událostí za využití řetězce příčin, které mohou vést k vybrané vrcholové události. Metoda FTA je graficko-analytická popř. graficko-statistická metoda. Názorné zobrazení stromu poruch představuje rozvětvený graf s dohodnutou symbolikou a popisem. Hlavním cílem analýzy metodou stromu poruch je posoudit pravděpodobnost vrcholové události s využitím analytických nebo statistických metod. Proces dedukce určuje různé kombinace

hardwarových a softwarových poruch a lidských chyb, které mohou způsobit výskyt specifikované nežádoucí události na vrcholu. Metoda používá logická hradla stromu poruch, které popisují vzájemné vztahy mezi vstupy a výstupy popsaných událostí. Metoda FTA je s úspěchem používána v různých průmyslových odvětvích pro posuzování spolehlivosti provozu výrobní technologie [12].

3.2.5. Analýza lidské spolehlivosti – HRA (Human Reliability Analysis)

Analýza lidské spolehlivosti pravděpodobnostního hodnocení bezpečnosti (probabilistic safety assessment – PSA) zahrnuje identifikování lidských akcí z pohledu bezpečnosti, modeluje nejdůležitější akce v PSA modelu a hodnotí jejich pravděpodobnost. Jak už bylo projeveno mnoha incidenty a studiemi, lidské akce mohou mít jak pozitivní, tak negativní efekt na bezpečnosti a ekonomice [8].

Analýza lidské spolehlivosti je postup na posouzení vlivu lidského činitele na výskyt pohrom, nehod, havárií, útoků apod. či některých jejich dopadů. Koncept analýzy lidské spolehlivosti HRA směřuje k systematickému posouzení lidského faktoru (Human Factors) a lidské chyby (Human Error). Ve své podstatě přísluší do zastřešující kategorie konceptu předběžného posuzování PHA. Zahrnuje přístupy mikroergonomické (vztah „člověk-stroj“) a makroergonomické (vztah systému „člověk-technologie“). Analýza HRA má těsnou vazbu na aktuálně platné pracovní předpisy především z hlediska bezpečnosti práce. Uplatnění metody HRA musí vždy tvořit integrovaný problém bezpečnosti provozu a lidského faktoru v mezních situacích různých havarijních scénářů, tzn. paralelně a nezávisle s další metodou rizikové analýzy [12].

3.2.6. Metoda PSA (Probabilistic Safety Assessment)

Metoda stanovuje příspěvky jednotlivých zranitelných částí k celkové zranitelnosti celého systému. Tato technologie se používá např. k modelování scénářů hypotetických jaderných havárií, které vedou k tavení aktivní zóny a k odhadnutí četnosti takových havárií. V zemích OECD byly doposud zpracovány stovky studií PSA. Metodika PSA se skládá z: pochopení systému jaderného zařízení a ze shromáždění relevantních dat o jeho chování při provozu; identifikace iniciačních událostí a stavu poškození jaderného zařízení; modelování systému a řetězců událostí pomocí metodiky založené na logickém stromu; hodnocení vztahů mezi událostmi a lidskými činnostmi; vytvoření databáze dokumentující spolehlivost systému a komponent. PSA je významným nástrojem pro řízení bezpečnosti. Omezení metodiky PSA vyplývají z neurčitosti v datech. Nástroj se však neustále zdokonaluje a neurčitosti v datech se krok za krokem snižují v důsledku výsledků ze systematicky prováděných výzkumů [7].

3.2.7. Analýza příčin a dopadů – CCA (Causes and Consequences Analysis)

Analýza příčin a dopadů je směs analýzy stromu poruch a analýzy stromu událostí. Největší předností CCA je její použití jako komunikačního prostředku: diagram příčin a dopadů zobrazuje vztahy mezi koncovými stavy nehody (nepřijatelnými dopady) a jejich základními příčinami. Protože grafická forma, jež kombinuje jak strom poruch, tak strom událostí do stejného diagramu, může být hodně detailní, užívá se tato technika obvykle nejvíce v případech, kdy logika poruch analyzovaných nehod je poměrně jednoduchá. Jak už napovídá název, účelem analýzy příčin a dopadů je odhalit základní příčiny a dopady možných nehod. Analýza příčin a dopadů vytváří diagramy s nehodovými sekvencemi a kvalitativními popisy možných koncových stavů nehod [7].

Použití CCA vyžaduje znalosti následujících dat a informačních zdrojů, tj. znalosti [12]:

- Poruch komponent nebo nerovnováh procesu, které by mohly způsobit nehody;
- Bezpečnostních systémů nebo nouzových procedur, které mohou ovlivnit koncový stav nějaké nehody;
- Potenciálních dopadů všech těchto selhání.

3.3. Přijatelné a nepřijatelné riziko

Většina studií končí určením rizika. Pro rozhodovací proces je však nejvýznamnější porovnání vypočteného nebo odhadnutého rizika s úrovní přijatelného rizika. Jinými slovy jde o úlohu určování přijatelného rizika. Varianty, které mají riziko nižší než přijatelné riziko, mohou být akceptovány. Ostatní jsou z dalšího rozhodovacího procesu vyloučeny, nebo je třeba upravit parametry tak, aby byly přijatelné. Riziko je přijatelné, když ti, kteří jsou jím ovlivněni, si ho neuvědomují nebo jej vědomě podstupují. Při jeho určování vstupují do procesu následující podmínky [7]:

- Prahová podmínka – malé riziko se ignoruje;
- Podmínka status quo – nevyhnutelné riziko, které nelze změnit;
- Podmínka regulační – je určena důvěryhodnými institucemi;
- Podmínka de facto – je určena historickým vývojem;
- Podmínka dobrovolného zisku - vyplývá z ochoty tolerovat určité riziko, spojené s dosaženým ziskem.

4. ANALÝZA ZRANITELNOSTI INFORMAČNÍCH A KOMUNIKAČNÍCH TECHNOLOGIÍ

V následujících kapitolách bude analyzována kritická infrastruktura v oblastech komunikačních a informačních systémů vybrané společnosti. Analýza by měla ukázat a zhodnotit rizika, která mohou hrozit v podniku eBrána, s. r. o. Hlavní důraz je kladen na hodnocení zranitelnosti informačních a komunikačních technologií. První část analýzy je zaměřena na bezpečnostní opatření uvedené společnosti vzhledem k ochraně spravovaných dat, možným únikům citlivých informací a zajištění kontinuity pracovního procesu.

4.1. Řízený rozhovor

Pro provedení analýzy zranitelnosti informačních a komunikačních technologií bylo nutné zajistit sběr dat. K tomuto účelu posloužil řízený rozhovor s vedoucím pracovníkem podniku eBrána, s.r.o. a s vybraným zákazníkem této společnosti.

Cílem řízeného rozhovoru bylo získání informací o společnosti z hlediska zajištění bezpečnosti. Hlavní důraz byl kladen na zabezpečení ochrany citlivých informací a zajištění chodu pracovního procesu. Druhý řízený rozhovor vedený se zákazníkem společnosti byl zaměřen na konfrontaci výpovědí.

První řízený rozhovor s vedoucím zaměstnancem společnosti eBRÁNA, s. r. o. obsahoval 35 otázek, které byly rozděleny do několika skupin. Druhý řízený rozhovor s vybraným zákazníkem společnosti sloužil ke konfrontaci uvedených výpovědí. Úplné znění otázek obou řízených rozhovorů je uvedeno v příloze A.

4.2. eBrána, s. r. o.

Společnost eBrána, s. r. o. byla vybrána proto, že se již dlouhou dobu (9 let) pohybuje v oblasti informačních a komunikačních technologií. Její zkušenosti tak poslouží ke zhodnocení zranitelnosti zkoumaného prvku kritické infrastruktury

4.2.1. O společnosti eBrána, s. r. o.

Společnost eBrána, s. r. o. byla založena v roce 2003 Ing. Jiřím Janků ještě v době, kdy studoval na Univerzitě Pardubice. Se spolužákem Martinem Semerádem vytvořili portál www.sroty.cz a v zápětí přicházeli první nabídky na webová řešení a vznikla společnost eBrána, s. r. o.

V současnosti je tato společnost jednou z největších společností nabízejících webová řešení v ČR a zaměstnává okolo 50 pracovníků v pardubické centrále. Za dobu své existence spustila více než 2 500 webových projektů. Firma je držitelem mnoha ocenění jako jsou WebTOP 100, Web roku 2010, Firma roku 2011, Odpovědná firma pardubického kraje a Odpovědná firma ČR.

V eBráně, s. r. o. pracuje více jak 75 webových expertů, má pobočky po celé ČR (Praha, Liberec, Hradec Králové, Brno a Olomouc) a jednu pobočku v Indii. Dále je členem několika organizací jako jsou Asociace pro elektronickou komerci, Czech ICT Alliance a nebo Hospodářské komory ČR.

4.2.2. Produkty a výroba

Jak už bylo zmíněno společnost eBrána, s .r. o. se zabývá výrobou webových aplikací. Firma vyrábí webová řešení na míru, podle přání zákazníka. Kromě webových aplikací nabízí i internetový marketing, tvorbu e-shopu, software pro realitní kanceláře a jiná řešení B2B a B2C.

Proces výroby webových stránek má vždy na svých bedrech celý tým odborníků. Vše začíná u obchodního manažera, který domlouvá kontrakt se zákazníkem a je hlavním (a většinou jediným) prostředníkem pro komunikaci mezi výrobcem a klientem. Obchodní manažeři jsou pravidelně proškolováni, aby měli dostatečné znalosti o produktech, které prodávají a mohli zákazníkům zodpovídat jejich dotazy. Po té, co OM dohodne se zákazníkem podmínky a podpis smlouvy, vyžádá si od něho základní podklady pro tvorbu webových stránek a kompletně to předává spolu s takzvanou "průvodkou" do výrobního oddělení. Vedoucí výroby zkontroluje, zda dostal všechny potřebné informace a buď průvodku vrací obchodnímu manažerovi s připomínkami, nebo naplánuje výrobní proces. Zaúkoluje grafiky, kteří připraví grafické návrhy stránek a prostřednictvím obchodního manažera se předávají zákazníkovi ke schválení. Pokud klient schválil grafický návrh, přichází na řadu implementátoři aplikační logiky, kteří vytvoří funkční prototyp stránek. Poté se pustí do práce kodéři, kteří grafický návrh nasadí na funkční prototyp aplikace. Před samotným spuštěním stránek, ještě přichází na řadu plniči obsahu a testeři, kteří celou aplikaci otestují ještě před předáním výsledku zákazníkovi. Celé stránky "předává" (ne fyzicky, ale předává přístupová hesla k administraci stránek) zákazníkovi opět obchodní manažer.

4.2.3. Řízený rozhovor s vedoucím vývoje SW produktů

Řízený rozhovor byl veden s Ing. Davidem Hübnerem, který souhlasil odpovědět na pár otázek týkající se zabezpečení spolčnosti eBRÁNA, s. r. o.

Otázky a odpovědi:

Skupina otázek: Vnější hrozby

- *Kladete důraz na zabezpečení přístupu do budovy?*

  Ano, snažíme se dbát na zabezpečení přístupu do budovy. Budova je přístupná pouze zaměstnancům a přes hlavní vchod a recepci se do budovy mohou dostat také další osoby z řad klientů a školených osob.

- *Jakým způsobem zabezpečujete přístup do budovy?*

  Přístup do budovy je chráněn standardním bezpečnostním systémem napojeným přímo na bezpečností agenturu. Systém je aktivován vždy posledně odcházejícím zaměstnancem z budovy. Deaktivaci naopak provádí zaměstnanec, jenž první přijde do práce.

- *Monitorujete nějakým elektronickým zařízením vstup zaměstnanců/návštěv do budovy?*

  Ano zaměstnanci mají přístup do budovy pouze pomocí elektronického čipu, který je napojen na elektronické zámky řízené speciálním software.

- *Jaké druhy autentizace ve firmě používáte? (heslo, grafické heslo, biometrické údaje, pin, ...).*

  K přístupu k informačnímu systému, do interní a na pracovní stanice jsou využívány autentifikační hesla spravovaná pomocí adresářového systému LDAP. Vstupní dveře jsou pak přístupné pomocí bezpečnostních chipů.

- *Setkali jste se s nějakými útoky na vnitřní informační systém?*

  Informační systém nebyl napaden.

- *Máte připravené nějaké krizové plány, např. v případě živelných pohrom?*

  Jelikož naše klíčové servery jsou umístěny v renomovaných datových centrech v ČR, jenž mají vlastní krizové plány, společnost eBRÁNA nemá zpracovány speciální krizové plány ohledně živelných ani jiných pohrom.

Skupina otázek: Ochrana citlivých dat a prevence

- *Uchováváte citlivá data o svých klientech v rámci budovy?*

  Citlivé informace o klientech, jejich kontaktních a dalších údajích jsou uchovávána v rámci interního informačního systému, do nějž mají přístup pouze oprávněné osoby, jenž vlastní přístupový účet.

- *Máte citlivá data uložená v elektronické i papírové podobě?*

  Jelikož jsme společnost působící zejména v oblasti Internetu, máme většinu citlivých informací uloženu v elektronické podobě.

- *Jsou-li data v elektronické podobě, využíváte šifrování?*

  Využíváme standardních prvků zabezpečující přístup k datům, kdy jsou veškerá přístupová hesla k systémům uložena v kryptované podobě. Vlastní kryptování a šifrování dat není využíváno.

- *Jak často a jakým způsobem provádíte zálohování dat?*

  Zálohy dat webových prezentací jsou prováděny automaticky na denní bázi. Pro informační systém je použito inkrementální rozdílové zálohování.

- *Máte geograficky rozdělené zálohy dat?*

  V rámci České republiky ano, na mezinárodní úrovni ne. Záleží tedy na pohledu, jak velké geografické měřítko vezmeme.

- *Používáte nějaký systém pro detekci útoků?*

Ano naše datové servery jsou chráněny monitorovacím software či externími systémy, které neustále sledují stav serverů a varují při výpadcích služeb, přílišném zatížení či nestandardních požadavcích.

- *Spravujete citlivá data o zákaznících Vašich zákazníků?*

  Pouze v případě našeho software REAL Brána, který je informačním systémem pro realitní kanceláře. Zde si klienti evidují citlivé informace o zakázkách a klientech.

  Elektronické obchody by se svým způsobem také daly považovat za citlivá data, jelikož obsahují poptávky a objednávky od nových či stávajících klientů.

- *Poskytujete svým zákazníkům záruky zabezpečení a přístupnosti dat? Šifrujete citlivé informace?*

  Přístupové údaje k datům jsou šifrovány, vlastní data nikoliv. Přenos dat může být šifrován, pokud to klient požaduje a tuto službu si zaplatí.

- *Spolupracujete s nějakou třetí stranou v této souvislosti?*

  Dodávky hostingových služeb jsou outsourcovány třetí stranou, se kterou je podepsán dokument NDA.

Skupina otázek: Zaměstnanci

- *Rozlišujete úroveň autorizace v rámci pracovních pozic?(různá práva pro různé pozice vzhledem k přístupnosti citlivých dat)*

  Ano, interně společnost eBRÁNA pracuje s uživatelskými rolemi či pozicemi, kterým říkáme „klobouky“ a těchto rolí definujeme více než 50.

- *Jakou technikou? (technika ne/přenechání volnému uvážení)*

  Role jsou definovány na základě pracovní pozice a jsou popsány interními směrnicemi a pravidly.

- *Kdo ve firmě spravuje uživatelské účty?*

Oddělení administrativy dává požadavky na správu uživatelských účtu oddělení ICT. Uživatelské účty tedy spravuje oddělení ICT.

- *Jsou zaměstnanci proškolováni v oblasti práce a přístupu k citlivým datům?*

  V rámci jejich přijímacího řízení a zaškolení existují i některé směrnice týkající se citlivých dat a způsobům práce s těmito daty.

- *Byl někdy někdo ve firmě potrestán za porušení bezpečnostních pravidel?*

  Tuším, že zatím nikoliv.

Skupina otázek: Analýza rizik a kritičnosti chráněných aktiv

- *Máte vyčíslenou hodnotu všech citlivých dat?*

  Řádově se jedná o desítky milionů korun.

- *Máte klasifikovaná data? (např. důvěrné, soukromé, citlivé, veřejné)*

  Interně používáme dokumenty s označením „Tajný dokument“. Tajné dokumenty jsou určeny pouze pro zaměstnance společnosti eBRÁNA nebo vedení společnosti (zde je omezeno přístupem k různým typům dokumentů dle uživatelské role).

- *Kolika svým zákazníkům jste poskytli řešení B2C, B2B?*

  Řešení e-commerce společnost eBRÁNA poskytuje řádově stovkám klientů zejména z ČR, ale i jiných evropských zemí.

- *Jste schopni odhadnout kolik GiB dat spravujete?*

  Řádově se jedná o jednotky až desítky terabajtů dat.

- *Máte nějak omezen přístup k těmto datům? (Např. může každý programátor/grafik získat k těmto datům přístup?)*

  Aktuálně mají programátoři a grafici přístup k datům webových prezentací. Přistup je možný však pouze z interní počítačové sítě nebo po připojení se k této síti pomocí VPN. V žádném případě nemohou zaměstnanci odkudkoli přistupovat

k datům našich klientů. Přístup je vždy možný po autorizaci a ověření přístupových a uživatelských práv k požadovaným službám.

Skupina otázek: Úroveň risk managamentu

- *Co zahrnuje zaměstnání nových pracovníků z hlediska bezpečnosti citlivých dat?*

  Zaměstnanci podepisují konkurenční doložku pracovní smlouvy zakazující využití technologií, jiných citlivých informací či údajů z databáze klientů společnosti eBRÁNA. Za porušení hrozí smluvní pokuta.

- *Řídíte se nějakými bezpečnostními politikami, standardy, normami, postupy, procedurami? Jakými?*

  Zaměstnanci společnosti eBRÁNA se řídí interními pravidly společnosti, které obsahují veškeré potřebné údaje a jsou pravidelně rozšiřovány. Zaměstnanci jsou pravidelně podrobováni testům ze znalosti těchto pravidel.

- *Vytváříte nějaké analýzy rizik? Máte příklad?*

  Analýza rizik je prováděna u většiny pilotních projektů společnosti ať se již jedná o vývoj nového software či projekty dalšího rozvoje společnosti.

- *Investujete do licencí bezpečnostních programů (antivir, antispy, ...)?*

  Ano bezpečnostní software pro počítačové stanice je instalován.

- *Kolik licencí potřebujete na firmu?*

  Firma v současné době potřebuje řádově desítky licencí.

- *Máte připravené plány pro obnovu, kterými byste se řídili po pohromě?*

  Písemné dokumenty neexistují, v praxi se ovšem běžně setkáváme s požadavky na obnovu dat ze strany zaměstnanců i klientů. Tyto obnovy byly vždy provedeny k jejich plné spokojenosti.

- *Co je prioritou?*

  Prioritou je obnovení maximálního možného množství dat v jejich nejčerstvější možné podobě.

- *Jakým způsobem máte zajištěnou komunikaci v případě pohromy? (např.: vnitrofiremní komunikace, obeznámení zaměstnanců; s okolím [záchranné sbory])*

  Zaměstnanci jsou standardně proškoleni na BOZP a Požární směrnice. Vnitrofiremní komunikace by zřejmě proběhla elektronicky formou e-mailu či telefonicky. V rámci budovy kanceláří společnosti se v případě pohromy spustí poplach a zaměstnanci musí opustit budovu pomocí únikových východů.

- *Máte nějakou alternativní lokalitu v případě pohromy na primární lokalitě?*

  Konkrétní budova připravena není, asi jako u většiny firem podobného rozsahu. Naši výhodou však může být to, že provizorně by většina našich zaměstnanců mohla dočasně fungovat systémem tzv. „homeoffice“. Záleželo by samozřejmě ale na rozsahu způsobených škod. Při totálním zániku počítačové infrastruktury by situace byla složitější.

- *Provádíte cvičná testování plánů po pohromě?*

  Běžně se provádí požární cvičení.

Druhý řízený rozhovor s klientem firmy:

- *Uchovávali jste v aplikaci od firmy eBRÁNA citlivá data svých klientů?*

  Ano, ale jen nezbytně nutné kontaktní údaje na naše zákazníky.

- *Jste schopni vyčíslit hodnotu těchto dat?*

  Přesnou hodnotu dat vyčíslenou nemáme, nicméně data jsou to cenná v podstatě pouze pro naši firmu, popřípadě konkurenční firmu.

- *Jak byl zabezpečen přístup k těmto datům? Dalo se k nim získat přístup z jakéhokoliv počítače připojeného k Internetu?*

  Data byla chráněna uživatelským jménem a heslem, které jsme pravidelně měnili. Přístup byl možný z jakéhokoliv zařízení připojeného k Internetu.

- *Garantovala Vám společnost eBRÁNA obnovu dat v případě jejich ztráty?*

  Ano, společnost eBRÁNA provádí zálohování a případnou obnovu dat.

- *Zaznamenali jste pokus o neoprávněný přístup k Vašim stránkám nebo jiný útok na Vaše stránky?*

  Ne, žádné hackerské útoky jsme nezaznamenali.

- *Zaznamenali jste někdy dlouhodobější neplánovaný výpadek Vašich stránek?*

  Pravděpodobně ne.

4.3. Analýza rizik ve společnosti eBRÁNA

Pro následující analýzu byly získány informace o možných hrozbách a chráněných aktivech z rozhovoru s vedoucím pracovníkem společnosti.

V následující tabulce je zaznamenán vztah aktiva k hrozbě. Tento vztah lze vyjádřit jako zranitelnost aktiva ve vztahu k dané hrozbě. Škála hodnocení je 0 - 5, přičemž číslo 5 vyjadřuje největší hrozbu.

Tabulka 2: Vztah aktiva k hrozbě.

Aktivum/hrozba	krádež	Ztráta	poškození	napadení	požár	povodeň	vyzrazení	Celkem
Data	3	2	1	3	0	0	0	9
Servery	2	0	4	2	1	0	0	9
Počítače	3	1	4	0	1	0	0	9
Budova	0	0	3	0	4	1	0	8
Zaměstnanci	0	0	0	0	0	0	4	4

Zdroj: Vlastní zpracování

Z tabulky je patrné, že data jsou jedny z nejvíce ohrožených aktiv a to nejvíce krádeží nebo napadením. Nejméně jsou ohrožena požárem a povodní, a to proto, že data jsou nehmotná. Data je možné ztratit třeba nesprávným zálohováním, anebo poškodit například, nachází-li se na nefunkčním disku.

Na stejné pozici se nachází servery, na kterých nacházejí data klientů a které jsou nezbytné pro chod podniku. Největší hrozbou je poškození. Poškození může vzniknout například neprofesionální manipulací. Napadením serverů se v této tabulce myslí napadení zvenčí například hackerem, který by chtěl získat data nebo ochromit chod firmy. Krádež tohoto aktiva je skoro nemožná a to proto, že je budova chráněna kamerovým systémem a také číselným kódem u vstupu do budovy.

Počítače jsou nedílnou součástí každodenního chodu firmy. Zaměstnanci počítače používají hlavně k vytváření produktů. Z důvodu každodenního užívání počítačů je jejich poškození největší hrozbou. Poškodit se mohou nesprávným užíváním. Další velkou hrozbou je zde také krádež. Není pravda, že by se počítače kradly z budovy snadněji než servery, ale je to dané tím, že manažeři si na pracovní schůzky s sebou berou laptopy, na kterých mají potřebná data a informace. Laptop zapomenutý například v autě se snadnější kořist než počítač umístěný v budově, která, jak už bylo zmíněno, je chráněna proti případným zlodějům. U této skupiny aktiv je nepatrná šance, že by se vznítili.

Budova, jak už bylo zmíněno, je chráněna proti vniknutí a to zaměstnaneckými čipy, kamerovým systémem nebo bezpečnostním kódem. Do budovy se tak mohou dostat pouze pracovníci nebo návštěva procházející přes recepci. Je ohrožená vznikem požáru. V oblasti prevence požáru je zřízen zákon o požární ochraně. V tomto zákoně by se eBRÁNA kategorizovala do firmy bez zvýšeného požárního nebezpečí. Firma podle tohoto ustanovení musí například obstarávat a zabezpečovat v potřebném množství a druzích požární techniku, vytvářet podmínky pro hašení požárů a pro záchranné práce, označovat pracoviště a ostatní místa příslušnými bezpečnostními značkami, příkazy, zákazy a pokyny ve vztahu k požární ochraně, atd [13]. K této hrozbě má podnik vyhotovenou požární směrnici (viz příloha B). Budova může být také ohrožena nepřízní počasí, jako jsou například vichřice, které jsou častým jevem na území České republiky. Vzhledem k poloze podniku téměř nehrozí, aby byla zasažena záplavovou vlnou.

Obrázek 1: Nebezpečí povodně

Zdroj: [16]

Zaměstnanci jsou důležitou součástí dobrého chodu podniku. Pro dobrou kontinuity pracovního procesu je důležité, aby bylo utajeno know-how.

4.4. Shrnutí získaných poznatků

Z řízeného rozhovoru vyplývá, že podnik např. nemá připravené krizové plány. Výhodou této firmy je, že při menší hrozbě, například výpadku elektřiny, která je pro vytváření webových aplikací potřebná, mohou zaměstnanci pracovat z domova, ačkoli i tam hrozí výpadek proudu. Po zasažení podniku větší pohromou např. živelnou pohromou (povodeň, požár, zemětřesení, sesuvy, atmosférické poruchy, atd.) krizový plán připravený nemají.

V následující tabulce jsou shrnuté hrozby, které se mohou vyskytnout a hodnocení opatření. Opatření jsou hodnocena slovně, a to: výborné, velmi dobré, uspokojivé, neuspokojivé (řazeno od nejlepšího).

Tabulka 3: Hrozba a hodnota opatření proti potenciální hrozbě

Hrozba	Opatření
Krádež dat zvně společnosti	Výborné
Ztráta dat	Výborné
Krádež serverů	Výborné
Napadení serverů	Výborné
Povodeň	Výborné
Krádež dat zevnitř společnosti	Velmi dobré
Krádež počítače	Velmi dobré
Poškození serverů	Velmi dobré
Požár budovy	Velmi dobré
Poškození počítače	Uspokojivé
Zaměstnanci - vyzrazení know-how	Uspokojivé

Zdroj: Vlastní zpracování

Z tohoto vyhodnocení je zřejmé, na jaké hrozby by se podnik měl zaměřit. Vyzrazení know-how má společnost řešené pomocí konkurenční doložky a za vyzrazení se platí penále. Poškození počítačů je běžná záležitost. Krádeže fyzických aktiv, které mají své místo v budově, jsou chráněné přístupem do budovy. Servery obstarává vyškolený pracovník. Při vzniku požáru se pracovníci řídí požární směrnicí. Otázkou je, jestli se zaměstnanci touto směrnicí řídí.

V další tabulce je shrnuta úroveň zabezpečení. Dělí se do čtyř sloupců. První obsahuje název aktiva, druhý jeho množství, ve třetím sloupci je popsaná hodnota aktiva, která je uvedena v korunách nebo slovně pomocí kvalitativního vyjádření, a čtvrtý sloupec obsahuje hodnocení přijatého opatření na ochranu proti potencionální hrozbě. Hodnocení se pohybuje na škále 1 -5, přičemž číslo 1 je nejlepší a 5 nejhorší.

Tabulka 4: Úroveň zabezpečení

název chráněného aktiva	Množství	hodnota	přijatá opatření (hodnocení)
kontinuita podnikání	--	vysoká	1
Budova	--	několik milionů	2
Data	až desítky terabajtů	řádové desítky milionů	3
Zaměstnacni	okolo 50 zaměstnanců	nevyčíslitelná	3

Zdroj: Vlastní zpracování

Z výsledků je možné vyčíst, že nejlépe zaopatřeným aktivem je kontinuita podnikání. Je to proto, že v případě menší hrozby (jako je třeba výpadek proudu), je možné pracovat z domova. To ale neznamená, že je se jedná o nejúčinnější řešení, například pokud je

pracovník z Pardubic a dojde k výpadku proudu v celém městě sídle centrály. Společnost by tudíž nemohla dále pracovat na zakázkách a dodržet termín, který byl dohodnut s klientem.

Dalším dobře chráněným aktivem je budova, která má dobrou polohu v případě živelné pohromy, jakou může představovat třeba povodeň. Do budovy je také těžké se dostat, jak už bylo řečeno výše.

Data má podnik chráněn především proti útoku zvenčí. Ochrana dat je řešena pomocí monitorovacího software, externími systémy, které neustále sledují stav serverů a varují při výpadcích služeb, přílišném zatížení či nestandardních požadavcích, pravidelným zálohováním nebo kryptováním.

Hodnota zaměstnanců je nevyčíslitelná. Je to proto, že školení nového pracovníka je dražší než již zaškolený zaměstnanec, který má vyšší produktivitu. Zároveň je seznámen s podnikovým know-how, které má také nevyčíslitelnou cenu, protože obsahuje nové postupy, vylepšení a inovace. Ty jsou cenné například pro konkurenci.

Tabulka 5 obsahuje hodnocení kritičnosti aktiva, jeho zranitelnost, opatření proti zranitelnosti, pravděpodobnost ohrožení aktiva a opatření ke snížení výskytu hrozby. Hodnocení se pohybuje na škále 1 – 5. Číslo 1 zde představuje nejlepší možnost a číslo 5 nejhorší.

Tabulka 5: Kritické hodnoty

Hrozba	Aktivum	kritičnost aktiva	zranitelnost aktiva	opatření proti zranitelnosti	pravděpodob-nost ohrožení	opatření ke snížení výskytu hrozby
Krádež	Data	4	3	4	4	4
Krádež	Počítače	3	4	3	3	3
Krádež	Servery	5	1	4	2	4
Poškození	Počítače	3	4	2	5	2
Poškození	Servery	5	3	3	3	3
Poškození	Budova	2	3	3	3	3
Napadení	Servery	5	2	4	4	4
Požár	Budova	2	3	4	3	3
Povodeň	Budova	2	1	1	1	1
Vyzrazení know-how	Zaměstnanci	4	4	2	3	3
Ztráta	Data	4	2	4	2	4

Zdroj Vlastní zpracování

Pro výpočet celkového rizika byl použit následující vzorec:

$$celkové\ riziko = kritičnost \times (zranitelnost - opatření\ proti\ zranitelnosti) \times (pravděpodobnost - opatření\ proti\ výskytu\ pravděpodobnosti).$$

Pro lepší přehlednost je uvedena následující tabulka, která obsahuje aktiva a hrozby z výše uvedené tabulky a výpočet celkového rizika podle předchozího vzorce.

Tabulka 6: Celkové riziko

Hrozba	Aktivum	celkové riziko
Krádež	Data	0
Krádež	Počítače	0
Krádež	Servery	30
Poškození	Počítače	18
Poškození	Servery	0
Poškození	Budova	0
Napadení	Servery	0
Požár	Budova	0
Povodeň	Budova	0
Vyzrazení know-how	Zaměstnanci	0
Ztráta	Data	16

Zdroj: Vlastní zpracování

Tabulka ukazuje celkové riziko i se započítáním vlivu přijatých protiopatření. V případě hrozeb, jejichž celkové riziko vůči danému aktivu vychází vyšší než nula, je možné hovořit tak, že by bylo vhodné, aby společnost zvážila přijmout další opatření proti těmto hrozbám resp., aby se zvýšila odolnost resp. snížila zranitelnost chráněných aktiv. Rozhodnutí o přijetí opatření je však podmíněno ekonomickou rentabilitou takového opatření a proto by byla nutná další analýza ekonomických nákladů a míry snížení rizika dodatečných opatření.

4.5. Závěry a doporučení

Důležitou součástí ochrany společnosti jsou všechny prvky kritické infrastruktury. Z analýzy a prozkoumání společnosti eBRÁNA vyplynulo, že je nutné se blíže věnovat zranitelnosti některých prvků.

4.5.1. Doporučení pro společnost eBRÁNA, s. r. o.

Největší hrozbou pro společnost eBRÁNA je z uvedených analýz ztráta serverů, které pracovníci používají ke každodennímu pracovnímu procesu. Na serverech běží již dokončené práce, jako jsou webové stránky nebo webová řešení. Ztráta těchto serverů by znamenala nespokojené zákazníky. Případné reklamace a náklady na opětovné zhotovení jejich projektu by byly příliš vysoké. Servery v podniku kontrolují a spravují specialisté, ztráta nebo zničení serverů hrozí jen zastaráním nebo úmyslným poškozením některého z pracovníků a proti těmto hrozbám se dá zakročit například včasnou výměnou serverů a omezeným přístupem do

místnosti, kde se toto aktivum nachází, zabezpečit jej například čipem, který by vlastnil pouze specializovaný pracovník.

Počet zaměstnanců se neustále zvyšuje, je důležité věnovat pozornost hrozbě zneužití dat zevnitř společnosti. Data mají v podniku hodnotu několika milionů. V úvahu přicházejí například důkladná rozdělení přístupových práv, monitoring vnitřní sítě a politika tvorby přístupových hesel. Náklady na toto doporučení nejsou nijak vysoké, v podstatě jde pouze o nastolení lepších pravidel, kterým je potřeba věnovat několik hodin práce zaměstnanců IT oddělení a vedení firmy.

Dalším doporučením je například vytvoření krizových plánů po obnově pro případ živelné pohromy a jiné události mající vliv na chod firmy. Zde se jedná opět pouze o investici časovou a možná o investici na konzultaci odborníků. Tímto plánem by firma předešla nepříjemnému momentu překvapení, který byť s malou pravděpodobností, by mohl nastat. Například by se mohlo jednat o následující hrozby: povodeň, požár, atmosférické poruchy (poryvy větru, vichřice, ale i tornáda), sesuvy půdy, zemětřesení.

ZÁVĚR

Jedním ze záměrů práce bylo zdůraznit důležitost kritické infrastruktury a jejích prvků. Bez zabezpečení kritické infrastruktury by mohlo dojít k velmi chaotickému jednání při pokusu o nápravu škod vzniklých nečekanou událostí, což by mohlo vést v krajním případě ještě k větším škodám. Důležitou součástí kritické infrastruktury jsou také informační a komunikační systémy, které společnost používá téměř neustále a bez nichž by si život jen stěží mohla představit, protože ho výrazně ulehčují.

V první kapitole byly vymezeny základní pojmy týkající se kritické infrastruktury. Byly také definovány její elementární prvky a objekty a subjekty kritické infrastruktury. V další kapitola následovalo seznámení se s technologiemi informačních a komunikačních systémů, definování útočníků a způsobů jejich útoků a obrany proti nim. Třetí kapitola obsahovala analýzu rizik a její zásady a řízení rizik a také blíže seznámila s metodami analyzování rizik. V závěrečné kapitole byly prakticky použity analýzy na vybraném subjektu. Subjektem byla společnost eBRÁNA, s. r. o., která byla ochotna zodpovědět otázky v dotazníkovém šetření. Tato kapitola také blíže seznamuje s historií podniku a jeho současným stavem. Je zde uvedeno také jaké produkty společnost nabízí a výrobní postup webového řešení. Produkty se vyrábí na přání klienta a výrobní proces se neustále zdokonaluje s vývojem nových technologií.

Z výsledků analýz bylo patrné, že nejdůležitějšími aktivy pro kontinuitu pracovního procesu subjektu, který byl vybrán, jsou servery, data a počítače. Protože podnik je částečně součástí jednoho z prvků kritické infrastruktury, jsou tato aktiva důležitá i pro jeho klienty. Na serverech se nachází data zákazníků a při narušení správnosti jejich chodu by měla hrozba ztráty dat nevyčíslitelné následky. Bez řešení B2B nebo B2C, které podnik poskytuje řádově stovkám klientů, by tito zákazníci nemohli pokračovat v podnikání. Citlivá data má eBRÁNA, s. r. o. vyčíslena do několika desítek milionů.

Největší hrozbou je poškození serverů, a to z jedné strany opotřebením a zastaráním, nebo úmyslným poškozením z vnitřního kolektivu pracovníků. Z vnitřního okolí proto, že vstup do budovy je chráněn bezpečnostními opatřeními, jako jsou zaměstnanecké čipy, kódový zámek, kamerovým systémem. Také návštěva nebo jiná osoba do budovy prochází po ohlášení přes recepci. Byla doporučena pravidelná kontrola stavu serverů a případná včasná výměna za nové a vstup do místnosti, kde se toto aktivum nachází, zabezpečit čipem. Tento čip by sloužil pouze obsluze těchto serverů.

Dalším doporučením bylo vytvoření plánů po pohromě, které by, v případě například živelné pohromy, pomohly vrátit podnik v co nejkratším čase do původního chodu a nepřerušila by se tím kontinuita pracovního procesu.

Domnívám se, že cíl této práce, analyzovat zranitelnosti informačních a komunikačních systémů a návrh vhodných opatření, byl splněn.

POUŽITÁ LITERATURA

[1] BAUER, Michael D. *Building Secure Servers with Linux*. Sebastopol: O'Reilly Media, 2003. ISBN 978-0-596-00217-6.

[2] BITTO, Ondřej. *Microsoft Windows 7: Podrobná uživatelská příručka*. Brno: Computer press, a. s., 2009. ISBN 987-80-251-2647-9.

[3] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Brno: Computer press, 2004. ISBN 80-251-0106-1.

[4] LINHART, Petr a Radim ROUDNÝ. *Ochrana obyvatelstva a terorismus*. Vyd. 1. Pardubice: Univerzita Pardubice, 2009, 238 s. Distanční opora. ISBN 978-80-7395-165-8.

[5] KYSELA, Martin. *Linux*: *Kapesní průvodce administrátora*. Praha: Grada Publishing a. s., 2004. ISBN 80-247-0733-0.

[6] MOZGA, Jaroslav, Miloš VÍTEK a František KOVÁŘÍK. *Kritická infrastruktura společnosti*. 1. vyd. Hradec Králové: Gaudeamus, 2008. ISBN 978-80-7041-299-2.

[7] PROCHÁZKOVÁ, Dana a Josef ŘÍHA. *Krizové řízení*. 1. vyd. Praha: Ministerstvo vnitra, Hasičský záchranný sbor ČR, 2004. ISBN 80-86640-30-2.

[8] PYY, Pekka. Human reilability analysis methods for probabilistic safety assessment. Lappeenranta: VTT, 2000. ISBN 952-30-5585-6.

[9] ŘÍHA, Josef. Typologické znaky kritické infrastruktury. In: *The science for population protection*. 1/2009. Pardubice: QUADRO.CZ, spol s r.o., 2009, s. 19. ISSN 1803-568X.

[10] SCAMBRAY, Joel, George KURTZ a Stuart MCCLURE. Hacking bez záhad. 5. vyd. Praha: Grada Publishing, a. s., 2007. ISBN 978-80-247-1502-5.

[11] STEWART, Ed TITTEL a Mike CHAPPLE. *CISSP*: *Certified Information Systems Security Professional - study guide*. Indiana: Wiley Publishing, Inc., 2008. ISBN 978-0-470-27688-4.

[12] ŠENOVSKÝ, Michail, Vilém ADAMEC a Pavel ŠENOVSKÝ. *Ochrana kritické infrastruktury*. Ostrava: Knižnice SPBI, 2006. ISBN 978-80-7385-025-8.

Legislativa

[13] Zákon č. 133/1985 Sb., o požární ochraně

[14] Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu (stavební zákon)¨

Internetové stránky

[15] Česká národní banka [online]. [cit. 2012-04-15]. Dostupné z: www.cnb.cz

[16] Building intelligent solutions with geospatial data [online]. [cit. 2012-04-15]. Dostupné z: www.intermaps.cz

[17] eBrána, s. r. o. [online]. [cit. 2012-04-15]. Dostupné z: www.ebrana.cz

[18] Ministerstvo průmyslu a obchodu [online]. [cit. 2012-04-16]. Dostupné z: www.mpo.cz

[19] Ministerstvo zdravotnictví České republiky [online]. [cit. 2012-04-15]. Dostupné z: www.mzcr.cz

[20] Policie České republiky. [online]. [cit. 2012-04-15]. Dostupné z: www.policie.cz

[21] Portál veřejné správy České republiky. [online]. [cit. 2012-04-15]. Dostupné z: http://www.portal-verejne-spravy.cz/

SEZNAM PŘÍLOH

Příloha A

- Uchováváte citlivá data o svých klientech v rámci budovy?
- Kladete důraz na zabezpečení přístupu do budovy?
- Jakým způsobem zabezpečujete přístup do budovy?
- Monitorujete nějakým elektronickým zařízením vstup zaměstnanců/návštěv do budovy?
- Máte citlivá data uložená v elektronické i papírové podobě?
- Jsou-li data v elektronické podobě, využíváte šifrování?
- Jak často a jakým způsobem provádíte zálohování dat?
- Máte geograficky rozdělené zálohy dat?
- Rozlišujete úroveň autorizace v rámci pracovních pozic? (různá práva pro různé pozice vzhledem k přístupnosti citlivých dat)
- Jakou technikou? (technika ne/přenechání volnému uvážení)
- Kdo ve firmě spravuje uživatelské účty?
- Jsou zaměstnanci proškolováni v oblasti práce a přístupu k citlivým datům?
- Jaké druhy autentizace ve firmě používáte? (heslo, grafické heslo, biometrické údaje, pin, …)
- Setkali jste se s nějakými útoky na vnitřní informační systém?
- Byl někdy někdo ve firmě potrestán za porušení bezpečnostních pravidel?
- Máte přiravené nějaké krizové plány, např. v případě živelných pohrom?
- Pokud ano, proti jakým hrozbám?
- Používáte nějaký systém pro detekci útoků?
- Pokud ano, jedná se o systém aktivní, pasivní či hybridní?
- Máte vyčíslenou hodnotu všech citlivých dat?
- Máte klasifikovaná data? (např. důvěrné, soukromé, citlivé, veřejné)
- Co zahrnuje zaměstnání nových pracovníků z hlediska bezpečnosti citlivých dat?
- Řídíte se nějakými bezpečnostními politikami, standardy, normami, postupy, procedurami? Jakými?
- Vytváříte nějaké analýzy rizik? Máte příklad?
- Investujete do licencí bezpečnostních programů (antivir, antispy, …)?
- Kolik licencí potřebujete na firmu?
- Máte připravené plány pro obnovu, kterými byste se řídili po pohromě?
- Co je prioritou?
- Jakým způsobem máte zajištěnou komunikaci v případě pohromy? (např.: vnitrofiremní komunikace, obeznámení zaměstnanců; s okolím [záchranné sbory])

- Máte nějakou alternativní lokalitu v případě pohromy na primární lokalitě?
- Provádíte cvičná testování plánů po pohromě?
- Spravujete citlivá data o zákaznících Vašich zákazníků?
- Kolika svým zákazníkům jste poskytli řešení B2C, B2B?
- Poskytujete svým zákazníkům záruky zabezpečení a přístupnosti dat?
- Šifrujete citlivé informace?
- Spolupracujete s nějakou třetí stranou v této souvislosti?
- Jste schopni odhadnout kolik GiB dat spravujete?
- Máte nějak omezen přístup k těmto datům? (Např. může každý programátor/grafik získat k těmto datům přístup?)

Příloha B

Zpráva o nebezpečí povodně

Adresa		
	Kraj: Pardubický	**Ulice, č.p./č.o.:** Na Třísle 145
	Okres: Pardubice	**PSČ:** 53002
	Obec - část obce: Pardubice - Bílé Předměstí	

Riziková zóna pro vybranou adresu

Zóna 2 zóna s nízkým nebezpečím výskytu povodně.

Doplňující informace

Souřadnice S-JTSK: X: -646987 **Y:** -1060636
Souřadnice GPS: N: 50°2'24,05" **E:** 15°46'48,39"
Kód adresy: 7778449 (dle číselníku poskytovaného MPSV)
Přesnost: adresa byla zaměřena s přesností na stavební objekt

Copyright Central European Data Agency, a. s.

Vysvětlivky pojmů

Na základě vyhodnocení všech aspektů jsou definovány 4 povodňové zóny podle nebezpečí výskytu povodní:

- **Zóna 1 – zóna se zanedbatelným nebezpečím** výskytu povodně.
- **Zóna 2 – zóna s nízkým nebezpečím** výskytu povodně.
- **Zóna 3 – zóna se středním nebezpečím** výskytu povodně.
- **Zóna 4 – zóna s vysokým nebezpečím** výskytu povodně.

Souřadnice S-JTSK (Systém jednotné trigonometrické sítě katastrální) - geodetický souřadnicový systém používaný v ČR
Kód adresy - předávací kód adresního místa dle standardu (AA0109) poskytovaného MPSV

Poskytovatel služby: Intermap Technologies, s.r.o. Více informací na www.intermap.cz.

Příloha C

Za účelem rychlého přivolání pomoci v případě vzniku požáru a rychlého a organizovaného vyhlášení požárního poplachu vydávám pro:

eBRÁNA

eBRÁNA s.r.o., Milheimova 1010, 530 02 Pardubice, IČ: 25984764

POŽÁRNÍ POPLACHOVÉ SMĚRNICE

Tato požární poplachová směrnice je interním právním předpisem a je zpracována na základě ustanovení §32 vyhl. č. 246/2001 Sb.

I. POVINNOSTI OSOBY, KTERÁ ZPOZORUJE POŽÁR

Každý je povinen v souvislosti se zdoláváním požáru:

a) provést nutné opatření pro záchranu ohrožených osob,
b) uhasit požár, jestliže je to možné, použitím všech dostupných hasebních prostředků (hasicí přístroje, požární vodovody), nebo provést nutná opatření k zamezení jeho šíření,
c) ohlásit neodkladně zjištěný požár nebo zabezpečit jeho ohlášení,
d) poskytnout osobní pomoc jednotce požární ochrany na výzvu velitele zásahu, velitele jednotky požární ochrany nebo obce.

II. ZPŮSOB A MÍSTO OHLÁŠENÍ POŽÁRU, ZPŮSOB VYHLÁŠENÍ POŽÁRNÍHO POPLACHU

Každý, kdo zpozoruje požár, je povinen:

a) ohlásit vznik požáru telefonicky přímo na ohlašovnu požáru Hasičského záchranného sboru kraje.

Telefonní číslo tísňového volání na veřejnou ohlašovnu požáru HZS je 150

b) Požární poplach pro osoby nacházející se v objektu se vyhlašuje **voláním HOŘÍ !!!**

III. POVINNOSTI OSOB PŘI VYHLÁŠENÍ POŽÁRNÍHO POPLACHU

a) provést evakuaci všech osob ze zasaženého úseku (objektu, prostoru), následně zajistit evakuaci materiálu, hořlavých látek, apod.; evakuace osob a materiálu musí být provedena únikovými cestami a východy, které jsou vyznačeny v grafické části evakuačního plánu,
b) zabezpečit volné přístupové a únikové cesty,
c) v případě požáru vypnout přívod elektrického proudu,
d) na výzvu velitele zásahu jednotky požární ochrany poskytnout osobní pomoc, dopravní prostředky, spojová zařízení a jiné věci potřebné ke zdolání požáru; uposlechnout příkazů členů zasahujících jednotek.

V případě ohrožení životů osob provádějících hasební zásah nebo záchranné práce, musí tyto osoby okamžitě opustit objekt (prostor); největší pozornost musí být věnována záchraně lidských životů!

IV. DŮLEŽITÁ TELEFONNÍ ČÍSLA

Při vyžadování pomoci, jakož i při ohlášení vzniku požáru nezapomeňte na tyto údaje:
- jméno osoby hlásící požár a důvod volání, v jakém rozsahu je požár, kde a co hoří, číslo telefonu

Hasičský záchranný sbor	*V Pardubicích*	*150*
Zdravotnická záchranná služba	*V Pardubicích*	*155*
Policie ČR	*V Pardubicích*	*158*
Vodovody a kanalizace, a.s.	*V Pardubicích*	*466 310 357*
Východočeská energetika, a.s.	*V Pardubicích*	*840 850 860*

Obdobně podle těchto požárních poplachových směrnic jsou zaměstnanci povinni postupovat, zjistí-li v objektu jiné vážné závady nebo dojde-li k jiné mimořádné události.

Zpracoval: Michal Kolman, tel. 606 901 676
Odborná způsobilost: Z – OZO-65/2002
Dne: 1.9.2011, Pardubice
Schválil: Ing. Jiří Janků, výkonný ředitel