VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV MANAGEMENTU

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF MANAGEMENT

NÁVRH BEZPEČNOSTNÍ POLITIKY ČESKÉ POBOČKY NADNÁRODNÍ SPOLEČNOSTI

THE PROPOSAL OF A SAFETY POLICY IN THE CZECH BRANCH OF AN INTERNATIONAL COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE
AUTHOR
Bc. TOMÁŠ FILIP

VEDOUCÍ PRÁCE
SUPERVISOR
Ing. VIKTOR ONDRÁK, Ph.D.

BRNO 2009

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2008/2009
Ústav managementu

ZADÁNÍ DIPLOMOVÉ PRÁCE

Filip Tomáš, Bc.

Řízení a ekonomika podniku (6208T097)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh bezpečnostní politiky české pobočky nadnárodní společnosti

v anglickém jazyce:

The Proposal of a Safety Policy in the Czech Branch of an International Compan

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004, 80-251-0106-1
NORTHCUTT, S. et al. Bezpečnost počítačových sítí. Praha: Computer Press, 2005, 80-251-0697-7
TVRDÍKOVÁ, M. Aplikace moderních informačních technologií v řízení firmy. Praha: Grada Publishing, 2008, 978-80-247-2728-8
MLÝNEK, J. Zabezpečení obchodních informací. Praha: Computer Press, 2007, 978-80-251-1511-4

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2008/2009.

L.S.

PhDr. Martina Rašticová, Ph.D.	doc. RNDr. Anna Putnová, Ph.D., MBA
Ředitel ústavu	Děkan fakulty

V Brně, dne 12.05.2009

Abstrakt

Bezpečnostní politika se zabývá procesy podnikové bezpečnosti v zájmu chránění aktiv bez ohledu na velikost pobočky. V dnešní době je podnik vystaven mnohým hrozbám a rizikům, kterým musí čelit tak, aby nebyl ohrožen jeho chod. Tato rizika a hrozby však nemusí být jenom konkurenčního zaměření, mohou vzniknout nahodile, nepravidelně a proti některým se ani nelze bránit nebo je jejich obrana příliš drahá. Naopak proti některým hrozbám se lze chránit lehce anebo levně. Pro správné posouzení se provádí analýza a vhodná bezpečnostní opatření.

Tato práce se zabývá kompletním návrhem bezpečnostní politiky pro malou českou pobočku jedné nadnárodní firmy. Obsahuje požadované analýzy, návrhy, teoretická východiska řešení, řízení změn a rolí pro snadnější návrh potřebných bezpečnostních dokumentů. Při zpracování byly využívány aktuální informace z oboru bezpečnosti, byl však kladen důraz na sestavení konceptů tak, aby dokument svým obsahem brzy nezestárl.

Klíčová slova

Bezpečnostní politika, analýza rizik, analýza hrozeb, bezpečnostní normy, bezpečnostní opatření.

Abstract

Safety policy deals with processes of security in company to protect assets regardless of a branch office size. Nowadays is the company exposed to a lot of threats and risks, which the company has to face to prevent work threats. This risks and threats don't have to be caused by competition, they can caused randomly, sporadically and someone can't be avoided or its protection is too expensive, whereas protection against some hazards can be easy or cheap. Analysis and appropriate safety actions are made for correct examination.

This thesis put mind to create complete suggestion of safety policy for a small Czech branch of an international company. It contains required analyses, tips, theoretical solutions, policy for personal management and changes for easier suggestion of necessary safety documents. I made use of up-to-date information from the domain of security during the process, but special care has been made while writing the concepts, so that the document's contents wouldn't age so quickly.

Key words

Safety policy, risk analysis, threads analysis, security standards, security techniques.

FILIP, T. Návrh bezpečnostní politiky české pobočky nadnárodní společnosti. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2009. 91 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

NÁVRH BEZPEČNOSTNÍ POLITIKY ČESKÉ POBOČKY NADNÁRODNÍ SPOLEČNOSTI

Prohlášení

Prohlašuji, že jsem diplomovou práci „Návrh bezpečnostní politiky české pobočky nadnárodní společnosti“ vypracoval samostatně pod vedením Ing. Viktor Ondráka, Ph.D.

Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Poděkování

Rád bych poděkoval svému vedoucímu Ing. Viktorovi Ondrákovi za poskytnutou literaturu, cenné rady a připomínky. Dále bych chtěl poděkovat managementu firmy Advantech Czech, s.r.o. za poskytnuté materiály, podměty a inspiraci při vytváření této práce.

v Brně, 22. 5. 2009

.....

Tomáš Filip

OBSAH

ÚVOD

Bezpečnostní politika je proces zabývající se řešením bezpečnosti u těch složek firmy, které vytvářejí pro firmu hodnotu nebo přispívají svou činností k plnění cílů firmy. Správné zabezpečení nám může chránit aktiva před poruchami, živelnými pohromami, kriminalitou, vandalismem, neoprávněným přístupem a celkově i jejich zneužitím.

Mnohá aktiva jsou pro firmu klíčová, jejich ztráta nebo poškození může způsobit vážné finanční ztráty, pro které není ani dnes a ani v budoucnosti místo. Doba, která uběhne, než se ztrátu podaří plně nahradit, může znamenat nejen výrazné oslabení pozice na trhu a snížení případných zisků, ale i čerpání prostředků, které by mohly být pro firmu mnohem lépe v budoucnu využity.

Se vzrůstající významem výpočetní techniky ve firmě rostou také další možnosti, jak se úspěšně prosadit v konkurenčním boji a to ať za pomoci informací uložených v nich, ale i prostředků, které nám informační systémy pro práci umožňují. Výpočetní technika navíc svým vhodným užíváním šetří náklady. Právě tyto firemní informační systémy se v dnešní době stávají snadnými oběťmi útoků různých druhů lidí a programů. Vlivem globalizace a celkového propojování systému je útok o to zákeřnější, že může být proveden z libovolného počítače, pokud je připojen k systému.

Bezpečnost podniku však nelze omezit jen na bezpečnost informačních systému, aktiva mnohých podniků nejsou tvořena jen z informací uložených v informačních systémech, ale i z tištěných dat, různých specializovaných zařízení a v neposlední řadě i samotného know-how.

Je tak v zájmu každé organizace chránit si svá aktiva jako jsou informace, majetek a know-how, ať jsou uložena v informačních systémech počítačů, v bankách, v papírových složkách nebo v hlavách zaměstnanců. Bezpečnost podniku obecně pojednává jak o fyzické tak i o personální a informační bezpečnosti.

Tato diplomová práce navrhuje řešení bezpečnosti podniku pro malou pobočku nadnárodní společnosti v pěti kapitolách.

- V první kapitole jsou vymezeny problémy a cíle, které vedly k zadání a vytvoření této práce.
- V druhé kapitole je provedena analýza současného stavu bezpečnosti pobočky pro všechny složky podniku.

- V třetí kapitole jsou rozebrána teoretická východiska řešení bezpečnosti, včetně požadované míry definic a informací k sestavení bezpečnostní politiky. Součástí kapitoly jsou i doporučená opatření a odkazy na vhodné dokumenty, které mohou pomoct při samotném návrhu.
- Kapitola čtvrtá obsahuje již samotné řešení problematiky, včetně analýzy aktiv, hrozeb a rizik. Další částí je i seznam rolí a odpovědností, je tak představen celkový koncept bezpečnostní politiky. V poslední části kapitoly je uvedena i analýza nákladů pro zavedení bezpečnosti v pobočce.
- V poslední páté kapitole je provedeno zhodnocení a závěr diplomové práce.

Součástí práce jsou i přílohy bezpečnostních dokumentů z oblasti informační bezpečnosti nadnárodní pobočky, ke kterým bylo při vytváření návrhu přihlédnuto.

1 VYMEZENÍ PROBLÉMŮ A CÍLE PRÁCE

Současná bezpečnostní politika firmy pro českou pobočku je definovaná v hlavě managementu. Existují sice firemní dokumenty, které řeší část bezpečnostní politiky, ale tyto dokumenty nejsou již delší dobu obměňovány a jsou tak zastaralé.

IT tým sídlící v německém Mnichově kontroluje a definuje počítačovou bezpečnost pro všechny evropské pobočky. Bohužel česká pobočka svým rozsahem plně neodpovídá běžným pobočkám v sítí firmy a tak je spousta věcí řešena za běhu, operativně a nesystematicky, za použití speciálních pravomocí místního vedení. Firemní bezpečnost je prováděna intuitivně bez řádného konceptu.

Cílem práce je shrnout potřebné úkony a požadavky na vytvoření dokumentu bezpečnostní politiky pro českou pobočku, ve kterém bude

- Shrnut aktuální stav zabezpečení,
- analyzovány hrozby a aktiva podniku a
- navržena bezpečnostní opatření řešící nové zabezpečení české pobočky,
- vypočteny hrubé náklady na zavedení bezpečnostní politiky do pobočky.

2 ANALÝZA SOUČASNÉHO STAVU

2.1 Česká pobočka fy. Advantech

Společnost Advantech Europe GmbH - Czech, organizační složka, na kterou je tato studie zaměřena, je českou pobočkou zahraniční firmy Advantech v Mnichově. Jedná se jmenovitě o organizační složku zahraniční osoby, umístěnou na území ČR, která jejím prostřednictvím v ČR podniká. V české pobočce je umístěno vývojové centrum pro zákaznické výrobky, firma má sídlo v Brně. Česká pobočka zaměstnává devět lidí. Předmětem podnikání a pracovní náplň pobočky je:

- Vývoj a výzkum zákaznických projektů,
- výroba prototypů a pomocné dokumentace,
- servisní a poradenská činnost v oblasti elektrotechniky,
- specializovaný maloobchod.

Samotná pobočka zaměstnává vlastního český mluvícího vedoucího složky, sekretářku, vývojové pracovníky a jednoho obchodníka.

- Vedoucí je zodpovědný za chod a řízení pobočky, má jako jediný práva k přístupu k citlivým informacím firmy a zastává mimo jiné i pozici bezpečnostního ředitele pobočky.
- Sekretářka řeší logistiku ve firmě a kooperuje učetnictví s Mnichovskou pobočkou, jako jediná kromě vedoucího má přístup k účetním informacím,
- Vývojoví pracovníci svou náplní přímo spadají pod vedoucího pobočky, provádějí vývoj a výzkum zákaznických projektů, mají přístup k běžným a výrobně-výzkumným informacím, tým je sestaven převážně z absolventů elektrotechnických škol.
- Obchodník spadá pod vedení Italské pobočky, která zajišťuje prodejní podporu jedné z divize fy. Advantech pro východní Evropu.

Zjednodušená rozvaha firmy ke dni 31.12.2008 je uvedena v tabulce 1.

Aktiva Σ	4249	Pasiva Σ	4249
A. Pohledávky za upsaný základní kapitál	**0**	**A. Vlastní kapitál**	**1525**
B. Dlouhodobý majetek	**0**	Základní kapitál	0
Dlouhodobý hmotný majetek	0	Fondy ze zisku	0
Dlouhodobý nehmotný majetek	0	Výsledek hospodaření minulých let	34
Dlouhodobý finanční majetek	0	Výsledek hosp. běžného účetního období	1491
C. Oběžná aktiva	**4134**	**B. Cizí zdroje**	**2627**
Zásoby	0	Rezervy	0
Dlouhodobé pohledávky	0	Dlouhodobé závazky	35
Krátkodobé pohledávky	1336	Krátkodobé závazky	2591
Krátkodobý finanční majetek	2798	Bankovní úvěry a výpomoci	1
D. Časové rozlišení	**115**	**C. Časové rozlišení**	**97**

údaje v celých tisících Kč

Tabulka 1: Rozvaha ve zjednodušeném rozsahu

2.1.1 Informace o mateřské firmě[1]

Hlavní firma Advantech Co., Ltd. byla založena na Taiwanu v roce 1983. Současnou strategií firmy je vývoj, podpora a prodej výpočetně řídících elektronických zařízení určených pro průmysl, případně specializovaných zařízení na přání zákazníka.

Postupem času vznikla řada produktů protínajících celé spektrum lidské činnosti. Jak byla firma rok od roku úspěšnější, rozšiřovala své působiště z Taiwanu i na další regiony, státy a kontinenty. Dosáhla řady ocenění a vybudovala si významnou pozici na celosvětovém trhu.

Firma Advantech v roce 2007 rozšířila svoji působnost na evropském trhu koupí menší německé firmy podobného zaměření, s kterou česká pobočka v Brně spolupracovala.

Mezi vybrané mise firmy patří:

- Přechod z modelu samostatných podniků umístěných po celém světě na jeden fungující globální model, označovaný ve světe jako GIE (Global Integrated Enterprise, tvůrcem projektu je fa. IBM).

1 *[1] ADVANTECH. Informace o firmě (online dokument)*

- Nadále vytvářet inovace v aplikacích a v poskytovaném servisu pro ePlatform aplikace.
- Dodržovat „Good to Great“ principy navržené Jimmym Collinsem.

Firma Advantech aktuálně působí v 18 zemích, 36 hlavních městech a zaměstnává přibližně 3700 zaměstnanců, z toho 1330 v Taiwanu. Většina evropských poboček má status prodejních kanceláří s lokální podporou zákazníků. Výjimku tvoří vývojová centra v Německu a v České republice. V Polsku je umístěno servisní středisko pro evropský trh.

Hlavní evropské sídlo se nachází v německém Mnichově, kde pracují účetní, projektoví manažeři, obchodníci. Úkolem Mnichovské pobočky je řídit obchodní transakce s evropskými zákazníky, vytvářet obchodní příležitosti, dohlížet a řídit chod ostatních obchodních poboček.

2.2 Analýza bezpečnostní politiky

Byla provedena analýza aktuálního stavu české pobočky, bylo shledáno, že v současné době není k dispozici žádný ucelený dokument řešící firemní bezpečnost. Jsou tak částečně nebo úplně ignorovány tyto body bezpečnostní politiky:

- Definování bezpečnostních rolí v pobočce,
- řízení přístupu, zodpovědnosti a pravomocí,
- analýza aktiv a hrozeb pro podnik,
- pravidelná bezpečnostní školení,
- metodika ověření funkčnosti zabezpečení,
- havarijní plány,
- řízení informační bezpečnosti a jejich složek,
- řízení personální bezpečnosti.

V případě, že se objeví nové incidenty, jsou dané problémy řešeny intuitivně, neefektivně a zřídkakdy s úspěchem (např. vymazané data již nelze v plné míře obnovit). Za období chodu pobočky nebyl prozatím zaznamenán žádný významný incident, který by způsobil výrazné škody na aktivech firmy.

Během chodu pobočky však byly zaznamenány tyto bezpečnostních incidenty:

- Firemní počítačové systémy, včetně počítače vedoucího pobočky, byly napadeny různými druhy škodlivého software,
- při zavádění inovací ve struktuře uložených informacích na místním serveru byla bez náhrady smazána část firemních dat,
- vyskytly se výpadky serveru způsobené jeho přetížením, nedostatkem volného místa na discích nebo selháním samotné techniky.

2.3 Analýza informační bezpečnosti

Po analýze informační bezpečnosti lze rozdělit podnikové informace do tří skupin. V pobočce se pracuje s citlivými informacemi, s běžnými informacemi a s produkčně-vývojovými informacemi.

Citlivé informace lze dále dělit na dvě skupiny. Do první skupiny patří informace, ke kterým má přístup pouze vedoucí pobočky, jako jsou smlouvy se zaměstnanci, interní smlouvy s nadřazenou firmou a smlouvy s externími dodavateli a poskytovateli služeb. Druhou skupinou jsou informace z finančního učetnictví (stavy pokladny, bankovních účtů, objednávek, pohledávek, stav zásob, rozpočtu, atd.), osobní informace zaměstnanců a dalších podnikové informace, ke kterým má přístup vedoucí a jeho sekretářka.

Produkčně-vývojové informace vznikají během procesu vývoje a výroby a jsou zpřístupněny všem zaměstnancům. Takto jsou přístupné i běžné informace, jako jsou manuály, příručky všeho druhu, technická dokumentace k cizím výrobkům, letáky, magazíny, katalogy, knihy, apod., tedy informace, které vedoucí pobočky nepovažuje za citlivé.

2.3.1 Práce s nedigitalizovanými informacemi

Většina citlivých informací z první skupiny je uložena v šanonech v uzamykatelné skříni s jednoduchým zámkem, ke kterému má klíč jen vedoucí pobočky. K dispozici jsou většinou jen v papírové podobě, neexistuje tedy jejich elektronická forma.

Citlivá data z druhé skupiny většinou zpracovává sekretářka pomocí počítače. Papírová data jako účty, objednávky, faktury jsou uloženy do šanonů ve volně dostupné neuzamykatelné skřínce. Každý měsíc je vždy část těchto papírových informací

posílána do externí firmy, která zpracovává účetnictví firmy. Po této akci je dostupnost citlivých informací silně omezena, je nutné je totiž vyžádat od externí firmy, pokud nebyly oskenované a uložené na místní server.

Běžné a produkčně-vývojové informace se skladují v celé firmě na různých místech. Jejich likvidace probíhá bez nějakých úprav vyhozením do koše s běžným odpadem(např. skartací nebo rozstříháním).

2.3.2 Práce s digitalizovanými informacemi

Digitalizované citlivé informace jsou uloženy na serveru, případně lokálně na přenosném počítači vedoucího pobočky anebo počítači sekretářky. K citlivým informacím nemají běžní zaměstnanci přístup. Povolený přístup k těmto citlivým informacím do vybraných adresářů na místní server má pouze vedoucí, sekretářka a účetní v Mnichově a IT oddělení.

Tištěné dokumenty se dle potřeby převádějí pomocí scanneru do elektronické podoby a ukládají do potřebných adresářů na server. Citlivé informace tak mají různou vnitřní strukturu od naskenovaných kopií, po tabulkové soubory, dokumenty a jiné speciální formáty, které vznikaly v průběhu práce v organizaci.

Běžné a produkčně-vývojové digitalizované informace jsou umístěny podle kategorií na místním serveru, případně lokálně u zaměstnanců. Tato data jsou dostupná všem lokálním zaměstnancům pobočky a k vybraným adresářům mají přístupová práva také ostatní zaměstnanci firmy Advantech, neboť jednotlivé pobočky jsou navzájem propojeny.

2.3.3 Bezpečnostní firemní dokumenty

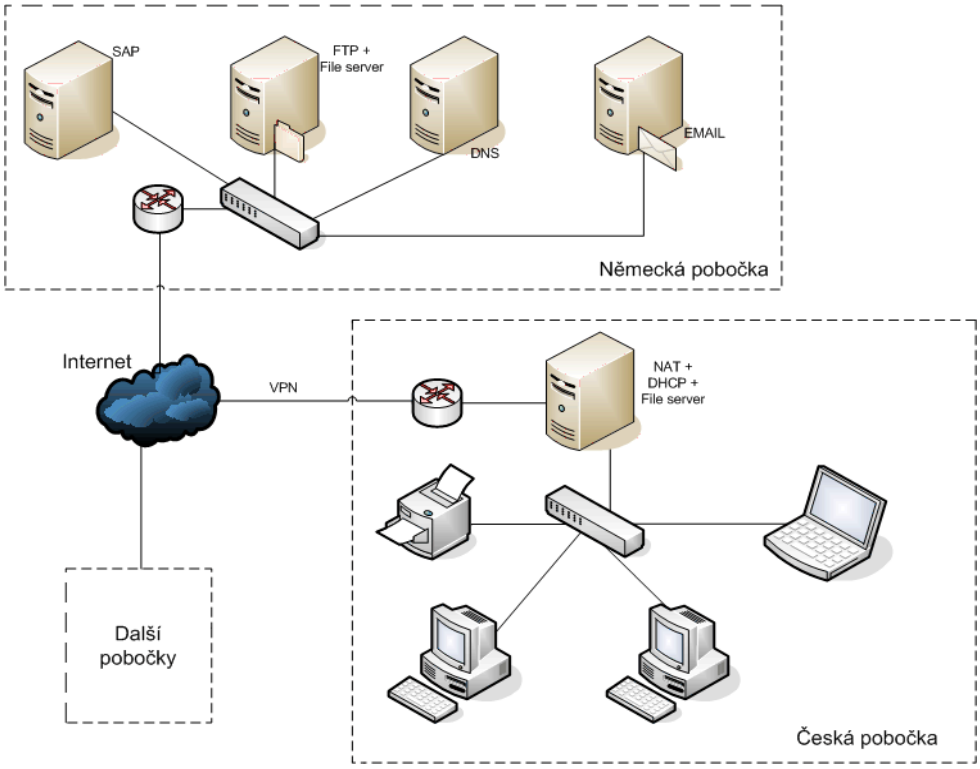
V roce 2004 byla sestavena sada dokumentů řešících informační bezpečnost podniku. Osoba, která tyto dokumenty vytvářela, však ve firmě již nepracuje a ani v dokumentech není zaznamenáno, zda tato informační bezpečnostní politika byla vytvářena podle některé známé bezpečnostní normy.

Dokumenty jsou napsány v anglickém jazyce a obsahem je lze zařadit někde mezi systémovou a celkovou bezpečnostní politikou. Dokumenty jsou sice závazné pro každého zaměstnance, ale za poslední dva roky neproběhla žádná osvěta zaměstnanců, tudíž pro některé nové zaměstnance můžou být tyto dokumenty utajeny. Jednotlivé dokumenty jsou zařazeny do příloh takto:

- Příloha A: Internet usage policy, str. 76 – pojednává všeobecně o chování uživatelů k internetové sítí, používání emailu, síťovým službám, říká, co je povoleno, co je zakázáno.
- Příloha B: Internet and Intranet Security Policy, str. 81 – v dokumentu jsou všeobecně řešena řízení přístupu, členění, rozdělení a přístup k informacím.
- Příloha C: Email Policy, str. 88 – dokument upřesňuje povolené a zakázané chování uživatelů k emailovým službám.

2.4 Analýza informační bezpečnosti IS/ICT

Ve firmě se používají počítače, na kterých běží operační systém Windows XP, tyto počítače jsou svěřeny jednotlivým uživatelům, kteří zodpovídají za jejich bezpečnost. Pobočka obsahuje lokálním server, na kterém běží operační systém Windows Server 2003. Zaměstnanci využívají přímé služby místního serveru, včetně aplikací umístěných na dalších serverech umístěných v Německu. Na vnitřní počítačovou síť pobočky jsou napojeny lokální počítače, tiskárny, přepínací prvky a jeden hlavní server, přibližná struktura zapojení je zobrazena na obrázku 1. O bezpečnost IS/ICT se stará ve větší míře mnichovské oddělení IT, kde je k dispozici i Čech jako kontaktní osoba, dále v menší míře má speciální práva k řízení bezpečnosti i vedoucí podniku.



Obrázek 1: Počítačová síť

Analýzou bezpečnosti byly zjištěny tyto skutečnosti:

- Nebyla a ani nejsou prováděna pravidelná bezpečnostní školení v oblasti bezpečnosti IS/ICT.
- Pravidelně se stahují bezpečnostní záplaty, které jsou vždy v čase 15:00 instalovány. Na některých je počítačích je instalován interní firewall fy Microsoft, některé počítače mají firewall vypnutý.
- Dále je instalován na všech počítačích antivirový program AVG a další program OfficeScan nasazený oddělením IT, který je nasazován na všechny počítače firmy. Úkolem programu OfficeScan je zamezit proniknutí všech forem škodlivého software. Úspěšnost obou programů v zabránění proniknutí škodlivého software na počítač je však slabá, jak bylo v minulosti několikrát ověřeno.
- Kontroly a plánování vytížení výpočetních prostředků za účelem ověření, zda je k dispozici dostatek výpočetních kapacit a pracovního místa, probíhají sporadicky a nepravidelně.
- Bezpečnostní záznamy za účelem auditních záznamu nejsou speciálně vyhotovovány, používají se jen ty, které systém implicitně poskytuje. Žádná další analýza se již neprovádí.
- Používání emailu je pod kontrolou uživatelů, v poštovním serveru je instalován poměrně účinný spamový filtr (mnohdy zachytí také běžnou poštu).
- Uživatelé mají právo si instalovat libovolný software, protože mají administrátorská práva. Běžně se připojují pod tímto administrátorským účtem a spouštějí na něm programy. Povolení administrátorského účtu je daní za statut vývojového centra, kde často probíhá nevyhnutelná instalace různých testovacích programů.
- Vývojové a provozní prostředí pobočky není odděleno, data jsou umístěna na jednom serveru na stejném fyzickém disku.
- Hesla jsou sestavena vedoucím podniku podle kriterií uvedených v kapitole 3.15.1. Pro určité pracovníky se však nemění. U novějších pracovníků (mladší jednoho roku) se mění pravidelně každého čtvrt roku. Zřejmě se jedná o chybějící nastavení systému pro starší pracovníky.
- Neprovádí se žádná forma zálohování informací a dat.

- Při testování, ale i ostrém provozu pobočky, se používá celá řada komunikačních protokolů, jak šifrovaných tak i nešifrovaných. Připojení cizích počítačů není nijak omezováno, k přístupu na server je však zapotřebí se autentizovat. WiFi síť se aktuálně nepoužívá, ale plánuje se její zavedení. Celá vnitřní síť je zapouzdřena do privátní sítě propojující jednotlivé pobočky. Do této sítě je možné se připojit vzdáleně z cizí sítě speciálním programem firmy Nortel.

2.5 Analýza majetkové bezpečnosti

Česká pobočka je zabezpečena trojími běžnými dřevěnými dveřmi s bezpečnostními zámky, které jsou dostupné z chodby po průchodu dalšími uzamykatelnými dveřmi. Zabezpečení je dostačující proti běžnému zloději, ale při použití řezací techniky jsou dveře lehce překonatelné. Na chodbě je však umístěna bezpečnostní kamera, která je sledována bezpečnostní službou objektu 24 hodin denně. Místnosti firmy nejsou ale dále nijak více zabezpečeny.

Lokální server spolu s potřebnými síťovými prvky je umístěn na přístupové chodbě, jako celek jsou prostředky zabezpečeny drátěnou kovovou klecí uzamykatelnou jednodušším zámkem. Server je vybaven zdrojem UPS, který vydrží napájet síťové prvky včetně serveru přibližně 20 minut.

Další ochranné prvky jako alarmy nebo signalizace požáru nejsou instalovány. Je zavedeno bezpečnostní pravidlo, kdy poslední pracující zaměstnanec před odchodem z firmy vypíná aktivní zásuvky v místnosti. Server je ale trvale napájen.

Firma má uloženu většinu finančních prostředků na jednom bankovním účtu, součásti firmy je i pokladna, kterou spravuje a uchovává ve svém přenosném kufru vedoucí pobočky, uvnitř se nachází maximálně 1% celkových finančních prostředků firmy.

2.6 Analýza personální bezpečnosti

Po analýze personální bezpečnosti lze konstatovat, že funguje intuitivně a operativně dle aktuálních potřeb podobně, jak je uvedeno v kapitole 3.17. Avšak vzhledem k absenci bezpečnostního dokumentu nejsou ošetřeny nutné kroky, které je zapotřebí učinit, když je zaměstnanec propuštěn. Je pravděpodobné, že některá z uvedených bezpečnostních opatření budou opomenuta.

3 TEORETICKÁ VÝCHODISKA ŘEŠENÍ

Bezpečnostní politika je proces zabývající se řešením bezpečnosti u těch složek firmy, které vytvářejí pro tuto firmu hodnotu (aktiva) nebo přispívají svou činností k plnění cílů firmy. Bezpečnostní politika je tak souhrnem kontrol, opatření, postupů, pravidel a zásad sloužící k nastavení a udržování stupně (míry) ochrany u těchto složek.

Bezpečnostní politika je základním dokumentem pro řešení firemní bezpečnosti. Pro bezpečnostní politiku není obecně dán předpis na formu, rozsah a úroveň detailů zpracovaných v ní[2]. Tento dokument může splňovat své hlavní cíle a přitom může mít mít rozsah pouze několika stránek formátu A4 nebo naopak se může jednat poměrně o rozsáhlý dokument řešící komplexně a detailněji podnikovou bezpečnost.

Celkovou firemní bezpečnost lze rozdělit podle typů aktiv na tři specifické oblasti:

- Informační bezpečnost,
- majetkovou bezpečnost a
- personální a osobní bezpečnost.

Problematiku bezpečnosti je nutné řešit adekvátně, účelně a komplexně pro všechny uvedené oblasti. Tedy tak, aby byla eliminována veškerá slabá místa v zabezpečení společnosti. Samotné vyspělé a špičkové zabezpečení v jedné oblasti bezpečnosti nemusí a ani nemůže pokrývat celkovou firemní bezpečnost. Příkladem může být opomenutí personální stránky bezpečnosti, kde při nedostatečném zabezpečení mohou uživatelé a zaměstnanci svou nedbalostí či úmyslem podkopat (obejít) informační anebo majetkovou bezpečnost a tak lehce oslabit celkovou bezpečnost.

Toto dokládá a více rozebírá pro informační bezpečnost TVRDÍKOVÁ[3]: „*Při posuzování bezpečnosti je třeba si uvědomit, že každý systém je silný jen tak, jak silný je jeho nejslabší článek. V případě zabezpečení informačních systémů je nejslabším článkem jednoznačně uživatel.*“

Při rozdělení bezpečnosti na jednotlivé oblasti je u středních a velkých organizací svedena odpovědnost na konkrétní osoby, případně celé bezpečnostní útvary, jejíž hlavní pracovní náplň je starost a odpovědnost za konkrétní bezpečnost (hlídači a vrátní,

2 *[15] MLÝNEK (2007), str. 9-12*

3 *[20] TVRDÍKOVÁ (2008), str 164-165*

správci IT, atd). U menších firem dochází ke kumulaci funkcí a to může snižovat celkovou firemní bezpečnost, na druhou stranu v rámci optimalizace lidských zdrojů je tento krok pochopitelný.

Dalším důležitým aspektem je i pohled na řízení bezpečnosti managementem podniku. Samotná formální podpora zdaleka nestačí. Projevovat se může například schválením bezpečnostních pravidel bez jejich následné realizace a kontroly. Nekomplexnost řízení, přehlížení varovných indikátorů, včetně vysokého bezpečnostního mínění, je dalším častým místem oslabení podnikové bezpečnosti.

Úroveň bezpečnosti by však měla odpovídat velikosti firmy a velikosti aktiv. Je pravděpodobné, že management bez řádné analýzy může mít námitky proti celkové ceně a rozsahu navrhovaných opatření zahrnující nové zabezpečení. Zavedení nové bezpečnosti a i s tím spojené náklady by měly být mnohem menší než důsledky a ztráty způsobené prolomením zabezpečení, případně ztráty daného aktiva. Bezpečnost na úrovni managementu by neměla být podceňována, musí být podporována a schválena vrcholným vedením.

Pro zdárné řešení bezpečnosti je nutné informovat management o úspěšnosti zavedeného bezpečnostního systému zpětnou vazbou. Výsledkem této zpětné vazby je zhodnocení vynaložených nákladů na bezpečnost firmy a jejich aktiv.

Mohou totiž nastat dvě stěžejní situace. První situace, kdy je případný bezpečnostní incident eliminován důsledně zavedenou bezpečnostní politikou, nebo druhá situace, kdy incident ještě nenastal a je pro systém hrozbou. V obou případech firemní aktiva nejsou (zatím) ohrožena.

Z pohledu managementu v rámci šetření finančních prostředků a vynaložených zdrojů může být zajímavé snížit (omezit) výdaje na bezpečnost, pokud nepřinášejí firmě zřetelnou hodnotu. To je důvodem pro zavedení dostatečné kontroly, zpracování získaných údajů o účinnosti opatření a revizí bezpečnosti, aby zabezpečení setrvala na úrovni definované na začátku bezpečnostní politikou.

Mezi činnosti a části systému firemní bezpečnosti patří[4]:

- Identifikace aktiv a jejich analýza z hlediska rizik,
- identifikace všech hrozeb, které firmě při vykonávání činnosti hrozí,
- identifikace rolí a odpovědnosti uvnitř organizace,
- zhodnocení současného stavu bezpečnosti,
- vypracování bezpečnostní politiky,
- školení zaměstnanců,
- řízení změn, realizace a prosazování bezpečnosti,
- výběr a implementace vhodných ochranných opatření,
- strategie havarijních plánů a plánů obnovy systémů a
- kontrola a revize bezpečnosti.

Ne vždy je nutné vytvářet dokumenty firemní bezpečnosti na tzv. „zelené louce“, tedy úplně od začátku, nově. Podporou pro vytváření dokumentů firemní bezpečnosti mohou být bezpečnostní standardy (normy) ISO/IEC, které se v plné míře zabývají vhodnými doporučeními ohledně bezpečnosti ve všech oblastech působení firmy.

V rámci postupné globalizace firem, rozšiřování trhu o nové pobočky a snižování nákladů roste zájem o používání internetu k sdílení firemních informací. S tímto faktem mimo jiné souvisí i jednotná bezpečnostní politika pro všechny pobočky firmy. V této fázi vzniku bezpečnostní politiky pobočka de facto přejímá již vytvořenou politiku nebo její části od své mateřské společnosti a snaží se jí v rámci místních podmínek a legislativy napasovat na chod pobočky.

3.1 Outsourcing

Další variantou, jak lze řešit vytvoření bezpečnostní politiky, je využití služeb třetích firem, které nabízejí služby v oblasti návrhu, sestavení a vypracování bezpečnostní politiky pro konkrétní firmu.

4 *[15] MLÝNEK (2007), str. 9-12; [20] TVRDÍKOVÁ (2008), str. 164-165*

Také dohled nad firemní bezpečností lze řešit externí organizací, tzv. outsourcingem. Podstatou outsourcingu je přenesení těch činností firmy, které netvoří podstatu podnikání, na jinou firmu.

Mezi výhody využití externí společnosti pro řešení firemní bezpečnosti patří:

- Nižší náklady firmy na pořízení nákladného hardware, specializovaného software a samotných zaměstnanců – bezpečnostních specialistů.
- Řešení incidentů, kontrola firemní bezpečnosti, revize bezpečností a nastavených pravidel a pravidelně se opakujících školení zaměstnanců mohou být podmíněny smluvními podmínkami a jsou jednodušeji postihovány. V případě incidentů mohou být i rychleji řešeny.
- Dobrá externí organizace zaměstnává odborníky, kteří se zabývají bezpečností, pro než je vyhledávání nových hrozeb a potenciálních útoků takřka každodenní činností. Jsou tak na potenciální problémy více soustředěni než interní zaměstnanci, pro které je bezpečnost pouze okrajovou záležitostí řešenou formou příplatku nebo částečného úvazku.

Mezi základní nevýhody patří:

- Náročný výběr na kvalitní firmu, sestavení bezpečnostních otázek a smlouvy.
- Větší důraz na zajištění bezpečnosti zpracovávaných informací externí společností (především citlivých informací).
- Částečná alokace interních zdrojů pro komunikaci a operace s externí firmou, nejen pro případ výskytu incidentu, kdy je nutné kvalifikovaně informovat externí firmu o problému, ale je také možné problém lokálně řešit.

3.2 Forma bezpečnostní politiky

Při zavádění bezpečnosti ve firmě může být žádoucí vystavit zprvu zjednodušenou formu bezpečnostní politiky, jak pro vedení podniku, tak pro zaměstnance. Takto obecnější a jednodušší bezpečnostní politika má řadu výhod. Jednak je snáze prosaditelná ve vedení, lépe se vysvětluje zaměstnancům a rychleji se aktualizuje.

Po uveřejnění a zavedení jednodušší a obecnější bezpečnosti lze řešit podrobnou bezpečnostní politiku důkladněji a to ve větším časovém horizontu, ať pro omezenou

skupinu uživatelů nebo v postupných krocích všem. Důkladnější bezpečnostní politika již nemusí a v určitých případech ani nemůže být určena všem zaměstnancům. Například z důvodu omezení informovanosti o hrozbách a možných napadení bezpečnosti firmy. Stručná politika bezpečnosti by měla obsahovat alespoň[5]:

- Vysvětlení pojmu bezpečnosti, zřetelnou deklaraci vedení podniku politiku bezpečnosti podporovat, v praxi ji prosadit a její plnění vyžadovat od všech zaměstnanců, organizačních útvarů a podřízených složek.
- Stanovení odpovědnosti organizačních a interesovaných útvarů podílejících se na zajištění bezpečnosti, včetně povinností a bezpečnostních opatření pracovníků ve všech stupních.
- Způsob řízení, kontroly bezpečnostní dokumentace, případně zmocnění k vydání prováděcích předpisů, standardů a pokynů a výjimek při krizových situacích.

Hlavní nevýhodou obecné formulace politiky je to, že pod některými formulacemi obecného dokumentu si mnoho pracovníků nedokáže představit jejich konkrétní obsah a tak může docházet ke špatné interpretaci obecných principů. Detailní politika by proto měla ve zvolené míře podrobností obsahovat i tato témata:

- Zacházení s citlivými informacemi v organizaci, případně schéma klasifikace aktiv,
- zajištění personální bezpečnosti, s cílem snížit rizika lidského faktoru, tj. rizika chyby, krádeže, podvodu nebo nesprávného užití či zneužití informací,
- zajištění fyzické bezpečnosti s cílem snížit rizika neoprávněného vniknutí, poškození nebo zničení prostor a technických zařízení,
- řízení přístupu uživatelů, stanovení přístupových práv, včetně vzdáleného přístupu, práce s mobilními počítači a práce mimo firmu,
- přehled bezpečnostních opatření a zpracovávání informací,
- řízení kontinuity všech činností a havarijního plánování,
- ochrana aktiv organizace, přístupy k nim a zpracování aktiv třetí stranou na základně smluvních vztahů,
- kontrola plnění, aktualizace, zajištění shody s legislativou, smluvními závazky.

5 *[16] POŽÁR (2005), str. 90*

Vzhledem k neustálému vývoji informačních systémů, bezpečnostních hrozeb a incidentů může být výhodné nejen pro velké společnosti rozdělit bezpečnostní politiku podle určitých činností a kritérií na sadu podpůrných dokumentů, které se svým menším rozsahem snáze aktualizují a poskytují jak výhody, tak eliminují nevýhody uvedené výše.

Cílem snažení je seznam dokumentů, který je schválen vedením, je závazný pro všechny zaměstnance a pracovníky externích společnosti. Při vytváření seznamu by se také měly definovat jednotlivé úrovně oprávnění přístupu k jednotlivým dokumentům a nejdelší doba aktualizace těchto dokumentů.

Dále lze rozdělit dokument bezpečnostní politiky na dvě formální části, na celkovou a systémovou bezpečnostní politiku organizace[6].

3.2.1 Celková bezpečnostní politika

Celková bezpečnostní politika se nezabývá konkrétními opatřeními, ale pojednává o konceptu budování bezpečnosti v organizaci. Dokument celkové bezpečnostní politiky může být poměrně stručný, ale je nutný a nesmírně důležitý, neboť z něj budou vycházet veškeré další práce[7]. Celková bezpečnostní politika obsahuje mimo jiné:

- Popis organizace a její činnosti,
- definici cílů bezpečnostní politiky,
- bezpečnostní infrastrukturu,
- identifikaci aktiv, citlivých dat a jejich vlastnictví,
- obecné hrozby,
- popis současného stavu bezpečnosti,
- popis bezpečnostních opatření a havarijní plány,
- relevantní zákony a normy,
- kontrolu dodržování celkové bezpečnostní politiky a sankce,
- odpovědnosti jednotlivých uživatelů a
- způsoby hlášení bezpečnostního incidentu.

6 *[20] TVRDÍKOVÁ (2008), str. 163*

7 *[16] POŽÁR (2005), str. 100*

3.2.2 Systémová bezpečnostní politika

Systémová bezpečnostní politika již definuje způsob implementace bezpečnostní politiky v konkrétním prostředí daného systému.

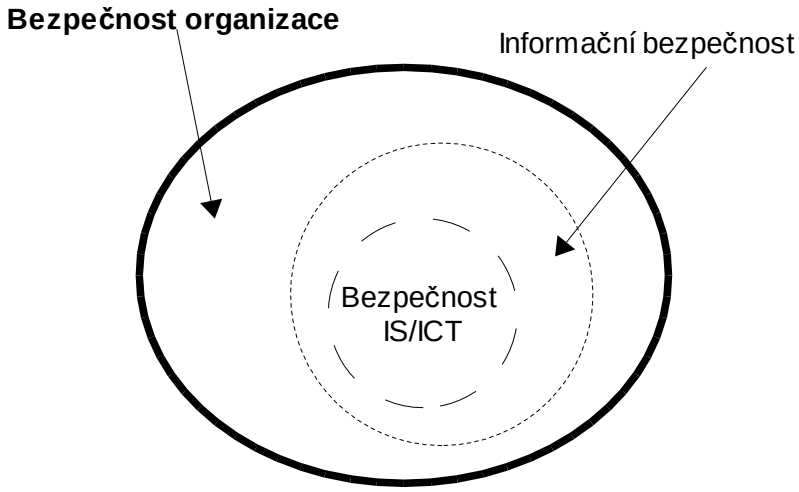
Systémová bezpečnostní politika je tedy etapa konkretizace bezpečnostních požadavků na určité komponenty systému, určitého uživatele. Nejedná se jen o technické zabezpečení, ale o celý komplex opatření mající vliv na každého pracovníka organizace, organizační složky a techniku organizace.

Systémová bezpečnostní politika typicky obsahuje následující bezpečnostní prvky:

- Popis rolí,
- řízení přístupu,
- zodpovědnosti a pravomoci,
- právní a etické otázky,
- vzory dokumentů,
- realizace osvěty a školení,
- řešení incidentů a
- testování bezpečnosti.

3.3 Bezpečnost organizace

Pro každou organizaci bez ohledu na zaměření platí, že pro celou škálu svých činností je plně závislá na svých pracovnících a dostupných hmotných i nehmotných statcích (aktivech). Nezbytnou úlohou managementu podniku jsou mimo jiné i plány, jak pracovníky a aktiva organizace chránit. Samotnou bezpečnost organizace lze rozdělit podle hierarchie nadřízenosti a podřízenosti na tři kategorie, které jsou znázorněny na obrázku 2.



Obrázek 2: Vztah úrovní bezpečnosti ve firmě

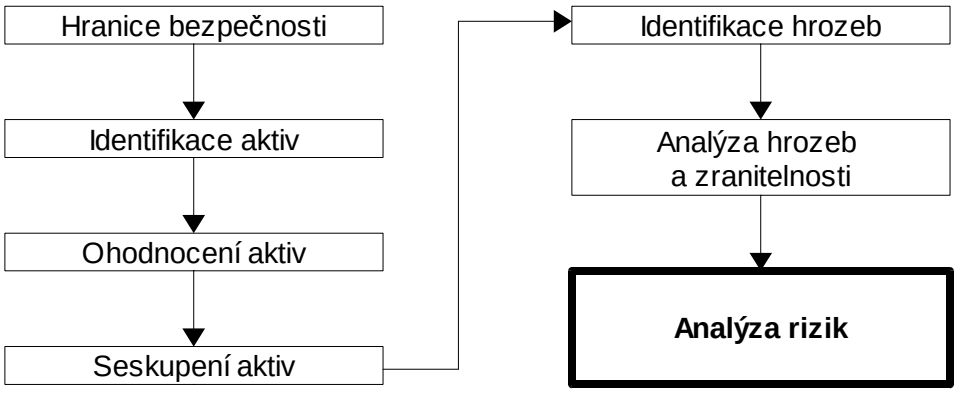
Nejvyšší kategorií je bezpečnost organizace. Její součástí je zajištění majetkové bezpečnosti majetku, jako například ostraha, řešení přístupů a fyzické oprávnění přístupu do budov, atd. Podřazenou částí je informační bezpečnost. Cílem a úkolem řízení bezpečnosti je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů, tedy nejen s informacemi v digitální podobě.

Informační bezpečnost řeší mimo jiné způsob uložení a správy archívu nedigitálních dat, zásady skartace materiálů, nakládání s informacemi během jejich transportu, zásady pro poskytování informací novinářům, zásady pro veřejné vystupování pracovníků organizace, apod.

Bezpečnost informačního systému a použitých informačních a komunikačních technologií (dále jen IS/ICT) je poslední, nejužší úrovní bezpečnosti ve firmě. V této oblasti se chrání taková aktiva, která jsou součástí informačního systému organizace podporovaného informačními a komunikačními technologiemi.

Aktiva organizace mají svoji hodnotu, která je v absolutní většině případů pro organizaci z hlediska jejího fungování kritická. V případě ztráty nebo závažného poškození některých aktiv tak může dojít i k ukončení činnosti organizace a tím ke značným finančním ztrátám majitele nebo akcionářů, nemluvě o obchodních partnerech, zákaznících i zaměstnancích.

Pro účelné zavedení bezpečnosti je zapotřebí provést analýzu rizik, včetně stanovení úrovně, na kterou chceme analyzovaná rizika eliminovat. Tato analýza může být provedena pro dílčí části aktiv firmy, jako je internetové bankovnictví, personální systém či pobočku společnosti, anebo plošně v rámci celé společnosti. Výběr rozsahu probíhá v prvotním kroku nazvaném obecné stanovení hranic bezpečnosti[8]. Další kroky analýzy rizik zahrnuje obrázek 3:



Obrázek 3: Obecný postup realizace analýzy rizik

3.4 Identifikace aktiv

Identifikace spočívá ve vytvoření seznamu aktiv, která leží uvnitř námi zvolené hranice bezpečnosti. Pro stanovení této hranice lze vyjít ze záměrů managementu společnosti, nebo požadavků, ať povinných nebo doporučených pro zabezpečení organizace. Budou sem patřit ta aktiva, která mohou být ohrožena nějakou hrozbou. Aktiva, která nejsou ohrožována, nejsou předmětem identifikace a další analýzy. Při sepisování seznamu aktiv se uvádí jejich název a umístění.

8 *[15] MLÝNEK (2007), str. 19*

Může se jednat například o tyto skupiny aktiv:

- Informace (účetní doklady, smlouvy, skladové informace, obchodní informace, strategické záměry, atd.),
- hmotný majetek,
- zásoby,
- peněžní prostředky,
- mentální, nehmotná aktiva (image firmy, know-how, software, licence aj.).

Identifikovat aktiva lze na základě náplně jednotlivých útvarů organizačního schématu nebo na základě obchodních aktivit společnosti (nejvhodnějším přístupem je využití obou přístupů současně).

Informace společnosti se obvykle sdružují do větších celků, tzv. informačních jednotek[9]. Při praktické realizaci identifikace ve firmě je vhodné přiřadit ke každé existující agendě jednu informační jednotku (souhrn informací užívaných při provozování dané agendy). V praxi lze přidělit v případě potřeby více informačních jednotek jedné provozované agendě společnosti, nebo lze naopak užívané informace ve dvou nebo případně i více agendách sloučit do jedné informační jednotky.

Zbytečné vytvoření mnoha informačních jednotek pro identifikaci vede k menší přehlednosti v průběhu provádění analýzy rizik. Středně velká obchodní společnost (kolem 100 zaměstnanců) užívá přibližně 10 až 20 informačních jednotek, velké obchodní společnosti (více než 1000 zaměstnanců) užívají obvykle sto a více jednotek.

3.5 Ohodnocení aktiv

Dalším krokem provádění analýzy rizik je ohodnocení aktiv dle významu, důležitosti a případné vyčíslení ztráty pro podnik. Ohodnocení fyzických aktiv (hmotný majetek, zásoby, aj.) není obtížné, lze jej určit na základě pořizovací ceny nového aktiva, s přibližně stejnými parametry jako má oceňované aktivum.

Je však zapotřebí vzít v úvahu přidanou hodnotu aktiva v závislosti na tom, jak důležitou roli aktivum znamená pro firmu při jejím pořízení, zapracování nebo výpadku.

9 *[15] MLÝNEK (2007), str. 20*

Ocenění a vyjádření hodnoty nehmotných aktiv a informací je obtížnější a je jedinečné pro každou organizaci. Manažeři obchodních společností často požadují ohodnocení informační jednotky na základě vyčíslení její finanční hodnoty. Tento přístup však není příliš vhodný pro účely zabezpečení informační jednotky a může často vést k chybným závěrům[10].

Jeden z možných přístupů ověřený při praktických realizacích je hodnocení, které používá i metodika CRAMM. Při tomto postupu je informační jednotka (aktivum) ohodnocena náklady, které by byly způsobeny porušením **důvěryhodnosti, integrity a dostupnosti.**

Za důvěryhodnost je považováno zajištění, že informace jsou přístupné nebo sděleny pouze těm, kteří jsou k tomu oprávněni. Dostupnost zajišťuje, že informace je pro oprávněné uživatele přístupná v okamžiku její potřeby a integrita hodnotí zajištění správnosti a úplnosti informací. Tyto tři kritéria poskytují podklady pro ohodnocení aktiv. Výběr kritérií je záměrný, jsou na sobě nezávislé a nejsou vzájemně podmíněny. Je vhodné při hodnocení aktiv věnovat zvýšené úsilí detailnímu popisu a vyhledání, kde všude je dané aktivum používáno a vytvořit jednotlivé hodnocení pro každé z nich[11].

Pro každou oblast dopadu se stanovuje několik úrovní závažnosti. Každé úrovni v dané oblasti se tak přiřadí celočíselná hodnota mezi 1 až N (např. 1 až 5). Názorný příklad ukazuje tabulka 2.

Přiřazená hodnota	Úroveň dopadu
1	Žádný dopad na organizaci
2	Zanedbatelný dopad na organizaci
3	Potíže či finanční ztráty
4	Vážné potíže či podstatné finanční ztráty
5	Může znamenat existenční potíže organizace

Tabulka 2: Úrovně závažnosti

Při odhadu možných negativních dopadů pro společnost se doporučuje vzít v úvahu následující negativní dopady: přímé finanční ztráty, ztráta dobrého jména společnosti, porušení právních předpisů a smluvních závazků, narušení důvěrnosti ve vztahu k osobním údajům osob, zhoršení výkonu společnosti, ohrožení obchodních zájmů, narušení veřejného pořádku, ohrožení bezpečnosti zaměstnanců apod.

10 *[15] MLÝNEK (2007), str. 21*

11 *[12] CHLUP. ISMS - ohodnocení aktiv.*

Negativní dopady jsou obvykle také zkoumány ze všech tří pohledů podrobněji. Například z pohledu nedostupnosti se lze zaměřit na různé časové intervaly. U porušení důvěrnosti se lze zabývat rozsahem uvnitř firmy, dopadem na třetí stranu anebo mimo společnost. Také pro integritu lze vytvořit skupiny hodnocení: malé chyby, velké chyby a záměrné modifikace.

Pro získání výsledného hodnocení aktiva je vhodné také přihlédnout k dalším faktorům související s aktivem, jako úroveň náhrady (lze-li aktivum nahradit) a faktor závislosti společnosti na aktivu. Dalším faktorem jsou náklady při omezením firmy, než dojde k obnově aktiva. Výslednou hodnotu hodnocení aktiva pro firmu lze vypočítat jako vážený průměr hodnot podle všech použitých hledisek[12].

3.6 Seskupování aktiv

Vzhledem k tomu, že aktiv je obvykle veliké množství, je vhodné zredukovat jejich počet sloučením aktiv podle různých hledisek tak, aby se vytvořily skupiny aktiv podobných vlastností.

Seskupovat se tak mohou aktiva podobné kvality, ceny, účelu, umístění apod. Takto vytvořená skupina aktiv pak dále vystupuje jako jedno aktivum, kterému lze přiřadit stejné hrozby a zranitelnosti. Z pohledu bezpečnosti je pak důležité aplikovat protiopatření na všechna sloučená aktiva.

3.7 Identifikace hrozby

V souvislosti s identifikaci hrozby se setkáváme s pojmy:

- Hrozba,
- zranitelnost a
- bezpečnostní incident.

Pojem hrozba označuje jakoukoliv okolnost, skutečnost, akci či událost působící na zranitelné místo aktiva. Tato hrozba může způsobit potenciální škodu, kompromitaci, ztrátu důvěry nebo hodnoty aktiva. Hrozba je skutečnost možného ohrožení, kdy se zatím nic nestalo, ale stát se může.

12 *[18] SMEJKAL (2006), str. 87*

Zranitelnost je nedostatek, slabina nebo stav aktiva, na kterém se může hrozba uplatnit. Tato veličina je vlastností aktiva a vyjadřuje citlivost aktiva působením dané hrozby. Zranitelnost vzniká všude tam, kde dochází k interakci mezi hrozbou a aktivem.

Vlivem okolí a prostředí vznikají zranitelná místa v podniku a tato místa způsobují hrozby. Základní charakteristikou je její úroveň, ta se hodnotí podle následujících faktorů:[13]

- **Citlivost** – náchylnost aktiva být poškozené danou hrozbou.
- **Kritičnost** – důležitost aktiva pro analyzovaný subjekt.

Když událost hrozby nastane, vznikne bezpečnostní incident. Hrozbu lze dělit podle hledisek zejména na[14]:

- objektivní
  - **Přírodní –** fyzické jako např. požár, povodeň, výpadek napětí, poruchy, přepětí v sít, apod.
  - **Fyzikální** – např. elektromagnetické vyzařování při bouři, exploze, atd.
  - **Technické nebo logické –** porucha zařízení, špatné zabezpečení IS/ICT, atd.
- subjektivní
  - Neúmyslné působení neškoleného uživatele, pracovníka s aktivy firmy nebo i správce informačního systému.
  - Úmyslné působení představované potenciální existencí vnějších útočníků, jako jsou např. špióni, teroristé, kriminální živly, hackeři, ale i vnitřní útočníci. Odhaduje se, že až 80% útoků na firmu je vedeno zevnitř útočníkem, kterým může být propuštěný, rozzlobený, vydíraný, chamtivý zaměstnanec; velmi efektivní z hlediska útoků je součinnost obou typů útočníků.

Charakteristikou hrozby je její vnější či vnitřní zdroj, frekvence, kritičnost uplatnění hrozby a motivace potenciálního útočníka, jako je finanční zisk nebo získání konkurenční převahy. Rozmachem používání IS/ICT ve firmách lze najít celou řadu dalších typických hrozeb, jako například:

13 *[18] SMEJKAL (2006), str. 83*

14 *[16] POŽÁR (2005), str. 40*

- Neautorizovaná modifikace informací, informačních zdrojů a služeb, tj. porušení integrity zachytáváním a modifikací zpráv, vkládání a replikaci zpráv, falšování identity,
- neautorizované zpřístupnění informace odposlechem na přenosovém médiu – např. použitím škodlivého software nebo elektromagnetického vyzařování, použití zařízení pro práci se zvukem, instalovaných na mnoha počítačích,
- agregace citlivých informací z méně citlivých dílčích informací,
- dedukce ze znalosti, že jistá informace je uložena v databázi včetně neautorizovaného přístupu, tj. použití standardních hesel nebo prolomení systému pro přístup k informacím,
- krádeže hardwarových a softwarových komponent, včetně používání jejich neoprávněných kopií nebo neautorizovaných programů,
- popírání aktu zaslání nebo přijetí zprávy anebo autorství dané zprávy,
- hoaxy, spamy, spyware, malware a počítačové viry, cílený útok na systém pro jeho vyřazení, tzv. útoky DoS a zejména DDoS.

Obvykle se rozlišuje několik stupňů úrovně hrozby, jako velmi nízká, nízká, střední, vysoká. U objektivních hrozeb je prevence obtížná a je vhodné je spíše řešit minimalizací dopadů vhodným plánem obnovy definovaném v havarijním plánu. U subjektivních hrozeb může být prevence snazší, velikost případné ztráty lze snížit uplatnění konkrétních bezpečnostních opatření.

3.8 Analýza rizik

Jedna z definic rizika říká, že riziko je pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty[15]. Je to tedy míra ohrožení konkrétního aktiva, míra nebezpečí, že se uplatní hrozba a dojde k nežádoucímu výsledku vedoucímu ke vzniku škod. Výše rizika vyplývá z hodnoty aktiva, úrovně hrozby a zranitelností aktiva.

Způsob vyjádření veličin, s nimiž se v analýze rizik pracuje, lze použít jako základní hledisko pro rozdělení těchto metod. Existují přitom dva základní přístupy k jejímu řešení: kvantitativní a kvalitativní metody vyjádření veličin analýzy rizik. V analýze rizik se používá buď jeden z těchto dvou přístupů, nebo jejich kombinace.

15 *[16] POŽÁR (2005), str. 37*

3.8.1 Kvalitativní metody analýzy rizik[16]

Kvalitativní metody se vyznačují tím, že rizika jsou vyjádřena v určitém rozsahu, například číselnou stupnicí 1-10, pravděpodobností <0-1>, ale i slovně jako malé, střední, velké riziko. Úroveň je určována obvykle kvalifikovaným odhadem.

Získávání výsledků kvalitativních metod je jednodušší a rychlejší na úkor subjektivních nefinančně vyjádřených výsledků. Následné přisuzování finančních nákladů nutných k eliminací hrozby může být kvalitativní metodou charakterizováno jako „velké až kritické“.

Dominujícím zástupcem kvalitativní analýzy z pohledu neformálního přístupu analýzy je metoda účelových interview (metoda Delphi), která spočívá v řízeném kontaktu mezi experty a příslušnými představiteli hodnoceného subjektu. Oproti jiným metodám, založených na strojovém zpracování velkého počtu dotazníků, používá metoda Delphi pro rizikovou analýzu souboru otázek. Tento soubor je rozdělen na dvě části otázek – pevnou a variabilní, upravené dle průběhu pohovoru a postavení respondenta.

V metodě Delphi nedochází k vzájemné ovlivňování respondentů, protože interview probíhají mezi představiteli odděleně. Kritizovanou nefinanční stránku lze vhodně začlenit do kriterií pohovorů, které navíc k prosazení nejpodstatnějších hypotéz, výběrem po statickém zpracování, mohou probíhat vícestupňově – iteračně.

3.8.2 Kvantitativní metody analýzy rizik

Kvantitativní metody jsou založeny na matematickém výpočtu rizika z frekvence výskytu hrozby a jejího dopadu. Vyjadřují dopad obvykle ve finančních termínech jako tisíce Kč. Nejčastěji je vyjádřeno riziko ve formě sumy roční předpokládané ztráty (anglicky Annualized Loss Expectancy = ALE)[17], která je vyjádřena finanční částkou.

$$ALE = \sum_{i}^{n} P_i * c_i$$

Kde *i* je pořadí ohrožení, *n* je celkový počet ohrožení za rok, *c* je ztráta a *P* pravděpodobnost ztráty.

16 *[18] SMEJKAL (2006), str. 95*

17 *[16] POŽÁR (2005), str. 43*

Kvantitativní metody se ujaly především v oblasti bezpečnosti organizací jejich informačních systémů. Pro podporu provádění kvantitativní analýzy rizik se obvykle používají speciální nástroje, obvykle v podobě programů, často disponujících databází informací, ve kterých je metodika a postup provádění analýzy rizik již zpracován. Mezi takové představitele patří metodiky CRAMM a COBRA.

Pravděpodobně nejznámější je metodika CRAMM[18], kde analýza řeší ohodnocení systémových aktiv, seskupení aktiv do systému a stanovení požadavků na bezpečnost pro jednotlivé skupiny, jak bylo naznačeno v předchozích kapitolách. Na tomto základě jsou navržena bezpečnostní opatření, která jsou ve shodě s úrovní rizika při porovnání s již implementovanými systémovými opatřeními. Důležité je, že se vždy zkoumá model určitého systému – nikoliv systém samotný. CRAMM je silně závislý na výsledcích strukturovaných interview s odborníky uživatele.

Metodika COBRA využívá pro analýzu rizik expertní systém, který je sestaven ze tří části – první obsahuje proces sestavení, případně výběr otázek z vědomostní databáze, v další části již probíhá zodpovězení otázek vybranou skupinou uživatelů a poslední části, kde systém sestaví výsledky a návrhy možných řešení z vyplněných otázek[19].

3.8.3 Volba analýzy rizik

Před výběrem analýzy rizik je vhodné provést orientační analýzu rizik za účelem posouzení, která z aktiv jsou klíčová pro činnost společnosti a která jsou vystavena značným rizikům. Pro tato aktiva by měla být následně provedena detailní analýza rizik a to některou z výše uvedených metod, případně oběma. Rozhodnutí, který přístup je pro daný objekt vhodný, závisí zejména na následujících skutečnostech:

- Jakých cílů má být použitím analýzy rizik dosaženo,
- k jakým účelům aktiva slouží,
- jaká je hodnota aktiv,
- zda jsou funkce, které aktivum poskytuje jsou kritické a pro koho,
- jaká je úroveň investic do aktiva a jaká je výše nákladů na případné obnovení funkčnosti.

18 *[18] SMEJKAL (2006), str. 97*

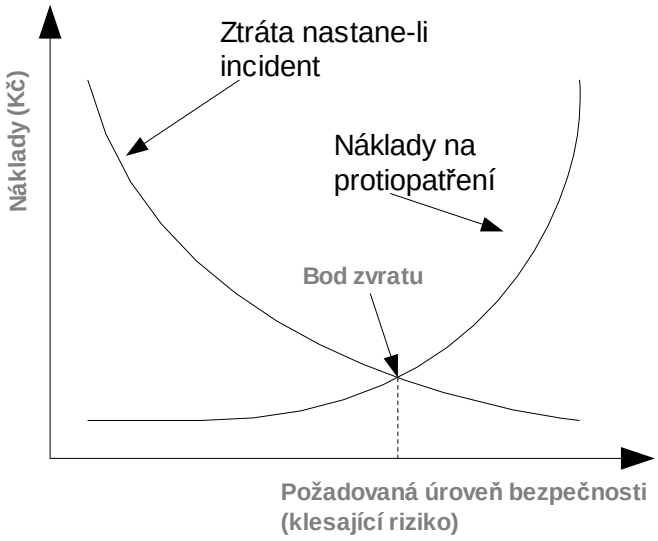
19 *[11] GREGORY (2008), str. 309*

Jestliže je libovolná uvedená skutečnost pro společnost spojená s aktivem kritická, pak je podrobná analýza rizik nezbytná. Na základě těchto rozhodnutí, může být pro aktiva prováděna analýza základním přístupem, neformálním přístupem, podrobnou analýzou rizika anebo kombinovaným přístupem. Kombinace metod je sice pravděpodobně nejvhodnější, ale současně nejnákladnější a nejzdlouhavější cestou.

3.9 Obecné způsoby potlačení rizik

Je zřejmé, že s existencí rizik se musí počítat, některá rizika lze přesunout a některá zadržet, v určitých situacích je vhodnější se riziku vyhnout nebo toto riziko redukovat[20]. Ochrana proti riziku a zabránění bezpečnostnímu incidentu je zejména otázkou ceny, čím vyšší míra zabezpečení, tím vyšší jsou náklady. Při návrhu vhodných protiopatření je základní otázkou cena chráněného aktiva.

Nejrozumnější je dosáhnout takové úrovně zabezpečení proti riziku, kde se vynaložené náklady vyrovnají případné ztrátě při události[21]. Výsledkem je hledání bodu průniku křivky nákladů a případné ztráty, jak ukazuje obrázek 4.



Obrázek 4: Analýza nákladů a přínosů

Možnosti jak dosáhnout adekvátních nákladů na protiopatření určují charakteristiky rizika samotného. Kritériem při tomto rozhodování je obvykle velikost rezerv firmy nebo schopnost firmy nést ztrátu.

20 *[18] SMEJKAL (2006), str. 112*

21 *[16] POŽÁR (2005), str. 43*

Každý způsob řešení rizika (zadržení, redukce, transfer) by měl být použít v situaci, kdy je nejvýhodnějším a nejméně nákladným způsobem dosažení cíle v podobě snížení či úplné eliminace rizika. Následující členění způsobů řešení rizik lze využít zejména ve fázi analýzy konkrétního rizika.

V souvislosti s rozlišením rizik do těchto tříd kategorií se používá pojem tvrdost rizika. Tvrdostí rizika se rozumí dopad ztráty v případě výskytu incidentu (nepříjemné události). Nízká tvrdost vyjadřuje nízký dopad ztráty na aktivum.

Shrnutí rozdělení rizik do zmíněných kategorií dle úrovně tvrdosti a výše pravděpodobnosti uvádí tabulka 3:

	Vysoká pravděpodobnost	**Nízká pravděpodobnost**
Vysoká tvrdost	vyhnutí se riziku, redukce	transfer (pojištění)
Nízká tvrdost	retence a redukce	retence

Tabulka 3: Doporučené metody pro obecné řešení problému rizika

3.9.1 Retence rizik

Retence rizik je pravděpodobně nejběžnější a legitimní metodou řešení rizik a v mnohých případech se jedná o metodu nejlepší. Spočívá v tom, že společnost běžně čelí neomezenému počtu rizik a ve většině případů se proti nim nedělají žádná bezpečnostní opatření. Retence rizik může být vědomá či nevědomá[22]. K vědomé retenci rizika dochází tehdy, je-li riziko rozpoznáno, ale nedojde k uplatnění nástroje proti tomuto riziku (např. transferu nebo redukce). Pokud není riziko rozpoznáno, je nevědomě zadrženo.

Retence je vhodná tehdy, pokud se riziko nevyplatí odstínit, protože může způsobit velmi malou škodu anebo se vyskytuje v dostatečně dlouhých intervalech. Retence spojená s redukcí je vhodná tam, kde jsou rizika charakterizovaná nízkou tvrdostí a vysokou pravděpodobností ztráty. Redukce je zde vhodná zejména pro redukci celkového objemu ztrát, které je třeba snést.

Retence rizika může být rovněž dobrovolná nebo nedobrovolná. Dobrovolná retence rizik je charakterizována rozpoznáním rizika a jejím tichým souhlasem s převzetím v něm obsažené ztráty.

22 *[18] SMEJKAL (2006), str. 114*

Nedobrovolná retence rizik existuje tehdy, jsou-li rizika nevědomě zadržena anebo riziko nemůže být transferováno či redukováno anebo se mu nelze vyhnout.

3.9.2 Redukce rizika

Pro rizika charakterizovaná vysokou pravděpodobností a vysokou tvrdostí je retence nereálná. Pojištění také nepřipadají v úvahu pro své vysoké náklady způsobené velkou pravděpodobností a tak je nejvhodnější se riziku vyhnout, případně riziko redukovat.

Metody na redukci rizika lze rozdělit na dvě skupiny podle způsobu aplikování redukce rizika. Do první skupiny patří ty metody, které se snaží odstranit příčiny vzniku rizika a tak preventivně působí tak, aby byl eliminován nebo alespoň částečně redukován výskyt krizových situací. Do druhé skupiny patří metody, které snižují nepříznivé důsledky rizika způsobené výskytem nepříznivých situací a kterým se nelze v podnikání vyhnout.

Redukce a retence rizik patří do kategorie ofensivního řízení rizik, které jsou zásadním způsobem ovlivňovány managementem firmy.

3.9.3 Transfer rizika (pojištění)

Poslední skupinou jsou metody charakteristické defensivním přístupem k riziku, jsou to rizika spojená s nízkou pravděpodobnosti, ale vysokou tvrdostí. Vysoká tvrdost zde znamená katastrofální dopad, pokud se ztráta skutečně objeví. Nízká pravděpodobnost naplnění hrozby znamená nízkou očekávanou hodnotu ztráty a nízké náklady transferu. Tato rizika tak lze nejvhodněji řešit pomocí pojištění proti možnému riziku (například pojištění budovy proti riziku požáru).

3.10 Identifikace rolí a odpovědnosti uvnitř organizace

Pro úspěšné prosazování firemní bezpečnosti je nezbytné definovat potřebné pracovní role a odpovědnosti uvnitř organizace, včetně potřebných procesů, kterými jsou realizovány bezpečnostní principy a bezpečnostní opatření.

Na vrcholu prosazování firemní bezpečnosti musí stát hlavní bezpečnostní ředitel[23]. Je zodpovědný za celkovou bezpečnostní organizaci ve firmě. Jeho postavení musí být jednoznačně zafixováno v organizačním řadu, aby se předcházelo zbytečným sporům a nedorozuměním. U menších společností může být tato pozice přidělena některé z

23 *[15] MLÝNEK (2007), str. 40 ; [16] POŽÁR (2005), str. 73*

vedoucích pozic ve společnosti. Hlavní činností bezpečnostního ředitele je vytvářet bezpečnostní strategii a koordinovat a kontrolovat práci spolupracovníků.

Další složkou v pokračování hierarchie rolí uvnitř organizace je pracovní tým bezpečnosti, jehož hlavním úkolem je prosazování rozhodnutí bezpečnostního ředitele.

Tento tým může být podle velikosti firmy sestaven ze specialistů z oblastí zajišťování bezpečnosti, především specialistů na IT bezpečnost, fyzickou bezpečnost, personální bezpečnosti, atd. Přitom není nutnou podmínkou, aby všichni členové byli do pracovního týmu začleněni na plný úvazek.

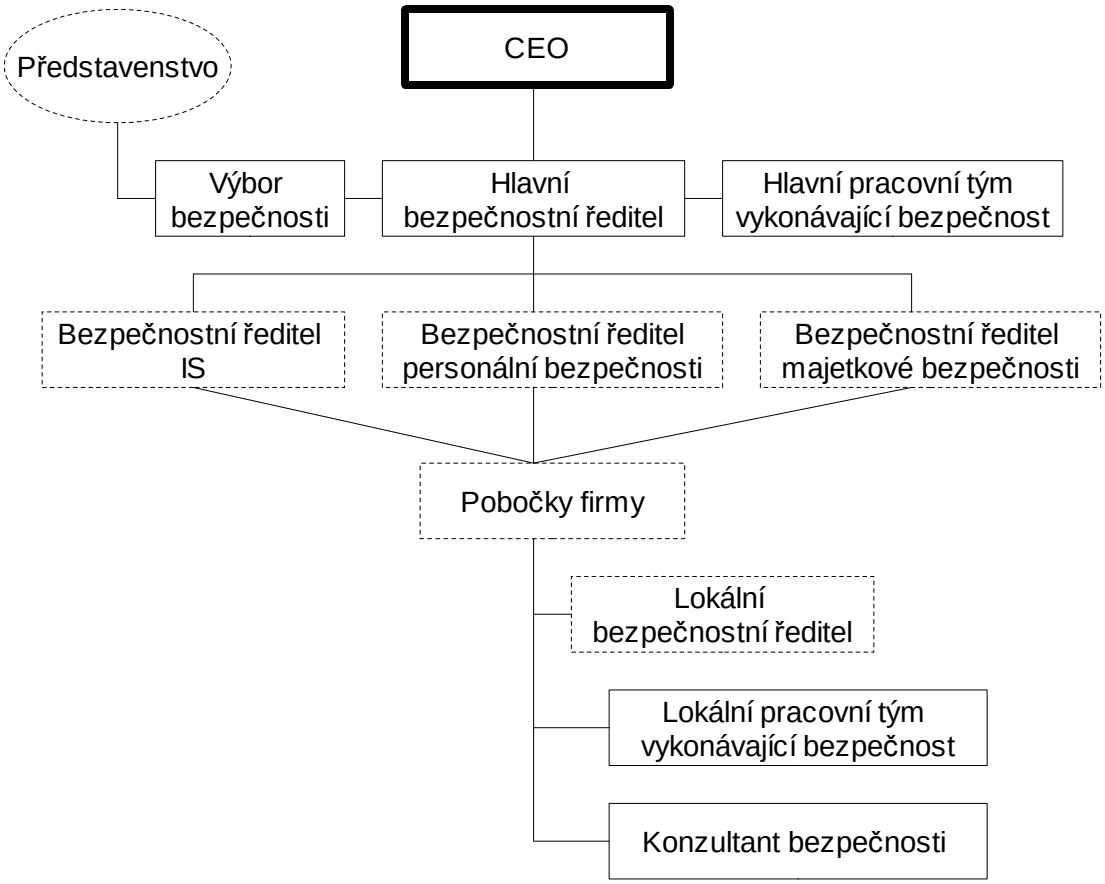
Pracovní tým vykonávající bezpečnost může být rozdělen na více části, jak ukazuje hierarchie na obrázku 5. Dle velikosti firmy a velikosti případných poboček je možné sestavit lokální týmy, které se starají o bezpečnost pobočky. Vykonávají úkoly nadřazeného (hlavního) pracovního týmu firmy. V rámci pobočky může existovat i lokální bezpečnostní ředitel, který podobně jako hlavní bezpečnostní ředitel dohlíží a koordinuje vykonávání bezpečnosti lokálního pracovního týmu.

Všichni pověření pracovníci týmu musí podle principu osobní odpovědnosti odpovídat za komplexní bezpečnost organizace. V určité míře do ní musí být zahrnuty všechny případy řešení bezpečnostní problematiky, včetně případů, kdy bezpečnostní opatření řeší, zajišťují nebo provádějí jiné úseky a jiní pracovníci. Kromě konkrétně zadaných kontrolních činností bezpečnosti je hlavní úlohou pracovníka týmu odborně dohlížet, navrhovat a vytvářet podmínky pro uskutečnění potřebných odborných opatření.

Další identifikace role v bezpečnosti podniku může být přiřazena konzultantovi bezpečnosti. Jeho úkolem je informovat o potřebách, nedostatcích a nových hrozbách v oblasti bezpečnosti s ohledem konkrétní pobočky, místní zákonů, atd.

POŽÁR[24] dále doporučuje zřídit bezpečnostní výbor za účelem umožnění vedoucím pracovníků iniciovat požadavky v oblasti bezpečnosti, vyjádřit se k návrhům bezpečnostního ředitele a projednat problematiku bezpečnosti ve vztahu k podřízeným útvarům (pobočkám).

24 *[16] POŽÁR (2005), str. 40*



Obrázek 5: Příklad rolí a orgánů bezpečnosti organizace

K zajištění řádného fungování těchto rolí musí být ze strany vedení zajištěny následující skutečnosti:

- Odpovídající postavení v organizační struktuře organizace, přesně stanovená působnost a pravomoci,
- určení kompetencí, práv a povinností,
- odpovídající materiální vybavení,
- dle potřeby personální obsazení podřízených funkcí,
- přesná specifikace vnitřních a vnějších vztahů,
- ohodnocení a sankce za prováděnou práci,
- definovaný časový rozsah pracovního úvazku.

3.11 Zhodnocení současného stavu bezpečnosti

Na základě vypracované analýzy rizik a sestavení rolí je dalším krokem k sestavení bezpečnostní politiky zhodnocení současného stavu bezpečnosti – bezpečnostní audit. V rámci bezpečnostního auditu by měl být analyzován skutečný aktuální stav implementace bezpečnostních opatření a mechanismů v různých oblastech organizace, jako je oblast technologická, personální, fyzická, organizační apod[25].

Výsledky stavů se porovnávají s interní nebo externí metrikou. Touto metrikou může být bezpečnostní politika organizace a s ní související interní dokumentace (směrnice, nařízení apod.) nebo relevantní bezpečnostní standardy, normy, technická a odborná doporučení a případně dodržování legislativy.

Výsledkem je hodnotící zpráva, která spolu s analýzou rizik a bezpečnostní politikou nastartuje změnové řízení ve firmě vedoucí k novému zabezpečení aktiv.

Cílem a přínosem bezpečnostní auditu je[26]:

- Zjištění aktuálního stavu podnikové bezpečnosti,
- identifikace nedostatků a rizikových faktorů,
- zvýšení bezpečnostního podvědomí v organizaci,
- nastartování komplexního řešení bezpečnosti,
- analýza potřebného rozpočtu pro změnové řízení.

25 *[17] SECUNET: Bezpečnostní audit. (online dokument)*

26 *[19] T-SOFT: Bezpečnostní audit IS/IT. (online dokument)*

3.12 Bezpečnostní normy

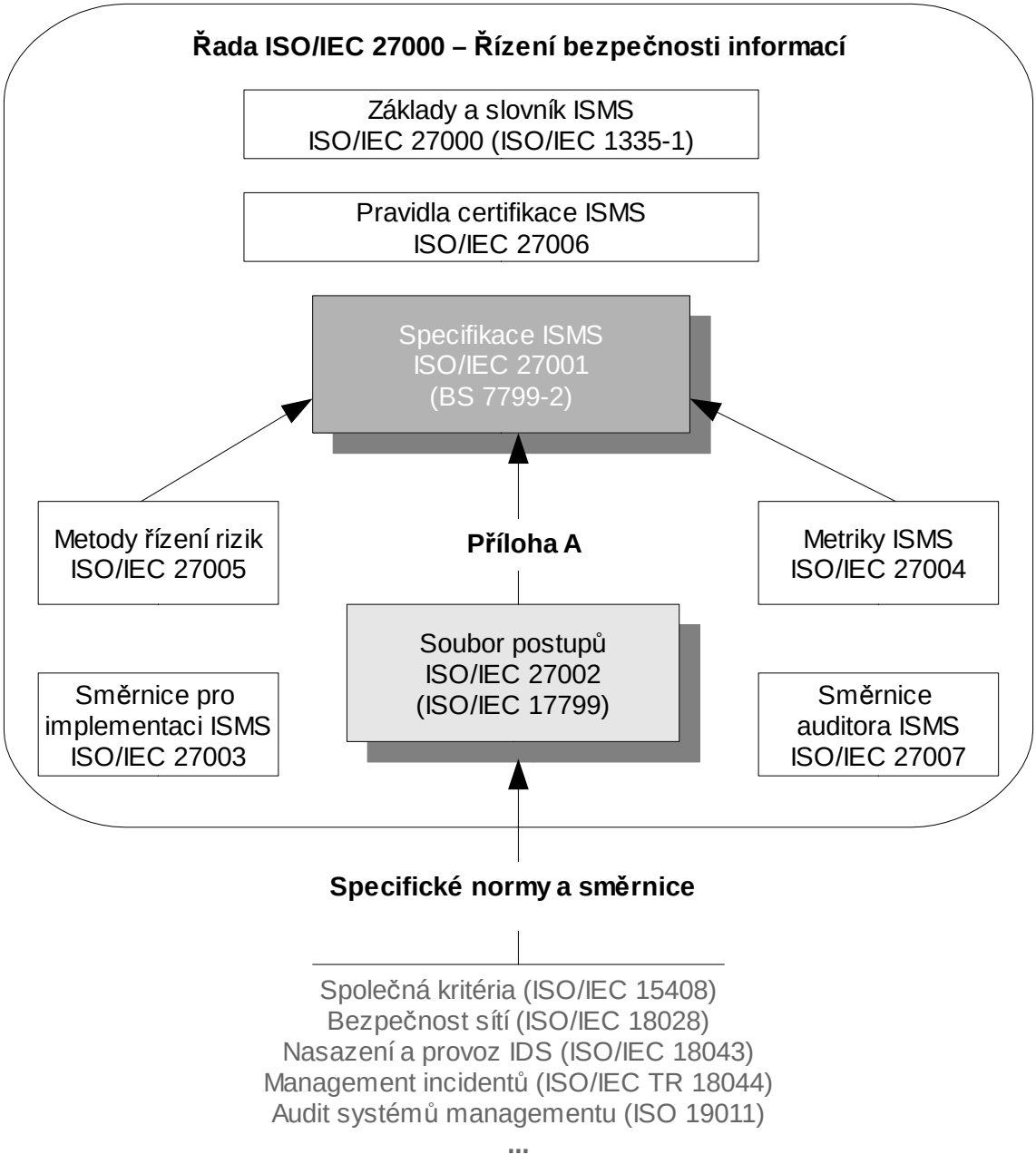
Významnou podporou pro zavádění systému bezpečnosti v organizaci jsou bezpečnostní standardy (normy) jako základní metodické nástroje. V oblasti zavádění informační bezpečnosti lze využít především normy ISO/IEC 17799 a ISO/IEC 27001. Tyto bezpečnostní normy umožňují sjednotit formy bezpečnostních opatření a přístupů k informační bezpečnosti využitím nejlepších zkušeností („best practices“) doporučených v příslušných normách. Implementace standardů však současně musí být konfrontována s realitou v dané organizaci.

Podle §4 zákona č. 22/1997 Sb. a předpisem č. 71/2000 Sb. se pojmem „česká technická norma“ označuje dokument schválený pověřenou právnickou osobou pro opakované nebo stálé použití, vytvořený podle výše uvedeného zákona, označený písmenným označením ČSN, jehož vydání bylo oznámeno ve Věstníku Úřadu pro technickou normalizaci, metrologii a státní zkušebnictví. Dále se stanoví, že česká technická norma není obecně závazná.

Normy a standardy tak vytvářejí určité východisko pro konkrétní implementaci systému řízení bezpečnosti v dané organizaci. Jde vlastně o nabídku technického řešení, která nemusí být využita.

Pro řešení bezpečnosti informací lze například využít série norem ISO 27000[27], viz obrázek 6.

27 *[8] DOUCEK (2008), str. 93*



Obrázek 6: Koncept série ISO 27000 pro ISMS

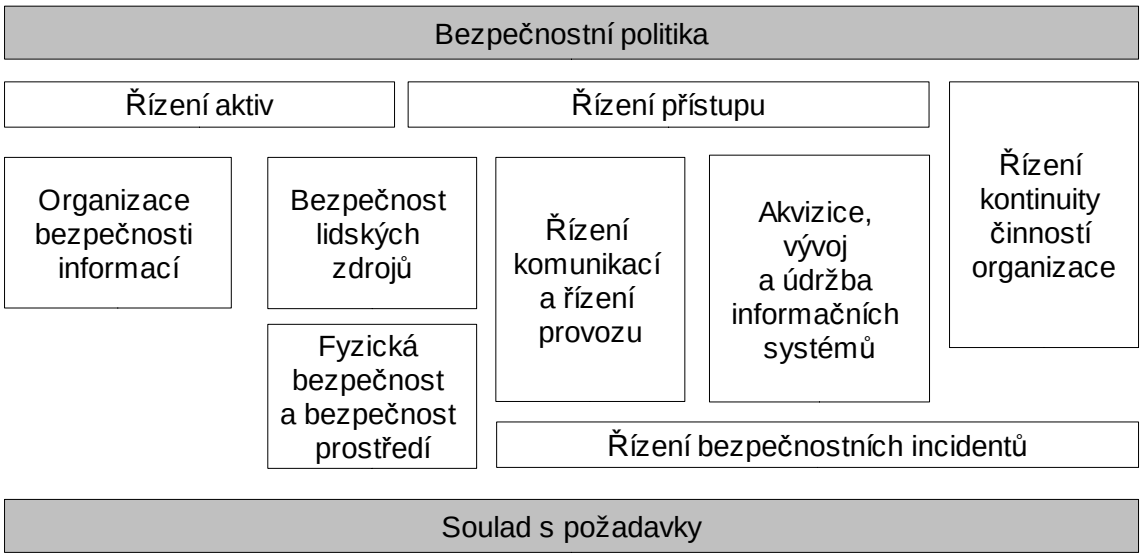
V rámci bezpečnosti informačních systémů jsou základními standardy v současné době následující normy[28]:

- Norma ISO/IEC 17799:2005 Information Technology – Security Techniques – Code of practice for Information Security Management.
- Norma ISO/IEC 27001:2005 Information Technology – Security Techniques – Information Security Management system – Requirements.

3.12.1 ISO/IEC 27002 – soubor postupů pro management bezpečnosti informací

Norma ISO/IEC 27002:2005 vychází z britské normy BS7799-1:1999 (resp. z následné mezinárodní normy ISO/IEC 17799:2000) a obsahuje soubor postupů pro řízení bezpečnosti informací v 11 oddílech a 39 oblastech bezpečnosti. Tento standard byl vytvořen soukromými společnostmi pod patronací British Standards Institution.

Norma popisuje nejlepší vžitou praxi („best practices“), norma z roku 2005 zahrnuje celkem 133 opatření. Jde o mezinárodně respektovanou soustavu doporučení. Jednotlivá opatření obsahují také popis způsobu implementace. Na obrázku 7 je uvedena hierarchie oblasti pro zabezpečení informace[29].



Obrázek 7: Rozdělení oblastí bezpečnosti informací v ISO/IEC 17799:2005

28 *[4] ČERMÁK (2007), str. 16*

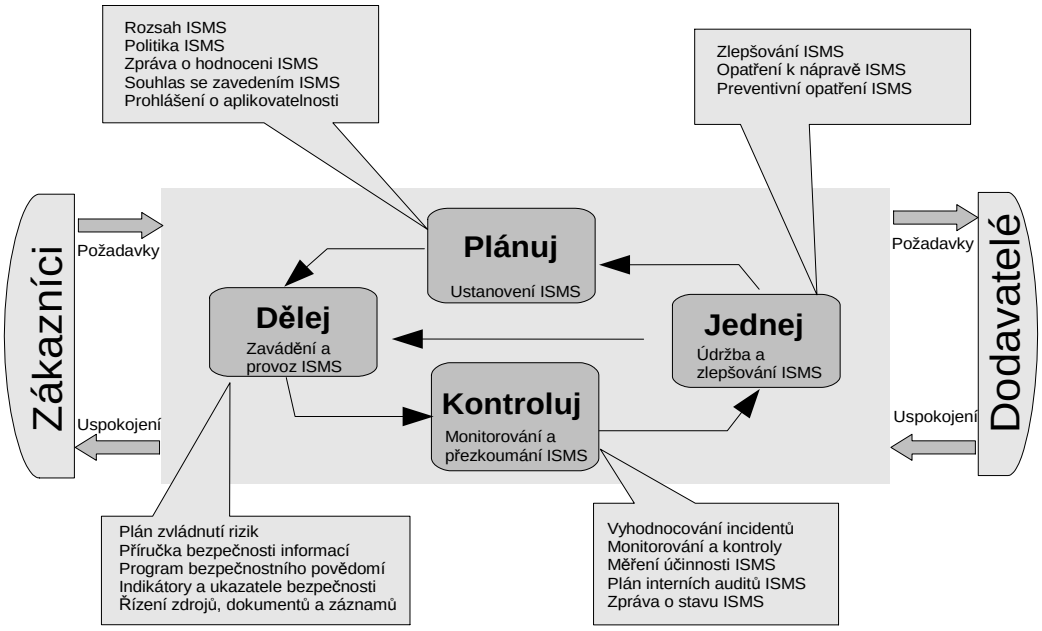
29 *[8] DOUCEK (2008), str. 131*

Předmluva normy upozorňuje na skutečnost, že další revize normy, plánovaná na rok 2007, vyjde jako ISO/IEC 27002. Český překlad normy pro edici 2005 vyšel v srpnu 2006 pod označením ČSN ISO/IEC 17799:2006.

3.12.2 ISO/IEC 27001 – Systém managementu bezpečnosti informací, požadavky

Norma ISO/IEC 27001:2005 (vycházející rovněž z britské normy BS7799-2:2002) obsahuje požadavky na systém řízení bezpečnosti informací (Information Security Management System - ISMS). Samotná norma podporuje procesní způsob řízení bezpečnosti, definuje metodický rámec řízení bezpečnosti jako procesu, ve kterém se na základě analýzy rizik vybírají opatření odvozené z normy ISO/IEC 17799:2005. Systém řízení bezpečnosti informací je zachycen na obrázku 8.

Na rozdíl od normy ISO/IEC 17799:2005 jsou požadavky v této normě formulovány jako povinné[30], podle normy ISO/IEC 27701:2005 také probíhá případná certifikace systému řízení bezpečnosti informací. Česká verze této normy označena jako ISO/IEC 27701:2006 vyšla v říjnu 2006.



Obrázek 8: Model řízení bezpečnosti informací

30 *[8] DOUCEK (2008), str. 95*

3.13 Zavádění bezpečnostní opatření

Dalším cílem po provedení analýzy rizik a bezpečnosti a zhodnocení aktuálního stavu je navrhnout postup k dosažení požadované úrovně zabezpečení pomocí bezpečnostních opatření a připravit tak prostředí pro udržování a zvyšování úrovně bezpečnosti. Některá bezpečnostní opatření mohou být realizována velmi rychle a s minimálními finančními náklady, aplikování jiných bezpečnostních opatření je náročnější časově a finančně a mohou být realizovány formou projektu[31].

Zaváděná bezpečnostní opatření by měla pokrývat všechny specifické oblasti firemní bezpečnosti, jakou jsou informační bezpečnost, majetková a personální bezpečnost. Pobočky nadnárodních firmy by při závádění bezpečnostních opatření měly vycházet z globální bezpečnosti politiky nadřazeného centra. Změny na základě lokálních podmínek by měly být projednány s konzultantem bezpečnosti a lokálním bezpečnostním ředitelem, po zpracování změnového řízení i s hlavním bezpečnostním ředitelem.

Bezpečnostní opatření lze dělit podle vztahu k případnému bezpečnostnímu incidentu na[32]:

- **Preventivní** – účelem je minimalizovat již samotné příčiny možného vzniku bezpečnostního incidentu,
- **dynamická (proaktivní)** – účelem je minimalizovat možné dopady aktuálně probíhajícího bezpečnostního incidentu, včetně zachyceného vzniku takového incidentu,
- **následná (reaktivní)** – účelem je minimalizovat možné dopady proběhlého bezpečnostního incidentu.

Mezi obecné bezpečnostní opatření firmy patří mimo jiné i pravidelné ověřování funkčnosti a aktualizace havarijních plánů obsažených v bezpečnostní politice a také pak následující skutečnosti:

Pravidelná školení zaměstnanců o bezpečnostní politice a bezpečnosti práce – za účelem udržování povědomí o bezpečnostní politice mezi zaměstnanci a sníženi rizika výskytu bezpečnostního incidentu.

31 *[15] MLÝNEK (2007), str. 61*

32 *[10] GÁLA (2006), str. 384*

Sestavení dokumentu pro libovolné změnové řízení – například při provádění aktualizace stávájícího software, zavádění nového informačního systémů, hardware a nových pracovních postupů. Součástí změnového řízení by měly být také stanoveny potenciální účinky dané změny a postupy určení odpovědnosti pro pro případ havarie, včetně sestavení havarijního plánu pro případ obnovy.

Pravidelné kontroly a údržby elektrických a neelektrických zařízení – součástí tohoto opatření je kontrola a údržba všech počítačových systémů (pravidelné čistění od prachu a nečistot včetně kontroly diskových medií), údržba elektromechanických částí založených na pohybu (ventilátory, motory, aj.) a dalšího elektronického vybavení firmy, které zanedbáním údržby může způsobit bezpečnostní incident. Pravidelná kontrola se musí zabývá také údržbou neelektrických zařízení, jako jsou hasicí přístroje, a kontrolou zabezpečení podniku včetně alarmů.

Kontroly služeb poskytovaných třetí stranou – je žádoucí provádět kontroly činností, které vykonává pro společnost externí firma (včetně outsourcingu), zda v jsou v oblasti bezpečnosti dodržovány povinnosti vyplývající z platné legislativy a smluvního ujednání mezi oběma stranami.

Uplatňování principu strukturované hierarchie funkcí uvnitř firmy – společnost v rámci svých schopností by měla udržovat funkční rozdělení rolí uvnitř podniku a zamezit prolínání funkcí. Pokud tak není, dochází k zvýšení rizika bezpečnostních incidentů[33].

3.14 Bezpečnostní opatření pro informační bezpečnost

V bezpečnostní politice podniku musí být uvedeny také metody pro bezpečnostní opatření k zachování bezpečnosti informací. V rámci informační bezpečnosti je třeba řešit i bezpečnost IS/ICT. V informační bezpečnosti navíc oproti bezpečnosti IS/ICT je vhodné řešit tyto bezpečnostní opatření:

Omezení přístupu k podnikovým nedigitálním informacím - omezit přístup jen pro určené osoby dle jejich pravomocí, pomocí bariér jako jsou uzamykatelné skříňky či trezory. Tato omezení mohou být řešena i umístěním dokumentů v externích organizacích, například určených pro dlouhodobou úschovu dokumentů. Přesun citlivých firemních dokumentů do těchto externích organizaci může být výhodné jak pro kvalitnější, tak i bezpečnější dlouhodobou ochranu než v samotném podniku.

33 *[15] MLÝNEK (2007), str. 62*

Způsob zpracování a zálohovaní nedigitálních dat – opatření mohou být řešena jejich kopií nebo převodem do digitální podoby pro zachování integrity a dostupnosti informací. Takto převedené digitální dokumenty lze ochránit vhodným kryptováním nebo přístupovými právy.

Měla by také být zavedena školení pro účelné veřejné vystupování pracovníků organizace při styku s externími subjekty, dodavateli, zákazníky, atd.

V bezpečnostní politice by měla být vyřešena vhodná metodika pro bezpečný transport a nakládání se všemi podnikovými informacemi, včetně zásad skartace a likvidace informací, ať v papírové či digitální podobě, (tedy všech přenosových medií jako diskety, CD/DVD, flash disky a všech tištěných dokumentů v jakékoliv podobě).

3.15 Bezpečnostní opatření pro bezpečnost IS/ICT

K bezpečnostním opatřením pro zabezpečení IS/ICT mohou patřit následující postupy a odpovědnosti:

Ochrana proti škodlivému software – opatření mají zajistit integritní ochranu a dostupnost informací a software. Uživatelé by měli být informování o nebezpečí škodlivého software a neměli by bránit funkčnosti kontrolních prostředků a programů k prevenci a detekování škodlivého software. Opatření jsou zaměřena na prevenci, detekci a případné ošetření poškozených informací.

Zálohování digitálních informací – jednou z nejúčinnějších ochran pro zajištění ochrany integrity a dostupnosti informací je jejich cílené zálohování. Má-li být zálohování smysluplné, musí být stanoven plán zálohování. Klíčové problémy jsou volba vhodného média, volba plánu zálohování (správná četnost záloh podle objemu změn) a volba místa uložení záloh (ne u místa originálních dat, atp.)[34]

Pravidelné stahování bezpečnostních záplat – opatření mají vynutit aktivaci stahování a aktualizaci bezpečnostních záplat. Moderní operační systémy umožňují automatickou kontrolu dostupných aktualizací a jejich instalaci téměř bez vědomí uživatele. Pravidelnost kontroly dostupnosti závisí na tom, jak často je systém připojen k internetu[35].

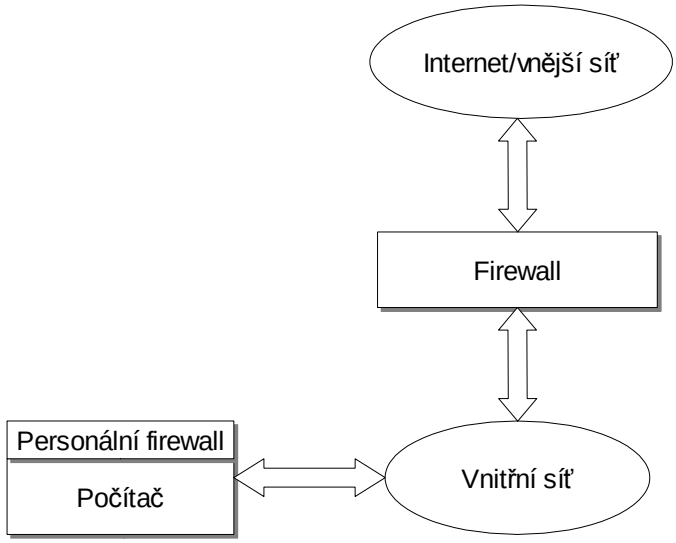
34 *[13] KOCH (2004), str. 161*

35 *[7] DOSEDĚL (2005), str. 20-21*

Systém kontrol a plánovaní vytížení výpočetních prostředků – bezpečnostní opatření by měla obsahovat pravidelnou kontrolu výpočetních prostředků, co se týká množství aktuálních volných paměťových kapacit a budoucích plánů rozvoje informačních systémů a výpočetních prostředků.

Vedení bezpečnostních záznamů – za účelem monitorování a vyhodnocování aktivit uživatelů vytváříme tzv. auditní záznamy[36], aby bezpečnostní pracovníci později věděli, co se v průběhu práce v systému dělo. Je to protokol se záznamy, který se zkoumá po bezpečnostním incidentu. Součástí každého záznamu je čas akce, program, který tento zápis vyvolal a popis akce, která k záznamu vedla, včetně položek o připojených uživatelích a spuštěných programem. Záznamy mohou také obsahovat neoprávněné pokusy o otevření souboru, přístup do adresářů jiných uživatelů, neoprávněná přihlášení do systému.

Řádně umístěný a nainstalovaný firewall – (obrázek 9). Firewall by měl být nainstalován, spuštěn a správně nakonfigurován na každém počítači včetně serveru, u kterého očekáváme připojení k internetu mimo chráněnou firemní síť. Výhodou těchto personálních firewallu je schopnost chránit počítač také v případě, když se ocitne mimo vnitřní chráněnou síť[37]. Dobře nakonfigurovaný Firewall umí ochránit jak vnitřní síť, tak může obsahovat antivirové programy, spam filter, ochranu proti DoS útoku apod.



Obrázek 9: Umístění firewallu

36 *[6] DOSEDÉL (2004), str. 49-50*

37 *[6] DOSEDĚL (2004), str 120-121*

Bezpečné používáni emailu – opatření souvisí s bezpečným používáním emailu uvnitř organizace i vně využitím vhodných softwarových nástrojů kombinujících případné kryptografické nástroje, včetně zákazu otvírání nevyžadovaných emailových příloh, které mohou složit k šíření virů.

Oddělení vývojového a provozního prostředí – pro zamezení incidentů je žádoucí oddělit prostředky vývojové centra od provozního prostředí, tj. rozdělit vývojový a provozní software na různé počítače včetně oddělení vývojových a provozních činností a vzájemných přístupů.

Instalace povoleného a ověřeného software – na každém počítači by měl být instalován jen software schválený a ověřený bezpečnostním ředitelem nebo bezpečnostním týmem. Instalace jiného software může způsobit bezpečnostní ohrožení, obzvláště pokud se vydávají za software, který má chránit počítač, jakou jsou anti-vírové, anti-spamové a anti-adware programy[38], které ve skutečnosti slouží k šíření malware na počítači.

Používání zabezpečeného přenosu dat – při přenosu dat prostřednictvím počítačové sítě se používají takzvané komunikační protokoly. Jiný protokol se používá pro odesílání a příjímání elektronické pošty, zcela jiný zase pro přenos souboru, další pro stahování internetových stránek a podobně[39]. Takto existuje celá řada nezabezpečených počítačových protokolů, kde datový tok je nezabezpečený a může být lehce odposloucháván. V případě přenosu citlivých dat je nutné používat zabezpečený přenosový kanál k zamezení odposlechu a zneužití získaných dat.

Fyzické zabezpečení komunikačních zařízení v sítí LAN - Lokální síť lze zabezpečit proti cizím potenciálně nezabezpečeným počítačům ochranou komunikačních portů, kdy se například znemožní použití prázdných zásuvek síťového provozu. Další vylepšenou variantou je řízení připojení do sítě, povolení připojení „cizího“ zařízení do sítě až jejím správcem. Třetím druhem je zabezpečení samotných kabelových spojů umístěním kabelových rozvodů tak, aby se na tyto spoje nemohl neoprávněný subjekt napojit[40], případně aby nebyly rušeny silovými rozvody. Pro sítě WLAN je nutné navíc zavést šifrování přenosu komunikace vhodným bezpečnostním standardem (např. WAP), neboť bez zabezpečení je možný mnohem jednodušší odposlech dat.

38 *[14] MACICH. Falešné antiviry obtěžují také české uživatele. (online dokument)*

39 *[6] DOSEDĚL (2005), str. 102*

40 *[16] POŽÁR (2005), str. 127-128*

3.15.1 Zavedení principu řízení přístupu

Přístup k informačním systémům je zapotřebí chránit z mnoha důvodů. Toto může vyplývat ze samotné podstaty ochrany informací a dat umístěných v informačních systémech, hierarchie pracovních rolí, atd. Proces, který povolí přístupu k informačnímu systému, se nazývá proces řízení přístupu.

Z hlediska fungování se řízení přístupu opírá o tři základní prvky, které jsou **identifikace**, **autentizace** a **autorizace**. V praxi to funguje tak, že libovolný uživatel, který se snaží přistoupit k nějakému objektu, se nejdříve identifikuje, tj. sdělí informačnímu systému svoje jméno ve formě LoginID. Tato informace je následně ověřena autentizací. Nejčastěji formou je vyzvání uživatele k zadání hesla. Existují i jiné možnosti, např. biometrika, kde se proces identifikace a autentizace spojuje dohromady.

Autorizace je poslední fází řízení přístupu, kdy se na základě prokázané identity ověřuje, zda má konkrétní entita nastavená oprávnění k provedení požadované akce[41].

Při autentizaci heslem je nutná pravidelná obměna hesel, aby se preventivně zabránilo přístupu nepovolaným osobám, které získaly v minulosti přístupové heslo. Také je nutné změnit přístupová hesla do systémů kdykoliv při podezření úniku hesla.

Vhodným bezpečnostním opatřením ze strany informačních systémů je tato nevyhnutelná a pravidelná změna hesla vyžadovaná po uživateli, včetně kontroly níže uvedených kriterií na bezpečnost hesla.

Pro vytvoření bezpečného hesla platí obecně tato pravidla:[42]

- Heslo musí obsahovat minimálně 8 znaků, nejlépe 14 a více znaků.
- V hesle se musí střídat malá a velká písmena.
- Heslo musí obsahovat speciální znaky.
- Heslo nesmí mít přímý význam ve slovníku, tedy nesmí dávat žádný smysl, nesmí být slovem.
- Heslo nesmí být údajem z okolí, například rodné číslo, datum narození, telefonní číslo, jména rodinných příslušníků, atd.

41 *[8] DOUCEK (2008), str. 144*

42 *[3] CAHA (2008), str. 11 (online dokument)*

3.16 Bezpečnostní opatření pro majetkovou bezpečnost[43]

K hlavním úkolům každého podniku patří nesporně vnější (obvodová) ochrana vlastních nebo užívaných objektů. Základem takovéto ochrany je zpravidla fyzická ochrana objektů doplňována technickými prostředky ochrany, ať mechanickými či elektronickými. Tato ochrana nespočívá v přímém odhalování spáchaných protiprávních jednání (přestupků či trestných činů), ale sehrává významnou úlohu v prevenci proti nim.

3.16.1 Metody fyzické ochrany

Z hlediska fyzické ochrany a ostrahy objektů lze definovat následující formy bezpečnostních opatření:

- **Strážní služba –** nepřetržité trvání v určitém časovém úseku s vymezením pevné nebo pohyblivé strážní stanoviště).
- **Bezpečnostní dohled –** např. při zabezpečování pořádku, bezpečnosti v obchodech, kasínech, stanovišť, atd.
- **Bezpečnostní ochranný doprovod –** doprovod osob, peněžních hotovostí, kamionové přepravy).
- **Kontrolní propustná služba –** zabránění propuštění osob a vozidel bez platného oprávnění, vedení knihy příchodů a odchodů, zabránění vnášení a vynášení předmětu z/do podniku, atd.
- **Bezpečnostní výjezd –** zásahová skupina, hlídka nebo pracovník podle stupně rizika na základě informace o narušení z elektronického zabezpečovacího systému vyjíždí na místo předpokládaného narušení.

3.16.2 Metody technické ochrany

Technická ochrana objektu představuje systémy a komponenty, pomocí nichž se vytvářejí relativně stále podmínky bránící nepovolaným osobám vniknout do chráněného objektu. Tyto systémy jsou složeny z různých technických zábran, které brání napadení objektu či proniknutí nepovolaných osob do objektu či chráněného prostoru (servery, místnosti, objekty atd.).

43 *[2] BRABEC (1996), str. 97-150*

Tato ochrana bývá zpravidla kombinována s metodami elektronické ochrany. Jako prostředky této metody se používají kovové mříže, mechanické bezpečnostní zámky, bezpečnostní dveře, bezpečnostní skla, bezpečnostní uzamykatelné systémy, úschovná místa, atp.

3.16.3 Metoda elektronické ochrany

Jde o systémy elektronické zabezpečovací signalizace, protipožární signalizace a elektronické signalizace různých stavů. Prvně jmenované systémy, elektronické zabezpečovací signalizace, plní úkoly preventivní (viditelné umístění některých prvků, či atrap odvracejí úmysl potenciálních pachatelů), také mohou informovat o narušení objektu, ztěžují nebo znemožňují neoprávněný pohyb v prostoru, atp.

Elektronické signalizace různých stavů mohou být sestaveny z čidel (tlaku, teploty, pohybu, úniku plynů, kapalin, tlaku), detektorů pohybu, elektronických zámků, požární signalizace, tísňových hlásičů, systémů ochrany vozidel atd.

V souvislosti s elektronickou ochrannou objektů je třeba si uvědomit dvě významné skutečnosti: neutrálnost elektronických zabezpečovacích systémů, kdy je vyloučen subjektivní lidský faktor a druhá skutečnost, kdy účinnost elektronické ochrany lze dosáhnout jen v návaznosti na fyzickou ochranu. Samotné elektronické systémy nestačí, např. nenavazuje-li signál o narušení objektu na zásah fyzické ochrany.

Pro řádný chod podniku může být žádoucí zavedení ochrany podpůrnými zařízeními, co např. zajišťuje nepřetržitou dodávku nezbytné elektrické energie, např. pomocí tzv. UPS. Některá zařízení mohou být závislá i na dodávce chladícího média jako je např. voda nebo některé plyny[44].

3.16.4 Metoda elektronického pozorování

Metodou je zajišťována ochrana objektů s využitím videokamer a elektronických dokumentačních prostředků. Mají především význam pro orgány činné v trestním řízení jako dokumentační prostředek, ale také mohou posloužit k dohledu bezpečnosti v podniku, který je realizován pomocí pracovníků fyzické ochrany, kteří v rámci realizace různých metod fyzické ochrany sledují situaci v těchto prostorách na monitoru.

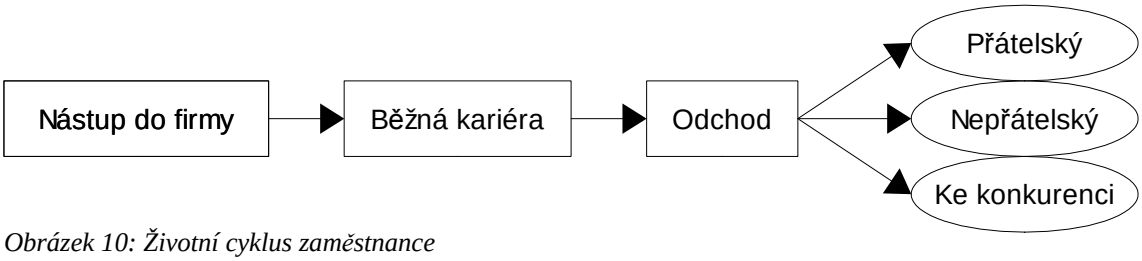
44 *[8] DOUCEK (2008), str. 141*

3.17 Bezpečnostní opatření pro personální bezpečnost

Personální bezpečnost z hlediska řízení lidských zdrojů se dotyká všech minulých, současných a budoucích zaměstnanců podniku, včetně pracovníků smluvních stran. Proto, aby byla zajištěna přiměřená úroveň bezpečnosti, je nutné provádět prověrky nových pracovníků či pracovníku smluvních stran. To zahrnuje jednoduché techniky, jako je ověření identity podle dokladů, ověření dokladů o vzdělání či o absolvovaných školeních, apod. Vyšší úrovní může být provedení analýzy osobnostního profilu, prověření referencí nebo kontrola obchodního rejstříku či rejstříků úpadců[45].

Mezi další bezpečnostní opatření při zavádění nového zaměstnance patří spolupráce personálního oddělení s oddělením IT. Obvykle po příchodu nového zaměstnance do podniku je nutno zřídit mu emailový účet, přidělit heslo, klíče, případně přidělit pracovní počítač a nainstalovat potřebný software, v neposlední řadě poskytnout řádné bezpečnostní školení.

Ve spojitosti s kariérním růstem musí být přidělována či odebírána oprávnění do různých částí informačního systému[46]. Takto každý zaměstnanec projde za svou firemní kariéru několika fázemi, což se nazývá životní cyklus zaměstnance, viz obrázek 10.



Obrázek 10: Životní cyklus zaměstnance

Poslední fází z pohledu bezpečnostních opatření je rozvázání pracovního poměru. Lze rozlišit tři druhy odchodů zaměstnance[47]:

- **přátelský –** zaměstnanec rozvázal pracovní poměr bez jakýkoliv problémů. Nemusí se tak očekávat, že by se pokoušel firmu po svém odchodu poškodit, vyloučit však nelze pokusy o pomstu vůči bývalému zaměstnavateli.

45 *[8] DOUCEK (2008), str. 139*

46 *[6] DOSEĎEL (2004), str. 178*

47 *[6] DOSEĎEL (2004), str. 180*

- **nepřátelský** – je vhodné očekávat, že se podle svých možností a schopností pokusí o pomstu.
- **konkurenční** – zaměstnanec byl „přetažen“ konkurencí. Lze očekávat, že se nebude pokoušet přímo o pomstu, možná ale nebude mít zábrany použít informace, které při své práci získal, případně které má možnost získat i po svém odchodu.

V rámci bezpečnosti je důležité prosadit vnitrofiremní proces, který bude řešit stav odchodu zaměstnance a kde by měly být přesně definovány úkony, které je nutno provést.

Kromě fyzického odebrání počítače a jeho případné reinstalace pro nového zaměstnance je třeba zrušit oprávnění v informačních systémech, zrušit nebo zapnout přeposílání emailů z poštovní schránky, změnit případná hesla, ke kterým měl zaměstnanec přístup, vyřadit adresu jeho notebooku z firewallu apod. Je zkrátka nutno odebrat všechna oprávnění, která zaměstnanec za svou kariéru ve firmě nasbíral.

4 NÁVRH ŘEŠENÍ

Z důvodu absence komplexní bezpečnostní politiky navrhuji vytvořit jak obecnější celkovou formu bezpečnostní politiky tak i dokument systémové bezpečnostní politiky. Návrh dokumentů jsem připravil v následujících podkapitolách, při vytváření návrhu jsem vycházel z poznatku čerpaných z teoretické části práce.

V první části návrhu řešení jsem sestavil obecná ustanovení, návrh dále pokračuje analýzou aktiv podle metodiky CRAMM. Identifikoval a ohodnotil jsem tak aktiva, sestavil je do společných skupin a stanovil hrozby, včetně možného řešení rizik pro tyto aktiva. Výsledkem analýzy byly společně s doporučenou informační bezpečnostní politikou firmy Advantech Europe, obecných doporučení normy ISO/IEC 27001 a ISO/IEC 27002 a aktuální analýzou stavu (uvedenou v přední části práce, kap. 2.2, str. 13) navrhnuta nová opatření. V závěru jsem také sestavil odpovědnostní role pro kontrolu a vykonávání navržených opatření.

4.1 Obecná ustanovení bezpečnostní politiky

4.1.1 Prohlášení k vedení firmy

V zájmu vedení firmy Advantech Czech s.r.o. musí být prosazování bezpečnostní politiky a všech její části. Účelem těchto bezpečnostních činností je nastolit a udržovat požadovanou míru fyzické, informační i personální bezpečnosti v celé pobočce firmy všemi zaměstnanci a externími subjekty[48].

Firma musí poskytnout veškeré nutné prostředky pro vytvoření požadované míry bezpečnosti, od subjektů firmy je však požadováno úplné dodržování této bezpečnostní politiky. V opačném případě má vedení firmy povinnost subjekty sankcionovat. Součástí bezpečnostní politiky firmy je i závádění kontrol a pravidelná školení, která mají za úkol dále prohlubovat a ověřovat kvalitu a dodržování bezpečnostní politiky ve firmě.

Součástí navrhované celkové bezpečnostní politiky by měly být dokumenty definující obecnou bezpečnostní politiku, která je platná pro všechny subjekty a systémovou bezpečnostní politiku, která je určena vybraným subjektům v ní popsané.

48 *V dalším textu se interní zaměstnanci firmy a zaměstnanci z externích firem budou považovat za jeden celkový pojem a to subjekt.*

4.1.2 Stanovení odpovědnosti a rolí

Vzhledem k velikosti pobočky a počtu zaměstnanců navrhuji, aby roli bezpečnostního ředitele vykonával nadále vedoucí pobočky, který je zodpovědný za vytváření a koordinaci bezpečnostní strategie včetně kontroly bezpečnosti.

Další odpovědnostní složkou by měl být pracovník, jehož úkolem by mělo být zavádění bezpečnostní politiky, včetně provádění pravidelných kontrol a vyhodnocování záznamů pro bezpečnostního ředitele. Tomuto pracovníkovi by měl být přidělen konzultant bezpečnosti a jeho zástupce v jedné osobě, který by spolu s ním měl připravovat zprávy o potřebách, nedostatcích a nových hrozbách, které jsou souhrnně připravovány pro vyhodnocení bezpečnostním ředitelem.

Většinu operací související s kontrolou a vykonáváním bezpečnosti by měl vykonávat bezpečnostní pracovník, konzultant by jej však v případě nepřítomnosti měl plně na požadovanou dobu nahradit. Oba tito pracovníci by vykonávali příkazy lokálního bezpečnostního ředitele. Ten však má za úkol zpracovávat nařízení vyššího vedení Mnichovské pobočky.

U obou těchto pracovníků je vhodné vyžadovat vysokoškolské vzdělání v oboru informačních technologií, neboť jak vyplynulo z analýzy, informační zabezpečení firmy je z větší části postaveno na zabezpečení počítačové techniky, které vyžaduje jak odborný lokální přístup tak i zkušenosti v oboru.

4.1.3 Proces řízení bezpečnostní dokumentace

Navrhuji, aby sestavením a aktualizací dokumentu bezpečnostní politiky firmy byl pověřen bezpečnostní pracovník, včetně bezpečnostního konzultanta. Výsledný dokument nebo sada dokumentů musí být ověřena a zhodnocena bezpečnostním ředitelem, který mimo jiné vydává rozhodnutí o provádění změn a sestavení prováděcího plánu.

Výjimky pro řešení krizových situací má právo vydávat pouze bezpečnostní ředitel nebo jeho zástupce, případně vyšší organizační složka. Dokumentace musí podléhat pravidelné aktualizaci, včetně analýzy aktiv, jak je naznačeno dále v textu. Tato aktualizace musí být zaznamenána a schválena. Navrhuji, aby se aktualizace bezpečnostních dokumentů prováděla každoročně a nepravidelně, při jakékoliv významné změně ve skladbě a množství firemních aktiv.

4.2 Realizace analýzy aktiv

Rozsahy všech části bezpečnosti politiky jsem zvolil vzhledem k zadání pouze na bezpečnost české pobočky firmy Advantech.

4.2.1 Identifikace aktiv

Aktiva firmy jsem rozdělil do skupin podle podobných nebo společných vlastností na:

- **Informace v elektronické podobě a v tištěné podobě** – do této skupiny jsou zařazeny veškeré informace, které jsou zpracovávány nebo uchovávány v podniku v digitalizované a tištěné podobě, jedná se o nejrůznější části účetních knih, papírové smlouvy, docházka a podobně.
- **Finance –** v této skupině jsou taková aktiva, která jsou bezprostředně spojena s peněžní stránkou firmy, patří sem finanční transakce, bankovní účet, pokladna atd.
- **Mentální aktiva –** do této skupině jsou zařazena dvě aktiva, ztráta know-how a poškození image firmy.
- **Majetek –** v této skupině jsou uvedena majetková aktiva, která působením hrozby mohou ohrozit nebo omezit chod pobočky.

4.2.2 Ohodnocení aktiv

Aktiva firmy byla ohodnocena podle stupnice čísel od jedné do pěti, jak bylo představeno v kapitole 3.5. Pro lepší přehlednost jsem barevně rozlišil jednotlivé skupiny, jak ukazuje tabulka 4.

Při ohodnocení jsem se také snažil vzít v potaz lokalizaci jednotlivých aktiv, která jsem také ohodnotil. Výsledek pro všechny tři sledované složky aktiva je zprůměrován a je uveden ve stejném řádku společně s aktivem. Poslední sloupec uvádí výslednou známku hodnocení aktiva, výsledky jsou uvedeny v tabulce 5.

Rozsah hodnot	Barva	Úroveň dopadu
<0 - 1,5)	šedá	**Žádný dopad na organizaci**
<1,5 -2,5)	fialová	**Zanedbatelný dopad na organizaci**
<2,5 -3,5)	zelená	**Potíže či finanční ztráty**
<3,5 -4,5)	oranžová	**Vážné potíže či podstatné finanční ztráty**
<4,5 – 5,0)	červená	**Může znamenat existenční potíže organizace**

Tabulka 4: rozsah a barevné rozlišení stupnice

Skupiny	Aktiva	Důvěryhodnost	Integrita	Dostupnost	Celková váha
Informace v elektronické a tištěné podobě	**Faktury**	**2**	**4**	**3,3**	**3,11**
	SAP	2	4	3	
	Účetní firma	2	4	3	
	Seznam v Excelu	2	4	4	
	Seznam závazků	**2**	**4**	**3,3**	**3,11**
	SAP	2	4	3	
	Účetní firma	2	4	3	
	Seznam v Excelu	2	4	4	
	Informace o obchodních partnerech	**3,5**	**2,5**	**3**	**3,00**
	NB šéfa	4	3	3	
	SAP	3	2	3	
	Skladové informace Lokální server	**2**	**2**	**2**	**2,00**
	Výrobní data	**3,66**	**3**	**3,33**	**3,33**
	Tištěná podoba	4	2	3	
Informace v elektronické a tištěné podobě	Lokální počítače	3	3	3	
	Lokální server	4	4	4	
	Seznam pohledávek	**2**	**4**	**3**	**3,00**
	SAP	2	4	3	
	Seznam v Excelu	2	4	3	
	Účetní knihy	**3**	**3,5**	**3**	**3,16**
	Účetní firma (fyzická kopie)	3	3	3	
	Seznam v Excelu	3	4	3	

Skupiny	Aktiva	Důvěryhodnost	Integrita	Dostupnost	Celková váha
	Výplatní pásky	**4,5**	**3**	**3,5**	**3,66**
	NB šéfa	5	3	4	
	Účetní firma	4	3	3	
	Docházkové listy Tištěná podoba	**1**	**2**	**1**	**1,33**
	Tištěné smlouvy Tištěná podoba	**4**	**4**	**3**	**3,66**
	Ztráta/Vyzrazení hesel	**4**	**3**	**2**	**3,00**
Finance	**Krádež pokladny**	**2**	**2**	**3**	**2,33**
	Valutová pokladna Kurzová ztráta	**4**	**4**	**3**	**3,66**
	Bankovní deposit (krach banky)	**4**	**4**	**5**	**4,33**
Mentální aktiva	**Ztráta know-how**	**5**	**5**	**4**	**4,66**
	Ztráta dobrého jména firmy	**4**	**4**	**4**	**4,00**
Majetek	**Znehodnocení licence klíčového software**	**4**	**4**	**4**	**4,00**
	Narušení lokálního serveru	**5**	**4**	**3**	**4,00**
	Ztráta VOIP	**2**	**2**	**2**	**2,00**
	Ztráta telefonního/faxového spojení	**2**	**2**	**2**	**2,00**
	Ztráta internetové konektivity	**3**	**3**	**4**	**3,33**
	Krádež skladových zásob	**2**	**2**	**2**	**2,00**
	Odcizení/poškození šéfova notebooku	**5**	**5**	**4**	**4,66**
	Odcizení/poškození lokálního PC/notebooku	**4**	**4**	**4**	**4,00**

Tabulka 5: Hodnocení aktiv metodou CRAMM

4.2.3 Seskupení aktiv

Na základě získaných informací z tabulky 5 jsem jednotlivá aktiva seskupil do společných skupin podle zaměření a podobné společné váhy ohodnocení. Dále však jsou uvedena jen ta aktiva, u kterých přesáhlo celkové hodnocení stupně 2 a více.

Výsledek sestavení zobrazuje následující tabulka 6, kde číslo v posledním sloupci uvádí společnou výslednou celkovou váhu, která byla sestavena jako průměr jednotlivých výsledných známek. Jednotlivá aktiva také získala nový společný název a jména skupiny byla nahrazena podle těchto zkratek: **I** - informace, **F** – finance, **K** – mentální část, **P** – majetek. Data jsou seřazena v každé skupině dle nejvyšších známek.

Pořadí	Skupina	Aktiva	Společný název	Váha
1.	K	Ztráta know-how	**Ztráta know-how**	**4,66**
2.	M	Odcizení/poškození šéfova notebooku	**Šéfův notebook**	**4,66**
3.	F	Bankovní deposit (krach banky)	**Bankovní deposit**	**4,33**
4.	K	Ztráta dobrého jména firmy	**Dobré jméno firmy**	**4,00**
5.	M	Narušení lokálního serveru	**Lokální server**	**4,00**
6.	M	Odcizení/poškození lokálního PC/notebooku	**Firemní počítač**	**4,00**
7.	M	Znehodnocení licence klíčového software	**Licence klíčového software**	**4,00**
8.	F	Valutová pokladna	**Valutová pokladna**	**3,66**
9.	I	Tištěné smlouvy, výplatní pásky	**Citlivé firemní informace, kategorie I**	**3,66**
10.	M	Ztráta internetové konektivity	**Internet**	**3,33**
11.	I	Faktury, seznam závazků, seznam pohledávek, účetní knihy, tištěné smlouvy	**Citlivé firemní informace, kategorie II**	**3,23**
12.	I	Výrobní data, přístupová hesla	**Produkčně vývojové informace**	**3,16**
13.	I	Skladové informace, informace o obchodních partnerech	**Běžné firemní informace**	**2,50**
14.	F	Krádež pokladny	**Krádež pokladny**	**2,33**
15.	M	Krádež skladových zásob	**Sklad**	**2,00**
16.	M	Ztráta VOIP konektivity, telefonního/faxového připojení	**Telekomunikační služby**	**2,00**

Tabulka 6: Seskupení aktiv

4.2.4 Identifikace hrozeb

Pro seskupená aktiva jsem dále provedl identifikace hrozeb, u každé skupiny jsou uvedeny samotné hrozby, možné útoky, včetně slabých míst, která tyto hrozby umožňují. Výsledek podle velikosti ohodnocení je uveden v následující tabulce 7.

1.	**Ztráta know-how**	**4,66**
	Hrozby	Odcizení firemních informací, odchod klíčových zaměstnanců, sankce.
	Možné útoky	Konkurence, nespokojený zaměstnanec.
	Slabá místa	Bezpečnostní zajištění informačních dat, zpracování tištěných materiálů, slabý věrnostní zaměstnanecký program.
2.	**Šéfův notebook**	**4,66**
	Hrozby	Odcizení, ztráta citlivých (jedinečných) informací.
	Možné útoky	Vloupání, elektronický útok (virus, trojský kůň), uživatelský omyl při manipulaci.
	Slabá místa	Manuální zpracování dat, možné bezpečnostní díry, bez zálohování.
3.	**Bankovní deposit**	**4,33**
	Hrozby	Porušení cash-flow, manipulace nepovolanými osobami.
	Možné útoky	Elektronický útok, uživatelský omyl při manipulaci, manipulace zaměstnanci.
	Slabá místa	Uložení financí v jednom bankovním ústavu, úroveň jištění přístupových míst s komunikací s bankou a počítačem.
4.	**Dobré jméno firmy**	**4,00**
	Hrozby	Ztráta trhu, důvěryhodnosti, potenciálních zisků.
	Možné útoky	Konkurence, zákaznici, elektronický útok.
	Slabá místa	Nedostatečná firemní politika, podpora zákazníkům, slabé výstupní kontroly elektronických informací k zákazníkům.
5.	**Lokální server**	**4,00**
	Hrozby	Odcizení firemních informací, narušení firemních dat a provozu.
	Možné útoky	Odcizení, virus, elektronický útok, přerušení napájení, nedostatečné chlazení.
	Slabá místa	Umístění a zabezpečení síťového serveru.
6.	**Firemní počítač**	**4,00**
	Hrozby	Odcizení firemních informací, uživatelský omyl při manipulaci.
	Možné útoky	Odcizení, virus, elektronický útok, nedostatečné chlazení.
	Slabá místa	Zabezpečení síťového serveru, zálohování.
7.	**Licence klíčového software**	**4,00**
	Hrozby	Nefunkčnost klíčového software, prodlužování vyřízení projektů, finanční sankce.
	Možné útoky	Virus, elektronický útok, vypršení licence.
	Slabá místa	Kontrolní mechanismy hlídající platnost licenčních souborů.
8.	**Valutová pokladna**	**3,66**
	Hrozby	Znehodnocení měny (převodního kurzu).
	Možné útoky	Elektronický útok, uživatelský omyl při manipulaci.
	Slabá místa	Úroveň jištění přístupových míst s komunikací s bankou a počítačem.
9.	**Citlivé firemní informace, kategorie I**	**3,66**
	Hrozby	Přístup k informacím nepovolanými osobami, odchod zaměstnance.
	Možné útoky	Uživatelský omyl při manipulaci, vloupání, odcizení.
	Slabá místa	Jištění úložiště jednoduchým zámkem.

10.	**Ztráta internetové konektivity**	**3,33**
	Hrozby	Narušení chodu firmy, komunikačních prostředků, ztráta aktuálních informací.
	Možné útoky	Útok, uživatelská chyba, chyby na straně poskytovatele internetu.
	Slabá místa	Absence záložních systémů a procesů v případě havárie.
11.	**Citlivé firemní informace, kategorie II**	**3,23**
	Hrozby	Odcizení, poškození, chybné zavedení do systému, ztráta, zneužití.
	Možné útoky	Vloupání, elektronický útok, uživatelský omyl při manipulaci.
	Slabá místa	Manuální zpracování dat, nedůsledně řešena digitalizace dokumentů, bezpečnostní zabezpečení elektronických systémů, ochrana heslem a přístupem.
12.	**Produkčně-vývojové informace**	**3,16**
	Hrozby	Ztráta firemních informací a narušení provozu, sankce.
	Možné útoky	Virus, elektronický útok, uživatelská chyba.
	Slabá místa	Manipulace a zabezpečení s firemními informacemi, absence zálohování, manipulace a ochrana s přístupovými hesly a personální politikou.
13.	**Běžné firemní informace**	**2,50**
	Hrozby	Odcizení, poškození, chybné zavedení do systému, ztráta, zneužití.
	Možné útoky	Vloupání, elektronický útok, uživatelský omyl při manipulaci.
	Slabá místa	Manuální zpracování dat, nedůsledně řešena digitalizace dokumentů, bezpečnostní zabezpečení elektronických systémů.
14.	**Krádež pokladny**	**2,33**
	Hrozby	Odcizení.
	Možné útoky	Vloupání, uživatelský omyl při manipulaci.
	Slabá místa	Fyzické zabezpečení pokladny, informační systém stavu pokladny.
15.	**Krádež skladových zásob**	**2,00**
	Hrozby	Odcizení.
	Možné útoky	Vloupání, uživatelský omyl při manipulaci.
	Slabá místa	Fyzické zabezpečení podniku.
16.	**Telekomunikační služby**	**2,00**
	Hrozby	Narušení chodu firmy, komunikačních prostředků.
	Možné útoky	Útok, uživatelská chyba, chyba na straně poskytovatele.
	Slabá místa	Nedostatek záložních systémů.

Tabulka 7: Identifikace hrozeb

4.2.5 Analýza rizik

Dalším krokem je analýza a zhodnocení možných rizik v komplexním měřítku na základě zjištěných hrozeb a aktiv podniku. Na základě předchozích údajů byly souhrnně lokalizovány hrozby. Jejich možné řešení je uvedeno v tabulce 8.

Hrozba	Aktiva	Možné řešení rizik
Finanční sankce / narušení chodu firmy	Ztráta know-how Ztráta internetové konektivity Telekomunikační služby Licence klíčového software	**Retence a redukce** – vhodnými prostředky
Manipulace s aktivem nepovolanými osobami	Bankovní deposit Citlivé informace, kat. I Citlivé informace, kat. II Běžné firemní informace Lokální server Šéfův notebook	**Redukce rizika** – vhodným bezpečnostním opatřením
Odcizení aktiva	Šéfův notebook Firemní počítač Krádež pokladny Krádež skladových zásob	**Transfer (Pojištění)** – proti vloupání, přenášení věcí
Porušení cash-flow	Bankovní deposit Valutová pokladna	**Transfer** – rozložení na víc bankovních účtů
Poškození aktiva	Citlivé informace, kat. I Citlivé informace, kat. II Produkčně-vývojové informace Běžné firemní informace Šéfův notebook Firemní počítač	**Retence a redukce** – maximální možná redukce vhodným bezpečnostním opatřením
Uživatelský omyl	Bankovní deposit Citlivé informace, kat. I Citlivé informace, kat. II Běžné firemní informace Lokální server Šéfův notebook	**Retence**
Znehodnocení měny.	Valutová pokladna	**Transfer** – rozložení na více měn, spořící účet

Tabulka 8: Řešení rizik

4.3 Nová bezpečnostní opatření

Na základě analýzy navrhuji následující bezpečnostní opatření, která mají za úkol snížit rizika dopadu hrozeb. Všeobecně pro všechny subjekty firmy platí, že v případě nejasností s prováděnou činností má subjekt firmy právo ověřit si u bezpečnostního týmu, zda činnost, kterou vykonává nebo chce vykonávat, je v souladu s bezpečnostní politikou. V případě, že tak neučiní a způsobí bezpečnostní incident, má firma právo subjekt sankcionovat.

V případě zjištění bezpečnostního incidentu je zapotřebí informovat bezpečnostní tým o aktuálním stavu. Bezpečnostní tým na základě havarijního plánu a povolení zásahu bezpečnostního ředitele začne bezpečnostní incident řešit. Výsledkem je zpráva, která informuje ředitele o výsledku akce.

4.3.1 Informační bezpečnost

Z analýzy vyplynulo, že firma dělí dokumenty na tři skupiny. Toto dělení může být zachováno, navrhuji však převést veškeré důležité dokumenty ze skupiny „citlivé informace, kategorie I“ (dokumenty, ke kterým má přístup jen vedoucí pobočky) do digitalizované podoby. Poté digitální kopie uchovat a vhodně kryptovat na lokálním serveru. Tištěné dokumenty je vhodné uchovat ve společnosti pro dlouhodobou úschovu dokumentů, kde budou dokumenty lépe chráněny proti odcizení, poškození a znehodnocení než uvnitř pobočky.

Část „citlivých informací, kategorie II“ je posílána do externí účetní firmy, kde by měla probíhat průběžná kontrola zpracování těchto dokumentů. Navrhuji, aby se veškeré dokumenty převáděly do digitální podoby a uchovávaly na lokálním serveru, pro jejich rychlou a snadnou dostupnost. Uložené digitální informace, včetně „citlivých informací, kategorie I“ by měly být umístěny na jiném diskovém poli nebo oddílu. Veškeré informace by měly být řádně zálohovány.

Dále navrhuji zakoupit skartovací stroj na fyzickou likvidaci všech tištěných produkčně-vývojových dokumentů a část běžných dokumentů, které mají jakoukoliv informační spojitost s pobočkou. Tento skartovací stroj by měli používat všechny subjekty firmy a měl by umožňovat i skartaci přenosných médií, jako jsou optické disky, diskety, apod.

Výsledné a dokončené produkčně-vývojové informace by měly být ukládány na server do specializované složky, která je podobně jak citlivé informace řádně zálohována proti ztrátě a poškození.

Plněním uvedených opatření se redukují tyto hrozby:

- **Poškození aktiva** – informační aktiva budou dvojitě chráněna, jak na lokálním serveru tak i v tištěné podobě, veškeré důležité informace se budou zálohovat.
- **Manipulace s aktivem nepovolanými osobami** – citlivá data první kategorie budou digitálně kryptována. Všechna citlivá data jsou umístěna mimo disk se společnými daty, tištěná data jsou uložena mimo pobočku.
- **Uživatelský omyl** – zálohování informací redukuje uživatelský omyl při smazání důležitých informací, informace se dají najít na dvou různých místech.

4.3.2 Informační bezpečnost IS/ICT

Na základě analýzy bezpečnosti a doporučení v normě ISO/IEC 27002 jsem sestavil následující body celkové bezpečnosti, které by měly být zahrnuty do bezpečnostní politiky:

- **Komunikace s elektronickými obchody** – Navrhuji, aby vedení podniku stanovilo podmínky a míru informací, které je možné uvádět při kontaktu s elektronickými obchody a firmami. Zároveň navrhuji vytvořit centralizovaný seznam přihlašovacích jednotných hesel a identifikací, včetně společné emailové adresy (např. obchod@advantech.eu), který je určený výhradně pro výměnu informací mezi pobočkou a externí firmou. Tento centralizovaný systém může být zaveden také pro získávání informačních brožurek, materiálů, součástek, návodů, atd. Každý interní zaměstnanec by měl mít možnost do tohoto seznamu nahlížet a k emailové schránce přistoupit. Pokud je to jenom možné, měli by si subjekty ověřit, že komunikují po zabezpečeném kanálu při výměně veškerých informací. Dále by mělo platit, že interní zaměstnanec by nikdy neměl svěřovat bezpečnostní heslo třetím stranám. Součástí výměny informace by mělo být používání dalších bezpečnostních mechanismů pro ověření autentizace a autorizace (kalkulačky kódu, mobilní telefon, atd.).

- **Mobilní a cizí přístroje** – Bezpečnostní tým má za úkol sestavit taková opatření a omezení, která povolí připojení mobilních a cizích zařízení až s jejím svolením. Možné je automatické připojení cizích přístrojů, ale to pouze a jen v ochranné zóně, která je mimo dosah počítačových systémů ve firmě.
- **Monitorování a hlášení** – Bezpečnostní tým by měl průběžně sledovat a vyhodnocovat vytížení internetového spojení, využití systémových prostředků, kontrolovat bezpečnostní záznamy o neúspěšných přihlášení a neoprávněných pokusech do systému. Součástí těchto monitorování by měla být také pravidelná kontrola výskytu škodlivého software na všech počítačích, kontrola instalovaného software a bezpečnostního nastavení. Výsledky by měly být pravidelně podávány ve strukturovaném hlášení bezpečnostnímu řediteli pobočky.
- **Ochrana internetového přípojení** – Bezpečnostní tým musí zabezpečit internetové připojení proti napadení škodlivým software, např. pomocí dobře nainstalovaného firewallu a antivirového programu. V zájmu bezpečnostního týmu je i vypracovat havarijní plán v případě výpadku internetového připojení.
- **Ochrana proti škodlivému software** – Uživatelé počítače nesmí bránit instalovaným prostředkům pro ochranu dat a informací na počítači. Bezpečnostní tým musí průběžně ověřovat zabezpečení instalovaného software. Pouze bezpečnostní tým může vydat povolení pro instalaci nového software. V zájmu bezpečnostního týmu je instalovat takové bezpečnostní prostředky, které v maximální míře ochrání bezpečnost organizace. V případě incidentu je zapotřebí informovat ředitele bezpečnosti o aktuálním stavu a možnostech způsobu řešení incidentu.
- **Operační procedury a zodpovědnost** – Navrhuji, aby zodpovědnost za informační bezpečnost konkretních počítačů byla svěřena samotným uživatelům počítače. Bezpečnost lokálního serveru by měla být svěřena lokálnímu bezpečnostnímu týmu. U přenosného počítače v době používání může být zodpovědnost přenesena na uživatele, po uvolnění však spadá bezpečnost a zabezpečení počítače na bezpečnostní tým. Při porušení pravidel lze tak postihovat konkrétní zaměstnance. Oprávnění uživatelů k zodpovědnosti za informační bezpečnost neumožňují oslabit další pravidla stanovená v bezpečnostní politice.
- **Použití počítačových prostředků** – Zaměstnanci firmy mohou používat počítačové prostředky a komunikační kanály jen a pouze k činnostem související

s jejich práci a smlouvou. Jakékoliv porušování a narušování bezpečnosti jiným použitím by mělo být sankcionováno. Uživatel by měl dodržovat nejvyšší míru bezpečnosti i při krátkodobém odchodu z pracoviště, jako je zamknutí počítače, soustavně udržovaný uklizený stůl, atd.

- **Řízení přístupových práv** – Úkolem bezpečnostního týmu je personální zabezpečení přístupových práv a řádné nastavení systému vyžadující periodickou výměnu hesel od všech uživatelů. Samotný systém by měl navíc při výběru nového hesla zabránit rotaci hesel (opětovné použití předchozích hesel). Samotní uživatelé nesmí hesla mezi sebou sdílet, ani je zapisovat na viditelné místa (monitory, klávesnice, počítač). Výjimkou jsou společné testovací prostředky nebo systémy, u kterých je nutné dodržet stejné heslo doporučené bezpečnostním týmem.
- **Služby třetí strany** – Měl by být ověřen způsob zajištění a ochrany dat u externích společností, které zpracovávají informace firmy, v konkrétním případě u účetní firmy by měl proběhnout audit informačních zabezpečení. V případě nedostatečného zabezpečení je zapotřebí provést nápravu nebo navrhnout vhodné opatření.
- **Systémové plánování** – Bezpečnostní tým by měl kooperovat s vývojovým týmem při obsazování prostředků a zpracovávat požadavky provádění činnosti bezpečnostního ředitele podle havarijního a změnového plánu. Bezpečnostní tým by měl také spravovat seznam nakoupených licencí programů a jejich data vypršení a podmínek aktualizace, včetně kontaktů na prodejce.
- **Výměna informací a datových nosičů** – Subjekty firmy by při výměně externích informací měli používat zabezpečených kanálů podle míry důležitosti informací. V případě citlivých dokumentů by za pomoci bezpečnostního týmu měly být vytvořeny šifrované bezpečnostní kanály určené pro jejich přenos. Při přenášení datových nosičů s citlivými informacemi by měl subjekt firmy vyžadovat předávací protokol, včetně způsobu přenášení a uložení tohoto media v externí firmě.
- **Zabezpečení přenosných počítačů –** Přenosné počítače by měly být vybaveny zvýšenou ochranou proti cizímu použití. Může se jednat o specializované klíče, čtečky prstů, HW karty. Důvodem je samotná mobilita a zvýšené bezpečnostní riziko ztráty a odcizení zařízení. Zároveň by na přenosném počítači mělo být uloženo minimum firemních informací, identifikačních údajů apod. Uživatel

spolu s bezpečnostní týmem by měl lpět na přesunu firemních informací na lokální server, kde jsou mnohem lépe chráněny. Současně musí být počítač vybaven účinným firewallem pro ochranu přípojení k cizí (nefiremní) síti.

- **Zálohování** – Bezpečnostní tým musí sestavit proces zálohování lokálního serveru. Navrhuji, aby se zálohování provádělo na vybraných adresářích lokálního serveru a aby se zálohy kopírovaly v nočních hodinách pravidelně přes internetovou síť na vybraný server v Mnichově. Nedílnou části je i vypracování havarijního plánu a pravidelné ověření možnosti obnovy.

Plněním uvedených opatření se redukují tyto hrozby: manipulace s aktivem nepovolanými osobami, odcizení aktiva, poškození aktiva, uživatelský omyl a narušení chodu firmy.

4.3.3 Majetková bezpečnost

V rámci majetkové bezpečnosti a výši aktiv uložených na bankovním účtu navrhuji rozložit prostředky uložené na bankovním účtu na dva účty. V dnešní době nabízejí banky také výhodné firemní spořící účty, které zhodnocují uložení financí s okamžitým přístupem k peněžním prostředkům. Podmínky bank jsou různé, nicméně lze najít vhodný produkt, který může vyhovovat konkrétnímu podnikateli. V rámci konkurenčního boje nabízejí některé banky vedení účtu zdarma, internetové bankovnictví zdarma, zdarma přesuny mezi spořícím a běžným firemním účtem, atd.

Prostředky může firma zhodnotit i jinými způsoby, zvolena varianta by však měla přinášet zisk, který může být využit pro případnou ztráty při znehodnocení měny. Rozložení financí by mělo být takové, aby se pokryla co nejvíce horní hranice jištění vloženého vkladu, pro případný krach banky.

Navrhuji dále instalovat ve firmě požární hlásič kouře, který vhodným způsobem upozorní vedoucího pobočky o výskytu incidentu (např. sms pager). Protože jsou ve firmě instalována elektrická zařízení, není vhodné pro bezpečnost zařízení a lidí používat automatický zhášecí vodní systém. Tento požární hlásič může být propojen s alarmem, spolu mohou obě zařízení zvýšit bezpečnost majetkové bezpečnosti.

Při pořízení alarmu a případných bezpečnostních dveří dále navrhuji zvážit smluvní pojištění proti odcizení a poškození majetku zaměstnanci.

V neposlední řadě by měl bezpečnostní tým sestavit mapku s umístěním bezpečnostních vypínačů, hasících přístrojů a dalších ochranných prvků. U hasících

přístrojů se musí hlídat datum pravidelné výměny, co půl roku by také měla probíhat kontrola hlídacích prvků a čistění vnitřků počítačů od prachu a nečistot.

Zavedením uvedených bezpečnostní opatření se mohou eliminovat tyto hrozby: narušení chodu firmy, znehodnocení měny, odcizení aktiva a porušení cash-flow.

4.3.4 Personální bezpečnost

Bezpečnostní ředitel a bezpečnostní tým musí být iniciátoři většiny akcí nutných pro hladké zavedení nového zaměstnance do firmy, včetně změny jeho přístupových práv vv případě pracovního postupu a případně i rušení jeho místa. Měl by být zdokumentován pracovní postup pro všechny uvedené případy.

Jedná se jak o školení pro nového zaměstnance tak i o pravidelná systémová školení, jejichž úkolem je seznámit subjekty s novými trendy v zabezpečení podniku. Školení by mělo informovat subjekty o nových hrozbách a ochrany vůči nim. Navrhuji, aby jako součást tohoto školení byly zavedeny účelné testy, které budou ověřovat znalosti bezpečnostní politiky u zkoušených subjektů.

Bezpečnostní školení, které nemůže vykonávat samotný bezpečnostní ředitel ani jeho tým, musí být obstaráno externími subjekty. Pro všechna školení musí být stanoven záznam o provedení, výsledku školení včetně periodicity opakování dalšího školení. Cílem školení je mimo jiné i zvýšení povědomí o firemní bezpečnosti u jednotlivých subjektů.

4.4 Pracovní vytížení bezpečnostního týmu

Navrhuji, aby většina pravidelných kontrolních a zaváděcích operací, které má vykonávat bezpečnostní technik, byla prováděna mimo běžnou pracovní dobu z důvodu co nejmenšího narušení chodu firmy. Studium problematiky, příprava dokumentace, změnového řízení a havarijních plánů může probíhat během normální pracovní doby.

S ohledem na nová bezpečnostní opatření uvádím také tabulku předpokládaných pracovních vytížení pro pracovníka vykonávající bezpečnost (tabulka 9) a konzultanta bezpečnosti (tabulka 10). Navrhuji, aby takovými pracovníky byli interní zaměstnanci, (nikoliv pracovníci externí firmy), kteří se již umí orientovat v aktuálním procesním řízení, oba jsou seznámeni s aktuální bezpečnostní politikou a mají vysokoškolské vzdělání v IT technologiích.

Navrhuji, aby sestavením havarijního plánu byl pověřen bezpečnostní technik, zatímco samotným testováním již bezpečnostní konzultant.

Činnost		Jednorázová	Opakovaná
Opravy stávájících bezpečnostních nařízení	Nastudovaní problematiky	2-3 dny	
	Provedení oprav	3 dny	2 hod / 2 týdny
	Kontrola opatření	3-4 dny	
Zavedení nových bezpečnostních opatření	Nastudovaní problematiky	5 dnů	
	Příprava změnového řízení	10 dnů	
	Příprava dokumentace	5 dnů	
	Zavedení změn	3-4 dny	
	Kontrola opatření	3-4 dny	1 hod / 2 týdny
Pravidelná kontrola bezpečnosti	Nastudovaní problematiky	2 dny	
	Příprava dokumentace	1 den	
	Instalace kontrolních mechanismů	3 dny	1 hod / 2 týdny
Školení	Nastudovaní problematiky	4 dny	1 hod / 6 měsíců
	Příprava dokumentace a průběh školení	3 dny	1 den / 6 měsíců
Zpracování reportů	Nastudovaní problematiky	2 dny	1 hod / 2 týdny
	Příprava dokumentace	2 dny	
Sestavení a kontrola havarijních plánů	Nastudovaní problematiky	2 dny	
	Revize havarijních plánů	3 dny	1 hod / 3 měsíce
	Zavedení havarijních plánů	5 dnů	1 hod / 3 měsíce
Činnosti pro majetkovou bezpečnost	Vytvoření dokumentace	1 den	
	Kontrola a provádění akcí		4 hod / 6 měsíců
Součet		**66 dnů**	**5 hod / 2 týdny + cca 2 dny / 6 měsíců**

Tabulka 9: Pracovní vytížení bezpečnostního technika

Činnost		Jednorázová	Opakovaná
Zjišťování nových hrozeb bezpečnosti	Nastudovaní problematiky	10 dnů	1 hod / 2 týdny
Školení	Průběh školení		1 den / 6 měsíců
Kontrola dokumentace	Změnové řízení	5 dnů	
Kontrola havarijních plánů	Provádění		4 hod / 3 měsíce
Součet		**15 dnů**	**2 hod / 2 týdny + cca 2 dny / 6 měsíců**

Tabulka 10: Pracovní vytížení bezpečnostního konzultanta

4.5 Analýza nákladů na nové zabezpečení

V této kapitole uvádím předpokládané výdaje a pravidelné náklady na zavedení a kontrolu nové bezpečnostní politiky v pobočce.

Z dat uvedených v tabulce 9 vyplývá, že pracovní vytížení bezpečnostního technika by měsíčně nemělo přesáhnout 10 hodin. Časová náročnost pro konzultanta bezpečnosti by neměla přesáhnout 4 hodiny měsíčně.

Navrhuji ohodnotit práci bezpečnostního technika měsíční částkou tisíc korun, práci bezpečnostního konzultanta částkou pět set korun. Předpokládám, že by provádění činností probíhalo nad rámec pracovní doby.

Z tabulky vytížení bezpečnostního technika dále vyplynulo, že zavádění bezpečnosti je plánováno na dobu tří až čtyř měsíců, které budou vyžadovat plné nasazení technika pro bezpečnost. Pro bezpečnostního konzultanta je kontrola práce bezpečnostního technika odhadována na dobu tří pracovních týdnů, zde se předpokládá přerušovaná činnost, protože bezpečnostní konzultant musí počkat na výsledky práce bezpečnostního technika.

Spolu s dalšími náklady firmy pro zavádění bezpečnosti jsem získal předpokládaný odhad celkových nákladů pro zavedení bezpečnosti

Položka	Cena od
Nové licence bezpečnostních programů[49].	20 000,-
Záložní testovací počítač, na kterém bude probíhat testování havarijních plánů, případně ochrana bezpečnostních pravidel.	10 000,-
Pomocný materiál pro vykonávání bezpečnosti (přenosné disky, záložní media, náhradní komponenty, atd.).	10 000,-
GSM alarm a hlásiče kouře[50].	15 000,-
Mzdové náklady bezpečnostního technika (super hrubá mzda).	120 000,-
Mzdové náklady bezpečnostního konzultanta (super hrubá mzda).	30 000,-
Celkem	**205 000,-**

Tabulka 11: Hrubý odhad nákladů na zavedení bezpečnosti

Sečtením položek v tabulce lze odvodit hrubý odhad na zavedení bezpečnosti v české pobočce, který vychází cca na 200 tisíc korun českých.

49 *[9] Nabídka firmy ESET. (online dokument)*

50 *[5]Nabídka elektronického zabezpečení firmy ČIP (online dokument)*

5 ZHODNOCENÍ A ZÁVĚR

Ve své diplomové práci jsem se vypracoval návrh bezpečnostní politiky české pobočky nadnárodní společnosti. Firma zaměstnává devět lidí, zabývá se vývojem a výrobou zákaznických prototypů a určitá aktiva související jak s vývojem a výrobou tak i s citlivými informacemi jsou pro firmu důležitá, neboť jsou jedinečná a aktuálně nepříliš dobře chráněna.

V praktické části práce jsem se snažil tato aktiva firmy identifikovat a ohodnotit je. Analýzou hrozeb a rizik jsem dále rozlišil aktiva dle důležitosti a zařazení na jednotlivé skupiny. Na základě této analýzy a absence významných dokumentů a procesů zabývajících se bezpečnostní politikou ve firmě jsem sestavil návrhy na zavedení nových bezpečnostních opatření. V neposlední řadě jsem navrhl také způsob řízení změn a personální obsazení nových bezpečnostních rolí v podniku.

V závěru práce jsem za pomocí vedení a osobních zkušeností sestavil jak analýzu pracovní vytíženosti, tak samotnou hrubou analýzu nákladů. Z této analýzy vyplynuly dvě podstatné skutečnosti.

První skutečnost říká, že pokud roli bezpečnostního technika bude pověřen někdo z interních zaměstnanců, je vhodné začít zabývat se bezpečností pro svou časovou náročnost v době vývojového útlumu, což jsou obvykle letní měsíce roku, protože zavedení bezpečnosti je odhadováno na období tří až čtyř měsíců. Druhá skutečnost říká, že náklady na celkovou bezpečnost jsou z větší části sestaveny z mzdových nákladů. Výše nákladů může být například hrazena z ušetřených prostředků z minulého roku, což činí necelých 15% z těchto rezerv.

Nemyslím si, že je účelné zaměstnávat nového pracovníka pro řešení bezpečnosti, ale je vhodnější rozšířit u vybraného interního pracovníka stávající smlouvu o novou pracovní náplň. Pokud se vedení firmy se rozhodne pro outsourcing, přinese to firmě dvě výhody. První výhodou bude neblokování interního pracovníka pro řešení bezpečnosti a druhou rychlejší nasazení bezpečnostní politiky (odpadne náročné studium bezpečnosti). Možnou nevýhodou bude ale bezesporu vyšší cena implementace. V tomto případě doporučuji přiřadit místo bezpečnostního konzultanta internímu pracovníkovi, který by dohlížel na provádění prací externí firmy.

Práce odhalila výrazné bezpečnostní mezery v dosavadní bezpečnosti pobočky, ať se firma rozhodne jakkoliv, měla by se pokusit implementovat z počátku alespoň jednoduší

návrhy bezpečnosti, protože je víceméně náhoda, že zjištěné bezpečnostní mezery a hrozby zatím nezpůsobily podniku značné škody na aktivech.

S ohledem na složitost zavedení a sestavení podnikové bezpečnosti je ucelený koncept řešení nevyhnutelný, jeden z možných přístupů byl představen právě v této práci.

5.1 Další kroky

Vzhledem k omezenému rozsahu práce se návrh bezpečnostní politiky nezabývá v zákonnou legislativou, která se podobně jak informační systémy vyvíjí. Jedním z důvodu realizace firemního zabezpečení je i plnění povinností vyplývající z platných zákonů a vyhlášek. V České republice dosud neexistuje zákon, který by komplexně řešil informační prostředí elektronického zpracování informací[51]. Je ale možné, že časem takový ucelený zákon vznikne. Zatím lze vycházet z různých pouček z obchodního zákoníku, zákonu o ochraně osobních údajů[52] a zákonu o elektronickém podpisu[53] vztahujících se alespoň částečně k problematice zabezpečení pro obchodní společnosti.

Další částí, kterou jsem se v práci nevěnoval, je zavedení systému kryptování informací a emailových zpráv, tj. seznámení s problematikou, vytvoření ověřujících certifikátů, výměny případných privátních a veřejných klíčů mezi adresáty atd[54]. Důvodem tohoto rozhodnutí je skutečnost, že by nutné změny přesáhly rozsah pobočky, což je vzhledem k malému množství důležitých citlivých zpráv nehospodárné. Druhým důvodem je nejednotný systém kryptování, který mimo jiné vyžaduje sjednocení komunikačních prostředků na obou stranách, což obzvláště u externích subjektů, kde by kryptování komunikace bylo žádoucí, je mnohdy nerealizovatelné.

Na vedení firmy je rozhodnutí, jakým způsobem bude řešena firemní bezpečnost v pobočce, zda se možnosti bezpečnostních opatření navýší i o pojištění majetku, kdo bude zodpovědný za řešení bezpečnosti a soustavnou aktualizaci potřebných dokumentů. Nechat však stávající bezpečnost podniku na úrovni, která je udržována doposud je velmi riskantní a může způsobit firmě značné ztráty v budoucnosti.

51 *[15] MLÝNEK (2007), str. 125*

52 *[21] Zákon č. 101/2000 Sb. ze dne 4.dubna 2000 o ochraně osobních údajů.*

53 *[22] Zákon č. 227/2000 Sb. ze dne 29.června 2000 o elektronickém podpisu a novely tohoto zákonu: zákon č. 226/2002 Sb. a zákon č. 440/2004 Sb.*

54 *[16] POŽÁR (2005), str 191*

6 SEZNAM POUŽITÉ LITERATURY

[1] ADVANTECH. *Informace o firmě* [online]. [cit. 2009-01-05]. URL: http://www.advantech.com.tw/Job/Default.aspx?sta=AboutAdvantech

[2] BRABEC, František. 1996. *Ochrana bezpečnosti podniku*. 1. vydání. Praha: EUROUNION, 1996. 204 s. ISBN 80-85858-29-0

[3] CAHA, Luděk. 2008.*Zabezpečení souborů v kanceláři*. Dostupné z: http://crypto-world.info/casop10/crypto78_08.pdf, vydáno v e-zine Crypto-World 78/2008, 2008, str.: 11-17. ISSN 1801-2140

[4] ČERMÁK, Igor. 2007.*Bezpečnostní hrozby a stav informační bezpečnosti na veřejných vysokých školách v ČR*, ve sborníku *Bezpečnostní politika IS*. Plzeň: Západočeská univerzita v Plzni, 2007, str.: 12-17. ISBN 978-80-7043-554-0

[5] ČIP. *Nabídka elektronického zabezpečení* [online]. [cit. 2009-04-05]. URL: http://cip.inshop.cz/

[6] DOSEDĚL, Tomáš. 2004. *Počítačová bezpečnost a ochrana dat*. 1. vydání. Praha: Computer Press, 2004. 190 s. ISBN 80-251-0106-1

[7] DOSEDĚL, Tomáš. 2005. *21 Základních pravidel počítačové bezpečnosti*. 1. vydání. Praha: Computer Press, 2005. 52 s. ISBN 80-251-0574-1

[8] DOUCEK, Petr - NOVÁK, Luděk - SVATÁ, Vlasta. 2008. *Řízení bezpečnosti informací*. 1. vydání. Praha: Professional Publishing, 2008. 239 s. ISBN 978-80-86946-88-7

[9] ESET. *Nabídka firmy ESET* [online]. [cit. 2009-04-05]. URL: http://www.eset.cz

[10] GÁLA, Libor - POUR, Jan - TOMAN, Prokop. 2006. *Podniková informatika*. 1. vydání. Praha: Grada Publishing, 2006. 482 s. ISBN 80-247-1278-4

[11] GREGORY, Peter. 2008. *IT Disaster Recovery Planning For Dummies*. 1st edition. United States: John Wiley & Sons, 2008. 360 s. ISBN 978-0-470-03973-1

[12] CHLUP, Marek. *ISMS - Hodnocení aktiv* [online]. [cit. 2009-03-20]. URL: http://www.chrantesidata.cz/cs/art/1149-dil-3/

[13] KOCH, Miloš - ONDRÁK, Viktor. 2004. *Informační systémy a technologie*. 1. vydání. Brno: Akademické nakladatelství CERM, 2004. 166 s. ISBN 80-214-2725-6

[14] MACICH, Jiří. *Falešné antiviry obtěžují také české uživatele* [online]. [cit. 2009-03-21]. URL: http://www.lupa.cz/zpravicky/falesne-antiviry-obtezuji-take-ceske-uzivatele/

[15] MLÝNEK, Jaroslav. 2007. *Zabezpečení obchodních informací*. 1. vydání. Brno: Computer Press, 2007. 154 s. ISBN 978-80-251-1511-4

[16] POŽÁR, Josef. 2005. *Informační bezpečnost*. 1. vydání (?). Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 311 s. ISBN 80-86898-38-5

[17] SECUNET. *Bezpečnostní audit* [online]. [cit. 2009-03-12]. URL: http://www.secunet.cz/pdf/PL_Bezpecnostniaudit.pdf

[18] SMEJKAL, Vladimír - RAIS, Karel. 2006. *Řízení rizik ve firmách a jiných organizacích*. 2. vydání. Praha: Grada Publishing, 2006. 300 s. ISBN 80-247-1667-4

[19] T-SOFT. *Bezpečnostní audit IS/IT* [online]. [cit. 2009-03-12]. URL: http://www.tsoft.cz/index.php?q=cz/audit-bezpecnostni

[20] TVRDÍKOVÁ, Milena. 2008. *Aplikace moderních informačních technologií v řízení firmy*. 1. vydání. Praha: Grada Publishing, 2008. 176 s. ISBN 978-80-247-2728-8

[21] Zákon č. 101/2000 Sb. ze dne 4.dubna 2000 o ochraně osobních údajů.

[22] Zákon č. 227/2000 Sb. ze dne 29.června 2000 o elektronickém podpisu a novely tohoto zákonu: zákon č. 226/2002 Sb. a zákon č. 440/2004 Sb.

7 PŘÍLOHY

A. INTERNET USAGE POLICY

【 Advantech Europe Policies & Procedures】

Policy No.: AEUITP-004

Subject: INTERNET USAGE POLICY

Version: V1

Effective Date: June 30, 2004

Prepared By: Advantech Europe Holding

Approved By: Managing Director / Financial Controller

a) Objective

Advantech Europe is committed to preventing the occurrence of inappropriate, unethical, or unlawful behaviour by any of the users of its computing systems and telecommunications networks. These responsibilities are not only mandated by the facility's business interests but by legal and ethical obligations concerning the welfare and privacy of its customers and business partners. This Internet usage Policy and its strict enforcement is an important and necessary part of the overall usage strategy.

b) Scope

The scope of this policy includes the following information:

- Internet services;
- Resource usage;
- Expectation of privacy;
- Corporate image;
- Contacts for usage issues and questions;
- Periodic reviews.

The components outlined in this document focus on issues associated with Advantech Europe's host computers, PCs, routers, terminal servers, and other devices that support access to the Internet. The scope of this document does not include facility-specific usage policies, application usage, and non-Internet usage.

The Internet usage Policy applies to all Internet users (individuals working for Advantech Europe, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners, and vendors) who access the Internet through the computing or networking resources. Advantech Europe's Internet users are expected to be familiar with and to comply with this policy, and are also required to use their common sense and exercise their good judgment while using Internet services.

c) Requirements

Violations of the Internet usage Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination.

Additionally, Advantech Europe may at its discretion seek legal remedies for damages incurred as a result of any violation. Advantech Europe may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the Internet via company network is approved, the potential Internet user is required to read this Internet usage Policy and sign an acknowledgment form (located on the last page of this document). The signed acknowledgment form should be turned in and will be kept on file at the facility granting the access. For questions on the Internet usage Policy, contact the Information Technology (IT) Department.

Internet Services Allowed - Access to the Internet will be provided to users to support business activities and only on an as-needed basis to perform their jobs and professional roles.

Internet access is to be used for business purposes only. Capabilities for the following standard Internet services will be provided to users as needed:

E-mail - Send/receive E-mail messages to/from the Internet (with or without document attachments).

Navigation - WWW services as necessary for business purposes, using a hypertext transfer protocol (HTTP) browser tool. Full access to the Internet; limited access from the Internet to dedicated company public web servers only.

File Transfer Protocol (FTP) - Send data/files and receive in-bound data/files, as necessary for business purposes.

Telnet - Standard Internet protocol for terminal emulation. User Strong Authentication required for Internet initiated contacts into Advantech Europe.

Management reserves the rights to add or delete services, as business needs change or conditions warrant. All other services will be considered unauthorized access to/from the Internet and will not be allowed.

d) Personal Internet Usage

Using company computer resources to access the Internet for personal purposes, without approval from the user's manager and the IT department, may be considered cause for disciplinary action up to and including termination.

All users of the Internet should be aware that Advantech Europe network creates an audit log-reflecting request for service, both in-bound and out-bound addresses, and is periodically reviewed.

Users who choose to store or transmit personal information such as private keys, credit card numbers or certificates or make use of Internet do so at their own risk. Advantech Europe is not responsible for any loss of information, such as information stored in the wallet, or any consequential loss of personal property.

e) Prohibited Usage

Acquisition, storage, and dissemination of data which is illegal, pornographic, or which negatively depicts race, sex or creed is specifically prohibited.

Advantech Europe also prohibits the conduct of a business enterprise, political activity, engaging in any form of intelligence collection from our facilities, engaging in fraudulent activities, or knowingly disseminating false or otherwise libellous materials.

Other activities that are strictly prohibited include, but are not limited to:

Accessing company information that is not within the scope of one's work. This includes unauthorized reading of customer account information, unauthorized access of personnel file information, and accessing information that is not needed for the proper execution of job functions.

Misusing, disclosing without proper authorization, or altering customer or personnel information. This includes making unauthorized changes to a personnel file or sharing electronic customer or personnel data with unauthorized personnel.

Deliberate pointing or hyper-linking of company Web sites to other Internet/WWW sites whose content may be inconsistent with or in violation of the aims or policies of Advantech Europe.

Use, transmission, duplication, or voluntary receipt of material that infringes on the copyrights, trademarks, trade secrets, or patent rights of any person or organization. Assume that all materials on the Internet are copyright and/or patented unless specific notices state otherwise.

Transmission of any proprietary, confidential, or otherwise sensitive information without the proper controls.

Creation, posting, transmission, or voluntary receipt of any unlawful, offensive, libellous, threatening, harassing material, including but not limited to comments based on race, national origin, sex, sexual orientation, age, disability, religion, or political beliefs.

Unless specifically authorized under the provisions of section Personal Internet Usage, the following activities are also strictly prohibited:

Unauthorized downloading of any shareware programs or files for use without authorization in advance from the IT Department and the user's manager.

- Any ordering (shopping) of items or services on the Internet.
- Playing of any games.
- Forwarding of chain letters.
- Participation in any on-line contest or promotion.
- Acceptance of promotional gifts.

Bandwidth both within Advantech Europe and in connecting to the Internet is a shared, finite resource. Users must make reasonable efforts to use this resource in ways that do not negatively affect other employees. Specific departments may set guidelines on bandwidth use and resource allocation, and may ban the downloading of particular file types.

f) Software License

Advantech Europe strongly supports strict adherence to software vendors' license agreements. When at work, or when company computing or networking resources are employed, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Questions regarding lawful versus unlawful copying should be referred to the IT Department for review or to request a ruling from the Legal Department before any copying is done.

Similarly, reproduction of materials available over the Internet must be done only with the written permission of the author or owner of the document. Unless permission from the copyright owner(s) is first obtained, making copies of material from magazines, journals, newsletters, other publications and online documents is forbidden unless this is both reasonable and customary. This notion of "fair use" is in keeping with international copyright laws.

g) Privacy

Users should consider their Internet activities as periodically monitored and limit their activities accordingly.

Management reserves the right to examine E-mail, personal file directories, web access, and other information stored on company computers, at any time and without notice. This examination ensures compliance with internal policies and assists with the management of company information systems.

Users should be aware that clear text E-mail is not a confidential means of communication. Advantech Europe cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users should also be aware that once an E-mail is transmitted it may be altered. Deleting an E-mail from an individual workstation will not eliminate it from the various systems across which it has been transmitted.

h) Periodic Reviews

To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with usage policies.

Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of usage policies. These reviews may result in the modification, addition, or deletion of usage policies to better suit company information needs

i) Amendment of Procedure

This Policy / Procedure will be reviewed on a semi-yearly base starting the date stipulated above. This document will be effective unless a further announcement of amendment.

Andrea Zolli

Managing Director, Advantech Europe

B. INTERNET AND INTRANET SECURITY POLICY

【 Advantech Europe Policies & Procedures】

Policy No.: AEUITP-002

Subject: INTERNET AND INTRANET SECURITY POLICY

Version: V1

Effective Date: June 30, 20004

Prepared By: Advantech Europe Holding

Approved By: Managing Director / Financial Controller

a) Objective

Advantech Europe's computer network introduces new resources and new services through Intranet and Internet connectivity. This connectivity not only results in new capabilities, but also in new risks and threats. This document formally defines our official policy regarding Intranet and Internet security in response to potential risks. All Internet users are expected to be familiar with and to comply with this policy.

Unless specifically stated otherwise, all statements and policies will apply to both the Intranet and the Internet.

For the purposes of this document the Internet is defined as a worldwide “network of networks” using Transmission Control Protocol/Internet Protocol (TCP/IP) for communication. The Intranet is defined as Advantech Europe's internal infrastructure connecting our facilities by using TCP/IP.

The IT Department of Advantech Europe is responsible for properly securing the data maintained in and transmitted by its computing systems and telecommunications networks. In addition, Advantech Europe is committed to preventing the occurrence of inappropriate, unethical or unlawful behaviour by any of its users. These responsibilities are not only mandated by the facility’s business interests but by legal and ethical obligations concerning the welfare and privacy of its customers and business partners. This Intranet and Internet Security Policy and its strict enforcement is an important and necessary part of the overall security strategy.

b) Scope

The scope of this policy includes the following information:

- Security threats;
- Management controls required for access security;
- Information confidentiality and protection;
- Expectation of privacy;
- Contacts for security issues and questions;
- Backup, recovery, and change management;
- Periodic reviews.

c) Requirements

The components outlined in this document focus on connectivity issues associated with Advantech Europe's host computers, PCs, routers, terminal servers, and other devices that support access to the Intranet and to the Internet. The scope of this document does not include facility-specific security policies, application security, and non-network security.

The Intranet and Internet Security Policy applies to all Intranet/Internet users (individuals working for the company, including permanent full-time and part-time employees, contract workers, temporary agency workers, business partners and vendors) who access the Intranet or Internet through the computing or networking resources. The company's Intranet/Internet users are expected to be familiar with and to comply with this policy.

Violations of the Intranet and Internet Security Policy will be documented and can lead to revocation of system privileges and/or disciplinary action up to and including termination. Additionally, the company may at its discretion seek legal remedies for damages incurred as a result of any violation. The company may also be required by law to report certain illegal activities to the proper enforcement agencies.

Before access to the company network is approved, the potential Intranet/Internet user is required to read this Intranet and Internet Security Policy and sign an acknowledgement form (located on the last page of this document). The signed acknowledgement form should be turned in and will be kept on file at the facility granting the access. For questions on the Intranet and Internet Security Policy, contact the Information Technology (IT) Department.

d) Procedures

Access Controls

User Strong Authentication - All Internet users who attempt to enter internal networks as allowed by this policy must authenticate themselves through the authentication mechanism established by the company network. Authentication prevents unauthorized users from gaining access to internal systems. Authentication techniques may employ strong authentication devices.

Strong authentication techniques enhance password level authentication through various cryptographic and bi-directional data exchanges involving dynamically generated single use passwords and/or challenge-response techniques. User authentication must be used to gain access to the network for Telnet or FTP regardless of data classification level. In addition, passwords chosen by the users must meet the requirements of the Password Policy.

Under no circumstances should users establish Internet or other external connections that could allow unauthorized outsiders to gain access to company systems and information. These connections include, but are not limited to, multi-computer file systems, Internet home pages, and FTP servers.

Traffic Flow - Unauthenticated (through strong authentication) in-bound traffic from the Internet will not be permitted except for E-mail and access to public web servers. Only authenticated users who have been approved by the IT department for access to their internal networks will be allowed in from the Internet.

Dial-up Control - Networked workstations should not be connected to separate analogue lines or modems unless required for performance of business functions and specifically authorized by the facility's IT department.

At no time should networked workstations with modems be left in an accessible state that could potentially allow unauthorized access. Direct remote dial-in to the Intranet is not allowed.

Physical Security - Physical access security measures must be taken to protect against the intentional or accidental intrusion by unauthorized individuals into any area where sensitive information may be readily accessible. Questions or issues should be brought to the attention of the IT department.

All vital system hardware must be physically protected against unauthorized access. Violations should be brought to the attention of the IT Department.

Classification and Responsibility of Information

Information Classification - Information must be classified according to the most sensitive detail it contains. Any questions about classification should be addressed to the IT Department. The following levels are to be used for classifying information:

- ✗ Level 1: Confidential Information:

This class represents important and/or highly sensitive material that is confidential according to state or federal law. Unauthorized disclosure, modification, or destruction of this information could cause serious damage to the company and its customers.

Examples of Level 1 information includes personnel information, payroll information, system access passwords, information file encryption keys, and all customer information.

- ✗ Level 2: Company Information:

This class represents information important to the company. Its destruction and/or modification could result in serious losses. This information must have controls to ensure its integrity and accuracy. Its use is therefore subject to certain restrictions.

Examples of Level 2 information includes accounting, budget, company-wide memos, local operations manuals, and company policies and procedures.

- ✗ Level 3: Unrestricted Information:

This class represents information that does not fall into one of the above classifications and is appropriate for all Advantech Europe personnel in addition to the general public. This information is not considered confidential, and its disclosure, modification and/or destruction does not need to be controlled.

Examples of level 3 information include general correspondence, newsletters, articles, speeches, photographs, brochures, advertisements, displays, and presentations.

Information Responsibilities - All Level 1 and 2 information must have an owner. Originators of information communications must determine appropriate information classifications and are the information owners. Recipients of data and information assume responsibility for subsequent handling of data and information in a manner consistent with the originators classification.

Information owners must determine appropriate information classifications, maximum acceptable unavailability, resource protection measures, and user access requirements. Level 1 and 2 information should be marked with its classification and with all other relevant handling instructions for all transmissions. Information owners must review all Level 1 and 2 information annually and re-certify their classification.

The information ownership role should not be confused with legal ownership. All company information is the property of the company.

Message Source Authentication and Integrity - Message source authentication ensures that information or data in transit is received from the named source. This is achieved with digital signatures. Digital signatures indicate that a message came from the person it is alleged to have come from.

Digital signatures not only indicate that a message came from the person it is alleged to have come from, they also indicate that a message has not been altered during transit. Digital signatures should be used whenever message integrity is considered important.

This can be used when communicating data at all classification levels. This feature should be available for Advantech Europe internal communication in the near future.

Encryption - The following data transfers over the Intranet and Internet are prohibited unless the data is encrypted by a company approved public or private key standard:

- ✗ Company information classified as Level 1,
- ✗ Credit card numbers, telephone calling card numbers,
- ✗ Login passwords and other parameters that can be used to gain access to goods or services.

In addition, Level 2 data sent over the Internet must be encrypted. It may be unencrypted on the Intranet.

Virus Detection - All software downloaded from non-company sources through the Intranet or Internet must be screened with virus detection software before being invoked. The most current release of the virus detection software and definition files must be used. These updates will be distributed as soon as they are released. When available on the market, virus detection software with the capability of checking Intranet and Internet E-mail attachments, web traffic, and FTP must be used in addition to the regular scanning of disk drives on the users' workstations.

Automatic scanning for virus must be installed on all PCs and servers accessing the Internet and should not be turned off by the user. In addition, all users must periodically scan their PCs and take responsibility for - 9 - Advantech Europe ensuring that all files sent out are free of virus infections.

If any networked workstation of Advantech Europe does not have virus software, the user should be responsible for contacting the IT department immediately.

Prohibited Usage - Activities that are strictly prohibited include, but are not limited to:

Any unauthorized, deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration;

Wilful or negligent introduction of computer viruses, Trojan horses or other destructive programs into company systems or networks or into external systems and networks;

Unauthorized decryption or attempt at decryption of any system or user passwords or any other user's encrypted files;

Packet sniffing, packet spoofing, or use of any other means to gain unauthorized access to a computing system or network. If you have any questions about Prohibited Usage, contact the IT Department.

Reporting Security Problems -

Lost or Stolen - It is the responsibility of the user to report any known or suspected breach of security, such as passwords or other system access control mechanisms to the IT department.

Virus Infection - Immediately report any virus infections or attacks to the IT department.

System Problems - Unusual system behaviour such as missing files, frequent system crashes, or miss-routed messages, should be immediately reported to the IT Department, who will refer the situation to the appropriate parties for investigation. These types of system behaviour may be related to virus infections or other security problems and must be promptly reported and investigated. The specifics of security problems should not be discussed except on a business need-to-know basis.

Confidentiality Violation - If proprietary information (Level 1 or Level 2 information as defined above) is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IT Department must be notified immediately.

Periodic Reviews

Security Compliance Reviews - To ensure compliance with this policy, periodic reviews will be conducted. These reviews will include testing the degree of compliance with security policies.

Policy Maintenance Reviews - Periodic reviews will be conducted to ensure the appropriateness and the effectiveness of security policies. These reviews may result in the modification, addition, or deletion of security policies to better suit company information needs.

e) Amendment of Procedure

This Policy / Procedure will be reviewed on a semi-yearly base starting the date stipulated above. This document will be effective unless a further announcement of

amendment.

Andrea Zolli

Managing Director, Advantech Europe

C. EMAIL POLICY

【 Advantech Europe Policies & Procedures】

Policy No.: AEUITP-003

Subject: E-Mail POLICY

Version: V1

Effective Date: June 30, 2004

Prepared By: Advantech Europe Holding

Approved By: Managing Director / Financial Controller

EXECUTIVE SUMMARIES

a) Objective

To define the guidelines concerning the Advantech Europe E-mail system.

b) Scope

This procedure applies to all Advantech Europe employees, and any other personnel granted access to the Advantech Europe E-mail system.

The term E-mail refers to text-based electronic communication systems used to deliver messages asynchronously

c) Requirements

The Advantech Europe's E-mail system is company property and is intended for Advantech Europe business. Staff and contractors who violate any aspect of this policy will be subject to disciplinary action up to and including dismissal. The severity of such disciplinary action will be dictated and prescribed - 1 - Advantech Europe according to Human Resource policies. Business associates who violate any aspect of this policy will have their E-mail access revoked.

d) Procedures

E-mail Access - All full time and part time Advantech Europe employees shall be extended E-mail privileges upon employment with the company. Temporary workers and contractors will be extended such privileges on a case-by-case basis depending on job necessity. Terminated employees' E-mail access will be canceled upon leaving

Advantech Europe.

Permissible Uses - The use of E-mail and related resources should be for company business only. Employees may want to use E-mail for personal communication that is not directly related to their role within the company, and a minimal amount of such use is acceptable. However, employees are expected to use good judgment and to limit the amount and frequency of such use.

E-mail users should use the same care and judgement in creating and transmitting E-mail messages that they would in formal business correspondence. Language that would not be used in face-to-face communication or in formal business correspondence should not be used in E-mail. Language that can create or further hostile attitudes or give offence on the basis of race, colour, religion, national origin, citizenship, ancestry, marital status, sex, mental or physical challenge, disability, age, veteran's status, or sexual orientation must not be used.

E-mail users should exercise caution and judgment when transmitting information that requires authorization, verification, or disclosure protection. E-mail is not certified to be encrypted or authenticated.

The use of E-mail must be in compliance with all applicable local, state, and federal statutes (ADL), and all Advantech Europe policies and procedures.

Prohibited Uses - Use of the Advantech Europe E-mail systems for any of the following purposes is prohibited:

The solicitation of funds, political messages, threats, harassment, slander, defamation, obscene messages, gambling, non-Advantech Europe Business/commercial activities, fraud, or other illegal activities;

The unauthorized disclosure of personal, Advantech Europe, or other information;

The sending of chain letters, Spam, unsolicited commercial email, or junk email;

The intimidation of others or interference with the ability of others to conduct business;

The transmission of information to individuals inside or outside Advantech Europe who do not have a legitimate need to receive the information;

The copying and/or illegal transportation of any document, software, or other work protected by copyright and/or patent law;

The sending of messages to which access is restricted by laws or regulations;

The construction of E-mail messages so that they appear to be from someone else (e.g. by forging E-mail headers).

The following access to Advantech Europe E-mail systems is also prohibited:

Obtaining access to the files or communications of others for the purpose of satisfying idle curiosity, with no substantial Advantech Europe business purpose;

Attempting to intercept any E-mail transmissions without proper authorization;

Attempting to breach any security measures on any E-mail system without proper authorisation;

Capture and "opening" of undeliverable E-mails, except as required in order for authorised employees to diagnose and correct delivery problems.

Privacy and Disclosure - Advantech Europe E-mail is NOT private. E-mail messages, files, and calendars are business records. Advantech Europe reserves the right to, without prior notice and for any reason, monitor, access, review, copy, delete, disclose, and distribute to any party any message sent,received, or stored on the Advantech Europe E-mail system.

Advantech Europe will make reasonable efforts to maintain the integrity and effective operation of its E-mail systems, but users are advised that those systems should in no way be regarded as a secure medium for the communication of sensitive or confidential information. Because of the nature and technology of E-mail, Advantech Europe can assure neither the privacy of an individual user's use of the Advantech Europe E-mail resources nor the confidentiality of particular messages that may be created, transmitted, received, or stored thereby.

E-mail information is occasionally visible to IT staff engaged in routine testing, maintenance, and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of E-mail messages.

Requests to disclose E-mail will be submitted in writing on the E-mail Disclosure Request form. The form will be delivered to the Chief Operating Officer with a copy to legal counsel. Administration and Company’s lawyer will convene to determine the appropriateness of such a request.

E-mail Retention - Most E-mail messages are a form of temporary communication and may be discarded routinely by either the sender or the recipient. However, depending on the content of the E-mail message, it may be considered a more formal record and should be retained.

E-mail backups are created for the purpose of business recovery. Information stored electronically is subject to the legal discovery process and can be subpoenaed.

e) Amendment of Procedure

This Policy / Procedure will be reviewed on a semi-yearly base starting the date stipulated above. This document will be effective unless a further announcement of amendment.

Andrea Zolli

Managing Director, Advantech Europe