

Projekt eliminace rizik elektronického podnikání ve firmě HP TRONIC, spol. s r. o.

Bc. Miroslav Poštolka

Diplomová práce
2005



Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav podnikové ekonomiky
akademický rok: 2004/2005

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Bc. Miroslav POŠTOLKA**
Studijní program: **N 6208 Ekonomika a management**
Studijní obor: **Podniková ekonomika**

Téma práce: **Projekt eliminace rizik elektronického podnikání ve firmě HP TRONIC, spol. s r. o.**

Zásady pro vypracování:

1. Vymezte rámec aktuálních projektových příležitostí firmy HP TRONIC, spol. s r. o.
2. Provedte analýzu dostupných literárních pramenů a informačních zdrojů k dané problematice.
3. Stanovte východiska pro zpracování projektu.
4. Vypracujte projekt eliminace rizik elektronického podnikání ve firmě HP TRONIC, spol. s r. o.
5. Verifikujte projektové řešení v návaznosti na bod 4.
6. Prezентуйте a zdůvodněte efektivnost daného projektového řešení spolu se závěrečným doporučením pro firmu HP TRONIC, spol. s r. o.

ABSTRAKT

Diplomová práce se zabývá bezpečností elektronického podnikání a informačního systému ve firmě. Zaměřuje se na nejdůležitější rizika spojená s provozem informačního systému pro podporu elektronického podnikání a řeší možnosti, jak je eliminovat. V první části práce je zpracována literatura vysvětlující pojmy z oblasti elektronického podnikání a bezpečnosti informačních systémů. Druhá, analytická část představuje firmu HP TRONIC, spol. s r. o. a zhodnocuje stav informační bezpečnosti v tomto podniku. Poslední, projektová část pak navrhuje možnosti a opatření, jak eliminovat bezpečnostní rizika a slabé stránky informačního systému ve firmě HP TRONIC, spol. s r. o.

ABSTRACT

The diploma work deals with the security of information system in a company engaged in e-business. The final thesis concentrates on the most important risks connected with the information system operation supporting the electronic business. The main aim of the work is to solve the possibilities how to eliminate these risks. The first part of the thesis processes the literature explaining important terms from the e-business and the information systems security area. The second, analytical part introduces the firm HP TRONIC, spol. s r. o. and evaluates the state of the information security in this company. The last, practical part suggests possibilities and solutions how to eliminate the security risks and weaknesses of the information system in HP TRONIC, spol. s r. o.

Děkuji vedoucímu své diplomové práce Mgr. Romanu Jaškovi, Ph.D. za odborné vedení cenné rady a připomínky a panu Stanislavu Šimčíkovi za poskytnutí podmínek ke zpracování diplomové práce.

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a použitou literaturu jsem citoval.

Ve Zlíně 5.5. 2005

.....
Miroslav Poštolka

ÚVOD.....	6
I. TEORETICKÁ ČÁST	7
1 POJMY A DEFINICE V ELEKTRONICKÉM PODNIKÁNÍ.....	8
1.1 EDI (ELECTRONIC DATA INTERCHANGE).....	8
1.1.1 Důvody zavádění EDI	9
1.2 TECHNOLOGIE INTERNETU V OBCHODU A PODNIKÁNÍ	10
1.2.1 Elektronické podnikání	10
1.2.2 Elektronické obchodování.....	11
1.2.3 B2B	12
1.2.4 B2C	13
2 INFORMAČNÍ SYSTÉM V PODNIKU	16
2.1 DEFINICE BEZPEČNÉHO INFORMAČNÍHO SYSTÉMU.....	16
2.2 INFORMAČNÍ BEZPEČNOST	16
2.2.1 Definice informační bezpečnosti.....	17
2.2.2 Cíle informační bezpečnosti.....	17
2.2.3 Závislost prosperity firmy na bezpečnosti informací.....	17
2.3 PROCES ŘEŠENÍ INFORMAČNÍ BEZPEČNOSTI	18
2.3.1 Strategie řešení informační bezpečnosti	19
2.3.2 Analýza rizik IS.....	20
2.3.3 Bezpečnostní politika IS	20
2.3.4 Bezpečnostní směrnice a standardy	21
2.3.5 Implementace bezpečnosti IS.....	21
2.3.6 Monitorování a kontrola.....	21
2.4 ANALÝZY BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU	22
2.4.1 Efekty bezpečnostní analýzy	22
3 HROZBY INFORMAČNÍCH SYSTÉMU V ELEKTRONICKÉM PODNIKÁNÍ.....	24
3.1 POČÍTAČOVÉ VIRY	24
3.1.1 Typy virů.....	25
3.2 HACKING.....	26
3.3 LIDSKÝ FAKTOR UVNITŘ ORGANIZACE	27
3.4 OSTATNÍ HROZBY	27
3.5 NEJČASTĚJŠÍ OHROŽENÍ ZABEZPEČENÍ V SÍTÍCH	27
3.5.1 Předstírání identity (Spoofing).....	27
3.5.2 Neoprávněné změny (Tampering).....	27
3.5.3 Odvolatelnost (Repudiation)	28
3.5.4 Zveřejnění informací (Information disclosure).....	28
3.5.5 Odepření služby (Denial of Service).....	28
3.5.6 Zvýšení oprávnění (Elevation of privilege)	28
4 NEJDŮLEŽITĚJŠÍ MOŽNOSTI OCHRANY DAT PŘED HROZBAMI.....	29
4.1 ANTIVIROVÉ PROGRAMY	29
4.2 FIREWALLY	30

4.3	KRYPTOGRAFIE	32
4.3.1	Symetrické šifrovací algoritmy	32
4.3.2	Asymetrické šifrovací algoritmy	33
4.4	KONTROLA PŘÍSTUPU	33
4.4.1	Autentizace pomocí znalosti, kterou disponuje daná osoba	33
4.4.2	Autentizace pomocí fyzického znaku dané osoby – biometrie	34
4.4.3	Autentizace pomocí daného bezpečnostního předmětu	34
4.4.4	Šifrování dat na discích a v lokální síti	34
4.5	ZÁLOHOVÁNÍ A ARCHIVACE	35
4.5.1	Zálohování dat	35
4.5.2	Zálohování hardwaru	36
4.5.3	Zálohování zdrojů napájení	36
4.6	ZABEZPEČENÍ KOMUNIKACÍ PROSTŘEDNICTVÍM SSL (SECURE SOCKET LAYER)	36
4.7	ELEKTRONICKÝ (DIGITÁLNÍ) PODPIS	37
5	NORMY Z OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ	39
5.1	NORMA ISO 17799 – KOMPLEXNÍ CHÁPÁNÍ BEZPEČNOSTI INFORMACÍ	39
II.	ANALYTICKÁ ČÁST	40
6	PŘEDSTAVENÍ FIRMY HP TRONIC ZLÍN, SPOL. S R. O.	41
6.1	HISTORIE SPOLEČNOSTI	41
6.2	PŘEDMĚT ČINNOSTI	41
6.3	FILOZOFIE FIRMY	42
6.4	VYBRANÉ EKONOMICKÉ ÚDAJE SPOLEČNOSTI	42
6.5	ORGANIZAČNÍ USPOŘÁDÁNÍ SKUPINY HP TRONIC	43
6.6	ELEKTRONICKÉ OBCHODY FIRMY HP TRONIC, SPOL. S R. O.	44
6.6.1	Elektronický obchod typu Business to customer (B2C) – ePROTON	44
6.6.2	Elektronický obchod typu Business to Business (B2B) – HPONLINE	45
7	ANALÝZA STAVU INFORMAČNÍ BEZPEČNOSTI VE FIRMĚ HP TRONIC, SPOL. S R. O.	46
7.1	ZODPOVĚDNOST ZA BEZPEČNOST INFORMAČNÍHO SYSTÉMU	47
7.2	SPRÁVA MÍSTNÍ SÍTĚ (LAN)	47
7.3	OPERAČNÍ SYSTÉM	49
7.4	ANTIVIROVÁ OCHRANA DAT V PODNIKU	50
7.5	PODNIKOVÉ FIREWALLY	52
7.6	PŘÍSTUP K SÍTI INTERNET	52
7.7	ZÁLOHOVÁNÍ	53
7.8	PŘÍSTUP K POČÍTAČŮM, SÍTI, DATŮM A SYSTÉMU	54
7.9	AUDIT (PROTOKOLOVÁNÍ, KONTROLA)	56

7.10	ZABEZPEČENÍ KOMUNIKACÍ NA WEBU	56
8	SILNÉ A SLABÉ STRÁNKY STAVU ZABEZPEČENÍ VE FIRMĚ HP TRONIC, SPOL. S R. O.	57
9	STAV INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE	59
III.	PROJEKTOVÁ ČÁST.....	64
10	PROJEKT ELIMINACE BEZPEČNOSTNÍCH RIZIK ELEKTRONICKÉHO PODNIKÁNÍ.....	65
10.1	NÁVRH ÚTVARU BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU	68
10.2	ZLEPŠENÍ BEZPEČNOSTI V OBLASTI ANTIVIROVÉ OCHRANY.....	70
10.3	ZVÝŠENÍ ÚROVNĚ ZABEZPEČENÍ INTERNETU	72
10.4	VYŠŠÍ BEZPEČNOST V OBLASTI KONTROLY PŘÍSTUPU (K POČÍTAČŮM, SÍTI, DATŮM).....	74
10.5	NÁVRH PRO BEZPEČNÉ ULOŽENÍ ZÁLOHOVANÝCH DAT	76
10.6	EVIDENCE, KONTROLA A ÚDRŽBA HARDWARU A SOFTWARE SÍŤE	77
10.7	PLÁN KONTINUITY IS	78
10.7.1	Postup vytváření plánu kontinuity	79
10.7.2	Oblasti, které pokrývá plán kontinuity IS	81
11	SHRNUTÍ PROJEKTOVÉ ČÁSTI.....	83
11.1	ZHODNOCENÍ NAVRHOVANÝCH ŘEŠENÍ	83
	ZÁVĚR.....	86
	SEZNAM POUŽITÉ LITERATURY	87
	SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK	89
	SEZNAM OBRÁZKŮ	90
	SEZNAM TABULEK A GRAFŮ	91
	SEZNAM PŘÍLOH.....	92

ÚVOD

V dnešní postindustriální době za probíhající technologické revoluce se stává nejdůležitějším zbožím globalizované společnosti informace. Informace se staly hlavním prostředkem i produktem nové doby. Vzájemné propojování informačních a komunikačních technologií vede ke vzniku a rozvoji informační společnosti. Kdo nehraje aktivní úlohu v dnes dynamicky rozvíjející se informační společnosti a nepřijímá jejich atributy se postupně dostává na okraj informační společnosti, kde je odsouzen k zániku. Dochází ke gigantickému rozmachu informačních technologií a tím i informačních systémů. Pryč jsou doby kartoték a papírových podnikových archivů. Již několik let se tyto kartotéky a archivy digitalizují. Na internetových sítích najdeme obrovské databáze informací. V souvislosti s rozvojem internetových technologií vznikají pro organizace a podniky nové příležitosti a možnosti pro podnikání.

V moderním světě elektronického obchodu jsou úspěšné organizace schopny rychle vyhledávat nové příležitosti k elektronickému podnikání (e-business), současně ale zjišťují, že bezpečnost informací je klíčovým podnikatelským problémem. Přesné, dostupné a bezpečné informace jsou absolutně nezbytné pro řízení a provozování moderního podnikání. Vznikly a etablovaly se nové velmi úspěšné dot.com organizace a vznikají stále další s nezměněnou intenzitou. K nim musíme přiřadit i stávající organizace a podniky, které se chopily nových technologií elektronického obchodování (e-commerce) dostupných přes Internet. Vznikají firmy, jejichž podstata je založena na nabídce svých produktů pouze prostřednictvím Internetu. Tyto firmy si však musí uvědomit, že bezpečnost jejich informačních systémů je pro ně klíčovým pojmem. Je však třeba říci, že v novém, rychle se vyvíjejícím globálním prostředí elektronického podnikání (e-business) nejsou požadavky informační bezpečnosti adekvátně chápány. To má za následek, že se některé z podniků mohou ocitnout v kritickém ohrožení.

Právě výše zmíněné skutečnosti mě vedly k tomu, abych se ve své diplomové práci zabýval tématem souvisejícím s informační bezpečností a to konkrétně v podniku, který se zabývá elektronickým podnikáním. Zajímalo mě, jaká rizika může takové podnikání pro podnik znamenat v souvislosti s bezpečností informačního systému a jaké jsou možnosti jejich eliminace. Byl jsem proto velmi potěšen, když mi byl ve firmě HP TRONIC, spol. s r. o. umožněn přístup k důležitým informacím a poznatkům, které jsem mohl ve své práci využít.

I. TEORETICKÁ ČÁST

1 POJMY A DEFINICE V ELEKTRONICKÉM PODNIKÁNÍ

Mladým a přitom bouřlivě se rozvíjejícím oborem informatiky je elektronické podnikání. Snad právě pro svou mladost zatím disponuje mnoha názvy. Můžeme se setkat s označením elektronický obchod, elektronické obchodování, e-commerce či e-business. Dokonce ani obsah elektronického podnikání ještě není přesně vymezen. Podstatné je, že se jedná o nabídku obchodních aktivit prostřednictvím počítačové sítě, většinou Internetu, a že přinejmenším část komunikace mezi obchodujícími subjekty probíhá na základě elektronické výměny informací. [12]

1.1 EDI (Electronic Data Interchange)

EDI (Electronic Data Interchange) je elektronická výměna strukturovaných standardních zpráv mezi dvěma aplikacemi dvou nezávislých subjektů. V systémech EDI spolu přímo komunikují počítačové aplikace nebo informační systémy obchodních partnerů a mohou si tak automatizovaně nebo s minimem lidských zásahů předávat obchodní dokumenty, jako jsou faktury a objednávky, dvacet čtyři hodin denně. Hlavním cílem těchto systémů je postupné nahrazování papírových dokumentů elektronickými, které mají nakonec stejnou právní váhu jako dokumenty klasické. Jsou však daleko bezpečnější a jejich předávání je efektivnější a levnější. EDI se nasazuje všude tam, kde se pravidelně předávají standardní doklady.[13]

EDI je elektronická výměna dat (zpráv), mezi nezávislými subjekty, splňující tyto charakteristiky:

1) integritu

- změna zprávy během přenosu bude odhalena,
- zpráva byla odeslána konkrétní osobou,
- zpráva přišla ve správném pořadí,

2) autentičnost

- určení osoby, která zprávu odeslala,
- neodmítnutí původu zprávy,
- neodmítnutí příjmu zprávy,

3) důvěrnost zprávy

- zajištění obsahu zprávy před nepovolanými osobami,

4) připuštění v právním rámci

- metody, které byly použity, jsou v souladu s právním kodexem. Toto vyžaduje, aby všechny zúčastněné strany pečlivě smluvně vymezily vztahy mezi sebou navzájem.[13]

1.1.1 Důvody zavádění EDI

V zavádění EDI lze vysledovat tři stupně realizace podle toho, jak hluboko EDI zasahuje do aktivit podniku:

1. **Náhrada papírových dokladů** je z těchto tří stupňů nejméně náročná a také nejméně nákladná. Kritériem její úspěšnosti je dostatečné množství informací (dostatečný počet zpráv) vyměňovaných s obchodními partnery. Její výhody se projevují ve snížení nákladů na administrativu a na poštovné, v omezení výskytu chyb a v úspoře času při výměně informací.
2. Integrace EDI do stávajících informačních systémů **představuje (užitečný) zásah do podnikových informačních systémů**. Aby se využily výhody EDI, jako je například rychlost komunikace s obchodními partnery, musí tato rychlost mít odpovídající odezvu i uvnitř podniku. Například systém přijímání objednávek bude vyžadovat zlepšení evidence zásob, rychlejší zadávání objednaného zboží do výroby apod. Nebo odesílání faktur cestou EDI by mělo navazovat na pohotový systém pro získání dat potřebných k vystavení faktury. **Výhodou tohoto stupně je** snížení skladových zásob, nová logistická koncepce, zlepšení toků peněz, vyšší produktivita práce a omezení výskytu chyb.[13]
3. EDI jako zprostředkující technologie **umožňuje radikálním způsobem změnit obchodní koncepci firmy a vztahy k jejím partnerům**. EDI se zde stává nedílnou součástí provozní technologie moderního podniku, jehož všechny funkce jsou optimalizovány a vzájemně plně sladěny. V tomto stupni EDI také umožňuje činnost flexibilním obchodním organizacím, které jsou schopné pružně se přizpůsobit a reagovat na proměnlivé požadavky zákazníků a vlivy okolí. EDI je

zde prostředkem k dosažení nové kvality podniku a úspora nákladů je přitom jen sekundárním efektem celkové obchodní strategie. [13]

1.2 Technologie internetu v obchodu a podnikání

Nové technologie umožňující šíření informací nejen uvnitř podniků a organizací, ale i směrem k jejich klientům a zákazníkům spolu se vzrůstající popularitou Internetu mezi všemi vrstvami obyvatelstva vytváří zcela nové podmínky pro velké, střední i malé podnikání. V souvislosti s pronikáním nových technologií do ekonomických strategií podniků se objevuje celá řada nových pojmů a termínů. Většina z nich začíná prefixem „E-“ nebo „e-“, který byl převzat ze všeobecně používaného označení elektronické pošty – „e-mail“. Jako příklady lze uvést pojmy „e-business“, „e-commerce“, „e-tailing“, „e-service“, „e-payment“. Všechny tyto pojmy označují určité ekonomické aktivity nebo děje, které probíhají s podporou nebo prostřednictvím elektronických technologií. V tomto kontextu lze považovat elektronické technologie za technologie, které se označují jako technologie Internetu.[7]

1.2.1 Elektronické podnikání

E-business je způsob podnikání využívající technologie Internetu jak v oblasti řízení podniku, tak v oblasti spolupráce s partnerskými podniky, v oblasti nákupu a prodeje, poskytování služeb zákazníkům atd. E-business tedy představuje komplexní řešení založené na elektronických (Internetových) technologiích.

Pojem e-business se stále častěji objevuje v ekonomicko podnikových tématech již od r.1997, kdy firma IBM realizovala rozsáhlou kampaň, jejíž záměrem byla popularizace nových možností, které do podnikání a obchodování přinesl stále se rozvíjející a rozšiřující se Internet. V současnosti se většina podniků nachází v některém z vývojových fází zavádění business a snad neexistuje podnik, jehož management by si alespoň nezbytnost zavedení nového systému podnikání neuvědomoval.[7]

Základem pro úspěšné naplnění záměru zavést v podniku e-business (ale též pro realizaci ecommerce, e-service atd.) je:

- kvalitní, průchodná, spolehlivá infrastruktura lokální podnikové sítě zaručující bezpečné datové přenosy
- propojení páteřního segmentu lokální sítě do Internetu vysokorychlostním spojem

- servery určené k poskytování klientských služeb vybavené robustním hardwarem s vyhovujícími technickými parametry a vhodným operačním systémem, který garantuje bezpečnost dat uložených v tomto výpočetním systému
- aplikační programové vybavení, splňující veškeré funkční a bezpečnostní požadavky a poskytující srozumitelné a pohodlné uživatelské rozhraní
- kvalifikovaný a vyškolený personál, zajišťující funkčnost všech výše vyjmenovaných složek.[7]

Pojem e-business je chápán v širším měřítku než e-commerce, asi tak, jako je obchodování podmnožinou samotného podnikání.[7]

1.2.2 Elektronické obchodování

Elektronické obchodování (*e-commerce*) je prodej a nákup zboží a služeb prováděný na základě elektronických technologií zpravidla v rámci internetového systému WWW . Pro přímý internetový maloobchodní prodej se používá někdy označení *e-tailing* nebo *e-retail*.

Oblast e-commerce je tvořena obchodními kanály mezi zúčastněnými obchodními stranami. Podle typu těchto zúčastněných stran lze obchodní kanály označit jako:

- **B2B** (*Business-to-Business*) kanály, kde na obou koncích obchodního kanálu jsou obchodní partneři, kteří s podporou internetových technologií provádějí mezipodnikové obchodní transakce.
- **B2C** (*Business-to-Customer*) kanály, kde jednou stranou je obchodník nebo poskytovatel služby a druhou stranou je koncový zákazník nebo klient.

Společným rysem obchodních kanálů B2B a B2C je to, že představují permanentně funkční virtuální spojení mezi klientem a poskytovatelem. Celá obchodní transakce probíhá bez přímého fyzického kontaktu zúčastněných stran. Geografická vzdálenost mezi pracovišti obchodních partnerů je nevýznamná.[7]

Základním rozdílem mezi B2B a B2C komercí je vzájemný vztah zúčastněných stran. U B2B obchodování se jedná zpravidla o dlouhodobější obchodní vztah mezi firmami (např. firma dodávající materiál a firma vyrábějící z tohoto materiálu určitý produkt, výrobce určitého produktu a jeho dealer, apod.). Tyto obchodní vztahy bývají mnohdy i smluvně podloženy. U B2C obchodování se jedná o prodej zboží koncovému zákazníkovi nebo o poskytování placených služeb. Typické pro B2C jsou jednorázově navazované vztahy prodávající - spotřebitel, bez nutnosti jejich dlouhodobého smluvního podchycení.

Další pojmy související s *e-commerce* oblastí jsou např.:

- ***E-marketplace***, což je virtuální, internetové tržiště, kde se on-line stýká nabídka s poptávkou. Jeho hlavní výhodou je možnost efektivního a pohodlného srovnání cen, dodacích a platebních podmínek a především technických parametrů jednotlivých produktů. Rozlišujeme *spotřebitelský e-marketplace*, kde se uplatňuje B2C, a *firemní e-marketplace*, kde mezi sebou obchodují pouze firmy formou B2B. Virtuální tržiště (používá se i termín burza) mohou být *vertikální B2B marketplace*, který se specializuje na určité průmyslové odvětví (např. hutní průmysl, chemický průmysl) a *horizontální B2B marketplace*, specializovaná na určitý typ zboží (např. potřeby pro zdravotnická zařízení, kancelářské potřeby, apod.). Účelem *e-marketplace* je zefektivnit vztahy uvnitř dodavatelsko-odběratelského řetězce a vytvořit prostředí pro navázání nových partnerských obchodních vztahů mezi podniky.
- ***E-mall***, což je virtuální nákupní centrum, zahrnující soustavu elektronických obchodů, pokrývajících určitý segment trhu. *E-mall* poskytuje zákazníkům další přidané služby jako např. možnost zapojit se do diskusních fór, populární souhrny „otázek a odpovědí“ (tzv. FAQs) apod.
- ***E-procurement***, což je "obstarávání" něčeho prostřednictvím Internetu. V podstatě jde o realizaci nákupu -- poptávky směrem od klienta, obvykle velkého podniku (např. podnik tímto způsobem zajišťuje nákup kancelářských potřeb, čistících a hygienických potřeb apod.). Poptávající subjekty specifikují svoje požadavky a *e-procurement* zajistí jejich naplnění. Cílem je tvorba hodnoty, resp. úspora nákladů kupujícího.[7]

1.2.3 B2B

Cílem B2B je zajištění bezpečné komunikace mezi obchodujícími partnerskými firmami, tj.: předávání dokumentů, uzavírání obchodních kontraktů, navazování dlouhodobých obchodních vztahů a realizování vlastních obchodních transakcí. Jeho smyslem je zjednodušení komunikace v dodavatelsko-odběratelském řetězci. Vztahy mezi jednotlivými firmami B2B trhu jsou téměř vždy formálně smluvně upraveny a výměna dokumentů probíhá podle mnohdy zákonem stanovených pravidel. Elektronicky prováděný obchod mezi podniky má především zvýšit efektivnost jednotlivých procesů a snižovat transakční náklady. [7]

Síťové přenosy dat zvyšují operativnost obchodních procesů, neboť doba oběhu dokladů se zkracuje ze dnů na minuty, nejvýše hodiny. Elektronické dokumenty jsou odolné proti chybivosti (u „papírových“ dokumentů může dojít k zavlečení chyby např. při přepisování údajů) a lze je snadno archivovat na elektronických paměťových médiích. [7]

Pro mnohé partnerské firmy je automatizovaná výměna elektronických dokladů již běžnou praxí. Je založena na systému EDI (Electronic Data Interchange) podporujícím elektronickou výměnu strukturovaných standardních zpráv mezi dvěma aplikacemi běžících na nezávislých subjektech. Systém EDI zaručuje integritu, autentičnost a důvěrnost zpráv. Vlastní zprávy jsou standardizovány. V rámci standardu jsou definovány formáty položek, číselníky a typové zprávy. Jako příklad jednoho z mnoha EDI standardů lze uvést UN/EDIFACT (United Nations/EDIFACT for Administration Commerce and Transport), který definuje velký počet různých zpráv pro státní správu, obchod a dopravu (objednávky, faktury, platební příkazy, daňová přiznání, celní deklarace atd.). [7]

Přenosy zpráv v systému EDI zajišťuje komunikační systém VAN (Value Added Network). VAN je nezávislá třetí strana, která obchodujícím stranám poskytuje nejen technické služby (přenosy zpráv, archivace dokumentů, technická podpora uživatelů), ale i služby administrativní (řeší smluvní vztahy uživatelů atd.). [7]

Mnohé podniky využívají pro svá řešení B2B systémy EDI, z nichž se začínají derivovat nové implementace integrující internetové služby a technologie, zvláště pak e-mail a technologie WWW. Jeden z možných nástupců EDI je bezesporu standard XML. [7]

Vývoj v oblasti B2B komerce probíhá velmi dynamicky a zatím nelze jednoznačně předvídat, zda směřuje k vytvoření jediného universálního B2B standardu nebo k vytvoření řady více i méně kompatibilních B2B systémů. [7]

1.2.4 B2C

B2C - zkratka „business to consumer“ - označuje elektronické komerční a marketingové aktivity či transakce mezi firmou a konečným spotřebitelem zboží či služby. Spotřebitelem přitom může být jak soukromá osoba, tak firma či podnikatel. Jedná se vlastně o obdobu klasického "kamenného" obchodu na Internetu. B2C se stává součástí obchodních strategií firmy a rozšiřuje tak významně oblast jejich obchodních aktivit. Některé obchody na

Internetu dokonce nemají žádnou „kamennou“ část, jsou to tedy obchody pouze virtuální. Takový typ obchodů bývá označován jako „*dot-com*“ („*.com*“) obchod.

B2C obchody přinášejí oběma partnerům, tj. obchodníkovi i zákazníkovi mnohé výhody. Jsou to zejména:

- snížení transakčních nákladů
- zjednodušení administrace obchodu
- přesná znalost nakupujícího
- individuální přístup k zákazníkovi
- možnost rychle a pružně reagovat na požadavky zákazníka
- optimalizace výroby a skladu
- trvalá dostupnost (7 dní v týdnu, 24 hodin denně)
- možnost využití B2C portálů
- levný a globální marketing
- získání konkurenční výhody

Obzvláště možnost získání konkurenční výhody a získání pevné pozice na trhu je významné pro menší a začínající firmy, které by v „kamenném“ obchodním světě jen stěží uspěly v konkurenci s velkými a zavedenými obchody. Zavedení internetového obchodu představuje zautomatizování veškerých procesů, které při obchodní transakci proběhnou mezi zákazníkem a obchodníkem. Velmi důležitou roli hraje též zajištění předprodejní a poprodejní fáze, i když vlastní obchodní transakci nevytvářejí.[7]

Zaujmout potenciálního zákazníka a přesvědčit ho o výhodnosti nákupu je možné prostřednictvím katalogů zboží, technickým popisem produktů a referencemi zveřejněnými na Web site obchodu. Do poprodejní péče o zákazníka patří především tzv. „call“ centrum, kam může zákazník zasílat své dotazy a připomínky prostřednictvím elektronické pošty, přímo z Web stránky obchodu nebo telefonicky. Protože o dotyčném zákazníkovi existují v zákaznické databázi záznamy o jeho nákupech, může s ním být jednáno zcela individuálně. Obchodní transakce mezi zákazníkem a obchodníkem prochází několika stádii. Jsou to:

- výběr zboží
- objednání zboží
- vyřízení objednávky

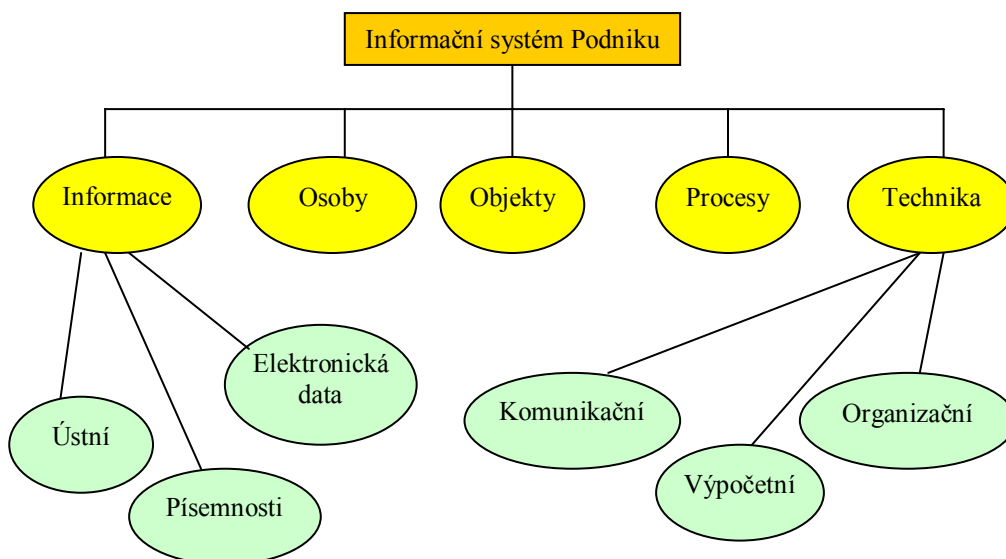
- účtování a platba [7]

Samostatným úkonem je dodávka zboží. Způsob dodávky je dán charakterem obchodovaného zboží. Jiný způsob dodávky lze samozřejmě použít u zboží nehmotného charakteru (např. softwarové produkty je jednoduše možné doručit zákazníkovi prostřednictvím Internetu) a jiný způsob volí obchodník u dodávky zboží hmotného charakteru (doručení poštou, vyzvednutí ve skladu apod.).

Řešení B2C využívá celou řadu internetových technologií. Kromě jazyka HTML je to zejména DHTML (dynamické HTML), jazyk XML, WML (pro možnost přístupu do internetového obchodu přes mobilní zařízení) a další programátorské nástroje a technologie jako: Java Applets, Java Scripts, VB Script (Visual Basic Script), ASP (Active Server Pages), PHP (Professional Home Pages), databázové servery a další. Vytvářejí na straně serveru i na straně klienta interaktivní uživatelské rozhraní, reagující na zadání zákazníka, pro něhož má být celý postup obchodní transakce jednoduchou a transparentní operací. [7]

2 INFORMAČNÍ SYSTÉM V PODNIKU

Informační systém podniku (IS) je definován jako systém informací procházejících firmou. Za účelem uskutečnění cílů IS je využíváno IT (informačních technologií) což jsou podpůrné prostředky technického charakteru.[4]



Obr. 1: Informační systém podniku [4]

2.1 Definice bezpečného informačního systému

Bezpečný informační systém definujeme jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti. Protože se každý informační systém (IS) skládá z více součástí, může být bezpečný IS vybudován pouze aplikací komplexních ochranných mechanismů. Ovšem i zde je nutné si uvědomit, že absolutní bezpečnost neexistuje a tedy vždy nutně existuje míra akceptovatelného rizika.[4]

2.2 Informační bezpečnost

Informační bezpečnost jako obor zabývající se zabezpečením informací v počítačových technologiích je relativně nový pojem. Jeho počátky je možné vysledovat v první polovině osmdesátých let v období, kdy se v masovém měřítku začínají přesouvat agendy a data všeho druhu do privátních výpočetních systémů. Tyto systémy, jejichž hodnotu zatím představovala jen jejich pořizovací cena, se rázem stávají centrem soustředění nesmírných

hodnot. Finanční domy vedou ve svých informačních systémech evidence účtů svých klientů, podniky je používají pro řízení výroby, armády do nich umísťují i ty nejutajovanější informace o obraně států. [4]

2.2.1 Definice informační bezpečnosti

Informační bezpečnost chápeme jako zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto hodnot. [4]

2.2.2 Cíle informační bezpečnosti

Základním cílem je ochrana a eliminace hrozeb včetně jejich dopadů. Hrozbami jsou například:

- kompromitace
- nedovolená modifikace (změna hodnot)
- destrukce části, nebo celého informačního systému
- zneužití citlivých informací
- použití klamných dat, ze kterých budou odvozeny chybné výsledky a závěry
- špatná interpretace hodnot
- neoprávněný přístup k hmotným (hardware) i nehmotným (data, informace) hodnotám
- únik informací (kopie, krádež, odvození požadovaných údajů ze získaných zdrojů dedukcí [4])

2.2.3 Závislost prosperity firmy na bezpečnosti informací

Informační bezpečnost, bezpečnost informací, prosperita firmy, konkurenceschopnost podniku. Toto vše jsou slovní spojení vázající se k ochraně informací s cílem zabezpečit jejich přiměřené utajení. Cílem je zajištění, aby někdo jiný nezískal takové možnosti, které by mu umožnily získat na úkor „mé“ společnosti větší část pomyslného nabízeného tržního koláče v jeho podnikatelské působnosti, aby nezískal konkurenční výhodu. Jde tedy o to, aby nedošlo k nechtěnému úniku významných informací, případně aby nedošlo k fyzickému odstavení informační bezpečnosti s příslušným odborným personálním

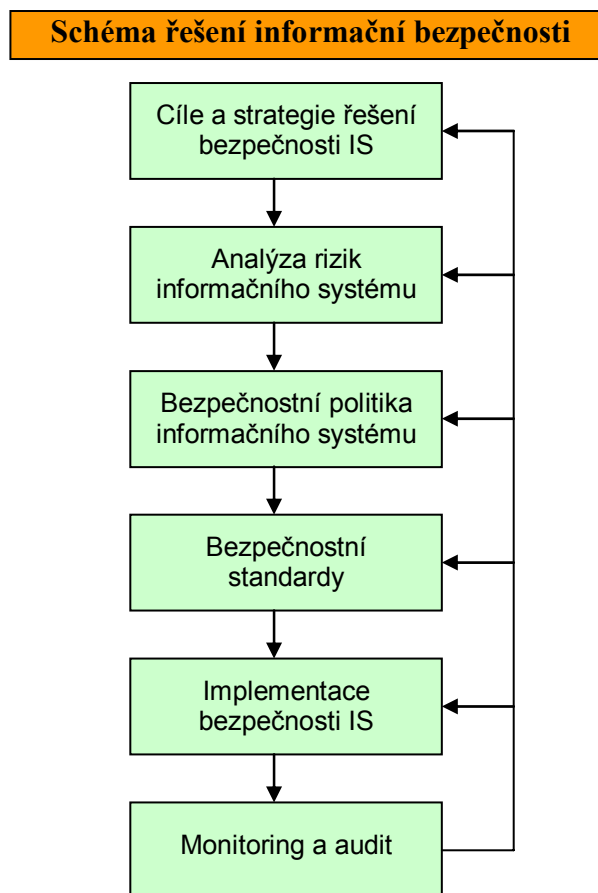
obsazením v podobě informačního managementu a bezpečnostního informačního managementu. Přístup k této problematice je v každé organizaci specifický. Jsou však jistá základní pravidla a postupy, které by měly být pro zajištění bezpečnosti naplněny. [4]

2.3 Proces řešení informační bezpečnosti

Prvním zlomem pro řešení informační bezpečnosti je vůbec rozhodnout se pro její řešení. Tomuto říkáme **mentální krok**. Až na výjimky, se management nerozhoduje na základě jasných a ověřitelných informací. Takové informace (výskyt hrozby v čase a jejich dopady na společnost) nejsou dopředu k dispozici a výpočty typu návratnosti investic jsou většinou spekulativní. Je zde nutné si pokládat otázky: „**co by se stalo, kdyby to tam nebylo**“, „**jak vysoké by byly nutné náklady na návrat do původního stavu, bylo-li by to vůbec možné?**“, atd. Je proto vhodné a užitečné, považovat náklady spojené s řešením a řízením informační bezpečnosti za určitý specifický druh pojištění. Komplikací pro rozhodnutí je dále fakt, že informační bezpečnost vyžaduje nezanedbatelnou finanční investici. Jakousi náplastí je ale fakt, že bez vynaložení těchto nákladů by společnost ztratila mnohem více. Cílem mentálního kroku je tedy rozhodnutí pro efektivní řešení informační bezpečnosti. To konkrétně znamená následující:

- Ochotu managementu společnosti se informační bezpečností seriózně zabývat
- Rozhodnutí managementu nastartovat proces řešení a přesně stanovit termíny splnění jednotlivých kroků
- Vyčlenění potřebných lidských zdrojů
- Ochotu managementu do projektů investovat
- Uvědomit si skutečnost, že je nutné spolupracovat s externími dodavateli bezpečnostních produktů a služeb
- Připravenost managementu na možné organizační změny

Informační bezpečnost je záležitostí čistě nákladovou, a to s velice obtížně vyjádřitelnými přínosy. V takové situaci je proto **naprosto nezbytná a klíčová podpora managementu firmy**. [2]



Obr. 2: Schéma řešení informační bezpečnosti dle ISO 13335 [4]

2.3.1 Strategie řešení informační bezpečnosti

V tomto kroku je potřeba udělat dva hlavní kroky:

- definovat hlavní cíle v oblasti informační bezpečnosti (co a jak chránit),
- navrhnout a schválit parametry dalších kroků, ideálně ve formě projektu/ů

První krok vlastně představuje zhmotnění "mentálního kroku". Management stanovuje priority řešení a ty se musí promítnout do cílů a parametrů. Typickými výstupy této části bývá definiční projektová dokumentace a ideálně také Celková bezpečnostní politika - stručný dokument deklarující podporu managementu v oblasti bezpečnosti (nejen informační).[15]

2.3.2 Analýza rizik IS

Riziko je "sexy" pojem a analýza rizik bývá často demonizována. Řada manažerů od týmů provádějících analýzu rizik (informací, informačních systémů) očekává zázraky a nečekané odpovědi a je pak zklamána, když dostanou odpovědi, které "... dávno a dobře znají".[15]

Analýza rizik musí poskytnout odpovědi na *tři základní otázky*:

- Co se stane, když nebudou informace chráněny?
- Jak může být porušena bezpečnost informací?
- S jakou pravděpodobností se to stane?

Existuje řada specializovaných metodologií na provádění analýzy rizik (např. FRAP, IRIS, CRAMM) a tento krok typicky vyžaduje spolupráci s externími experty. Standardním výstupem analýzy rizik je *zpráva se sumarizací a prioritizací rizik plus návrh doporučených opatření na jejich eliminaci nebo alespoň snížení*. [15]

Bezpečnost je především o prioritách - jde o to netrávit čas chráněním něčeho, co nemá pro společnost cenu. Hlavním cílem analýzy rizik musí být tyto priority co nejdříve a nejpřesněji určit.[15]

2.3.3 Bezpečnostní politika IS

Analýza rizik provedená v předchozím kroku vede k detailnímu poznání organizace, jejích problémů a potřeb. To umožňuje vytvořit klíčový bezpečnostní dokument - bezpečnostní politiku - a zohlednit v něm specifika dané organizace. Jedná se o dokument, který je po přijetí managementem závazný pro celou společnost a který definuje východiska pro všechny další aktivity společnosti v oblasti informační bezpečnosti. Hlavním cílem informační bezpečnostní politiky je:

- definovat hlavní cíle při ochraně informací,
- stanovit způsob, jak bezpečnost řešit,
- určit pravomoci a zodpovědnosti.

Doporučuje se vyvarovat se přebírání již hotových bezpečnostních politik bez posouzení vlastních specifik. Špičková bezpečnostní politika banky bude pravděpodobně nepoužitelná pro výrobní podnik.[15]

2.3.4 Bezpečnostní směrnice a standardy

Bezpečnostní politika definuje hlavní pravidla a zásady bezpečnosti. Ty je potřeba ještě dále konkretizovat do podoby detailních pravidel a postupů - bezpečnostních směrnic a standardů. Směrnice a standardy jsou součástí interní legislativy a jako takové se stávají závaznými pro organizaci.

Při rozhodování o tom, co má být ještě součástí bezpečnostní politiky a co již dát do standardů, může pomoci časové měřítko. Zkušenost ukazuje, že ustanovení politiky by se neměla významně měnit alespoň 2 roky.[15]

2.3.5 Implementace bezpečnosti IS

Zásady a pravidla politiky, resp. standardů a směrnic, se nenaplní automaticky jejich vytvořením a přijetím. Je potřeba nastartovat aktivity (projekty), které bezpečnostní zásady uvedou do života. Z tohoto pohledu se nejedná o uzavřený krok, ale spíše moment, kdy jsou zahajovány jednotlivé bezpečnostní projekty, koordinované ustaveným bezpečnostním managementem. Příklady bezpečnostních projektů mohou zahrnovat:

- bezpečnostní vzdělávání,
- havarijní plánování,
- zabezpečení připojení na internet,
- implementace infrastruktury veřejných klíčů.[15]

2.3.6 Monitorování a kontrola

Pokud je ustaven bezpečnostní management a jsou schváleny klíčové bezpečnostní dokumenty, je nutné zajistit dodržování definovaných pravidel a zásad a ovšem také zpětnou vazbu, která zajistí, že se významné změny promítnou do příslušné dokumentace a do procesu řízení bezpečnosti. [15]

Reakce na nově se objevující rizika, změny priorit organizace a změny okolního prostředí mohou vyvolat potřebu vrátit se k některému z předchozích kroků řešení bezpečnosti a provést například doplňkovou analýzu rizik, či doplnění chybějících bezpečnostních standardů a směrnic. Tento fakt je na schématu řešení naznačen šipkami vedoucími vzhůru.

Obrázkem toho, jak organizace chápe smysl trvalého řešení bezpečnosti, je způsob vyrovnání se monitorováním a kontrolou. Neřešit tuto část znamená, že náklady byly vynaloženy jednorázově a že po čase budeme začínat s bezpečností opět prakticky z nuly. [15]

2.4 Analýzy bezpečnosti informačního systému

Při analýze bezpečnosti informačního systému je naším cílem prověřit aktuální stav bezpečnosti, odhalit slabá místa a najít nejvhodnější opatření k jeho odstranění. Výsledkem analýzy je podrobná dokumentace o bezpečnostní situaci IS společnosti. Ochrana a bezpečnost informací ovšem nezahrnuje jen počítačovou část. Zahrnuje také veškeré činnosti a subjekty, které s informacemi přicházejí do styku a to jak s informacemi v elektronické, tak i papírové i jiné podobě. Z tohoto důvodu je třeba při analýze neopomenout a významně se zabývat sociální oblastí, tedy lidským faktorem, neboť opomenutí něčeho v této oblasti se stává místem informačního úniku. Tohoto pak samozřejmě mohou využít jak neloajální zaměstnanci, tak i další pracovníci, kteří vůbec nemusí být nutně specialisté v oblasti informatiky. Může jít například o ostrahu objektů, opraváře, obslužný personál kanceláří, externí průnikáře a to jak počítačové, tak využívající metod sociálního inženýrství.[4]

2.4.1 Efekty bezpečnostní analýzy

- **Zvýšení důvěryhodnosti společnosti** – podobně jako certifikáty řady ISO 9000, lze jasnou bezpečnostní politiku prezentovat jako konkurenční výhodu.
- **Zabránění poškození dobrého jména společnosti medializací úniku dat** – bezpečnostní politika jasně říká, jaký bude postup v případě úniku dat.
- **Ochrana stability organizace** – minimalizuje nebezpečí úniku dat z informačního systému vnějším narušitelem. Způsobů jak proniknou je mnoho. Je třeba mít na vědomí, že protokol TCP/IP je zcela otevřený a proto není problém sledovat obsah jakékoliv otevřené, nešifrované komunikace firmy prostřednictvím internetu.
- **Chrání investice do výzkumu a vývoje před zneužitím** – vývoj a výzkum je nesmírně drahou záležitostí a jakýkoliv únik těchto dat by mohl na straně konkurenta vést k urychlené výrobě a uvedení na trh za zcela jiných podmínek nežli my.

- **Chrání společnost před útokem hackerů či virů** – společnost je chráněna před hackery, tedy před osobami, které ať už pro zábavu nebo s jiným cílem (vydírání, krádeže) pronikají do cizích systémů. Nebo je chráněna před viry, které rovněž působí destruktivním charakterem.
- **Chrání práci zaměstnanců před zneužitím** – chrání ji před zneužitím konkurencí, ale také před zneužitím jinými zaměstnanci.
- **Chrání informace obchodního charakteru** – zde jde převážně o databáze klientů, předměty smluv, apod.
- **Omezuje absolutní moc uživatelů nad informačním systémem** – jsou dána přesná pravidla platná pro všechny zaměstnance a jejich pozice ve společnosti. Pravidla jsou jasná a srozumitelná.
- **Schopnost analyzovat podezřelé situace** – jakýkoliv pokus o průnik je rozpoznán a umožňuje připravit adekvátní reakci.
- **Společnost je připravena na technické selhání** – v případech selhání technických zařízení společnosti nastupují předem určené náhradní prostředky. [4]

3 HROZBY INFORMAČNÍCH SYSTÉMU V ELEKTRONICKÉM PODNIKÁNÍ

Výpočetní systém je systém, kde jsou zpracovávána a uchovávána data, která jsou nositeli informací. Výpočetní systém zahrnuje hardware, software a vlastní data. Tyto tři složky jsou aktiva, která je nutno zabezpečit proti hrozbám a útokům pasivním i aktivním. V oblasti bezpečnosti dat jsou specifikovány čtyři typy hrozeb namířených proti bezpečnosti výpočetního systému. Jsou to:

- **přerušeni**, kdy aktivum výpočetního systému se ztratí, stane se nepoužitelným nebo nepřístupným. Příkladem je zničení hardware zařízení, výmaz programu nebo datového souboru nebo selhání operačního systému při vyhledávání souboru na disku.
- **odposlech**, při kterém neoprávněná strana získá přístup k aktivu. Neoprávněná strana může být jak osoba, tak program nebo výpočetní systém. Příkladem může být nepovolené kopírování programů nebo datových souborů nebo tajný odposlech prováděný při datových přenosech po síti. Ztráta aktiva může být odhalena bezprostředně, ale „tichý“ odposlech nemusí zanechat stopy, podle nichž by byl odhalitelný.
- **pozměnění**, kdy neoprávněná strana nejenže získá přístup k aktivu, ale také tohoto přístupu využije k jeho pozměnění. Příkladem může být nelegální provedení změn v datech databází, pozměnění programů tak, že se ovlivní jejich běh, nebo provedení změn na datech v průběhu jejich přenosu v síti. V některých případech se pozměnění aktiva projeví ihned, ale některé případy je téměř nemožné detekovat.
- **vytvoření falsifikátu** určitého objektu neoprávněnou stranou. Příkladem může být neoprávněné vložení falešných záznamů do databází nebo vytvoření falešné zprávy a její následné odeslání po síti. Mnoho škod na programovém vybavení počítačů a na datech. [7]

3.1 Počítačové viry

Počítačový virus je kus programového kódu, který je schopen se prostřednictvím hostitelské aplikace replikovat a to více než jednou. Přeloženo do srozumitelného jazyka je to program, který se šíří, aniž by o tom člověk sedící u počítače věděl. Vedle toho, že zabírá část paměti žádnou jinou vlastnost vzhledem k této definici nemá. Nemusí tedy více

škodit a ani se jinak projevovat. Škodlivost patří mezi určité projevy navíc, které do virů jejich autoři z rozličných důvodů přidávají. Viry také často obsahují obranné mechanismy proti detekci a některé druhy (polyformní viry) jsou schopny mutace. Šíření virů je dáváno převážně do souvislosti s oběhem volně distribuovaných programů. Následky virové nákazy mají tedy nejružnější podobu a to od převážně neškodných zvukových či obrazových efektů, které rozptylují uživatele a zatěžují počítač a jeho paměť, až po možnost rozsáhlého zničení dat a programů. [4]

3.1.1 Typy virů

- **„Pravé“ viry** – Jsou to malé počítačové programy, které se spojí s legitimním programem a spustí se spolu s ním. Když se tento virový program spustí, reprodukuje se a může způsobit nežádoucí nebo poškozující chování počítače. Tyto viry se šíří většinou na disketách obsahujících infikovaný program. Nyní lze bohužel takové infikované programy stáhnout z Internetu. Často je v něm také zabudováno zpoždění mezi skutečnou infekcí a destruktivními činnostmi viru, takže ten má šanci nakazit další počítače ještě dříve, než bude odhalen. Tyto viry napadají spíše samotný operační systém než aplikace a data uložená v počítači. [5]
- **Trojské koně** – Pojmenované podle legendárního dřevěného koně, jedná se také o počítačové programy, které se vezou na hřbetě legitimního programu, ale obvykle se nereprodukuje. Když trojský kůň vklouzne do vašeho počítače, změní některá jeho nastavení bez vašeho vědomí. Dalším použitím trojského koně je vytvoření „zadních vrátek“ ve vašem operačním systému tak, aby se do vašeho počítače mohl dostat jiný uživatel bez vašeho vědomí (proto ten název). [5]
- **Červi** – Tyto programy se nepřipojují k jiným programům, ale běží úplně samy, reprodukuje se tak, až zahltní systém, v němž jsou. Mají tendenci se objevovat v sítích, z nichž Internet je samozřejmě největším příkladem. Někdy před 12 lety jeden červ ucpal podstatnou část Internetu ně několik hodin, dokud nebyl úplně odstraněn s vynaložením značných nákladů a úsilí. Nezničil data nebo programy, ale spotřeboval značné množství počítačových zdrojů. [5]
- **Makroviry** – Moderní aplikační programy jako MS Word vám umožňují připojit k datovým souborům malé programy, zvané makra, které mají udělat něco užitečného. Makra mohou být bohužel také zhoubná a označují se jako makroviry.

Tyto viry mohou infikovat a infikují datové soubory a postupně je ničí. Například, když otevřete infikovaný dokument aplikace Word, který jste třeba dostali jako přílohu elektronické pošty, spustí se makrovirus a infikuje váš systém. Potom, kdykoli vytvoříte nebo otevřete neinfikovaný dokument, makro to zjistí a ihned tento soubor infikuje. Makroviry mohou způsobit zmatek ve vašich datech, například tím, že změní jeho formátování. Nedávný virus ILoveYou byl z určitého hlediska hybridní infekcí makrovirem a červem. Jednalo se o červa, ve kterém byl samostatný program, jenž se rozšířil po síti Internet, ale choval se jako makrovirus.

- **Virová elektronická pošta** – To je ve skutečnosti nesprávný název. Dosud neexistují žádné viry, červi, trojské koně či jiné infekce, které by se šířily textem samotné elektronické zprávy. Viry se zatím vždy přenášely v přílohách elektronické pošty a svou špinavou práci prováděly tehdy, když příjemce přílohu otevřel. Takže buďte ujištěni, že pouhé otevření a přečtení samotné elektronické pošty není nebezpečné. Nicméně otevření přílohy může být něco jiného. [5]

3.2 Hacking

Hacking – hackování – je činnost, při které se hacker nebo skupina hackerů snaží vniknout do cizího systému. Tato činnost je většinou prováděna on-line, je tedy zapotřebí připojení (například k LAN nebo internetu). Hackování ale může být prováděno i na lokálním počítači bez sítě, pokud k němu má hacker fyzický přístup. Existují různé druhy útoků. Některé směřují k získání administrátorských práv, další ke shození serveru ("zamrznutí" systému). [8]

Hacker je pak člověk s ohromujícími znalostmi počítačů, operačních systémů, přenosových počítačových protokolů a programování. Zná silné stránky i nedostatky programů, dokáže objevit nové bezpečnostní díry atd. Tyto znalosti samy o sobě jsou prospěšné, ale někteří lidé jich využívají k nabourávání a průniku do systémů, o kterých si jejich majitelé myslí, že tam nikdo cizí nemá co dělat. [8]

Právě jejich znalosti, inteligence, schopnost inovace a improvizace je činí nebezpečnějšími než viry. Vir provádí jen to, co mu programátor zadal, hacker dělá, co ho napadne. Naštěstí se hackeři nedají kopírovat a tak jsou jejich útoky méně časté, než útoky virů. [8]

3.3 Lidský faktor uvnitř organizace

Ve velké míře mohou informační systém podniku ohrožovat také jeho vlastní zaměstnanci. Jedná se často o tzv. interní útok, kdy se zaměstnanec firmy snaží vědomě způsobit firmě škodu. Patří sem ale také neúmyslné poškození dat informačního systému zaměstnancem plynoucí např. z neznalosti a nedostatečného proškolení v práci s určitým programovým vybavením.

3.4 Ostatní hrozby

Mezi další hrozby, které mohou způsobit poškození nebo ztrátu dat informačního systému dále můžeme zahrnout:

- události způsobené přírodními jevy (ohně, voda, zásah bleskem)
- poruchy techniky (např. výpadky napájení, porucha zařízení)

Fyzická poškození způsobená přírodními katastrofami a závadami techniky obvykle zjistíme okamžitě. Informační systém přestane být jednoduše funkční a způsobené škody lze celkem přesně definovat. Horší situace nastává při nelegálním úniku informací.

3.5 Nejčastější ohrožení zabezpečení v sítích

3.5.1 Předstírání identity (Spoofing)

Existuje několik druhů předstírání identity. *Předstírání adresy IP* znamená vytváření paketů, které vypadají, že přišly z jiné adresy IP. Tato možnost se využívá zejména u jednocestných útoků (například útoky typu DoS). Pokud se paket tváří, že je odeslán z počítače ve vnitřní síti, je možné, že projde přes bránu firewall (která je navržena na ochranu proti externím útokům). Tyto útoky lze těžko detekovat. Vyžadují znalosti pro sledování a analýzu datových paketů.

3.5.2 Neoprávněné změny (Tampering)

Neoprávněné změny se týkají úpravy obsahu paketů při přenosu v Internetu nebo změny dat na disku počítače po průniku do sítě. Útočník může například umístit na síťový kabel odposlouchávací zařízení, které bude číst pakety opouštějící síť. Může tak zachytit či pozměnit odchozí informace.

3.5.3 Odvolatelnost (Repudiation)

Odvolatelnost je schopnost uživatele nepravdivě popřít akci, kterou nemohou ostatní strany dokázat. Například uživatel, který odstraní určitý soubor, může úspěšně tento čin popřít, pokud neexistuje průkazní mechanismus (například auditování).

3.5.4 Zveřejnění informací (Information disclosure)

Zveřejnění informací je jejich poskytnutí někomu, kdo by k nim neměl mít běžně přístup.

3.5.5 Odepření služby (Denial of Service)

Útoky typu DoS jsou počítačové útoky prováděné útočníkem, který se pokouší přetížit či zastavit síťovou službu, jako je webový nebo souborový server. Útočník může například natolik zatížit server požadavky, na které se bude snažit odpovědět, že začne ignorovat skutečné oprávněné požadavky na připojení. V roce 2003 byl masivní útok DoS veden proti několika hlavním organizacím na webu, včetně Yahoo a Microsoft, s cílem znepřístupnit jejich servery.

3.5.6 Zvýšení oprávnění (Elevation of privilege)

Zvýšení práv je proces, kdy uživatel oklame systém, aby získal neoprávněnou úroveň přístupu, kterou může obvykle zneužít k jeho poškození či zničení. Útočník se může například přihlásit k síti pomocí účtu Guest a poté zneužít nedostatky v softwaru, které mu umožní získat oprávnění správce.

4 NEJDŮLEŽITĚJŠÍ MOŽNOSTI OCHRANY DAT PŘED HROZBAMI

Informační systémy, jejich aktivita, mohou být za určitých okolností cílem působení různých nebezpečí. Mohou to být lidé (vlastní zaměstnanci), události způsobené přírodními jevy (ohněň, voda, zásah blesku, atd.), poruchy techniky (výpadky napájení, porucha zařízení). Lidské hrozby představují agenti rozvědky, průmysloví agenti, teroristé, organizovaní nebo jednotliví zločinci, zlomyslní nebo pomstychtiví lidé, dobrodruzi, počítačová nadšenci, avšak také vlastní zaměstnanci či přátelé. Od útočníka musíme očekávat, že použije libovolný způsob průniku. Nemusí jít vždy o nejzřejmější metodu a také o útok na nejsilnější místo ochrany. Fyzická poškození způsobená přírodními katastrofami a závadami techniky obvykle zjistíme okamžitě. Informační systém přestane být jednoduše funkční a způsobené škody lze celkem přesně definovat. Horší situace však nastává při nelegálním úniku informací. Zde nelze téměř nic dokázat, pokud získané informace nejsou někde zjevně použity (dokazuje se tedy až důsledek průniku). Provozovatel informačního systému většinou nemá zájem na negativní publicitě a tak dochází k představě, že se vlastně nic nestalo a že ochrana informačního systému je vlastně zbytečná. Většina útoků právě z uvedeného důvodu zůstává neodhalena a ty odhalené neproniknou na veřejnost i z toho důvodu, aby narušitel neměl potvrzen rozsah svého úspěchu a uživatel informačního systému neztratil svou pověst. Informační systém se před působením hrozeb brání řadou protiopatření. Ta pak mohou mít různé podoby:

- ✓ administrativní (zákaz přístupu, či manipulace s daty)
- ✓ logická (nastavení přístupových práv)
- ✓ fyzická (zabránění přístupu nepovolaných osob, ochrana objektů)
- ✓ technická (disková pole, šifrovací a kryptografické systémy) [10]

4.1 Antivirové programy

Přítomnost počítačových virů v systémových prostředcích informačních systémů je závažný problém. Protože je existence virů v těchto prostředcích nežádoucím jevem, přijímají se různá opatření, aby se zabránilo jejich vniknutí do informačních systémů anebo aby se úspěšně podařilo eliminovat jejich účinky. Proto významným prvkem bezpečnosti informačních systémů je ochrana před počítačovými viry. Existují různé druhy

antivirových testů. Patří mezi ně srovnávací test, heuristická analýza, antivirový test, rezidentní antivirová kontrola, kontrola pošty.[1]

Antivirové systémy – v současnosti patří k nejfrekventovanějším antivirovým programům. Antivirový systém se skládá z částí, které sledují všechny nejpodstatnější vstupní místa, kterými by případná infiltrace mohla do počítačové systému proniknout. Antivirový systém se obvykle skládá z částí:

- *vykonávající nepřetržitý dohled* – antivirovou kontrolu nad daty, se kterými uživatel pracuje (tzv. on-access skener).
- *umožňující provést antivirový test na vybrané oblasti*. Test je vyvolán na základě požadavku uživatele (on-demand) a obvykle se tak tato část označuje jako on-demand skener.
- *udržující antivirový systém v aktuální podobě*. Zajišťuje stahování aktualizací antivirového systému z Internetu.
- *vykonávající automatickou antivirovou kontrolu příchozí a odchozí elektronické pošty*. [1]

4.2 Firewallly

Firewall je hardwarové nebo softwarové zařízení instalované na vstupní bráně do internetu. Cílem je účinně oddělit lokální a veřejnou síť a kontrolovat přenos dat mezi nimi.[6]

Z bezpečnostního hlediska přináší následující funkce:

- funguje jako „škrtící místo“ – všechna data směřující z lokální sítě do Internetu nebo naopak musí tímto místem projít. Zde mohou být analyzována a podle bezpečnostních pravidel lze rozhodnout, zda mohou opustit síť nebo zda mohou být do sítě vpuštěny.
- firewall může zaznamenávat statistické i konkrétní údaje o datech přes něj procházejících. Ty poté mohou sloužit jako zdroj dat pro kontrolu funkčnosti bezpečnosti systému.
- omezuje nebezpečí průniku do sítě zvenčí, ze strany Internetu.[6]

Druhy firewallů:

1. **Paketové filtry** – Jde vlastně o selektivní směrování IP paketů. Filtr registruje každý paket, který přijde na firewall, chce skrz něj projít a čte jeho hlavičku, kde je uvedeno na jakou adresu paket směřuje.

Výhody paketového filtru:

- ✓ vysoký výkon,
- ✓ flexibilní konfigurace,
- ✓ relativní jednoduchost a spolehlivost implementace.

Nevýhody paketového filtru:

- nemožnost detailní konfigurace na aplikační úrovni,
- nutnost dodatečného překladu adres.[6]

2. **Aplikační brány** – Aplikační bránou rozumíme program, ale také počítač, na kterém tato brána běží. Její postup je odlišný od filtrování paketů. Bývá umístěna mezi lokální a rozsáhlou sítí. Uživatelský klientský program místo toho, aby komunikoval se skutečným serverem poskytujícím dané služby, komunikuje s aplikační bránou. Aplikační brána musí rozumět protokolu, kterým klient se serverem komunikují. To jí umožňuje vyhodnocovat požadavky obou stran a zabraňovat tak nepovolaným operacím. [1]

Výhody aplikační brány:

- ✓ Co není povoleno, je zakázáno. Služby, pro které neexistuje proxy brána, jsou automaticky zakázány.
- ✓ Umožňují přesné nastavení filtrování obsahu paketů
- ✓ Proxy umožňují skrýt adresy počítačů ve vnitřní síti
- ✓ Aplikační brány obvykle umožňují vytváření velmi podrobných protokolů o jejich činnosti [6]

Nevýhody aplikační brány:

- Jednotlivé proxy mohou překladem adres zpomalovat průchodnost paketů [6]

4.3 Kryptografie

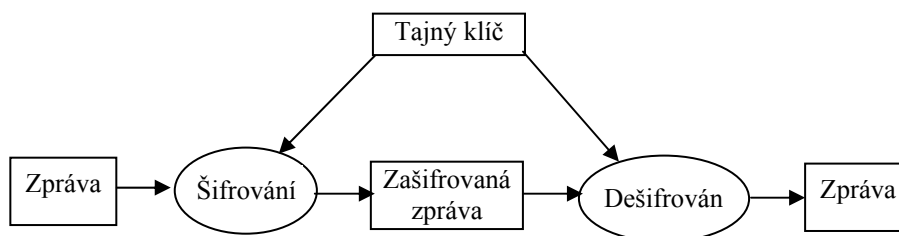
Šifrování, neboli kryptografie je proces, kdy z otevřeného textu pomocí šifrovacího algoritmu a šifrovacího klíče vytvoříme text šifrovaný. Ten nelze převést zpět na otevřený text bez znalosti příslušného šifrovacího klíče a algoritmu. Celková bezpečnost je tedy dána nejen kvalitou šifrovacího algoritmu, ale také kvalitou uložení šifrovacího klíče. Klíčem rozumíme posloupnost jedniček a nul určité délky, obvykle udávané v bitech.

Podle principu činnosti lze šifrovací algoritmy rozdělit do dvou skupin: na symetrické a asymetrické. [6]

4.3.1 Symetrické šifrovací algoritmy

Symetrické šifrování využívá jak pro šifrování, tak pro pozdější dešifrování dat tentýž klíč. Pokud tedy uživatel A zašifruje metodou symetrického šifrování nějaký soubor a uživatel B chce později tento soubor dešifrovat, musí pracovat oba uživatelé se stejným klíčem, jenž spolu sdílí. Sdílení společného tajného klíče se však netýká pouze uživatelů, nýbrž také klientských a serverových počítačů v síti, neboť i ty pracují s tímto klíčem. Proces symetrického šifrování probíhá v podstatě následovně:

1. Uživatel A použije symetrický klíč k zašifrování souboru.
2. Uživatel B dešifruje soubor stejným klíčem, který předtím použil uživatel A. [3]

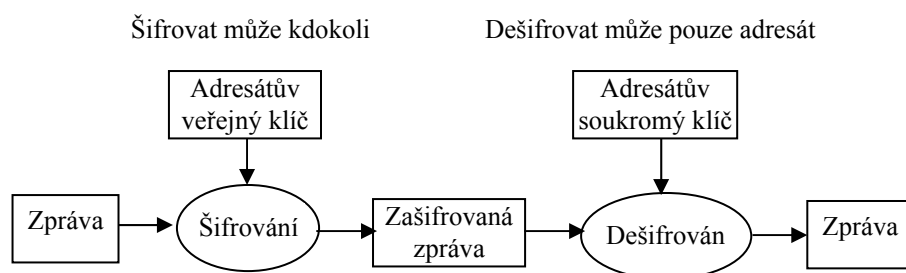


Obr. 3: Šifrování a dešifrování dat pomocí symetrických algoritmů [6]

4.3.2 Asymetrické šifrovací algoritmy

V případě asymetrického šifrování se na rozdíl od symetrického šifrování pracuje s párem klíčů. Tento pár klíčů poskytne nadřazený úřad v síti, přičemž jeden z klíčů je k dispozici všem uživatelům sítě, zatímco druhý je dostupný pouze pro jeho „vlastníka“. Proto se tento pár klíčů také dělí na tzv. „veřejný“ klíč, který slouží k šifrování dat a na „soukromý“ klíč, který je určen k dešifrování. Proces asymetrického šifrování probíhá v podstatě následovně:

1. Uživatel A použije veřejný klíč uživatele B k zašifrování souboru.
2. Uživatel B, jemuž je zašifrovaný soubor určen použije svůj soukromý klíč, aby soubor dešifroval. [3]



Obr. 4: Šifrování a dešifrování dat pomocí asymetrické kryptografie [6]

4.4 Kontrola přístupu

Základní technologií pro identifikaci uživatelů je jejich **autentizace**. Autentizací rozumíme proces, kdy se uživatel snaží představit IS a ten se naopak snaží ověřit, že se jedná skutečně o daného uživatele. Princip ověřování je jednoduchý. Bezpečnostní systém a uživatel mají společné tajemství (přístupové heslo), jehož platnost je schopen bezpečnostní systém ověřit. V praxi je tímto tajemstvím obvykle přihlašovací heslo. Proces autentizace uživatele pak spočívá v zadání přihlašovacího jména a hesla. Bezpečnostní systém pak ověří jeho správnost a podle výsledku buď uživatele do systému vpustí, nebo nikoliv. [6]

4.4.1 Autentizace pomocí znalosti, kterou disponuje daná osoba

Autentizace pomocí znalosti, což je zadání správného hesla, kterou disponuje pouze daná osoba. Přihlašování do systému pomocí jména (login) a hesla (password) je zcela nepochybně nejpoužívanější způsobem.[4]

4.4.2 Autentizace pomocí fyzického znaku dané osoby – biometrie

Metody biometrie jsou založeny na snímání jedinečných znaků osoby a typicky se jedná o snímání otisků prstů nebo oční duhovky. Po technologické stránce jsou biometrické metody mnohem náročnější, jak na použitý hardware, tak i obslužný software. [4]

4.4.3 Autentizace pomocí daného bezpečnostního předmětu

Velice zajímavým způsobem, jak vyřešit identifikaci osoby přistupující k důvěrným datům, je použití některého z hardwarových autentizačních prostředků, jako jsou různé čipové nebo magnetické karty či např. tzv. tokeny. Tento druh identifikace bývá někdy označován jako identifikace pomocí něčeho, co konkrétní člověk vlastní. Existuje dlouhá řada těchto zařízení od mnoha světových výrobců. [4]

4.4.4 Šifrování dat na discích a v lokální síti

Nejvhodnějším způsobem účinné ochrany osobních dat je kombinovat více těchto ochranných složek. Tedy hesla, šifrování i hardwarové klíče. Pravděpodobnost úspěšného útoku se pak stává téměř zanedbatelnou. Šifrování představuje pomyslný „druhý sled“ ochrany dat v počítači. Pokud se již totiž útočník dostane do počítače, má sice k souborům jako takovým přístup, ale jejich obsah je pro něj nečitelný. Může je sice zničit, ale v žádném případě nemůže zneužít jejich obsah.

On-line šifrování - jedná se o šifrování dat, které probíhá při čtení, nebo při ukládání souboru na disk. Při požadavku na otevření konkrétního souboru je ověřeno, zda má uživatel k tomuto souboru povolen přístup a zda disponuje příslušným šifrovacím klíčem, Pokud ano, je soubor dešifrován a otevřen. Pokud nejsou podmínky splněny, je uživateli přístup k souboru odepřen. Při ukládání je uvedený postup obrácený.

Off-line šifrování - tato technologie na rozdíl od on-line nešifruje data v reálném čase, ale jednorázově při přihlášení nebo odhlášení příslušného uživatele. Při přihlášení uživatele jsou jeho soubory dešifrovány, při odhlášení naopak zašifrovány. Tato metoda je vhodná zejména pro zabezpečení menších objemů zvolených dat.

On-demand šifrování - je nejjednodušší varianta pro zajištění ochrany důvěrných dat. Jedná se o zašifrování souboru na požádání uživatele. Jde o doplnění funkce zašifrování a dešifrování souborů přímo do operačního systému. [4]

4.5 Zálohování a archivace

Zatímco zálohování je proces uchování dat za účelem obnovení v případě havárie, archivace je proces uchování dat pro jejich pozdější využití v případě potřeby starých údajů (např. archivace několik let starých smluv, účetnictví apod.).

4.5.1 Zálohování dat

Zálohování dat patří mezi nejúčinnější preventivní nástroje v ochraně informační báze organizace. Proto je její funkčnost pro hladký chod organizace klíčovou záležitostí. Proces zálohování závisí na konkrétním instalovaném systému. U malých a středně velkých systémů se doporučuje dále rozdělit zálohovaná data do dalších kategorií a podle zařazení zvolit konkrétní postup. [6]

Cílem zálohování je rychle obnovit plně funkční stav informačního systému, jaký byl těsně před katastrofou. Zálohování (backup) je možné popsat jako vytváření bezpečnostní kopie dat nebo celého operačního systému tak, abychom mohli v případě havárie některé součásti počítače obnovit stav, který existoval těsně před vznikem poruchy. [1]

Kategorie zálohovaných dat

1. Operační systém, instalace databázových a jiných aplikací. Jednoduše data, která se často nemění a která se dají s trochou úsilí obnovit i z instalačních médií. Citlivost takovýchto dat je nejnižší.
2. Vytvořená data, která jsou velmi málo používána a je možné je rekonstruovat. Mohou to být záznamy registru operačního systému a data podobného charakteru.
3. Kritická data, která jsou často modifikována a jsou zásadní pro provoz systému. V praxi to může být datová část informačního systému, datové a indexové soubory apod. [6]

Mezi základní **způsoby zálohování** patří:

- **výchozí** – je to kopie původního systému. Provádí se po první instalaci, zálohuje všechny soubory a programy.
- **kompletní** – při každém zálohování jsou vždy zálohována všechny data najednou. Kompletní zálohování patří mezi nejznámější a nejjednodušší způsob zálohování. Za výhodu je považována jednoduchost obnovy v případě potřeby. Mezi nevýhody

kompletního zálohování patří skutečnost, že je náročnější na výpočetní prostředky a zabírá výrazně větší množství úložného prostoru

- **inkrementální** (přírůstkové) – při prvním spuštění se provede kompletní záloha, ale při dalších se již provádí záloha těch dat, která byla od posledního spuštění modifikována. Po nějakém časovém intervalu, resp. po určitém počtu spuštění zálohování, se celý postup opakuje.
- **diferenční** (rozdílové) – jde o obdobu inkrementálního zálohování s tím rozdílem, že při každém dalším spuštění nezalohují změny pouze od posledního spuštění, ale od poslední kompletní zálohy. Diferenční zálohování představuje zálohu pro všechny data od poslední úplné zálohy. [1]

4.5.2 Zálohování hardwaru

Problematika zálohování se netýká jen zálohování dat, ale i zálohování hardwaru a například přívodu energie. Zálohování hardwaru se ve většině organizací řeší na několika úrovních. Nejkritičtější jsou disky a ostatní magnetická média. Zálohování disků obvykle organizace řeší tzv. zrcadlením disků nebo tvorbou diskových polí. Výhodou těchto řešení je, že v případě poruchy disku pracuje celý systém bez přestávky dále. Porušený disk se prostě vymění za běhu bez nutnosti pozastavit celý systém.

Zálohování ostatního hardwaru se v praxi obvykle řeší malou zásobou jednotlivých komponent uložených na bezpečném místě. [6]

4.5.3 Zálohování zdrojů napájení

Před rozmary napájecí sítě mohou systém ochránit rozličné záložní zdroje napájení (UPS). Jsou k dispozici v mnoha variantách, od malých pro zálohování jednotlivých PC až po malé elektrárny, které jsou schopny dodávat energii celé budově včetně výtahů. [6]

4.6 Zabezpečení komunikací prostřednictvím SSL (Secure Socket Layer)

Vzhledem k tomu, že Web systém se stále masivněji uplatňuje v nejrozličnějších odvětvích, je stále silněji požadováno zabezpečení informací přenášených ve webovských transakcích. Bez tohoto zabezpečení by nebylo možné představit si používání webových

technologií v elektronickém obchodování. V současné době je vyvinutý (a dále rozvíjený) protokol pro zabezpečení Webových transakcí na Internetu označený jako HTTPS (Hyper Text Transfer Protocol – Secure) a navazující na základní transakční protokol Web systému HTTP.

Protokol HTTPS je postavený na protokolu SSL (Secure Societ Layer), který globálně řeší bezpečnost protokolové sady TCP/IP. SSL poskytuje bezpečný komunikační kanál mezi dvěma uzly Internetu na úrovni spojení vytvořeného protokolem TCP. Takto umožní protokol SSL bezpečnou implementaci běžných aplikačních protokolů podporujících internetové služby (např. FTP, TELNET, http). SSL používá kryptografické technologie. Komunikující uzly si vymění jednou své veřejné klíče a pro každou další následující relaci si vytvoří tajný klíč, tzv. „session key“, který po ukončení této relace zanikne. [1]

4.7 Elektronický (digitální) podpis

Elektronický podpis je v dnešní době nová, postupně se zavádějící technologie, jejímž cílem je vedle klasického podpisu postavit nástroj, který dostatečně potvrzuje autorství dotyčného člověka. Má tedy být v kybernetickém světě tím, čím je běžný podpis v normálním životě. [4]

Digitální (elektronický) podpis je způsob, kterým je možno zajistit:

- **autenticitu zprávy (dokumentu)**, tzn., že příjemce s určitostí ví, kdo je autorem dokumentu
- **integritu zprávy (dokumentu)**, tzn., že příjemce s určitostí ví, že obsah podepsaného dokumentu nebyl následně po jeho podpisu pozměněn
- **nepopiratelnost zprávy (dokumentu)**, tj. příjemce může prokázat, kdo je autorem dokumentu s daným obsahem. [7]

Jestliže se určitý subjekt rozhodne využívat výhod zaručeného elektronického podpisu, je nutné, aby se spojil se společností, která poskytuje certifikační služby. Po prokázání své identifikace obdrží soukromý klíč, který je tajný. Odesílatel tedy vytvoří dokument spustí speciální program, který vygeneruje z obsahu dokumentu a informací o autorovi (resp. informací z jeho soukromého klíče) určitou řadu znaků, kterou připojí k posílané zprávě a odešle ji.

Adresát obdrží takto podepsanou zprávu a potřebuje nástroj, který by mu ověřil, zda je podpis pravý a v pořádku. K tomu slouží veřejný klíč. Ten je možné získat různými

způsoby. Jak přímo od adresáta, tak i veřejně na internetu. Zde ale nastává problém pravosti veřejného klíče. Tuto pravost zaručuje opět poskytovatel certifikačních služeb, který vydá osvědčení jehož účelem je zjistit identitu osoby. Pokud je vše v pořádku a veřejný klíč potvrdí pravost soukromého a identitu odesílatele, splňuje tedy datová zpráva veškeré náležitosti pravosti a ověřenosti ve smyslu zákona. [14]

Elektronický podpis je možno uplatnit aplikacích jako je elektronická pošta, v právnických systémech, v podnikových a obchodních aplikacích, kde dochází k výměně dokumentů, v aplikacích pro státní správu, při distribuci software nebo pro zajišťování integrity obsahu databází. [7]

5 NORMY Z OBLASTI BEZPEČNOSTI INFORMAČNÍCH TECHNOLOGIÍ

Bezpečnostní normy zahrnují bezpečnostní techniky, obecné bezpečnostní protokoly a specifické aplikační protokoly. Do skupiny mezinárodních norem patří normy vyvíjené v ISO, IEC, ITU a IEEE. Tyto organizace vyvíjejí i společné normy ISO/IEC, ISO/ITU-T. Na americké straně do skupiny organizací vydávajících mezinárodně uznávané normy patří organizace ANSI a NIST.

Vedle výše uvedených organizací existují dále normy CEN/CENELEC s evropskou působností, nebo normy vydávané národními normalizačními úřady, například britská BSI (British Standardisation Institut) nebo ČSNi (Český normalizační institut) s národní působností. [4]

5.1 Norma ISO 17799 – komplexní chápání bezpečnosti informací

Jedná se o řešení, které vychází z úspěšné a obecně přijímané britské normy BS7799. Bezpečnost je zde chápána jako ucelený systém vyvážených bezpečnostních opatření doplněných jasně definovaným systémem řízení. Cílem je ochrana informací celé organizace.

Při řešení bezpečnosti organizace by měl být dodržen následující postup:

- Řešení bezpečnosti musí mít podporu vrcholového vedení
- Vstupním dokumentem řešení bezpečnosti je zpracování úvodní studie posouzení bezpečnosti
- Následuje analýza rizik, která může být zpracována některým ze specializovaných nástrojů (CRAMM, Proteus), či provedena na základě metodik navazujících úzce na ISO/IEC 17799:2000
- Na základě výsledků analýzy rizik je zpracována celková bezpečnostní politika organizace.
- Závěrečným a pro organizaci velmi důležitým krokem je implementace politiky do praxe, kde jsou vytvářeny směrnice či politiky pro jednotlivé druhy bezpečnosti informací spolu s tvorbou plánu obnovy funkčnosti. [4]

II. ANALYTICKÁ ČÁST

6 PŘEDSTAVENÍ FIRMY HP TRONIC ZLÍN, SPOL. S R. O.

6.1 Historie společnosti

Firma HP TRONIC byla založena panem Milanem Hradilem v roce 1990. Hlavní činností v době vzniku firmy byl maloobchodní prodej spotřebního zboží s postupnou specializací na domácí elektrospotřebiče. V následujících letech firma rozšířila své aktivity také na velkoobchodní prodej a začala budovat odběratelskou síť, která plošně zahrnuje celou ČR. Sídlo společnosti je dnes ve Zlíně – Prštném.

6.2 Předmět činnosti

Hlavním předmětem činnosti firmy je zejména velkoobchodní prodej spotřební elektroniky, domácích elektrospotřebičů a dalšího drobného zboží, jako jsou záznamová média, osvětlovací technika apod. V rámci těchto obchodních aktivit firma úspěšně realizuje projekt PROTON.

Firma HP TRONIC se zabývá prodejem především značkové spotřební elektroniky, proto mezi její dodavatele se řadí převážně renomované společnosti. Mezi nejznámější patří firmy Moulinex, Rowenta, Tefal, Philips, Grundig, Elektrolux, Braun, Zelmer, Eta, Thomson-Calex, Whirlpool, Tatramat, Indesit aj. Mimo spotřební elektroniku firma zaměřuje svou činnost na prodej záznamových médií od společností TDK, Sony, BASF. Od roku 1996 je firma výhradním dovozcem centrálních vysávacích systémů kanadské firmy Ultra Clean Manufacturing. Na druhou stranu mezi nejvýznamnější odběratele patří především síť velkoobchodních prodejen Makro, Euronova, Magnum Trade aj.

V roce 1996 firma vstoupila jako jedna z prvních na trh splátkového prodeje domácích spotřebičů a spotřební elektroniky. Dnes tato činnost právě v oblasti domácích spotřebičů a spotřební elektroniky významným způsobem doplňuje škálu služeb, které HP TRONIC nabízí.

Od roku 1997 provozuje firma několik hotelových zařízení a vyvíjí tak aktivity v oblasti cestovního ruchu a nabídek služeb pro volný čas. Právě oblast tuzemského cestovního ruchu se v posledním období velmi dynamicky rozvíjí a očekává se tedy, že tento trend bude pokračovat.

6.3 Filozofie firmy

HP TRONIC je zákaznický orientovaná firma. Proto je velký důraz kladen právě na spokojenost zákazníka, proto má klíčovou úlohu ve struktuře firmy ZÁKAZNICKÉ CENTRUM (ZC) a proto je základním a společným krédem všech firemních aktivit „dělat vše pro spokojeného zákazníka“.

6.4 Vybrané ekonomické údaje společnosti

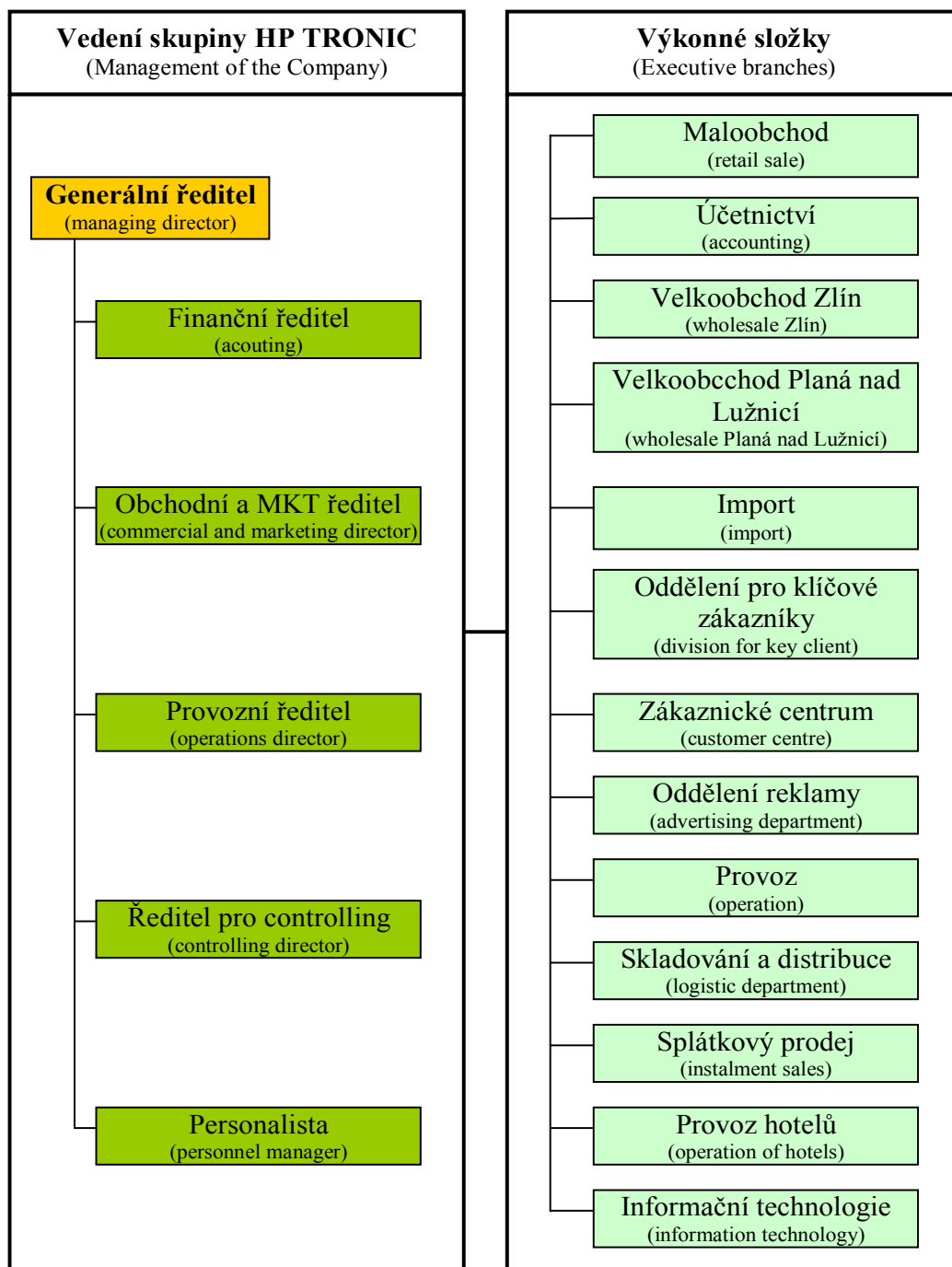
V roce 2003 překročila společnost dvě významné hranice. V měsíci listopadu se podařilo realizovat tržby ve výši 301,3 mil. Kč a překročit tak hranici 300 mil. Kč. Taky díky tomuto výsledku se podařilo dosáhnout ročních tržeb za prodej výrobků a služeb ve výši 2.062.994 tis. Kč a překročit tak hranici 2 mld. Kč. Z hlediska meziročního porovnání to pak znamená růst o 8 %. Segment spotřební elektroniky se na celkových tržbách podílel 22 % a tržby v tomto segmentu zaznamenaly meziroční nárůst 40 %. Jistý vliv na tento vývoj mělo taky úspěšné uvedení na trh značky Hyundai, kterou HP TRONIC na Českém a Slovenském trhu exkluzivně zastupuje. Segment velkých domácích spotřebičů se na celkových tržbách v roce 2003 podílel ze 38 % a rovněž tento segment zaznamenal meziroční růst ve výši 8 %. Segment malých domácích spotřebičů z hlediska tržeb společnosti HP TRONIC Zlín, spol. s r. o. meziročně narostl o 4,6 % a konečně segment mobilních telefonů a multimédií zaznamenal pokles 20 %. Vybrané ekonomické údaje společnosti jsou zobrazeny v následující tabulce.

Tab. 1: Vybrané hospodářské údaje společnosti [vlastní zpracování]

Údaje v tisících Kč	2003	2002	2001	2000	1999
Tržby za prodej zboží	2 018 663	1 870 893	1 769 629	1 510 400	1 218 878
Provozní HV	45 734	40 810	36 962	20 367	26 790
Oběžná aktiva	549 503	445 291	427 430	423 951	454 205
Vlastní kapitál	175 541	148 882	115 763	96 104	83 515
Počet zaměstnanců	149	118	101	101	60

6.5 Organizační uspořádání skupiny HP TRONIC

Nové dvoustupňové organizačně-řídící schéma firmy bylo definováno koncem roku 2000 a do dnešní doby nedoznalo téměř žádných změn. Za velmi významné však lze považovat změny na vedoucích pozicích některých výkonných složek. Personální posuny znamenaly ve všech případech významnou stabilizaci a posílení jednotlivých oddělení, což pak mělo pozitivní vliv na výsledky, jichž tato oddělení dosáhla.



Obr. 5: Dvoustupňové organizačně-řídící schéma firmy HP TRONIC, spol. s r. o.

6.6 Elektronické obchody firmy HP TRONIC, spol. s r. o.

6.6.1 Elektronický obchod typu Business to customer (B2C) – ePROTON

Firma HP TRONIC provozuje internetový obchod typu B2B pod názvem ePROTON. Tento obchod je určen pro maloobchodní zákazníky, který nabízí širokou nabídku domácích elektrospotřebičů, spotřební elektroniky, fototechniky a mobilních telefonů. Na adrese www.eproton.cz je možnost výběru z více než 7500 výrobků s možností přímého dovozu až k zákazníkovi.

Jedná se o klasický internetový obchod, kdy zákazník, před tím než chce v obchodu nakupovat, se musí nejdříve zaregistrovat. Zákazník musí při registraci zadat svou korespondenční adresu, tzn. jméno, příjmení, ulici, PSČ, město, stát, heslo, telefon. Po registraci zákazník vstupuje do obchodu na základě zadání svého uživatelského jména a hesla. Obchod je velmi přehledný, u každého zboží je uvedena cena a zákazník ho vkládá do košíku pomocí zvýrazněné ikony košíku. Pokud si nakupující zboží vybral, v dalším kroku volí způsob dodání, a to buď poštou, osobním odběrem nebo je mu zboží doručeno přímo firmou. V následujícím kroku si zákazník zvolí způsob placení. Placení je možno provést v hotovosti – při převzetí zboží, platbou na dobírku, platbou převodem na účet firmy u banky. Další možností je on-line platba prostřednictvím eBanky, která díky pokročilým informačním a komunikačním technologiím umožňuje pohodlné a bezpečné řešení všech peněžních transakcí. Úplně v posledním kroku má zákazník možnost provést rekapitulaci a kontrolu objednaného zboží.

Aby měl elektronický obchod úspěch u zákazníků, je třeba aby je ujistil o tom, že je bezpečný a měl by zajistit bezpečnost zákazníkem zadávaných dat. Společnost HP TRONIC své zákazníky ujišťuje, že veškerá zadávaná data jsou důvěrná a nejsou poskytována žádným jiným subjektům. Registrací zákazník pouze souhlasí se zpracováním jeho osobních údajů společností k marketingovým účelům.

eProton.cz je členem Asociace pro elektronickou komerci (APEK). Certifikovaný obchod je takový obchod, který poskytuje zákazníkům standardní úroveň základních služeb. To znamená, že například dodržuje slíbené dodací lhůty, odpovídá za kvalitu prodávaného zboží, odpovídá za zboží a řeší reklamace, zveřejňuje pravdivé informace atd. Jinými slovy

dodržuje tzv. certifikační pravidla stanovená Asociací pro elektronickou komerci jako nejvyšší tuzemské autority v oblasti elektronického obchodování.

6.6.2 Elektronický obchod typu Business to Business (B2B) – HPONLINE

HPONLINE je B2B řešení pro obchodní partnery společnosti HP TRONIC Zlín spol. s r.o. Je založen na stejném principu, jako je výše popsáný elektronický obchod ePROTON s tím rozdílem, že registraci obchodního partnera je nutno provést přímo v sídle firmy HP TRONIC, na základě potřebných údajů a dokladů. Po registraci dostane zákazník opět přiděleno uživatelské jméno a zvolí si heslo pro přístup do obchodu. Postup nákupu je pak již podobný jako u obchodu typu B2C. U obchodu HPONLINE je zákazníkům navíc umožněna bezpečná komunikace prostřednictvím protokolu SSL (secure socket layer).

7 ANALÝZA STAVU INFORMAČNÍ BEZPEČNOSTI VE FIRMĚ HP TRONIC, SPOL. S R. O.

Následující část diplomové práce se zabývá stavem bezpečnosti informačního systému ve firmě. Zhodnocení bylo provedeno na základě dotazníků, které jsou součástí nástroje pro analýzu rizik zvaného Cobra. Tento nástroj je produktem britské firmy C & A Systems Security Ltd., která se zabývá bezpečnostními a rizikovými analýzami. Použité dotazníky jsou součástí modulu, který se zaměřuje na bezpečnost e-commerce systémů a byly sestaveny na základě normy ISO17799/BS7799, o které je zmíněno a je popsána v teoretické části práce. Veškeré použité dotazníky jsou v původní anglické verzi přílohou diplomové práce.

Použitý modul „E-commerce“ je rozdělen do několika oblastí, z nichž jsem vybral ty, které jsem považoval pro hodnocení bezpečnosti daného informačního systému za nejdůležitější. Každou z těchto oblastí jsem pak dále rozšířil o další otázky, které jsem považoval za podstatné pro provedení této analýzy. Hodnocené oblasti jsem rozdělil do těchto samostatných kapitol:

- Zodpovědnost za bezpečnost informačního systému
- Správa místní sítě (LAN)
- Operační systém
- Antivirová ochrana dat v podniku
- Podnikové firewally
- Přístup k síti Internet
- Zálohování dat
- Přístup k počítačům, síti, datům a systém
- Audit (protokolování, kontrola)
- Zabezpečení komunikací na Webu

Cílem provedení tohoto zhodnocení je vytvořit celkový pohled na úroveň bezpečnosti informačního systému ve firmě a najít možné rizika a slabé stránky, jejichž eliminace a odstranění pak bude součástí projektové části diplomové práce.

7.1 Zodpovědnost za bezpečnost informačního systému

Ve firmě HP TRONIC není zřízeno žádné oddělení, které by se zabývalo výhradně bezpečností informačního systému a ochranou dat. Všechny tyto činnosti spadají pod oddělení informačních technologií, jehož pracovníci jsou velmi kvalifikovaní a zkušení lidé ve svém oboru. Je však třeba říci, že se starají spíše o technickou stránku fungování informačního systému a teprve na druhém místě je řešena bezpečnost. Řešení bezpečnosti není tedy považováno za samostatnou oblast. Právě absence takového oddělení, které by se jí zabývalo, je podle mého názoru slabou stránkou informačního systému firmy HP TRONIC. Ve firmě, takového rozměru, by měl být minimálně jeden pracovník vyčleněný na to, aby se zabýval výhradně komplexní bezpečností celého systému.

Silné stránky zabezpečení v této oblasti:

- ✓ kvalifikování a zkušení zaměstnanci oddělení IT

Slabé stránky zabezpečení v této oblasti

- absence útvaru zabývajícího se výhradně bezpečností informačního systému

7.2 Správa místní sítě (LAN)

Hlavním cílem této kapitoly je zhodnotit bezpečnostní opatření v oblasti lokální sítě. Správa a bezpečnost místní sítě je v této části rozebírána z toho důvodu, že pro podnik, který se zabývá elektronickým podnikáním je nezbytné zajistit, aby nedocházelo k poruchám, výpadkům a poškozením sítě. Pokud by tomu tak nebylo, docházelo by k nemalým finančním ztrátám.

Místní síť (LAN) firmy HP TRONIC je poměrně rozsáhlá a přesahuje areál podniku tzn. oblast lokální sítě je externí mimo areál podniku. K lokální síti firmy je připojeno více než 200 počítačů. Provoz tak rozsáhlé sítě si samozřejmě vyžaduje nemalé nároky na údržbu a bezpečnost a spadá v podniku pod Oddělení informačních technologií, konkrétně pod správce sítě. Správce sítě v podniku představuje zároveň centrální kontaktní bod, na který mohou uživatelé a systémový pracovníci hlásit veškeré problémy v oblasti lokální sítě. To umožňuje správci řešit ihned vzniklé potíže. Z pohledu bezpečnosti by měli být důkladně chráněny informace o nastaveních a konfiguraci sítě, což si pracovníci IT plně uvědomují a

přístup k těmto informacím je přísně kontrolován a omezen pouze na ty pracovníky, kteří jsou oprávněni je požadovat.

V síti může nastat situace, kdy se určité zařízení v síti může stát zdrojem neoprávněné aktivity. V takovém případě umožňují bezpečnostní opatření takové zařízení izolovat či oddělit od sítě. Dalším problémem, který může v provozu sítě vzniknout jsou potíže s hardwarem lokální sítě. Správa sítě je však proti takovým situacím zabezpečena mechanismem, který ji umožňuje včas varovat před potenciálními problémy s hardwarem. Snahou správce sítě je také zabránit tomu, aby žádný hardwarový prvek v síti nebyl pod nepřiměřeným tlakem v důsledku přetížení. Samozřejmě je dispozici také diagnostické a monitorovací zařízení sítě. Hardware, který tvoří hlavní komponenty sítě, je starý v průměru od 1 do 5 let. Po této době obvykle dochází k jeho výměně.

Údržba a veškeré postupy a pravidla související s údržbou hardwaru a softwaru nejsou ve firmě plně zdokumentovány a nejsou také plánovány ani schvalovány práce související s údržbou. To je menší nedostatek, protože pravidelnou a plánovanou údržbou hardwaru i softwaru se může předcházet jeho potížím. Pokud je třeba provést údržbu či opravu na nějaké součásti lokální sítě, je prováděna, pokud je to možné za chodu, aby nedošlo k přerušení provozu. Hardware ani software lokální sítě není nikdy nezávisle kontrolován a není prováděn jejich audit, což je třeba také označit za nedostatek. Je však třeba říci, že i přes tento nedostatek nedochází k nějakým vážnějším problémům a prostoje sítě se v průběhu posledních 12 měsíců pohybovaly pod úrovní jednoho procenta. Oddělení IT proto nepovažuje za důležité vypracovávat podrobné statistiky či záznamy příčin selhání lokální sítě.

Primárním médiem pro přenos dat v lokální síti je kroucená dvojlinka (točený kabel). Z hlediska bezpečnosti je vhodné, aby veškeré kabely byly usazeny v kabelovém vedení a umístěny pod podlahu či usazeny do zdi. V podniku tomu tak není u všech kabelových rozvodů, ale na druhou stranu je možné je kdykoliv zkontrolovat, zda u nich nedošlo k neoprávněné manipulaci či je možné je rychle vyměnit v případě jejich poškození. Neoprávněná manipulace s kabely je však v podniku zcela vyloučena a pracovníci IT nepovažují za důležité provádět u nich pravidelnou podrobnější kontrolu.

Fyzický přístup k volným nebo nepoužívaným portům (vstupům, výstupům) sítě není nijak omezen ani kontrolován. Z hlediska důkladného řešení bezpečnosti informačního systému

by nepoužívané kabely a porty měly být ihned vyřazeny nebo odpojeny, protože se můžou stát zdrojem neoprávněných aktivit.

Veškerý hardware je připojen na nepřetržitý napájecí systém, tak aby nedocházelo ke zbytečným výpadkům sítě. Zotavení či obnovení provozu lokální sítě není zahrnuto v žádném formálním plánu pro případ výjimečných událostí či plánu opětovného zahájení provozu.

Pokud jsou v síti přenášena citlivá či důvěrná data je pro jejich utajení využíváno kryptografie. Pro šifrování jsou využívány jak hardwarové, tak i softwarové šifrovací systémy. Pro vytváření a distribuci šifrovacích klíčů existují ve firmě přesně vymezené postupy a pravidla a dochází k pravidelným změnám klíčů.

Silné stránky v této oblasti zabezpečení:

- ✓ kvalifikovaná správa sítě
- ✓ informace o nastavení a konfiguraci sítě jsou předmětem přísné ochrany
- ✓ mechanismus varující před potencionálními problémy hardwaru v síti
- ✓ nízké stáří hardwarových komponent v síti
- ✓ nepřetržitý napájecí systém
- ✓ šifrování citlivých dat přenášovaných v rámci sítě

Slabé stránky v této oblasti zabezpečení:

- není prováděna pravidelná údržba hardwarových komponentů v síti
- hardware ani software lokální sítě není pravidelně kontrolován a není prováděn nezávislý audit
- není omezen ani kontrolován fyzický přístup k volným a nepoužívaným portům sítě
- zotavení a obnova provozu sítě není zahrnuta v žádném plánu pro případ výjimečných událostí

7.3 Operační systém

Ve firmě HP TRONIC je instalován operační systém Microsoft Windows XP (eXPerience – zkušenost). Je zatím posledním operačním systémem z dílny Microsoft, prodávaným u nás. Je to systém který slučuje obrovskou stabilitu a bezpečnost systému Windows 2000 a k tomu nabízí obrovskou podporu multimédií a nejnovějšího hardware. Je konstruován tak, aby bylo možno využít veškerého potenciálu dnešních osobních počítačů a obsahuje

proto celou řadu nových zajímavých nástrojů, např. možnost tzv. Active Windows Update za použití internetu. Je dodáván ve dvou verzích – MS Windows XP Professional a MS Windows XP Home Edition. V podniku je samozřejmě využíváno verze MS Windows XP Professional, která je určena pro firmy a pro náročné uživatele. Velkou výhodou tohoto systému a přínosem pro bezpečnost je právě zmíněná možnost Active Windows Update. Ta umožňuje pravidelné stahování aktualizací a záplat operačního systému ze serveru firmy Microsoft a okamžité odstranění bezpečnostních děr.

Silné stránky zabezpečení v této oblasti:

- ✓ velmi kvalitní a moderní operační systém
- ✓ funkce pravidelných automatických aktualizací
- ✓ vysoká podpora ze strany výrobce operačního systému

Slabé stránky zabezpečení v této oblasti:

- možná neznalost uživatelů operačního systému a jejich nedostatečné proškolení

7.4 Antivirová ochrana dat v podniku

Antivirové ochraně věnuje oddělení informačních technologií poměrně velkou pozornost, protože si uvědomuje, jaké následky může zavirování podnikové sítě přinést. Mechanismus pro detekci a prevenci virové infekce má formu velmi kvalitního softwarového produktu. Software poskytuje pro kontrolu virů část kódu, rezidentního v paměti, který průběžně hledá přítomnost viru. Antivirový program, který je v podniku využíván poskytuje všechny následující funkce:

- Kontrola programů
- Kontrola datových souborů
- Virový skener
- Kontrola velikosti souborů
- Kontrolu systémových oblastí pevného disku
- Prostředek pro automatické léčení a odstranění virů

Samozřejmě, aby byl antivirový program plně funkční, je třeba, aby byl neustále aktualizován. Aktualizace virové databáze si program stahuje automaticky z internetu, ze serveru výrobce programu.

Veškeré virové incidenty, ke kterým dochází jsou většinou velmi dobře a rychle zvládnuty a odstraněny. Pracovníci IT, vzhledem k nízkému počtu virových incidentů, nevedou žádné záznamy o jejich výskytu ani žádnou dokumentaci apod.

Pokud dochází ke kopírování a spouštění programů či dat z přenosných médií (CD, DVD, diskety), nedochází u nich vždy ke kontrole virové infekce. O kopírování dat a spouštění programů z přenosných médií a o tom jak kontrolu na přítomnost viru provést, nejsou všichni uživatelé dostatečně poučeni, což je významný nedostatek.

Problematika antivirové ochrany je ve firmě HP TRONIC velmi dobře zvládnuta a svědčí o tom i fakt, že v průběhu posledních 12 měsíců se potýkala pouze s jedním vážnějším virovým incidentem.

Běžné antivirové programy však neumí detekovat a odstranit všechny programy typu Spyware (ad-ware). Jsou to programy, které se starají o posílání důvěrných informací o uživateli a jeho počítači na vzdálené servery a to bez jeho vědomí. Tento druh softwaru bývá často implementován do freewarových programů (zdarma) a je velmi obtížné ho identifikovat.

Zjistil jsem, že v podniku není na počítačích instalován žádný software pro odstranění programů tohoto typu, které mohou významným způsobem snižovat výkonnost operačního systému a tím i produktivitu práce na počítači. Na jednom z počítačů jsem tedy nainstaloval freewarovou verzi programu pro detekci a odstranění spywaru. Provedený test pak prokázal obrovské množství těchto programů na počítači a nedostatečné opatření v této oblasti zabezpečení.

Silné stránky zabezpečení v této oblasti:

- ✓ velmi kvalitní softwarový produkt pro detekci a prevenci virové infekce
- ✓ pravidelná automatická aktualizace virové databáze

Slabé stránky zabezpečení v této oblasti:

- absence softwaru pro detekci a odstranění spywaru

7.5 Podnikové firewally

Firewall firmy HP TRONIC je jedna z mnoha silných stránek zabezpečení informačního systému (počítačové sítě). Veškerá spojení mezi sítí organizace a další vnější stranou či sítí internet jsou uskutečněna přes velmi kvalitní podnikový firewall. Firewall ověřuje veškeré pokusy o přístup do vnitřního okruhu firmy (sítě) zvenčí a nedovolí tak potenciálnímu útočníkovi, aby pronikl do počítačové sítě a tam jakkoliv manipuloval s daty.

Firewall je nastaven standardně tak, aby zamítl všechno a přijímá pouze protokoly, které jsou nezbytně nutné, k takovým IP adresám, které je požadují. Je velmi nepravděpodobné, že by firewall mohl selhat způsobem, že pustí pakety dál, než aby je blokoval.

Samozřejmě přístup k firewallu samotnému je vyhrazen pouze oprávněným osobám, kterými jsou pracovníci oddělení IT, konkrétně správce sítě. Firewall je umístěn v uzamčeném prostoru s ovládacími prvky pro připojené terminály a řídicími systémy. Je však třeba říci, že logický přístup k firewallu (tzn. účty administrátorů apod.) není předmětem přísných omezení a autentifikace a není pravidelně kontrolován. Není ani veden žádný kontrolní záznam všech změn prováděných při přihlášení k firewallu.

Na veškeré zabezpečovací prostředky, které společnost používá, jsou ze strany výrobců poskytovány plné podpory. Pracovník, který je správcem firewallu má stanovenou odpovědnost přijímat a hodnotit bezpečnostní varování od výrobce firewallu, ale taky jiných bezpečnostních poradních orgánů.

V oblasti zabezpečení podnikové sítě bránou firewall jsem nenašel žádné podstatné nedostatky a můžu ji tak označit za silnou stránku organizace.

7.6 Přístup k síti Internet

Přístup zaměstnanců firmy HP TRONIC k Internetu je samozřejmě nezbytným předpokladem pro úspěšné fungování jejich internetových obchodů a je formálně schválen a povolen zodpovědným správcem sítě. Dále je důležité poznamenat, že Internet je zpřístupněn přes autorizovanou bezpečnou bránu (mezisíťový počítač). Všichni zaměstnanci jsou velmi stručně informováni a o tom, jakým způsobem, správně a efektivně využívat Internet. Je jim také známo, že Internet v organizaci by měl být používán pouze pro účely spojené s obchodní činností firmy. Na druhou stranu však není veden žádný

registr či záznam přístupů jednotlivých uživatelů k internetu a jejich kontrola není zabezpečena žádným jiným mechanismem. Nutno taky poznamenat, že veškeré výše zmíněné skutečnosti nejsou v podniku žádným způsobem kontrolovány a nejsou zpracovány žádné zásady a pravidla ve formě určitého dokumentu či směrnic, které by pohyb uživatelů na internetu nějakým způsobem upravovaly. Zaměstnanci také nejsou poučeni o hrozbách, které jsou spojeny s jejich pohybem na internetu.

Internetu je ve firmě využíváno také k zasílání citlivých dat. V takovém případě jsou data přiměřeně chráněna proti odhalení, prozrazení či modifikaci většinou prostřednictvím šifrovacích metod. Pokud jsou z internetu stahovány spustitelné soubory, podléhají automatické antivirové kontrole, ale to jaké soubory či data jsou stahována není v podniku opět žádným způsobem kontrolováno.

Silné stránky zabezpečení v této oblasti:

- ✓ přístup k internetu přes autorizovanou bezpečnou bránu (mezisíťový počítač)
- ✓ možnost šifrování dat přenášených přes Internet
- ✓ antivirová kontrola dat stahovaných z Internetu

Slabé stránky zabezpečení v této oblasti:

- pohyb uživatelů po Internetu není žádným způsobem kontrolován
- neexistuje žádný dokument či směrnice formálně upravující pohyb uživatelů po Internetu

7.7 Zálohování

V případě dat je ztráta velmi nepříjemná, ale přesto nahraditelná. Jiná situace je u firemních dat, kdy ztráta může vést až k likvidaci firmy, neboť mohou být ztraceny nejen kontakty na partnery, ale i data účetní. Včasné zálohování uživatelských dat je bezesporu nejlevnější způsob, jak předcházet především finančním ztrátám.

Proti takovým ztrátám je organizace poměrně dobře zajištěna. Ve firmě existuje vybavení pro zálohování dat a softwaru, který je v systému uložen. Je využíváno různých druhů zálohovacích médií, od obyčejných disket, přes CD, DVD, externí pevné disky, až po páskové zálohovací mechaniky.

Co se týká typu zálohování, provádí se úplná záloha s přírůstkem změněných (nových) souborů. Úplná záloha je prováděna většinou každý den, přičemž jsou zálohována

aplikační a uživatelská data. Obvykle jsou vytvářeny dvě záložní kopie a není žádnými směrnice či jiným dokumentem v podniku stanoveno, na jakém místě by měly být uloženy. Většinou je tomu tak na místě, kde byly vytvořeny. Podle standardů a norem bezpečnosti by tomu však mělo být na ohnivzdorném a vodovzdorném úložišti.

Zálohování by bylo k ničemu, kdyby záložní kopie nebyly funkční. Funkčnost kopií umožňuje ověřit přímo zálohovací software, ale možnost ověření není v podniku vždy využívána. Neexistují taky žádné psané zásady pro zálohování dat.

Jestliže by došlo k přerušení hlavního přívodu elektrické energie, existují opatření, kdy by došlo k dodávce energie z alternativního zdroje. Podnik má svůj vlastní záložní generátor.

Pro případ, že by byl systém úplně zničen, jsou známa opatření taková, aby došlo k jeho rychlému nahrazení. Tato opatření však nejsou v podniku žádným způsobem zdokumentována. Není však garantován časový úsek, během kterého by mělo k jeho nahrazení dojít. V podniku není vypracován žádný plán k zajištění kontinuity podnikání, obsahující popis činností, které by měly být učiněny v případě vážnějších okolností (např. ztráta kanceláře v důsledku požáru apod.).

Silné stránky zabezpečení v této oblasti:

- ✓ provádí se pravidelná záloha dat
- ✓ existuje nástroj pro ověření funkčnosti zálohovaných dat
- ✓ existuje záložní zdroj elektrické energie
- ✓ vypracována opatření pro případ zničení či poškození systému

Slabé stránky zabezpečení v této oblasti:

- zálohovaná data nejsou uložena na bezpečném místě
- není vypracován podrobný plán kontinuity IS

7.8 Přístup k počítačům, síti, datům a systému

Data každého podniku jsou velmi cenná a ne každý zaměstnanec by měl mít přístup ke všem datům. Je třeba, aby pro každého uživatele byla vytvořena jednoznačná identifikace (uživatelský účet), která podle jeho funkce vymezí příslušná přístupová oprávnění do systému a v systému ho autentizuje. Tak to, více méně, funguje i ve firmě HP TRONIC. K systému zde mají přístup pouze pracovníci počítačové podpory a oprávnění interní uživatelé. Mechanismus autentifikace také umožňuje omezit uživatelům přístup pouze

k takovým funkcím, které jsou oprávněni používat. Přístup k samotnému operačnímu systému, registrům a dalším klíčovým oblastem je také omezen pouze na autorizované a zkušené uživatele. Všem zaměstnancům je zamezen přístup k důležitým utilitám jako je například formátování disku. K takovým funkcím mají přístup pouze pracovníci IT oddělení. Je možno zabránit přístupu ke konkrétním programům či datovým souborům pro vybrané uživatele nebo uživatelské skupiny.

Úspěšná i neúspěšná přihlášení do systému by měly být evidovány v protokolu a archivovány po určitou dobu. V podniku však k žádným takovým záznamům nedochází.

Každý počítač je nastaven tak, aby po určité době nečinnosti došlo k vypnutí obrazovky a je možno nastavit heslo pro to, aby mohl uživatel dále pokračovat v činnosti. Tato funkce je velmi důležitá pro to, aby bylo zamezeno přístupu k datům neoprávněným uživatelům v době nepřítomnosti uživatele oprávněného. Nastavení hesla spořiče obrazovky je však v podniku věcí jednotlivých uživatelů a není pravidlem, že je tato možnost zabezpečení využívána všemi pracovníky.

Mechanismus sloužící pro ochranu citlivých souborů umožňuje jejich šifrování, ale je v podniku využíván ve velmi malé míře.

Mechanismus pro kontrolu přístupu k počítačům vyžaduje autentifikaci prostřednictvím uživatelského jména a hesla. Přístupová hesla si vybírají vždy uživatelé samotní. Jestliže dojde k několika po sobě jdoucím chybným zadáním hesla, přístup není uživateli zamítnut. Z hlediska bezpečnosti by tomu tak mělo být. Změna hesla je možná, ale bezpečnostní mechanismus změnu hesel nevyžaduje a je na uživateli, zda a jak často si heslo mění. Všechna hesla jsou jedinečná pro každého uživatele a bezpečnostní mechanismus vyžaduje minimální délku hesla, která je 5 znaků. Při zadávání hesla je pole pro jeho zadání automaticky potlačeno. Pokud dochází ke změně hesla je nejdříve požadováno zadání hesla existujícího a nové heslo je pak nutné zadat dvakrát. Mechanismus pro kontrolu přístupu k počítačům neumožňuje přihlášení k počítači jako tzv. guest neboli veřejný uživatel.

Pracovníci IT oddělení si nejsou vědomi, kdo by, kromě konkurence, mohl mít zájem o získání dat posuzovaného systému a v průběhu posledních dvou let nebyly zaznamenány žádné případy neautorizovaného odhalení, prozrazení či modifikace dat.

Na závěr je třeba poznamenat, že ačkoliv v podniku existuje poměrně kvalitní systém autentifikace uživatelů, není využíván v plné míře. Nejsou zpracovány žádné zásady upravující tvorbu hesel a jejich pravidelné změny a uživatelé nejsou v této oblasti poučeni.

Silné stránky zabezpečení v této oblasti:

- ✓ kvalitní systém autentifikace uživatelů

Slabé stránky zabezpečení v této oblasti:

- neexistují zásady pro tvorbu a změnu hesel
- nepoučení zaměstnanci v této oblasti

7.9 Audit (protokolování, kontrola)

Aby byla zajištěna bezpečnost systému či sítě je třeba provádět podrobné monitorování těch činností, které mají vliv na zabezpečení tohoto systému či sítě. Cílem takového monitorování je zachytit nekorektní operace, pokusy o narušení bezpečnosti a průniky do systému ochrany. Zvláštní pozornost je třeba věnovat použití a rušení souborů a adresářů.

Ve firmě HP TRONIC není takový audit a protokolování prováděno. Vytvářejí se např. záznamy logů u hlavních systémů, avšak velkým nedostatkem je, že tyto logy již nejsou nikdy vyhodnocovány. Tyto záznamy jsou přitom cenným zdrojem informací, které by měly sloužit k dalšímu zlepšení bezpečnosti v organizaci. Tuto oblast zabezpečení je tudíž nutné označit za slabou stránku bezpečnosti IS.

7.10 Zabezpečení komunikací na Webu

Pro bezpečnou komunikaci firmy HP TRONIC a jejích obchodních partnerů prostřednictvím webových stránek je používán protokol SSL pro zvýšení bezpečnosti přenášených údajů. Tento protokol je zatím využíván pouze v obchodu typu B2B – HPONLINE, ale oddělení IT uvažuje o jeho zavedení i pro zákazníky obchodu B2C – ePROTON. Jeho použití, nejen že zabezpečí přenášená data proti odposlechu, ale také významně zvyšují důvěryhodnost firmy u zákazníků. Implementaci protokolu SSL lze považovat za silnou stránku.

8 SILNÉ A SLABÉ STRÁNKY STAVU ZABEZPEČENÍ VE FIRMĚ HP TRONIC, SPOL. S R. O.

Tab. 2.: Silné a slabé stránky bezpečnosti IS [vlastní zpracování]

SILNÉ STRÁNKY BEZPEČNOSTI IS	SLABÉ STRÁNKY BEZPEČNOSTI IS
Zodpovědnost za bezpečnost informačního systému	
kvalifikování a zkušenosti zaměstnanci oddělení IT	absence útvaru zabývajícího se výhradně bezpečností informačního systému
Správa místní sítě (LAN)	
kvalifikovaná správa sítě	není prováděna pravidelná kontrola a údržba hardwarových komponentů v síti
mechanismus varující před potencionálními problémy hardwaru v síti	není omezen ani kontrolován fyzický přístup k volným a nepoužívaným portům sítě
nízké stáří hardwarových komponent v síti	
nepřetržitý napájecí systém sítě	
možnost šifrování citlivých dat přenášených v rámci sítě	
Operační systém	
velmi kvalitní a moderní OS – Windows XP Professional	možná neznalost uživatelů operačního systému a jejich nedostatečné proškolení
funkce pravidelných automatických aktualizací OS	
vysoká podpora ze strany výrobce operačního systému	
Antivirová ochrana	
velmi kvalitní softwarový produkt pro detekci a prevenci virové infekce	absence softwaru pro detekci a odstranění spywaru
pravidelná automatická aktualizace virové databáze	
Firewally	
podnikový firewall	
Internet	
přístup k internetu přes autorizovanou bezpečnou bránu	pohyb uživatelů po Internetu není žádným způsobem kontrolován
možnost šifrování dat přenášených přes Internet	neexistuje žádný dokument či směrnice formálně upravující pohyb uživatelů po internetu
antivirová kontrola dat stahovaných z Internetu	

Audit	
	není prováděn audit a kontrola záznamů logů
Zálohování	
provádí se pravidelná záloha dat	zálohovaná data nejsou vždy uložena na bezpečném místě
existuje nástroj pro ověření funkčnosti zálohovaných dat	neexistuje plán continuity IS
existuje záložní zdroj elektrické energie	
vypracována opatření pro případ zničení či poškození systému	
Přístup k počítačům, síti, datům a systému	
existence systému autentifikace uživatelů	neexistují zásady pro tvorbu a změnu hesel
	nepoučení zaměstnanci v této oblasti
Zabezpečení Webu	
Zabezpečení komunikací na webu prostřednictvím SSL	

V předchozích kapitolách jsem se poměrně podrobně zabýval současným stavem informační bezpečnosti ve firmě HP TRONIC. Zjistil jsem, že bezpečnostní politika ve firmě je poměrně dobře řešena a není brána na lehkou váhu. Většina prvků informační bezpečnosti je ve firmě zavedena a tyto prvky jsou plně funkční. Některým oblastem však není v podniku věnována dostatečná pozornost či nejsou řešeny vůbec. V předcházející tabulce uvádím výčet nejdůležitější silných a slabých stránek zabezpečení informačního systému, které jsem získal v předchozí analytické části. Data v ní uvedená, mi poslouží k vytvoření plánu eliminace rizik plynoucích ze slabých stránek, kterým se budu zabývat v projektové části diplomové práce.

9 STAV INFORMAČNÍ BEZPEČNOSTI V ČESKÉ REPUBLICE

V České republice přisuzují největší váhu informační bezpečnosti banky a finanční instituce, kde velký význam této problematice přikládá 93 % respondentů. Zřejmě i proto banky a finanční instituce vykazují nejlepší výsledky takřka ve všech sledovaných oblastech informační bezpečnosti, mezi něž patří například existence bezpečnostní politiky, připravené plány obnovy funkčnosti informačních systémů či vyhrazený rozpočet na informační bezpečnost. Jen ve využívání a plánovaném využívání elektronického podpisu obsadily banky a finanční instituce druhou příčku a předstihly je firmy z oblasti telekomunikací a IT. Nejmenší důležitost své informační bezpečnosti přikládají podniky působící v elektrotechnice, strojírenství a dřevozpracujícím průmyslu. [11]

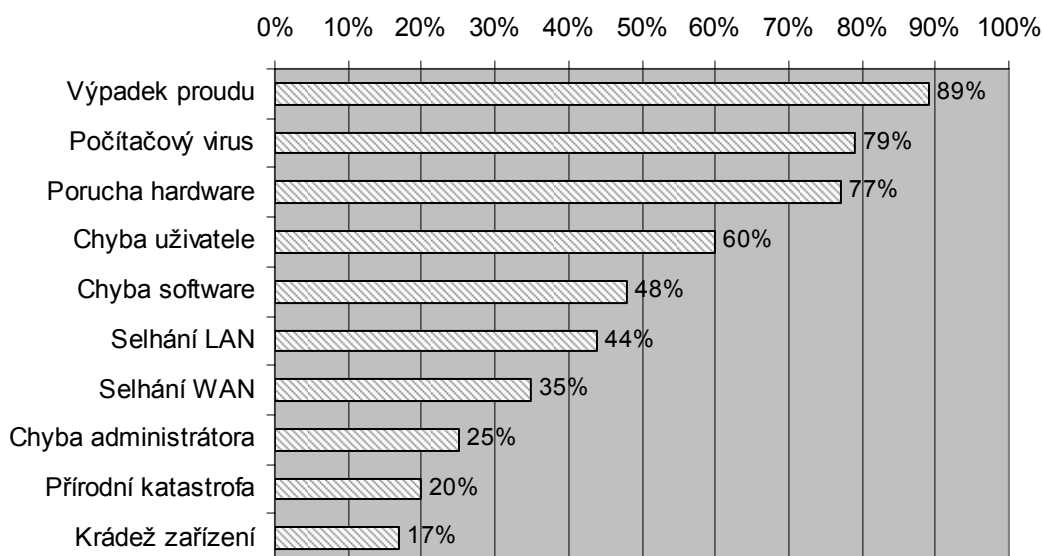
Oddělení odpovědné za informační bezpečnost v podniku je v České republice v drtivé většině oddělení IS /IT, navíc tento podíl dokonce roste. Celkem to je 78 % organizací. Pouze zcela výjimečně se jedná o útvar bezpečnosti, pouze ve 3 %. To je zcela nevyhovující situace, neboť bezpečnost by měla být od IS /IT oddělena a rozhodně by pracovník či pracovníci zodpovědní za bezpečnost neměli podléhat vedení IS/IT. [9]

Základním dokumentem, ze kterého by se mělo vycházet budování informační bezpečnosti, je bezpečnostní politika. Je to zásadní dokument, ze kterého by pak mělo vycházet budování bezpečnostního projektu, měla by být formálně dokumentována, schválena nejvyšším vedením atd. Přesto ve formě dokumentu má tuto bezpečnostní politiku přijatou pouze 46 % organizací. Jde ovšem o nárůst proti roku 1999 (35 %) i proti roku 2001 (42 %). Navíc i pokud má organizace bezpečnostní politiku přijatou, není jisté, jaké vlastně pokrývá oblasti. [9]

Povědomí o bezpečnosti informačních systémů v ČR stagnuje. Jediný nárůst zaznamenává oblast zabezpečení internetu. Zde 88 % firem používá firewall, zatímco před dvěma lety to bylo 76 % a v roce 1999 jen 52 %. Antivirové programy v roce 2003 využívalo 84 % firem, což představuje 16% nárůst oproti roku 2001 a 50% nárůst ve srovnání s rokem 1999. [11]

Takřka každý druhý podnik se v uplynulých dvou letech setkal s bezpečnostním incidentem v oblasti informačních systémů s přímými finančními dopady. Konkrétně se jedná o 49 % firem. Nejčastějšími bezpečnostními incidenty byly výpadky proudu, které postihly 89 % firem. Druhou příčku obsadily počítačové viry, s nimiž se setkalo 79 % firem. Počítačové viry ovšem zaznamenaly klesající trend oproti předchozím letům. Třetím

nejčastějším narušením informační bezpečnosti byly poruchy hardware, které zasáhly 77 % podniků. Výše popsané skutečnosti jsou zobrazeny v následujícím grafu. [11]



Graf 1: Nejčastější bezpečnostní incidenty ve firmách v ČR [11]

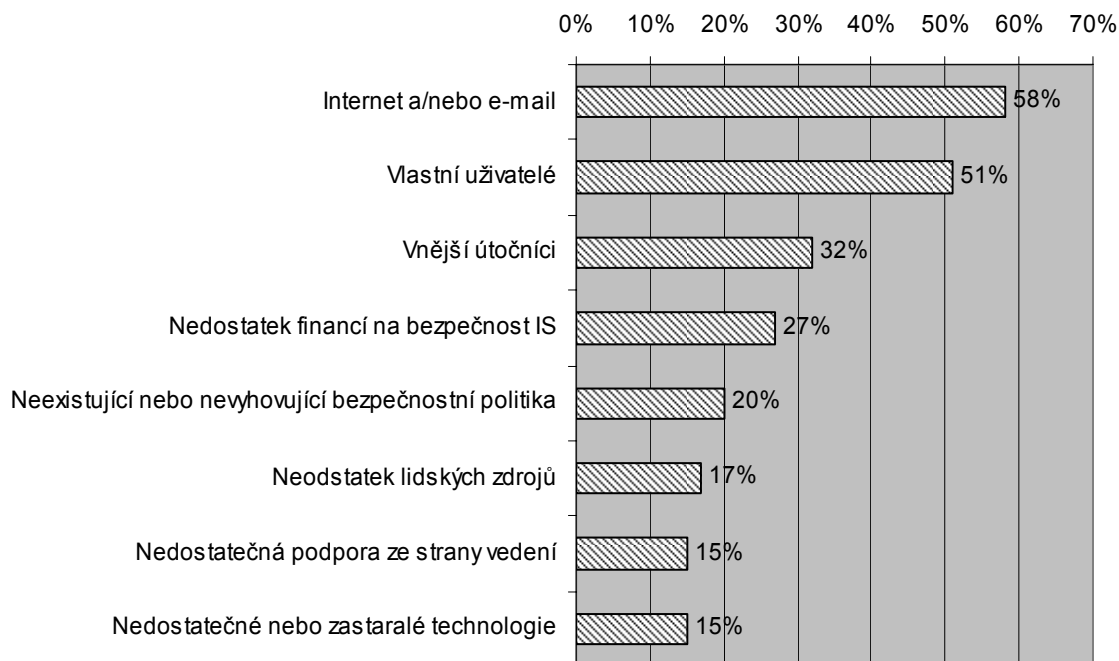
Kvalitní identifikace a autentizace je jedním z významných prvků zabezpečení. Identifikace a autentizace je pro přístup uživatelů do systému vyžadována u 99 % organizací. Některé organizace (13 %) vyžadují i jinou identifikaci a autentizaci kromě hesla, např. biometrickou autentizaci apod. Většina organizací sice provádí záznamy logování u hlavních systémů, ovšem většina organizací již tyto logy nevyhodnocuje. Pravidelně je vyhodnocuje 23 % organizací. Tyto záznamy jsou přitom cenným zdrojem informací, které by měly sloužit k dalšímu zlepšení bezpečnosti v organizaci.[9]

Popularitu si mezi českými firmami získává elektronický podpis. V současné době jej používá nebo plánuje v horizontu jednoho roku používat 51 % organizací. Firmy využívají elektronický podpis z 84 % k externí komunikaci se známými a definovanými obchodními partnery a zákazníky. Takřka třetina firem jej využívá k interní komunikaci.[11]

Prvenství ve finanční náročnosti jednotlivých bezpečnostních incidentů za rok 2003 obsadila přírodní katastrofa, reprezentovaná povodněmi. Průměrný přímý finanční dopad činil téměř 3,1 milionu Kč. Na druhém místě je chyba software, jejíž průměrný přímý finanční dopad je 1,9 milionu Kč. Na dalších místech v nejdražších narušeních bezpečnosti informačních systémů byla porucha hardware a chyba uživatele. [11]

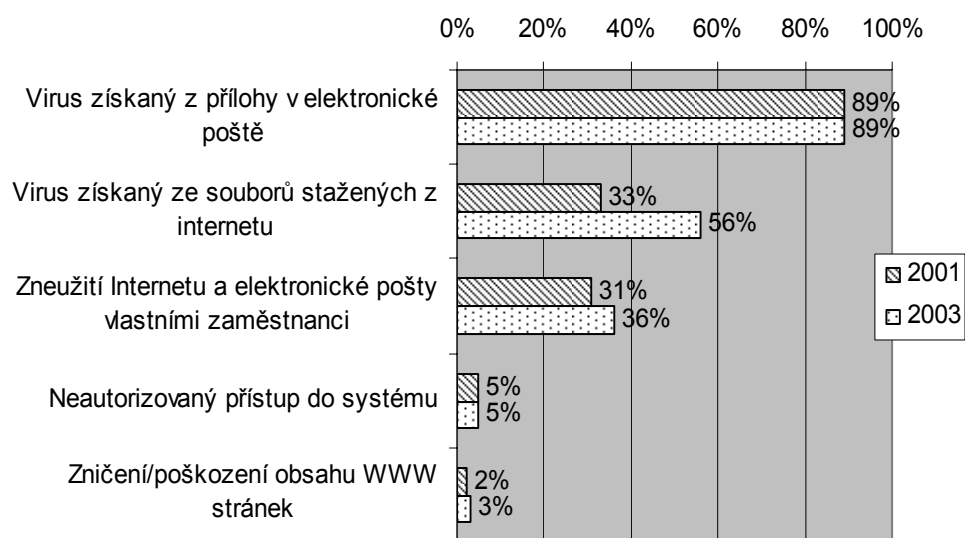
Za nejvážnější hrozbu informační bezpečnosti je podle 58 % respondentů považován internet společně s e-mailem. Padesát jedna procent organizací se domnívá, že největší

hrozbou jsou vlastní zaměstnanci, pro 32 % jsou to vnější útočníci. Na čtvrtém místě se objevil nedostatek financí na zabezpečení informačních systémů, který podle názoru firem ohrožuje 27 % z nich. Více než polovina firem, konkrétně 52 %, neví, co by dělala, kdyby byl jejich systém napaden. Nemají totiž žádné plány na obnovu svých informačních systémů. [11]



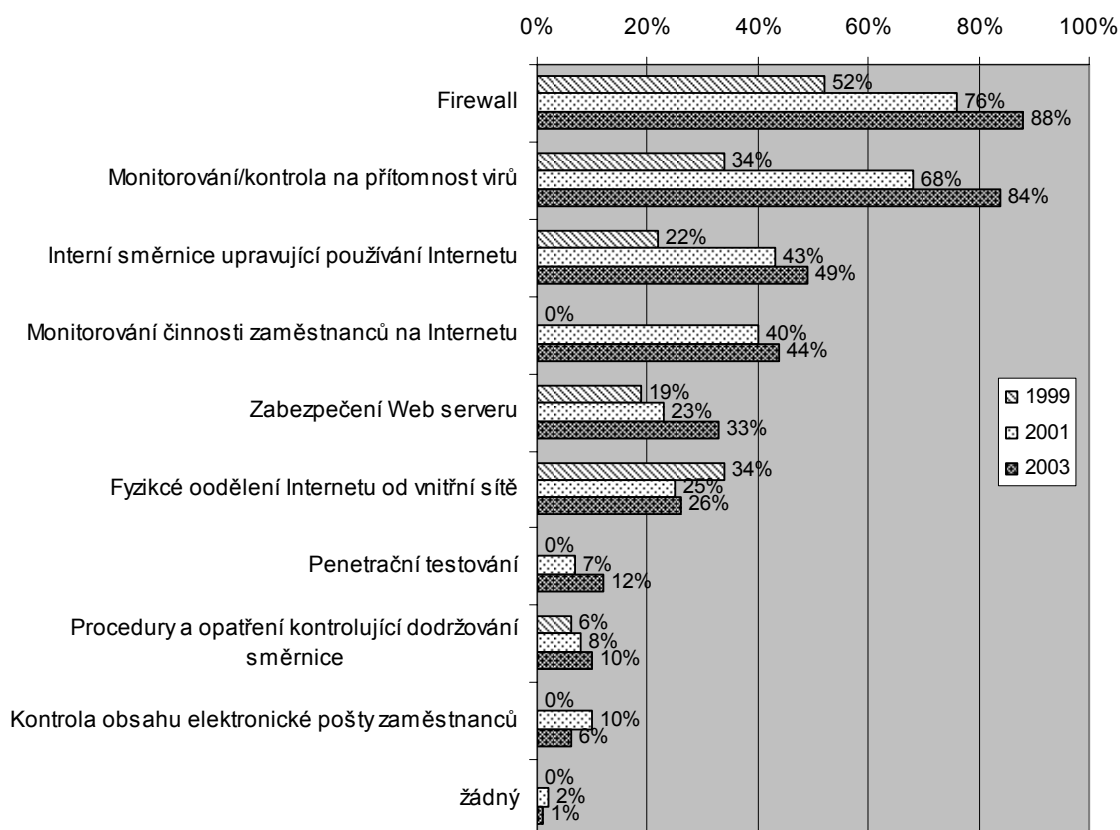
Graf 2: Největší hrozby z hlediska informační bezpečnosti [9]

Zatímco v roce 1999 mělo 17 % zaměstnanců přístup k internetu, v roce 2003 to již bylo 47 % zaměstnanců. Stejně rychlým tempem ale roste zejména počet virů stažených z internetu.[9]



Graf 3: Bezpečnostní incidenty a internet [9]

Stejně jako roste riziko bezpečnostních incidentů v souvislosti s internetem, tak se také vyvíjí způsoby zabezpečení internetu. To je znázorněno v následujícím grafu.[9]



Graf 4: Způsoby zabezpečení internetu [9]

Procento organizací se samostatným rozpočtem na informační bezpečnost se od roku 2001 prakticky nezměnilo. Relativní průměrná výše rozpočtu je 7,7 % ve srovnání s celkovým rozpočtem organizace na IS/IT. Platí, že čím větší organizace, tím větší pravděpodobnost existence samostatného rozpočtu na bezpečnost. [11]

Stále více firem řeší problematiku informační bezpečnosti ve spolupráci s externími firmami. Konkrétně se jedná o 57 % firem, které oblast bezpečnosti informačních systémů outsourcují. V této oblasti nastal v roce 2003 posun oproti roku 2001, kdy podniky, které outsourcovaly oblast informační bezpečnosti, tvořily 46 %. [11]

Celkově lze říci, že v některých oblastech bezpečnosti informačních systémů se situace oproti roku 2001 zlepšila (existence bezpečnostní politiky, využití firewallu, antivirové zabezpečení). V některých oblastech stav stagnuje a neočekávaně je v některých oblastech i horší – existence plánů obnovy. [9]

III. PROJEKTOVÁ ČÁST

10 PROJEKT ELIMINACE BEZPEČNOSTNÍCH RIZIK ELEKTRONICKÉHO PODNIKÁNÍ

V projektové části budu řešit problémy a slabé stránky IS a pokusím se *navrhnout opatření*, která povedou ke zvýšení informační bezpečnosti ve firmě a budou *eliminovat možná rizika* plynoucí ze slabých stránek. Při řešení těchto úkolů budu vycházet především z výsledků analytické části, tedy z analýzy silných a slabých stránek v podniku, která je prezentována v jejím závěru.

Cílem mého projektu je navrhnout ve firmě *správné a fungující opatření*, která povedou ke *snížení rizik* souvisejících s provozem informačního systému v podniku. Veškerá opatření budou vycházet ze současného stavu informační bezpečnosti. Mou snahou je navrhnout taková řešení, která s minimálními náklady budou problémy, slabé stránky a rizika s nimi spojené eliminovat na co nejnížší úroveň.

Hlavním problémem, na který se v této části zaměřím je fakt, že v podniku neexistuje útvar zabývající se komplexní bezpečností celého systému v podniku. Úkolem bude proto takový útvar či oddělení v podniku navrhnout a určit funkce a činnosti, které by takovému útvaru náležely.

Dalším podstatným problémem v oblasti antivirové ochrany, jak vyplynulo z předchozích kapitol, je nedostatečná ochrana informačního systému proti spywaru. Ze současných softwarových produktů na trhu vyberu nástroj, který bude nejvhodnější a splní v podniku svůj účel.

Nedostatek spatřuji také v nedostatečném poučení zaměstnanců o tom, jak se pohybovat na internetu. Úkolem bude tedy vytvořit zásady pohybu uživatelů na internetu, protože si myslím, že neznalost uživatelů v kombinaci s internetem je pro bezpečnost zásadní hrozbou, která zvyšuje riziko bezpečnostního incidentu.

Nepoučení uživatelů je patrné i v oblasti používání hesel. Co se týká autentizace, zjistil jsem, že někteří zaměstnanci používají velmi slabá hesla, v horším případě je nepoužívají vůbec. Vytvořím tedy postup, kterým by se zaměstnanci měli řídit při výběru, změnách a použití hesel.

Ačkoliv jsou všichni zaměstnanci chráněni proti nevyžádané poště tím, že jejich emailové adresy nejsou nikde zveřejněny, tedy ani na webových stránkách firmy, v poslední době se

zaměstnanci setkávají s větším množstvím spammu, který jsou nuceni odstraňovat. Proto navrhnu opatření, jak proti tomuto problému bojovat.

V podniku dále není věnována pozornost záznamům logů, ze kterých lze získat velmi užitečné informace v případě bezpečnostního incidentu. Tyto záznamy jsou sice v podniku prováděny, ale již nejsou uchovávány ani hodnoceny. To bude poslední slabá stránka, kterou se prostřednictvím svého projektu pokusím odstranit.

Oblast zálohování má nedostatek ve skutečnosti, že zálohovaná data jsou velmi často ukládána v místě, kdy byly zálohy vytvořeny. V podniku není bezpečné místo pro uložení důležitých záloh pro případ, že by došlo v budově k požáru či jiné katastrofě. Proto se tento nedostatek budu snažit odstranit návrhem vhodného řešení.

Dále z analýzy vyplynulo, že veškerý hardware, ale i software není řádně evidován, u hardwaru v síti nedochází k pravidelné a preventivní údržbě. Nedochází ani k pravidelným kontrolám nepoužívaných vstupů v síti ani k jejich zabezpečení proti případnému zneužití. Proto vypracuji nápravné opatření k tomuto nedostatku.

Zjistil jsem také, že firma HP TRONIC nemá vypracován podrobný plán kontinuity IS. V poslední části projektu navrhnu firmě doporučení jakým způsobem takový plán vytvořit a vymezím hlavní důvody pro jeho vypracování.

Historie projektu:

- Potřeba *navrhnout opatření pro eliminaci bezpečnostních rizik* elektronického podnikání
- Zlepšení bezpečnosti informačního systému v podniku

Požadavky managementu na projekt:

- Zhodnotit celkový stav bezpečnosti informačního systému ve firmě
- Vytvořit opatření eliminující rizika plynoucí ze slabých stránek bezpečnosti IS
- Navrhnout doporučení a zásady pro odstranění slabých stránek IS
- Nízké náklady na projekt

Co se již učinilo:

- Bylo provedeno podrobné zhodnocení stavu bezpečnosti IS ve firmě
- Byly nalezeny slabé stránky v oblasti bezpečnosti IS

Cíl projektu:

- Zvýšení informační bezpečnosti elektronického podnikání ve firmě

Kritéria úspěchu:

- Zájem zaměstnanců IT oddělení řešit problematiku bezpečnosti IS
- Úspěšná analýza současného stavu informační bezpečnosti ve firmě
- Vypracování vhodných a účinných opatření a postupů, které budou rizika plynoucí z hrozeb skutečně eliminovat

Co není součástí projektu:

- Do projektu nebudou zapojeny žádné jiné externí firmy či osoby
- Součástí projektu není kompletní inovace informačních systémů a technologií

Omezení projektu:

- Nelze získat takové informace týkající se existujícího zabezpečení informačního systému, které považuje vedoucí IT oddělení za citlivé a přísně tajné
- Není možný přístup ke všem počítačům a nelze libovolně využívat dostupnou výpočetní techniku
- Projekt musí být vypracován do xx.xx. xxxx

Rozpočet projektu:

- Při tvorbě opatření je třeba počítat s minimálními náklady na jejich zavedení
- Není stanovena maximální částka, kterou nesmí investice do zlepšení stavu bezpečnosti IS přesáhnout. Záleží na dohodě s managementem
- Není podmínkou, aby podnik veškerá navržená opatření a postupy zaváděl a jejich dodržování a funkčnost nebude možno ověřit

Rozvrh prací:**1. Návrh útvaru bezpečnosti IS**

- Přiřazení funkcí a činností tomuto útvaru
2. **Zlepšení bezpečnosti v oblasti antivirové ochrany**
 - Návrh účinného nástroje proti spywaru
 3. **Zvýšení úrovně zabezpečení internetu**
 - Vytvoření zásad pro bezpečný pohyb na internetu
 - Ochrana proti spammu
 4. **Vyšší bezpečnost v oblasti kontroly přístupu (k počítačům, síti, datům)**
 - Vytvoření zásad pro správné užívání hesel
 - Záznamy, evidence a kontrola logů
 5. **Opatření v oblasti zálohování**
 - Bezpečné uložení zálohovaných dat
 6. **Návrh evidence, kontroly a údržby hardwaru a softwaru v síti**
 7. **Postup a důvody vytvoření plánu kontinuity IS**

Organizace projektu:

Řídící tým: Ing. Stanislav Šimčík

Vedoucí projektu: Ing. Stanislav Šimčík

Projektový tým: Bc. Miroslav Poštolka

Zaměstnanci oddělení IT ve firmě HP TRONIC, spol. s r. o.

Sponzor projektu: projekt není sponzorován

10.1 Návrh útvaru bezpečnosti informačního systému

Oddělení IT ve firmě si je moc dobře vědomé důležitosti zabezpečení IS v podniku. Většina oblastí bezpečnosti IS je velmi dobře řešena a z analýzy vyplynulo, že v podniku neexistují nějaké významnější hrozby, které by mohly bezpečnost ohrozit. Myslím si však,

že pro podnik takové velikosti jako je HP TRONIC by nemělo být pro řešení celkové informační bezpečnosti pouhé oddělení IT dostačující. Toto oddělení se skládá z pracovníků správy sítě, systémových administrátorů a webmastera. Všichni z těchto pracovníků samozřejmě dbají o zabezpečení ve své oblasti působnosti. Myslím si však, že starat se o bezpečnost IS celkově není jejich prioritním úkolem a není to ani v jejich možnostech. Bezpečnost je až na druhém místě. V podniku neexistuje kontrola nad tím, zda je stanovená bezpečnostní politika v podniku dodržována a zda se zaměstnanci řídí stanovenými bezpečnostními zásadami a postupy. Neprovádí se pravidelné školení zaměstnanců v oblasti bezpečnosti a ti se pak můžou stát potenciální hrozbou informačního systému. Správce sítě nemusí být schopen se starat o všechny aspekty zabezpečení, které se v podniku vyskytují. Proto bych v rámci oddělení IT vyčlenil alespoň jednoho pracovníka, který by měl veškeré aspekty zabezpečení IS pod kontrolou. Jednalo by se tak o správce zabezpečení, který by dohlížel na dodržování stanovené bezpečnostní politiky v podniku a prováděl průběžná opatření pro její zlepšování. Dalším podnětem pro to, že jsem se rozhodl takového pracovníka v podniku nasadit je skutečnost, že administrátoři informačního systému ve firmě mají často plná práva na provádění změn v rámci systému a mají tak vlastně monopol na monitorování své vlastní činnosti. Neexistuje nad nimi žádná kontrola a možnost zasáhnout v případech, kdy překračují rámec svých pravomocí.

Hlavní funkce, úkoly a činnosti správce zabezpečení:

- kontrola dodržování stanovené bezpečnostní politiky
- zavádění nových prvků bezpečnostní politiky
- provádění analýzy stavu informační bezpečnosti v podniku
- vytváření účinných opatření k zajištění informační bezpečnosti
- kontrola účinnosti opatření k zajištění informační bezpečnosti
- řešení bezpečnostních incidentů
- pravidelné školení zaměstnanců v oblasti informační bezpečnosti

Z absence správce zabezpečení plynou další zjištěné slabé stránky informační bezpečnosti v podniku. Proto návrh na jeho vyčlenění považuji za klíčové řešení celého projektu.

10.2 Zlepšení bezpečnosti v oblasti antivirové ochrany

V podniku je instalován velmi kvalitní a účinný nástroj pro detekci a odstranění virové infekce. Jak jsem ale již v analytické části uvedl, tento nástroj není schopen odhalit všechny druhy škodlivých programů typu spyware a adware. Tyto programky, ač se může zdát, že v počítači nijak neškodí a pracují na pozadí, můžou být velmi nebezpečné. Dokonce i ta nejneškodnější forma spywaru představuje zásah do soukromí. Odborníci se domnívají, že v budoucnu bude spyware čím dál tím škodlivější a bude využíván pro zjišťování hesel, čísel kreditních karet a pro další formy krádeže identity.

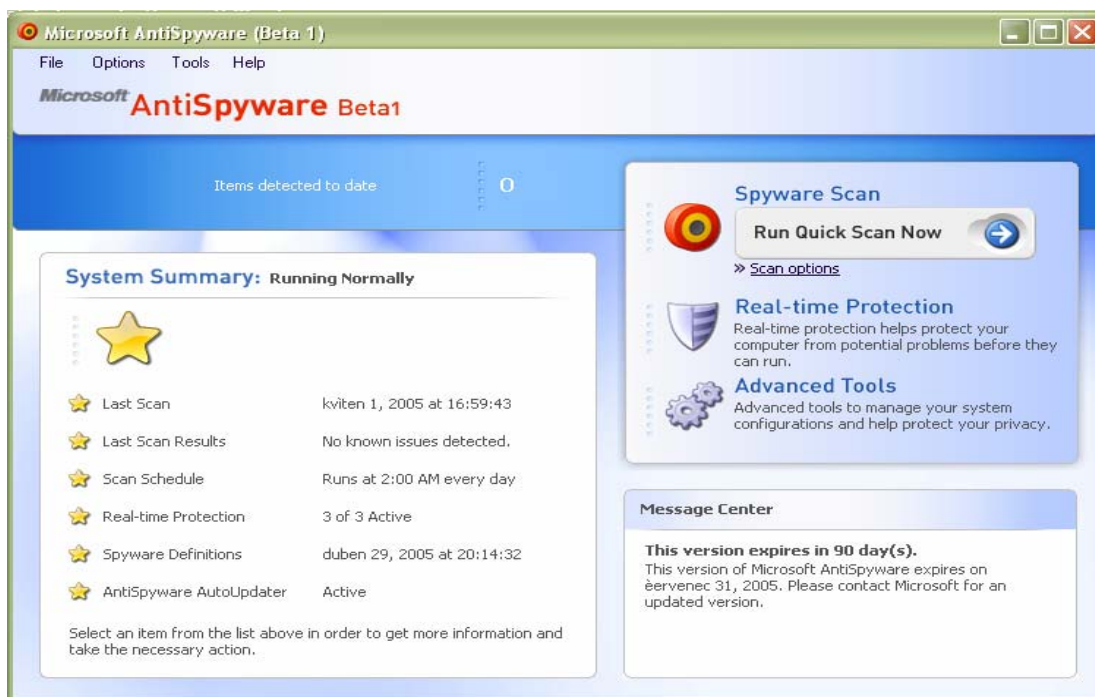
Proto jsem na jednom z počítačů nainstaloval software pro detekci a odstranění spywaru/adwaru, abych zjistil jaká je situace v této oblasti zabezpečení v podniku. Provedený test ukázal, že se na počítači vyskytuje velké množství programů tohoto typu.

Rozhodl jsem se proto firmě navrhnout instalaci softwaru typu antispysware na všech počítačích v síti. Na trhu je poměrně široká paleta programů tohoto typu a je z čeho vybírat. Na základě vlastních zkušeností a testů těchto programů v odborných časopisech jsem rozhodoval mezi dvěma:

- *Microsoft Windows AntiSpyware*
- *LavaSoft AdAware SE*

Tab.3: Navrhované nástroje proti spywaru [vlastní zpracování]

	Microsoft Windows Antispyware	LavaSoft AdAware SE
Výrobce	Microsoft Corp.	Lavasoft
Licence	Freeware	Shareware
Operační systém	Windows 2000/XP/2003	Windows 98/ME/NT/2000/XP/2003
Automatický update	Ano	Ano
Ochrana v reálném čase	Ano	Pouze v plné verzi
Čeština	Ne (zatím)	Ano
Cena plné verze programu	Zdarma možno stáhnout z internetu	Kč 986 (bez DPH 19 %)



Obr.6: Ukázka nástroje Microsoft AntiSpyware



Obr.7: Ukázka nástroje Ad-Aware SE

Z výše posuzovaných nástrojů jsem firmě doporučil instalaci softwaru od společnosti LavaSoft. Antispyware od Microsoftu lze sice oproti konkurenci zdarma stáhnout z internetu, a to v plné verzi, která podporuje funkci ochrany v reálném čase, avšak je třeba

řící, že produkt Microsoftu je zatím beta verzí. Je tedy plně funkční, ale je zatím určen pouze pro testovací účely a může mít ještě určité nedostatky a chyby. Ad-aware je zdarma ke stáhnutí pouze ve verzi pro nekomerční využití, která tuto funkci ochrany v reálném čase neumožňuje. Ad-Aware je však již na trhu delší dobu a je to poměrně dobře vyzkoušený nástroj. Z toho důvodu jsem doporučil zakoupení právě Ad-Awaru SE ve verzi Professional. Ten bude zakoupen s originální licencí. Výhodou produktu firmy LavaSoft je také fakt, že je k dispozici v českém jazyce.

10.3 Zvýšení úrovně zabezpečení internetu

Jak vyšlo najevo z analytické části, není v podniku kontrolován pohyb uživatelů po internetu. Neexistují v podniku žádné psané zásady a pravidla pro využití internetu zaměstnanci a ti také nejsou poučeni o hrozbách souvisejících s jejich pohybem na internetu.

Tato problematika souvisí také s mým návrhem zavedení správce zabezpečení. Tento pracovník by měl provádět právě taková školení a přednášky, které by zvyšovali povědomí zaměstnanců v oblasti informační bezpečnosti. Patří sem samozřejmě i oblast zmíněných hrozeb internetu.

S využíváním internetu nesouvisí pouze nebezpečí, které přináší v podobě nejrozumnějších virů, spywaru a dalších škodlivých jevů. Souvisí také s produktivitou práce, která může klesat v důsledku toho, že podnik nepřijme opatření ke kontrole používání internetu svými zaměstnanci.

Cílem této kapitoly je proto navrhnout v oblasti zabezpečení internetu nejdůležitější pravidla a zásady pro jeho používání, které by měli zaměstnanci dodržovat, aby nezpůsobily podniku ztráty, které by mohly plynout z potenciálních bezpečnostních incidentů. Mnou navržené zásady by měly být zaměstnancům prezentovány a předány ve dvou kopiích. Jednu kopii si ponechají a druhou podepsanou vrátí.

Tab.4: Zásady bezpečného používání internetu ve firmě [vlastní zpracování]

ZÁSADY BEZPEČNÉHO POUŽÍVÁNÍ INTERNETU VE FIRMĚ HP TRONIC		
1. Internet je určen pouze pro plnění pracovních úkolů ve firmě 2. Využit internetu pro soukromé účely je povoleno pouze v době pracovních přestávek a mimo pracovní dobu 3. Není povoleno jakkoliv měnit nastavení internetového prohlížeče 4. Zaměstnancům je zakázáno připojovat se k nedůvěryhodným serverům 5. Je zakázáno stahování a instalace jakéhokoliv softwaru z internetu 6. Je zakázáno stahovat a rozšiřovat materiály urážlivé, nedovolené nebo obtěžující povahy 7. Pracovní emailová schránka nesmí být použita k soukromým účelům 8. Nevyžádané a podezřelé e-maily či jejich přílohy nesmí být otvírány		
Vypracoval: Bc. Miroslav Poštolka Dne: 18. 4. 2005	Schválil: Ing. Stanislav Šimčík Dne: 20. 4. 2005	Podpis zaměstnance:

Od výše zmíněných zásad si slibuji, že zaměstnanci ve firmě budou internet používat zodpovědněji a uvážlivěji a jejich dodržování povede k minimalizaci rizika napadení či ztráty podnikových dat prostřednictvím útoků z internetu.

Do této oblasti zabezpečení jsem zahrnul také zabezpečení proti spammu. Jak už jsem popsal výše, přestože pracovní emaily nejsou zveřejněny na webových stránkách firmy HP TRONIC, zaměstnanci se velmi často setkávají s nevyžádanou poštou. Zjistil jsem, že firma používá ve většině případů pro práci s elektronickou poštou program Microsoft Outlook, jehož součástí je účinný antispamový filtr. Tento nástroj však není aktivní a nebyla nastavena pravidla pro filtraci příchozí pošty. Navrhoval bych proto, aby byla povolena funkce filtrace a byla vytvořena pravidla pro filtraci příchozí elektronické pošty. Toto opatření by vedlo k úspoře času, který musí zaměstnanci trávit ručním tříděním a mazáním nevyžádané pošty.

10.4 Vyšší bezpečnost v oblasti kontroly přístupu (k počítačům, sítí, datům)

V oblasti kontroly přístupu byly odhaleny dva podstatné nedostatky. Především se jedná o nepoučení uživatelů o tvorbě a používání hesel. Nepoučení zaměstnanců v tomto směru opět plyne z již popsané neexistence útvaru, který by se zabýval školením zaměstnanců v oblasti bezpečnosti IS, tedy absence mnou navrhovaného pracovníka – správce zabezpečení. O používání hesel by měla být provedena krátká přednáška, jejíž součástí by byla řešena i v předchozí kapitole zmíněná problematika hrozeb z internetu.

Dalším nedostatkem je, že oddělení IT nevěnuje pozornost záznamům logů, jejich evidenci a kontrole. Záznamy logů jejich evidence, vyhodnocování a kontrola by měla být opět úkolem navrhovaného správce zabezpečení, který by takovou činnost prováděl každý den.

V souvislosti s problematikou slabých hesel jsem navrhl seznam nejdůležitějších pravidel pro zaměstnance, které by měli dodržovat při jejich tvorbě a používání. Tato pravidla by každý zaměstnanec dostal po skončení zmíněné přednášky týkající se této oblasti. Nad dodržováním politiky hesel by pak měl mít kontrolu správce zabezpečení.

Tab.5: Doporučené zásady používání hesel [vlastní zpracování]

DOPORUČENÉ ZÁSADY POUŽÍVÁNÍ HESEL	
1. Heslo nesmí být sdíleno s více lidmi. 2. Heslo nesmí být příliš jednoduché (např. jména partnerů, dětí, datum narození apod.). 3. Heslo je tím bezpečnější, čím je delší. Minimální délka hesla by měla být 8 znaků. Je vhodné kombinovat písmena a číslice. 4. Maximální stáří hesla by mělo být 30 dnů. Po této době by mělo být heslo změněno. 5. Heslo je třeba uložit na chráněném místě (nejlépe v hlavě), nesmí být přilepené na stole vedle monitoru. 6. Není vhodné používat jedno heslo pro více aplikací.	
Vypracoval: Bc. Miroslav Poštolka Dne: 18. 4. 2005	Schválil: Ing. Stanislav Šimčík Dne: 20. 4. 2005

Co se týče nedostatečného auditu, evidence záznamů logů, jejich analýzy a kontroly, pro řešení daného problému ve firmě jsem doporučil základní postup a zásady, jak by se tyto činnosti měly v podniku provádět. Důvody pro jejich zavedení vidím zejména v:

- *možnosti odhalení útoku* – z logovacích souborů lze někdy odhalit právě probíhající útok na aplikaci a včas mu zabránit. I po úspěšném útoku jsou logy často jediným místem, ze kterého lze provedené vniknutí vůbec odhalit.
- *možnosti obnovy aplikace a vyvození odpovědnosti* - ze záznamů v logu lze zpětně vysledovat způsob vniknutí, průběh útoku a rozsah způsobených škod. To může administrátorovi pomoci při zpětné obnově aplikačních dat do stavu před vniknutím. Také lze často vystopovat útočníka a vyvodit vůči němu příslušné důsledky.
- *možnosti získat informace o uživateli* - rozbořením logů lze také získat cenné informace o svých uživateli, o jejich zvyklostech, typické cestě procházení aplikací, využívaných službách apod.

Zásady evidence, analýzy a kontroly logů:

1. Logovací záznam musí obsahovat základní informace, jako čas události, identifikaci uživatele, IP adresu a jméno počítače, ze které přistupuje.
2. Měly by být kontrolovány všechny důležité akce, zejména potenciálně nebezpečné
3. V aplikacích se doporučuje evidovat následující typy událostí:
 - čtení a zápis dat;
 - změny jakýchkoliv údajů včetně přístupových oprávnění, umístění v databázi či filesystému nebo vlastnictví;
 - smazání jakéhokoliv datového objektu;
 - síťová komunikace na všech úrovních;
 - autentizační události;
 - autorizační události;
 - administrační funkce;
 - všechny nastalé chyby;
4. Přístup k záznamům logů mají pouze osoby určené pro jejich kontrolu – správce zabezpečení.
5. Záznamy by měli být ukládány na bezpečném místě.

6. Doporučuje, aby administrátor prohlížel logy pravidelně, a to alespoň jednou denně.

Navrhované opatření se může jevit jako zbytečné a může se zdát, že pro správce zabezpečení je ztráta času tímto problémem se zabývat. Já se však domnívám, že pro předcházení a řešení již provedených útoků na informační systém je zavedení tohoto opatření velmi užitečné a jeho účinnost a opodstatnění by se projevilo právě až v situaci, kdy by došlo ke skutečnému bezpečnostnímu incidentu.

10.5 Návrh pro bezpečné uložení zálohovaných dat

Dotazníkového šetření, které jsou v podniku provedl, prokázalo, že ačkoliv samotnému zálohování dat je věnována značná pozornost, situace v oblasti uložení záložních médií je již podstatně horší. Záložní média jsou mnohdy uložena v místě, kde byly vytvořeny. V případě, že by došlo v budově firmy k požáru či jiné katastrofě by proto mohlo dojít ke zničení i těchto záložních médií. Je tedy třeba zavést opatření, kdy by zálohovaná data byla umístěna na ohnivzdorném místě nebo jejich kopie uloženy zvlášť mimo budovu nebo alespoň v jiné části budovy. Je třeba říci, že místo, které by bylo odolné vůči požáru v podniku neexistuje.

Z toho důvodu jsem podniku navrhl zakoupení ohnivzdorné bezpečnostní skříně uzpůsobené pro počítačové nosiče dat. Taková skříň je odolná také proti vlhkosti, požárním plynům a zmagnetizování. Na trhu je množství výrobců, kteří nabízejí takové skříně a ceny se pohybují od 40 000 Kč až po 250 000 Kč. Záleží na nejrůznějších parametrech a specifikacích, jako je velikost, doba ohnivzdornosti, bezpečnostní třída apd. Jako příklad uvádím trezor od firmy FORMAT. Tato skříň, typ „Fire Star Plus“ se řadí spíše do nižších cenových kategorií a pro podnik HP TRONIC by byla plně dostačující. Navrhovaný trezor by sloužil nejen pro uložení důležitých záložních médií, ale také k bezpečné ochraně důvěrných a citlivých dat.



Obr.8: Ohnivzdorná skříň Fire Star Plus

10.6 Evidence, kontrola a údržba hardwaru a softwaru sítě

Z dotazníků, které jsem dal pracovníkům IT oddělení ve firmě k vyplnění, jsem zjistil, že ve firmě HP TRONIC není věnována dostatečná pozornost evidenci, kontrole a údržbě hardwarových komponent v síti. K údržbě a kontrole hardwarových zařízení dochází většinou až v případě, že se na nich vyskytne nějaký problém. K preventivní údržbě hardwaru tedy dochází velmi zřídka.

Doporučoval bych proto, aby bylo zavedeno takové opatření, které by stanovovalo povinnost určeným pracovníkům IT oddělení provádět kontrolu a údržbu veškerého hardwarového vybavení minimálně jednou za 3 měsíce. Preventivní údržbou můžou být odhalovány a odstraňovány skryté závady, které by mohly při jejich včasném neodstranění výpočetní techniku poškodit a mohly by tak dojít k dalším problémům. Při preventivní údržbě by mělo být provedeno vnitřní i vnější očištění všech komponent výpočetní techniky. Každá počítačová stanice by měla být označena evidenčním číslem. Pro každou počítačovou stanici by pak měla existovat evidenční karta, ve které by byl uveden seznam hardwarového vybavení této stanice.

Dále bych doporučoval, aby v této evidenční kartě byl uveden seznam softwaru, který je na daném počítači instalován a při provádění údržby hardwaru byla prováděna také kontrola, zda zde není instalován další nelegální či nevhodný software. Na této kartě by bylo také uvedeno datum kontroly a kdo kontrolu prováděl. V poznámkách pak, jaké byly zjištěny nedostatky a provedeny opatření k jejich odstranění.

Tab.6: Evidenční karta počítačové stanice [vlastní zpracování]

Evidenční karta počítačové stanice							
Evidenční číslo stanice:			Umístění stanice:			Kontrola a údržba	
						Datum kontroly	Kontrolu provedl
Programové vybavení			Technické vybavení				
Název	Verze	Licenční číslo	Název	Sériové číslo	Invent. číslo		
Poznámky:							

Na základě takové karty by pak pracovník zodpovědný za kontrolu a údržbu hardwaru zkontroloval, zda skutečný stav souhlasí s údaji na kartě a zaznamenal možné změny. Záznamy z karet by pak byly pořízeny do elektronické podoby, kdy by byly veškeré údaje o hardwarovém i softwarovém vybavení vedeny v databázi programu MS Access.

Od navrženého opatření si slibují nejen přehlednou evidenci veškeré výpočetní techniky ve firmě. Pravidelná kontrola a údržba hardwaru by měla vést ke snížení rizika poruch a výpadků hardwarových prostředků v síti a ke snížení ztrát nich plynoucích. Kontrola softwaru pak zajistí, aby na počítačích nebyl instalován nelegální či nežádoucí software.

10.7 Plán kontinuity IS

Jak jsem zjistil z dotazníkového šetření, firma HP TRONIC nemá vypracován podrobný plán kontinuity IS. Podle mého názoru by společnost jako je HP TRONIC měla mít takový plán bezpodmínečně vypracován. Uvádím proto v této části diplomové práce důvody pro jeho vytvoření a stručný postup, podle kterého by měl být vytvořen. [16]

Plán kontinuity IS připravuje organizaci na potenciální havárie, omezuje jejich dopady na fungování informačního systému a stanoví postupy, jak řešit nestandardní situace. Jednotlivá narušení mohou být nejrůznějšího typu, například:

- přírodní nebo technické - technologické havárie,

- cílené útoky na informační systém,
- neúmyslné selhání obsluhy s důsledkem výpadku informačního systému,
- nedostatek obslužného personálu,
- výpadek subdodavatele např. elektrické energie, plynu, Internet providera, atp. [16]

Pro inicializaci projektu a vytváření plánu kontinuity IS je několik významných důvodů:

- dobré jméno společnosti zejména směrem k zákazníkům a veřejnosti,
- zvýšení hodnoty akcií společnosti,
- minimalizace ztrát společnosti v případě vzniku mimořádné situace ,
- Bezpečnostní politika - součástí bezpečnostní politiky je obvykle i kapitol definující podmínky a vytváření plánu kontinuity ,
- Standard BS7799 - Kapitola 11 - Řízení kontinuity podnikatelských činností
Řízení kontinuity podnikatelských činností by mělo obsahovat opatření k identifikaci a minimalizaci rizik, omezovat důsledky škodlivých incidentů a zajistit obnovení nezbytných činností.,
- Legislativní požadavky. [16]

10.7.1 Postup vytváření plánu kontinuity

Příprava

V první etapě jsou zmapovány výchozí podmínky, kdy vstupem je popis informačního prostředí (přehled systémů, komunikací, HW, SW, jejich vzájemné propojení) a zhodnocení aktuálního stavu havarijní připravenosti (havarijní procedury, zálohování, pojištění, plány) a výstupem je dokument, který je určen pro rozhodování managementu společnosti (stanovuje cíle, důvody, legislativní předpoklady a standardy, předpokládaný způsob řešení, potřebné kapacity, harmonogram a náklady). [16]

Analýzy a Strategie

V druhé etapě jsou provedeny analýzy, které slouží jako vstup pro stanovení strategie:

- analýza rizik, která hodnotí pravděpodobnost vzniku mimořádné události v důsledku působení daného rizika na aktiva společnosti;

- analýza obchodních dopadů, která hodnotí finanční dopady na společnost v případě výpadku kritického procesu, analyzuje důležitost dat, aplikací a IS z hlediska dopadů na organizaci a analyzuje reálnosti nezbytného rychlého a postupného obnovení stavu IS.

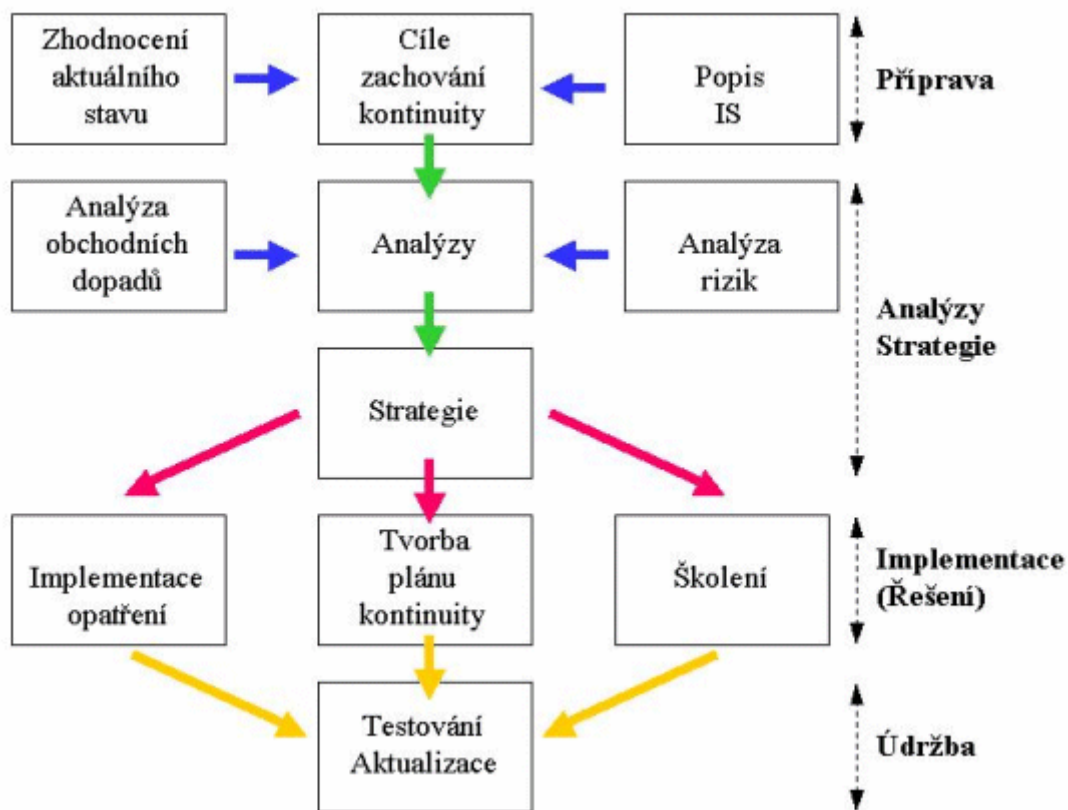
Strategie zachování kontinuity je dokument pro management společnosti, kde jsou na základě vypracovaných analýz vyjmenovány možné ztráty, optimalizovány investice do konkrétních opatření, navrženy dílčí procedury a plány, způsob školení, aktualizace, management rizik a další. [16]

Implementace (tvorba opatření a plánů)

Třetí etapa se skládá z vlastní implementace opatření (bezpečnostní opatření, zálohování, záložní centra, atd.), zavedení managementu kontinuity IS a tvorby jednotlivých detailních procedur a plánů.

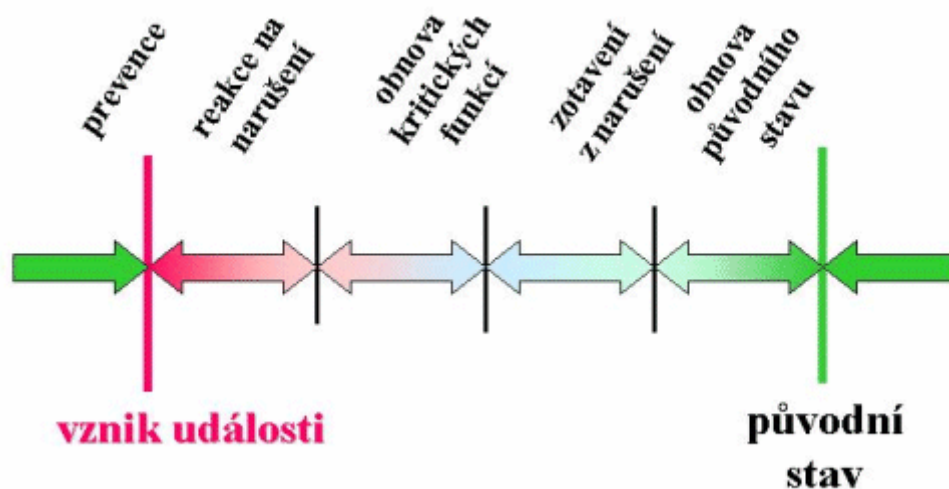
Údržba

Vytvořením plánů a realizací dílčích opatření celý proces nekončí, nedílnou součástí je i školení zaměstnanců, osvěta, testování jednotlivých procedur a jejich aktualizace. [16]



Obr. 9: Postup vytváření plánu kontinuity IS [16]

10.7.2 Oblasti, které pokrývá plán kontinuity IS



Obr. 10: Oblasti, které pokrývá plán kontinuity IS [16]

Prevence

Prevence znamená přípravu plánů a jejich realizačních opatření, přípravu lidí i technických prostředků pro případ havárie. Na kvalitě prevence závisí četnost a doba výpadků a náklady na obnovu funkčnosti. [16]

Reakce na narušení (mimořádnou událost)

Prvořadým zájmem každé společnosti je, aby škody vzniklé v případě havárie byly co nejmenší a co nejméně narušily chod společnosti. Do této fáze spadá také ochrana zdraví a lidských životů. Probíhají činnosti k zastavení, omezení rozsahu či zpomalení události. [16]

Obnova kritických funkcí organizace

Po prvotní reakci následuje obnova kritických procesů. Tato fáze má pro organizace velký význam, neboť zde se rozhoduje o velikosti následných škod, případně o samotné existenci organizace. Činnosti pracovníků se přitom řídí dle havarijních procedur. Jejich součástí je např. přesun provozu do náhradních prostor a náhradního zařízení, obnova provozu v nouzovém, havarijním stavu, atp. [16]

Zotavení z mimořádné události

Další fází procesu obnovy je obnova podpůrných činností a celkové zotavení organizace z narušení. Obnovují se především takové funkce, které z hlediska časové dostupnosti

a významu nejsou kritické, ale přesto se značnou měrou podílejí na kvalitě služeb, které organizace poskytuje. [16]

Obnova původního stavu

V této fázi se obnovuje původní stav provozu IS, je zjištěn rozsah škod, jsou rekonstruovány budovy místnosti, zajištěna technika, SW prostředky a přechod provozu z havarijního do normálního stavu. [16]

11 SHRUTÍ PROJEKTOVÉ ČÁSTI

V následující části diplomové práce shrnu nejdůležitější poznatky z navrhovaných opatření pro eliminaci bezpečnostních rizik elektronického podnikání. Zhodnotím jejich význam pro informační bezpečnost v podniku, efektivitu a přínos pro podnik.

Na začátek je třeba říci, že informační bezpečnost je záležitostí čistě nákladovou a přínosy jsou velmi těžce vyjádřitelné. Je tedy velmi obtížné spočítat efekt, jaký by navrhované opatření přinesly. Náklady na ně vynaložené je třeba chápat jako formu pojištění. Nelze předem určit zda a kdy může dojít k bezpečnostnímu incidentu. Avšak v případě, že by k němu došlo, podniku by se náklady do takových opatření ke snížení rizika mnohokrát vrátily.

11.1 Zhodnocení navrhovaných řešení

- o V případě zavedení navrhovaných řešení by došlo ke zvýšení celkové informační bezpečnosti v podniku.
- o Bylo přihlíženo k minimalizaci nákladů, které by musely být vynaloženy v případě realizace jednotlivých návrhů.
- o Nejvyšší náklady by si vyžádalo zavedení pracovníka pro správu zabezpečení a dále pak náklady na pořízení ohnivzdorné skříně pro uložení zálohovaných dat. Náklady na nákup programu pro detekci a odstranění spywaru jsou minimální, jestliže porovnáme efekt, který by přinesl. Další navržená opatření si již nevyžadají žádné náklady na jejich realizaci.

Návrh zavedení správce zabezpečení

- Rozsahem i náklady je to nejnáročnější opatření, které by však mělo největší efekt, co se týče zlepšení celkové informační bezpečnosti v podniku.
- Význam takové funkce by spočíval především v utváření bezpečnostní politiky a kontrole jejího důsledného uplatňování.
- Zavedení tohoto opatření by mělo vliv i na další návrhy v tomto projektu, protože by umožnilo zajistit jejich důsledné dodržování. Týká se to především politiky hesel a bezpečného pohybu na internetu.

- Přínos by spočíval také ve zvyšování povědomí zaměstnanců o informační bezpečnosti školeními, přednáškami a workshopy zaměřenými na tuto tematiku.

Návrh na zlepšení bezpečnosti v oblasti antivirové ochrany

- Spočívá v zavedení účinného nástroje proti spywaru.
- Náklady na toto opatření jsou minimální ve srovnání s efektem, který přinese.
- Detekcí a odstraněním nežádoucích programů dojde ke zvýšení bezpečnosti a eliminaci rizika ztráty dat.
- Nástroj odstraní další nežádoucí efekty těchto škodlivých programů, kterými mohou být snížení výkonu počítače či snížení produktivity práce spojené s úsilím zaměstnanců na odstranění nechtěných jevů (např. změna startovní webové stránky apod.).

Zvýšení úrovně zabezpečení internetu

- Opatření tohoto typu sebou nenese žádné náklady.
- Prostřednictvím přednášky by byli zaměstnanci poučeni o hrozbách spojených s internetem.
- Vytvořené zásady pro používání internetu ve firmě by měly vést k tomu, že zaměstnanci budou internet používat zodpovědněji a uvážlivěji, což povede k minimalizaci rizika napadení či ztráty podnikových dat prostřednictvím útoku z internetu.
- Zásady obdrží každý pracovník v tištěné podobě k podepsání. To by mělo vést k odpovědnosti za jejich dodržování.
- Jednoduché nastavení filtrace příchozí pošty by mělo zastavit nežádoucí příchozí zprávy. To bude znamenat vyšší úroveň zabezpečení počítačů a také vyšší produktivitu práce.

Vyšší bezpečnost v oblasti kontroly přístupu (k počítačům, síti, datům)

- Opatření k tvorbě a používání silných hesel všude tam kde je to nutné povede k zamezení přístupu do systému, k počítačům a důležitým datům nepovolaným a neoprávněným osobám.

- Zaměstnanci mají návod ve formě zásad, jak správně vybírat a používat hesla.
- Prováděním auditu, evidence záznamů logů, jejich analyzováním a kontrolou by se dalo předcházet potenciálním bezpečnostním incidentům a dále pak z nich zjistit, zda už k takovým incidentům nedošlo.

Opatření v oblasti zálohování

- Z důvodu, že v podniku není bezpečné místo pro uložení důležitých zálohovaných dat, bylo třeba se tímto problémem zabývat.
- Náklady na toto opatření ve formě zakoupení ohnivzdorné skříně pro ukládání zálohovacích médií jsou poměrně vysoké.
- V případě požáru či jiné katastrofy v budově by zálohovaná data byla bezpečně uchráněna před zničením.

Evidence, údržba a kontrola hardwarového a softwarového vybavení

- Pravidelnou preventivní údržbou a kontrolou hardwarového vybavení lze předcházet jeho výpadkům či poruchám. Ty pak mohou firmě způsobit zbytečné ztráty z nutnosti pořízení hardwaru nového či z prostojů, které jsou poruchami způsobeny.
- Kontrolou softwarového vybavení počítačů lze zjistit, zda na počítačích není instalován nedovolený, nežádoucí či nelegální software.

Plán kontinuity IS

- V podniku není vypracován podrobný plán kontinuity IS.
- Podnikání je z velké části závislé na nepřetržitém fungování informačního systému.
- Vypracováním navrženého doporučení by bylo možno obnovit chod organizace po havárii IS.
- Vypracování plánu kontinuity IS by vedlo k minimalizaci ztrát společnosti v případě vzniku mimořádné situace.

ZÁVĚR

Problematika ochrany bezpečnosti informačních systémů a digitálních dat - elektronická bezpečnost, nebo také e-security, se dostává čím dál tím víc do popředí zájmu managementu společností i řadových zaměstnanců. Společnosti, které přešly od původních způsobů ukládání informací v tištěné podobě k digitálnímu zpracování, jsou si dnes již dobře vědomy, že i takto uložená data je třeba chránit a zabránit jejich prozrazení neoprávněným osobám, jejich neautorizované modifikaci a manipulaci.

Na druhé straně jsou zde společnosti, které si plně problematiku informační bezpečnosti neuvědomují, včetně případných dopadů a důsledků na fungování samotné společnosti. U řady společností se lze setkat s názorem, že chránit interní systémy před vlastními pracovníky je zbytečné, případně to není na pořadu dne.

Úspěšné organizace jsou schopny ve světě elektronického obchodu rychle nalézat nové příležitosti a možnosti pro své podnikání. V tomto světě je však bezpečnost informací klíčovým problémem. Prudký rozvoj internetových technologií s sebou přináší také rizika nového typu, tzv. e-rizika, která je třeba řídit. V moderně řízeném podniku si dnes již nelze představit informační systém, který by nebyl alespoň částečně nějakým způsobem chráněn. Ne všechny podniky však věnují bezpečnosti informačního systému dostatečnou pozornost, protože náklady na její udržení jsou poměrně vysoké a efekt, který přinášejí není většinou nikde vidět. Tyto náklady totiž nepřinášejí přímý zisk. Není pak snadné přesvědčit management k tomu, aby uvolnil finanční prostředky na projekty zabezpečení informačního systému podniku. Management by si však měl položit otázku, co se může stát, jestliže nebudou informace dostatečně chráněny. Zcela jistě by někdo slabiny informačního systému objevil, začal data a informace krást a zneužívat. Takové činnosti by pak způsobily podniku jistě nemalé ztráty. Je však třeba si uvědomit, že nejde jen o bezpečnost, ale také o budování důvěry v bezpečí. Ta hraje v prostředí elektronického podnikání ještě významnější roli a k tomu, aby byla přijata, je třeba ji také prokázat. Společnost, která nebude schopna svá data dostatečně chránit, bude ztrácet zákazníky, protože ti takové společnosti nebudou důvěřovat. S rozvojem nových informačních technologií se budou vyvíjet i nové způsoby zabezpečení informačních systémů. Na závěr je třeba říci, že informační bezpečnost je třeba brát seriózně a organizace, které nebudou věnovat dostatek zdrojů a času na řízení rizik, můžou být odsouzeny k zániku.

SEZNAM POUŽITÉ LITERATURY

- [1] ČANDÍK, Marek. *Základy informační bezpečnosti*. 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004. 107 s. ISBN 80-7318-218-1.
- [2] DOBDA, L. *Ochrana dat v informačních systémech*. 1. vyd. Praha: Grada, 1998. 286 s. ISBN 80-7169-479-7
- [3] EISENKOLB, K., GÖKHAN, M., WEICKARDT, H., *Bezpečnost Windows 2000/XP*. 1. vyd. Praha: Computer Press, 2003. 501 s. ISBN 80-7226-789-2.
- [4] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. 1. vyd. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.
- [5] JONES, Dennis. *Jak využívat Internet*. 1. vyd. Praha: SoftPress s. r. o., 2001. 398 s. ISBN 80-86497-12-7.
- [6] KUCHAR, Miloš. *Bezpečná síť*. 1. vyd. Praha: Grada Publishing, spol. s r. o., 1999. 92 s. ISBN 80-7169-886-5.
- [7] KUNDEROVÁ, L., LIŠKA I. *Datová komunikace a informační zdroje*. 1. vyd. Brno: Mendelova zemědělská a lesnická univerzita v Brně, 2003. 126 s. ISBN 80-7318-095-2
- [8] BRBLA, Jan. *Viry a hackeři: Absolut beginner on WWW* [online]. c2003, poslední revize: 11. 7. 2004 [cit. 2005-04-13]. Dostupný z:
< <http://www.abowe.brbla.net/1/1basicsecurity/virandhacker.php> >
- [9] BRECHLEROVÁ, Dagmar. *Výsledky průzkumu stavu informační bezpečnosti v ČR: Systémonline* [online]. c2004, [cit. 2005-04-18]. Dostupné z:
< http://www.systemonline.cz/site/doc-management/04_08brechl.htm >
- [10] HVOZDECKÝ, Lukáš. *Ochrana dat a informací: konjunktura.cz* [online]. c2003, [cit.2005-04-16]. Dostupné z:
< <http://www.konjunktura.cz/index.php3?w=art&id=1220&rub=480&s=>>
- [11] KLAŠKA, Luboš. *Průzkum Ernst & Young: Svět sítí* [online].c2003, [cit. 2005-04-18]. Dostupné z:
<<http://www.svetsiti.cz/view.asp?rubrika=Aktuality&temaID=4&clanekID=414>>

- [12] KOPŘIVA, Petr. *Elektronické podnikání*: shopfinder.cz [online]. c2000, [cit.2005-04-14]. Dostupné z: < <http://www.shopfinder.cz/svet/clanek.asp?ID=7>>
- [13] POSPÍŠIL, Robert. *EDI v kostce*: shopfinder.cz [online]. c2000, [cit.2005-04-15]. Dostupný z: < <http://www.shopfinder.cz/svet/clanek.asp?ID=7>>
- [14] PLEYER, Jan. *Elektronický podpis – obsah a význam*: e-cokommerce.cz [online].c2000, [cit. 2005-04-14]. Dostupné z: <<http://www.ekommerce.cz/ec/ec.nsf/0/C6582649E88C4ABDC125690A003FBD8F>>
- [15] SEIGE, Viktor. *Informační bezpečnost? Proč ne!*: Systemonline [online].c2002, č. 7-8. [cit. 2005-04-14]. Dostupné z: < www.systemonline.cz/site/bezpecnost/its.htm >
- [16] T-SOFT, s.r.o., *Havarijní plán IS*: T-soft [online].c2002, poslední revize: 6. 5. 2005 [cit. 2005-04-20]. Dostupné z: < <http://www.tsoft.cz/cz/01-07-01.asp> >

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

APEK	Asociace pro elektronickou komerci
B2B	Business-to-Business
B2C	Business-to-Customer
EDI	Electronic Data Interchange
HTTPS	Hyper Text Transfer Protocol – Secure
IS	Informační systém
IT	Informační technologie
LAN	Local Area Network
SSL	secure socket layer
TCP	Transmission Control Protocol
UN/EDIFACT	United Nation/Electronic Data Interchange for Administration Commerce and Transport
VAN	Value Added Network

SEZNAM OBRÁZKŮ

Obr. 1. Informační systém podniku

Obr. 2. Schéma řešení informační bezpečnosti dle ISO 13335

Obr. 3. Šifrování a dešifrování dat pomocí symetrických algoritmů

Obr. 4. Šifrování a dešifrování dat pomocí asymetrické kryptografie

Obr. 5. Dvoustupňové organizačně-řídící schéma firmy HP TRONIC, spol. s r. o.

Obr. 6. Ukázka nástroje Microsoft AntiSpyware

Obr. 7. Ukázka nástroje Ad-Aware SE

Obr. 8. Ohnivzdorná skříň Fire Star Plus

Obr. 9: Postup vytváření plánu kontinuity IS

Obr. 10: Oblasti, které pokrývá plán kontinuity IS

SEZNAM TABULEK A GRAFŮ

Tab. 1. Vybrané hospodářské údaje společnosti

Tab. 2. Silné a slabé stránky bezpečnosti IS

Tab. 3. Navrhované nástroje proti spywaru

Tab. 4. Zásady bezpečného používání internetu ve firmě

Tab. 5. Doporučené zásady používání hesel

Tab. 6. Evidenční karta počítačové stanice

Graf 1. Nejčastější bezpečnostní incidenty ve firmách v ČR

Graf 2. Největší hrozby z hlediska informační bezpečnosti

Graf 3. Bezpečnostní incidenty a internet

Graf 4. Způsoby zabezpečení internetu

SEZNAM PŘÍLOH

P I Dotazníky – The e-security toolkit.

Access Control & Authentication

This module assess the security mechanisms installed to control access to the PC/workstation/etc.

THE E-SECURITY TOOLKIT

Question Module: SECPKG - Access Control & Authentication

Question 1 - Completion is REQUIRED. Please select only ONE response.

Is an access control mechanism in place for the PC/workstation/computer? If so, what type of authentication is required ?

No

☐

Go to END

Yes - User Id Only

☐

Go to question 13

Yes - Password Only

☐

Yes - User Id & Password

☐

Yes - User Id, Password & Token

☐

Yes - Smartcard/biometric Only

☐

Go to question 13

Yes - Smart/biometric With User/password

☐

Yes - Digital Signature

☐

Question 2 - Completion is REQUIRED. Please select only ONE response.

Who chooses the access passwords?

The User

☐

A System Administrator

☐

The User Manager

☐

It Is System Generated

☐

Other

☐

Question 3 - Completion is REQUIRED. Please select only ONE response.

Is access revoked after a set number of consecutive failed access attempts?

No

☐

Yes - After 3 Attempts

☐

Yes - After 4 Attempts

☐

Yes - After 5 Attempts

☐

Yes - After 5 - 9 Attempts

☐

Yes-after More Than 9 Attempts

☐

THE E-SECURITY TOOLKIT

Question Module: SECPKG - Access Control & Authentication

Question 4 - Completion is REQUIRED. Please select only ONE response.

Does the security mechanism enforce password change:

- | | |
|-----------------------|--------------------------|
| Weekly | ☐ |
| Monthly | ☐ |
| Quarterly | ☐ |
| Half Yearly | ☐ |
| Annually | ☐ |
| Less Frequent / Never | ☐ |

Question 5 - Completion is REQUIRED. Please select only ONE response.

Are passwords unique to each user or are they shared?

- | | |
|--------------------------|--------------------------|
| Unique | ☐ |
| Shared Within Department | ☐ |
| Common Password Used | ☐ |

Question 6 - Completion is REQUIRED. Please select only ONE response.

Does the security mechanism enforce a minimum length for new passwords?

- | | |
|-----------------------------|--------------------------|
| No | ☐ |
| Yes, Less Than 5 Characters | ☐ |
| Yes, 5 Or More Characters | ☐ |

Question 7 - Completion is REQUIRED. Please select only ONE response.

When passwords are input, is the input field automatically blanked to prevent display?

- | | |
|-----|--------------------------|
| Yes | ☐ |
| No | ☐ |

THE E-SECURITY TOOLKIT

Question Module: SECPKG - Access Control & Authentication

Question 8 - Completion is REQUIRED. Please select only ONE response.

When the access password is changed, is it necessary to first input the existing password for validation ?

Yes

☐

No

☐

Not Applicable

☐

Question 9 - Completion is REQUIRED. Please select only ONE response.

When the access password is changed, does the security facility enforce that the new password is input twice?

Yes

☐

No

☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

Does the security mechanism maintain a history file of previous passwords (to prevent re-cycling of the same password)?

Yes

☐

No

☐

Go to question 12

Question 11 - Completion is REQUIRED. Please select only ONE response.

How many previous generations of password does the security facility hold ?

1 - 3

☐

4 - 8

☐

8 - 12

☐

More Than 12

☐

THE E-SECURITY TOOLKIT

Question Module: SECPKG - Access Control & Authentication

Question 12 - Completion is REQUIRED. Please select only ONE response.

Does the security facility filter for obvious password choices, or plain words that could be perhaps discovered via a dictionary?

Yes

☐

No

☐

Question 13 - Completion is REQUIRED. Please select only ONE response.

Does the access control mechanism allow the use of a guest/general user-id facility (for the sharing of the PC/workstation/computer)?

Yes

☐

No

☐

Go to question 15

Question 14 - Completion is REQUIRED. Please select only ONE response.

Are the 'guest' users restricted to a subset of the facilities available?

Yes

☐

No

☐

Question 15 - Completion is REQUIRED. Please select only ONE response.

Are User-Ids/Access-Codes shared, or are they unique and specific to individuals (excluding any 'guest' facility)?

Shared

☐

Unique and Specific

☐

Not Applicable

☐

Audit & Logging

This question module will assess auditing and logging functionality and practices. All aspects are considered, including the type of audit data collected, the monitoring procedures and access to the audit log itself.

It is suggested that this question module is completed by the Manager of the area concerned, or by the relevant Security Administrator/Auditor, if one exists.

THE E-SECURITY TOOLKIT

Question Module: AUDIT - Audit Procedures

Question 1 - Completion is REQUIRED. Please select only ONE response.

Are unsuccessful access attempts audited and monitored (i.e. reports produced and examined)?

Audited And Monitored

☐

Audited Only

☐

Neither

☐

Question 2 - Completion is REQUIRED. Please select only ONE response.

Is an audit capability in use for other than initial system access (eg: for file/folder violations, registry/system

Yes

☐

No

☐

Go to END

Question 3 - Completion is OPTIONAL, and more than one response may be selected.

Please select from the list, those events that are applicable but are NOT being audited.

System Events (eg registry changes)

☐

File/Folder Access Violations

☐

Sensitive Programs Executed

☐

Internet Activity

☐

System Configuration Changes

☐

Question 4 - Completion is REQUIRED. Please select only ONE response.

Are audit reports labeled in any way (eg: date produced, owner, etc)?

Yes

☐

No

☐

Not Applicable

☐

Go to question 6

THE E-SECURITY TOOLKIT

Question Module: AUDIT - Audit Procedures

Question 5 - Completion is OPTIONAL, and more than one response may be selected.

Please select those items which are NOT included on audit report headers/labels.

Owner

☐

Date Produced

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Are the pages of the audit report numbered ?

Yes

☐

No

☐

Question 7 - Completion is OPTIONAL, and more than one response may be selected.

Please select those items for which data is NOT held in the audit log (where applicable).

User-id

☐

Date/time Of Event

☐

Name Of File/Folder/Site

☐

Type Of Event Recorded

☐

Question 8 - Completion is REQUIRED. Please select only ONE response.

How frequently is the audit log printed and checked?

Every Day

☐

Every Week

☐

Every Month

☐

Every Three Months

☐

Every Six Months

☐

Never Printed & Checked

☐

THE E-SECURITY TOOLKIT

Question Module: AUDIT - Audit Procedures

Question 9 - Completion is REQUIRED. Please select only ONE response.

Is access to the audit log itself restricted?

Yes

☐

No

☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

What access level does the auditor have to the audit log?

Read Only Access

☐

Read & Update Access

☐

Read, Update & File Delete

☐

Not Applicable

☐

Question 11 - Completion is REQUIRED. Please select only ONE response.

Are test 'unauthorized access' attempts ever made to ensure that the security and audit mechanisms are working as specified?

Yes

☐

No

☐

BackUp & Contingency

This questionnaire is designed to assess the back-up and contingency status of a PC or small LAN infrastructure.

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 1 - Completion is REQUIRED. Please select only ONE response.

Are any back-up facilities, features or practices in place for the DATA and SOFTWARE held on the system being reviewed ?

Yes

☐

No

☐

Go to question 15

Question 2 - Completion is REQUIRED. Please select only ONE response.

Please identify the type of media normally used for back up:

Removable Hard Disk

☐

Go to question 4

Off-Site Transmission

☐

Go to question 4

Another Internal Hard Disk

☐

Go to question 4

Recordable Media (eg: CD)

☐

(Other) LAN

☐

Go to question 4

Other

☐

Go to question 4

Question 3 - Completion is REQUIRED. Please select only ONE response.

Where applicable, is the write protection mechanism always set after the backup to the media is complete?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 4 - Completion is REQUIRED. Please select only ONE response.

What type of backup is performed ?

Full Backup Every Time

☐

Go to question 6

Periodic Full With Incremental

☐

Incremental Only

☐

Not Applicable

☐

Back-Up Area in Situ

☐

Go to question 6

Question 5 - Completion is REQUIRED. Please select only ONE response.

How frequently are incremental backups taken ?

Daily

☐

Weekly

☐

Fortnightly

☐

Less Frequent Than Fortnightly

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

How frequently are FULL back-ups taken ?

Daily

☐

Weekly

☐

Fortnightly

☐

Monthly

☐

Less Frequent Than Monthly

☐

Never

☐

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 7 - Completion is REQUIRED. Please select only ONE response.

Which of the following are normally backed-up (if applicable)?

Application/user Data	☐
System Data/programs	☐
Both	☐
Neither	☐

Question 8 - Completion is REQUIRED. Please select only ONE response.

How many back-up copies are normally taken?

1	☐
2	☐
More Than 2	☐

Question 9 - Completion is REQUIRED. Please select only ONE response.

Where are back-up copies held ?

On-site Only	☐
Off-site Only	☐
Both	☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

Are back-up copies held in Fire/Water proof storage?

Fire Proof Only	☐
Water Proof Only	☐
Both	☐
Neither	☐

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 11 - Completion is REQUIRED. Please select only ONE response.

How many GENERATIONS of the back-up are held ?

1 - 2

2 - 4

5 Or More

Question 12 - Completion is REQUIRED. Please select only ONE response.

Does the backup software verify that the backup is usable, and is the verification facility used ?

Yes

Yes - But Not Used

No

Not Applicable

Question 13 - Completion is REQUIRED. Please select only ONE response.

Is a copy of the operating system software and a copy of the restore utility (if applicable) also kept with the backup media ?

Yes

No

Not Applicable

Question 14 - Completion is REQUIRED. Please select only ONE response.

Are the master media of the software stored in a secure fire proof location ?

Yes

No

Not Applicable

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 15 - Completion is REQUIRED. Please select only ONE response.

Is there a backup system which could be used if this one was unavailable for a short period of time (e.g. 1 day) ?

Yes

☐

No

☐

Not Applicable

☐

Question 16 - Completion is REQUIRED. Please select only ONE response.

Is there a backup system available if this one was unavailable for 1 week ?

Yes

☐

No

☐

Not Applicable

☐

Question 17 - Completion is REQUIRED. Please select only ONE response.

If the system was totally destroyed, is there an arrangement in place to obtain a replacement? Are time scales by which the replacement will be supplied guaranteed?

Yes

☐

Yes - But No Guarantee

☐

No

☐

Question 18 - Completion is REQUIRED. Please select only ONE response.

Is there a business continuity plan containing details of actions to be taken in more serious circumstances (e.g. loss of office)?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: BACKUP - PC & LAN Infrastructure Contingency

Question 19 - Completion is REQUIRED. Please select only ONE response.

If the main power supply to the system was interrupted, are there any arrangements in place to obtain power from an alternative source (such as a back-up generator, or stand-by battery)?

Yes

☐

No

☐

Not Applicable/ Not Necessary

☐

Question 20 - Completion is REQUIRED. Please select only ONE response.

Are all of these contingency arrangements fully documented (so that use of the system can be restored in a timely, efficient, and secure manner)?

Yes

☐

No

☐

Data Access

This question module assesses the access control facilities in place on the system for both data and functionality.

It is suggested that this module is completed by the user, or by the relevant supervisor/manager. If necessary, reference should be made to the system or PC support staff.

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 1 - Completion is REQUIRED. Please select one or more response(s).

Please identify who has access to the system under review:

General Public	☐
Clients/customers	☐
PC Engineers	☐
PC Support Personnel	☐
Internal Users	☐
Other Computer Systems	☐

Question 2 - Completion is OPTIONAL, and more than one response may be selected.

Please identify if any of the following might be particularly interested in the data on the system under review.

Journalists	☐
Pressure Group(s)	☐
Other Unauthorized Persons	☐
Employees	☐

Question 3 - Completion is REQUIRED. Please select only ONE response.

Have there been any recorded instances during the last two years of unauthorized data disclosure, or data alteration ?

Neither	☐
Data Disclosure	☐
Data Alteration	☐
Both	☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 4 - Completion is REQUIRED. Please select only ONE response.

Has an illegal ATTEMPT to change or disclose data ever been encountered ?

Yes

☐

No

☐

Question 5 - Completion is REQUIRED. Please select only ONE response.

Does the system under review have any form of security & authentication mechanism in place to restrict access to it?

Yes

☐

No

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Is there a facility in place to restrict access to only those functions a user is authorized to use ?

Yes

☐

No

☐

Question 7 - Completion is REQUIRED. Please select only ONE response.

Is access to the operating system, registry, and other core areas restricted to authorized and experienced users ?

Authorized & Experienced

☐

All Authorized Users

☐

All Users

☐

System/PC Has Only One User

☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 8 - Completion is REQUIRED. Please select only ONE response.

Does the system or PC contain a facility which blanks the screen after a certain period of inactivity ?

Yes

☐

No

☐

Not Applicable

☐

Go to question 12

Question 9 - Completion is REQUIRED. Please select only ONE response.

Does the screen blanking facility require re-authentication (eg: the input of a valid user-id and password) before processing can be resumed?

Yes

☐

No

☐

Go to question 12

Question 10 - Completion is REQUIRED. Please select only ONE response.

Does the screen blanking facility allow ANY user to continue processing on the input of a valid security details (eg: their own user-id & password) ?

Yes

☐

No: Must Be Same User

☐

System/PC Has Only One User

☐

Question 11 - Completion is REQUIRED. Please select only ONE response.

When the screen blanking facility is activated, does it only prevent input from the keyboard, or is all processing on the system or PC suspended ?

Prevents Keyboard Input

☐

Stops All PC Processing

☐

User Definable

☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 12 - Completion is REQUIRED. Please select only ONE response.

Is access to the removable media drive(s) (eg: floppy disk drive) restricted in any way ?

Yes - Physical Locks

☐

Yes - Software Locks

☐

No

☐

Not Applicable

☐

Question 13 - Completion is REQUIRED. Please select only ONE response.

Is access to powerful utilities/functions (such as disk formatting utilities) restricted in any way ?

Yes - By Security Package

☐

Yes - Other Means

☐

Yes - Programs Removed

☐

No

☐

Question 14 - Completion is REQUIRED. Please select only ONE response.

Is access to data files and programs restricted or controlled in any way ?

Yes

☐

No

☐

Go to question 20

Question 15 - Completion is REQUIRED. Please select only ONE response.

At what level are the files protected ?

Individual File Level

☐

Directory/Folder Level

☐

Disk Partition or Drive Level

☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 16 - Completion is REQUIRED. Please select only ONE response.

Does the file protection mechanism allow for files to be assigned to owners (i.e. specific users or groups of users) ?

Yes

☐

No

☐

Question 17 - Completion is REQUIRED. Please select only ONE response.

When new files are created and protected, whose responsibility is it to assign access permission to users other than the owner ?

Security Administrator

☐

Owner Of The File

☐

Any User Requiring Access

☐

None Of These

☐

Not Applicable

☐

Question 18 - Completion is REQUIRED. Please select only ONE response.

Does the file protection mechanism provide encryption for highly sensitive files and is this always employed

No

☐

Yes

☐

Question 19 - Completion is REQUIRED. Please select only ONE response.

Do the files continue to be protected if they are copied onto non-fixed media, such as diskettes or CDs ?

No

☐

Yes-but Requires Special Attn

☐

Yes

☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 20 - Completion is REQUIRED. Please select only ONE response.

Are any existing security measures revoked during the installation or maintenance of programs/packages ?

During Installation

☐

During Maintenance

☐

During Both

☐

During Neither

☐

Not Applicable

☐

Question 21 - Completion is REQUIRED. Please select only ONE response.

Is non-fixed media (e.g. disks or CDs) holding sensitive data individually labelled and subject to stringent access controls ?

Labelled Only

☐

Access Controlled Only

☐

Access Controlled And Labelled

☐

Neither

☐

Not Applicable

☐

Question 22 - Completion is REQUIRED. Please select only ONE response.

If data becomes redundant, is it:

Deleted

☐

Go to question 24

Archived

☐

Nether Deleted Nor Archived

☐

Go to question 24

Not Applicable / No Redundancy

☐

Go to question 24

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 23 - Completion is REQUIRED. Please select only ONE response.

Is all archived non public domain data subject to access controls ?

Yes

☐

No

☐

Not Applicable / All Public

☐

Question 24 - Completion is REQUIRED. Please select only ONE response.

Is any of the data considered to be particularly sensitive (eg: personal data, financial data, etc.) ?

Yes

☐

No

☐

Go to END

Question 25 - Completion is REQUIRED. Please select only ONE response.

Is there a facility to detect and report unauthorized attempts to access ALL sensitive data ?

Yes

☐

No

☐

Question 26 - Completion is REQUIRED. Please select only ONE response.

When sensitive data is deleted is there a facility in place to actually overwrite it (eg: with zeros)?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: ACCESS - Access To Data

Question 27 - Completion is REQUIRED. Please select only ONE response.

What measures are taken when storage media containing sensitive data is re-used ?

None

☐

Overwriting / Re-format

☐

Not Applicable

☐

Question 28 - Completion is REQUIRED. Please select one or more response(s).

What measures are taken when magnetic storage media containing sensitive data is disposed of ?

Data Overwritten / Re-format

☐

Total Physical Destruction

☐

Other

☐

None

☐

Not Applicable

☐

Question 29 - Completion is REQUIRED. Please select only ONE response.

Does security software restrict the use of sensitive data to specific users or groups of users?

No

☐

Yes

☐

Question 30 - Completion is REQUIRED. Please select only ONE response.

In addition to logical access controls, are there any physical access controls for PCs/workstations/computers holding very sensitive data (e.g. PC key/lock, stored in locked cabinet, etc.) ?

Yes

☐

No

☐

Firewall Security

This module addresses the security issues pertaining to the use and deployment of firewalls.

THE E-SECURITY TOOLKIT

Question Module: FIREWALL - Firewall Security

Question 1 - Completion is REQUIRED. Please select only ONE response.

Are all connections between the organization's networks and external third party or public wide area IP networks made via a formally authorized firewall (or have equivalent approved controls over the data and protocols which are allowed through)?

Yes

☐

No

☐

No Firewalls are Employed

☐

Go to END

Not Applicable

☐

Go to END

Question 2 - Completion is REQUIRED. Please select only ONE response.

Are the firewalls protecting the organization's networks/resources owned and managed by the organization itself?

No

☐

Yes

☐

Not Applicable

☐

Question 3 - Completion is REQUIRED. Please select only ONE response.

Are all firewall connections formally authorized by a designated network owner?

Yes

☐

No

☐

Not Applicable

☐

Question 4 - Completion is REQUIRED. Please select only ONE response.

Are the firewalls configured to default to reject everything, only accepting those protocols that are explicitly required, to those IP addresses which specifically require them?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: FIREWALL - Firewall Security

Question 5 - Completion is REQUIRED. Please select only ONE response.

Could the firewalls fail in such a way that packets are allowed through rather than being blocked?

Yes

☐

No

☐

Not Applicable

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Where practical, is a 'double indemnity' approach used - in which two different technologies are used in the firewall implementation to ensure that a weakness exploited in one does not necessarily compromise the other?

Yes

☐

No

☐

Not Applicable

☐

Question 7 - Completion is REQUIRED. Please select only ONE response.

Is the firewall itself IP-addressable from either of the two networks it connects to?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: FIREWALL - Firewall Security

Question 8 - Completion is OPTIONAL, and more than one response may be selected.

Which of the following, if any, are NOT recorded (and held securely) by the firewall administrators. Only indicate where applicable.

Connectivity of the Firewall	☐
Location of the Firewall	☐
ID or Name of the Firewall	☐
The Owner of the Firewall	☐
Network Owners (where applicable)	☐
What is Allowed Through	☐
Who Authorized the Connection	☐

Question 9 - Completion is REQUIRED. Please select only ONE response.

Is physical access to firewalls restricted to authorized individuals only?

Yes	☐
No	☐
Not Applicable	☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

Is the firewall physically located within a locked cabinet with physical controls also in place for any connected terminals or management systems?

Yes	☐
No	☐
Not Applicable	☐

THE E-SECURITY TOOLKIT

Question Module: FIREWALL - Firewall Security

Question 11 - Completion is REQUIRED. Please select only ONE response.

Is the logical access to firewalls (admin user logons, etc) subject to tight restrictions and authentication... and is this regularly reviewed?

Yes

☐

No

☐

Not Applicable

☐

Question 12 - Completion is REQUIRED. Please select only ONE response.

Is an audit trail maintained for all changes carried out whilst logged on to the firewall(s)?

Yes

☐

No

☐

Not Applicable

☐

Question 13 - Completion is REQUIRED. Please select only ONE response.

Are firewall audit trails regularly reviewed and securely archived?

No

☐

Yes

☐

Not Applicable

☐

Question 14 - Completion is REQUIRED. Please select only ONE response.

Are logs produced and reviewed of attempted breaches of network security?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: FIREWALL - Firewall Security

Question 15 - Completion is REQUIRED. Please select only ONE response.

Are logs produced and reviewed of all successful and unsuccessful attempts to access the firewall itself?

Yes

☐

No

☐

Not Applicable

☐

Question 16 - Completion is REQUIRED. Please select only ONE response.

Have all manufacturer default userids and passwords been disabled for all the firewalls?

No

☐

Yes

☐

Not Applicable

☐

Question 17 - Completion is REQUIRED. Please select only ONE response.

Is formal responsibility assigned to receive and review security alerts from the firewall manufacturer and from security advisory bodies (with respect to the applicable firewall type)?

Yes

☐

Receive Only

☐

No

☐

Not Applicable

☐

Question 18 - Completion is REQUIRED. Please select only ONE response.

Are all firewall connections and controls regularly reviewed and tested from a security perspective?

Yes

☐

No

☐

Not Applicable

☐

Internet Access

This module covers the access to and use of Internet facilities.

THE E-SECURITY TOOLKIT

Question Module: INTERNET - Internet Access

Question 1 - Completion is REQUIRED. Please select only ONE response.

Is the Internet only be used for the organization's own business related activities (eg: not used for non-work activity)?

Yes

☐

No

☐

No Internet Access

☐

Not Applicable

☐

Question 2 - Completion is REQUIRED. Please select only ONE response.

Is internet access formally granted by the user's accountable manager or equivalent?

No

☐

Yes

☐

Not Applicable

☐

Question 3 - Completion is OPTIONAL, but only ONE response should be selected.

Is a log maintained of the access right of all internet users and is this regularly reviewed?

Yes

☐

Logged but Not Reviewed

☐

Neither Logged nor Reviewed

☐

Not Applicable

☐

Question 4 - Completion is REQUIRED. Please select only ONE response.

Have users specifically been made aware of appropriate and effective use of the internet ?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: INTERNET - Internet Access

Question 5 - Completion is REQUIRED. Please select only ONE response.

Is the internet accessed through an authorized secure gateway?

Yes

☐

No

☐

Not Applicable

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Is sensitive data ever sent across the internet?

Yes

☐

No

☐

Go to question 8

Question 7 - Completion is REQUIRED. Please select only ONE response.

When sensitive data is sent across the internet is it adequately secured to protect it against both unauthorized disclosure and modification (eg: by using robust and legal encryption techniques)?

No

☐

Yes

☐

Question 8 - Completion is REQUIRED. Please select only ONE response.

Is a disclaimer mandated for users when views are expressed over the internet (to ensure that no legal responsibility is accepted by the organization for those views)?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: INTERNET - Internet Access

Question 9 - Completion is REQUIRED. Please select only ONE response.

Are users specifically instructed not to download or distribute material of an offensive, illegal or annoying nature (eg: chain mail, pornography)?

Yes

☐

No

☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

Are all IP addresses authorized and unique?

Yes

☐

No

☐

Question 11 - Completion is REQUIRED. Please select only ONE response.

Are those IP addresses used only within the organization considered to be confidential?

Yes

☐

No

☐

Not Applicable

☐

Question 12 - Completion is REQUIRED. Please select only ONE response.

Are users made aware that executable files downloaded from the internet must be subject to stringent processes prior to use (eg: virus checks, authenticity checks, etc)?

Yes

☐

No

☐

Not Applicable

☐

LAN & Network Security

The prime focus of this module is to assess the security arrangements in place on/for a Local Area Network. However, as many of the areas covered are equally applicable to other network /server types, it is suggested that value may be obtained if it is also used to address the latter.

It is suggested that the module is completed by the Network Support Manager.

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 1 - Completion is REQUIRED. Please select only ONE response.

Has a central point of contact been established to which users and systems personnel can report Local Area Network problems?

Yes

☐

No

☐

Question 2 - Completion is REQUIRED. Please select only ONE response.

The prime focus of this module is to assess the security arrangements in place on/for a Local Area Network. However, as many of the areas covered are equally applicable to other network/server types, value may be obtained if it is also used to address the latter. In this scenario, please treat the term 'LAN' in the wider context.

Are you ready to proceed?

Yes

☐

Question 3 - Completion is REQUIRED. Please select only ONE response.

Is the Local Area Network:

Internal To One Office

☐

Internal To A Building

☐

Internal To A Site

☐

External To The Site

☐

Question 4 - Completion is REQUIRED. Please select only ONE response.

How many workstations are there connected to the Local Area Network ?

1 - 10

☐

11 - 30

☐

31 - 50

☐

50 - 200

☐

More Than 200

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 5 - Completion is REQUIRED. Please select only ONE response.

Is access to the Local Area Network configuration information strictly controlled and limited to those who legitimately require it?

Yes

☐

No

☐

Not Applicable

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Is it possible to isolate a device that is suspected of being the source of unauthorized activity?

Yes

☐

No

☐

Question 7 - Completion is REQUIRED. Please select only ONE response.

Are changes to the software used to control Local Area Network resources (such as LAN switches and hubs)

Not Authorized Or Scheduled

☐

Authorized Only

☐

Scheduled Only

☐

Authorized and Scheduled

☐

Not Applicable

☐

Question 8 - Completion is REQUIRED. Please select only ONE response.

Are changes to the software that controls Local Area Network security features pre-authorized and scheduled

Not Authorized Or Scheduled

☐

Authorized Only

☐

Scheduled Only

☐

Authorized And Scheduled

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 9 - Completion is REQUIRED. Please select only ONE response.

Does the LAN use switched or broadcast technology?

Switched

☐

Broadcast

☐

Question 10 - Completion is REQUIRED. Please select only ONE response.

Are MAC (Media Access Control layer) addresses checked to prevent the connection of unauthorized devices?

Yes

☐

No

☐

Not Applicable

☐

Question 11 - Completion is REQUIRED. Please select only ONE response.

Is the LAN pro-actively managed?

No

☐

Yes

☐

Question 12 - Completion is REQUIRED. Please select only ONE response.

Is logical access to management and configuration facilities strictly controlled?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 13 - Completion is REQUIRED. Please select only ONE response.

Is there any mechanism or procedure that provides early warning of potential problems with Local Area Network hardware ?

Yes

☐

No

☐

Question 14 - Completion is REQUIRED. Please select only ONE response.

Is any element of the Local Area Network hardware put under undue stress due to overuse?

Yes

☐

No

☐

Don't Know

☐

Question 15 - Completion is REQUIRED. Please select only ONE response.

Is Local Area Network diagnostic testing/monitoring equipment available?

Yes

☐

No

☐

Not Applicable

☐

Go to question 17

Question 16 - Completion is REQUIRED. Please select only ONE response.

Is the network diagnostic equipment used only under strict managerial control?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 17 - Completion is REQUIRED. Please select only ONE response.

Are all hardware and software maintenance procedures and contracts fully documented ?

Yes

☐

No

☐

Question 18 - Completion is REQUIRED. Please select only ONE response.

On average, how old is the hardware which makes up the main components of the Local Area Network ?

Less Than One Year

☐

One To Five Years

☐

Five to Eight Years

☐

More Than Eight Years

☐

Question 19 - Completion is REQUIRED. Please select only ONE response.

What was the percentage downtime of the Local Area Network during the last 12 months ?

Less Than 1%

☐

1 - 5%

☐

More Than 5%

☐

Don't Know

☐

Go to question 22

Question 20 - Completion is REQUIRED. Please select only ONE response.

Are statistics collated for the cause of all Local Area Network failures ?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 21 - Completion is REQUIRED. Please select only ONE response.

Is all maintenance work on the Local Area Network:

Procedurally Controlled

☐

Pre-Authorized

☐

Procedurally Controlled & Authorized

☐

Not Procedurally Controlled or Authorized

☐

Not Applicable

☐

Question 22 - Completion is REQUIRED. Please select only ONE response.

Is maintenance of any part of the Local Area Network ever performed whilst it is in production use ?

Yes

☐

Yes - But Meant To Be

☐

No

☐

Question 23 - Completion is REQUIRED. Please select only ONE response.

Is preventative maintenance performed on the components of the Local Area Network in accordance with manufacturer's recommendations ?

No

☐

Main Components Only

☐

Yes

☐

Not Applicable

☐

Question 24 - Completion is REQUIRED. Please select only ONE response.

Is there a dial-in facility available on this Local Area Network ?

Yes

☐

No

☐

Go to Module DIAL-IN

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 25 - Completion is REQUIRED. Please select only ONE response.

How often is Local Area Network software and hardware independently audited ?

Every 6 Months

☐

Every 12 Months

☐

Less Frequent

☐

Never

☐

Question 26 - Completion is REQUIRED. Please select only ONE response.

What is the primary medium used for transmission of data across the Local Area Network ?

Copper Wire/Twisted Pair

☐

Coaxial Cable

☐

Wireless

☐

Fibre Optics

☐

Other

☐

Go to question 29

Question 27 - Completion is REQUIRED. Please select only ONE response.

Can cables be inspected, or are they sealed in trunking and embedded in walls or under floors, etc. ?

Cannot Be Inspected/Not Sealed

☐

Can Be Visibly Inspected

☐

Sealed In Trunking & Hidden

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 28 - Completion is REQUIRED. Please select only ONE response.

Is a structured cabling approach taken (i.e. using secure wiring closets, floor sockets, patching facilities, risers, etc.) ?

Yes

☐

No

☐

Not Applicable

☐

Question 29 - Completion is REQUIRED. Please select only ONE response.

How frequently are cables, junction boxes and other physically exposed components inspected for unauthorized tampering ?

At Least Every Month

☐

Every 3 Months

☐

Every 12 Months

☐

Less Frequent Than 12 Months

☐

Not Applicable

☐

Question 30 - Completion is REQUIRED. Please select only ONE response.

Are LAN switches used to help ensure that data is only transmitted to its authorized recipient ?

Yes

☐

No

☐

Not Applicable / Don't Know

☐

Question 31 - Completion is REQUIRED. Please select only ONE response.

Are cables or junction boxes physically labelled with their function or purpose ?

Yes

☐

No

☐

Not Applicable

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 32 - Completion is REQUIRED. Please select only ONE response.

How frequently are LAN/Workstation ports re-assigned ?

Daily	☐
Weekly	☐
Monthly	☐
Quarterly	☐
Every 6 Months	☐
Every 12 Months / Never	☐
Not Applicable	☐

Question 33 - Completion is REQUIRED. Please select only ONE response.

Is physical access to spare or unused LAN ports strictly restricted and controlled ?

Yes	☐
No	☐
Not Applicable	☐

Question 34 - Completion is REQUIRED. Please select only ONE response.

Are unused ports locked down logically (eg: by LAN switch) ?

Yes	☐
No	☐
Not Applicable	☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 35 - Completion is REQUIRED. Please select only ONE response.

Are cables/ports promptly disconnected/disabled when they become redundant ?

Yes

☐

No

☐

Not Applicable

☐

Question 36 - Completion is REQUIRED. Please select only ONE response.

Are LAN port assignments and re-assignments fully logged and documented ?

Yes

☐

No

☐

Not Applicable

☐

Question 37 - Completion is REQUIRED. Please select only ONE response.

Do critical LAN hardware components operate from an uninterruptable power supply system ?

Yes

☐

No

☐

Question 38 - Completion is REQUIRED. Please select only ONE response.

Are adequate physical controls in place to prevent unauthorized access to the LAN patch panels, switches, hubs, management consoles and other active and passive components?

Yes

☐

No

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 39 - Completion is REQUIRED. Please select only ONE response.

Is the recovery of the Local Area Network included in a formal contingency/business resumption plan ?

Yes

☐

No

☐

No Recovery Plan In Place

☐

Question 40 - Completion is REQUIRED. Please select only ONE response.

Have the users of the Local Area Network defined their service level requirements, in terms of availability and performance ?

Yes

☐

No

☐

Question 41 - Completion is REQUIRED. Please select only ONE response.

How often are the contingency arrangements for the Local Area Network tested ?

Every 6 Months

☐

Every 12 Months

☐

Less Frequently

☐

Never / No Such Arrangements

☐

Question 42 - Completion is REQUIRED. Please select only ONE response.

Is cryptography being used to protect the confidentiality of data passing over the Local Area Network ?

No

☐

Go to question 45

Yes

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 43 - Completion is REQUIRED. Please select only ONE response.

Is an industry recognized strong cipher being used ?

Yes

☐

No

☐

Not Applicable

☐

Question 44 - Completion is REQUIRED. Please select only ONE response.

How is encryption being applied ?

LAN/PC Resident Software

☐

Hardware Cryptographic Device

☐

Both

☐

Neither

☐

Question 45 - Completion is REQUIRED. Please select only ONE response.

Is cryptography used to ensure the integrity of data passing over the Local Area Network ?

Yes

☐

No

☐

Go to question 47

Question 46 - Completion is REQUIRED. Please select only ONE response.

Is an industry recognized message authentication (MAC) technique used ?

Yes

☐

No

☐

Don't Know

☐

THE E-SECURITY TOOLKIT

Question Module: NETWORK - LAN & Network Security

Question 47 - Completion is REQUIRED. Please select only ONE response.

Are strict procedures in place for the creation and distribution of encryption keys ?

Yes

☐

Creation Only

☐

Distribution Only

☐

Neither

☐

Crypto Not Used

☐

Question 48 - Completion is REQUIRED. Please select only ONE response.

Is a key management system in place which allows key recovery to be carried out (eg: as required by RIP legislation) ?

Yes

☐

No

☐

Not Applicable

☐

Question 49 - Completion is REQUIRED. Please select only ONE response.

Are keys periodically changed?

Yes

☐

No

☐

Not Applicable

☐

Virus Management

This question module assesses the virus detection and prevention mechanisms and procedures.

It is suggested that the module is completed by the User or Manager of the system. If necessary, reference should be made to the relevant Support Personnel.

THE E-SECURITY TOOLKIT

Question Module: VIRUS - Virus Management

Question 1 - Completion is REQUIRED. Please select only ONE response.

Is there a mechanism in place to detect and prevent virus infection ?

Yes

☐

No

☐

Go to END

Question 2 - Completion is REQUIRED. Please select only ONE response.

Does this protection take the form of a software package/utility ?

Yes

☐

No

☐

Go to question 6

Question 3 - Completion is REQUIRED. Please select only ONE response.

Does the virus checking utility provide a memory resident portion of code that continually scans for viruses

Yes

☐

No

☐

Not Applicable

☐

Question 4 - Completion is OPTIONAL, and more than one response may be selected.

Please identify all those functions that the virus detection package performs. Once all selections have been made, press OK:

Checksum Of Programs

☐

Checksum Of Data Files

☐

Virus Scanner

☐

File Size Checking

☐

Checks Hard Disk System Areas

☐

Automatic Cleanup Facility

☐

Don't Know

☐

THE E-SECURITY TOOLKIT

Question Module: VIRUS - Virus Management

Question 5 - Completion is REQUIRED. Please select only ONE response.

Is the virus 'fingerprint' file updated at least every month ?

Yes

☐

No

☐

Question 6 - Completion is REQUIRED. Please select only ONE response.

Are all virus incidents managed in a secure manner, in that they are cleaned up, investigated, reported to management, and properly documented ?

No

☐

Reported Only

☐

Reported & Documented Only

☐

All The Above

☐

Question 7 - Completion is REQUIRED. Please select only ONE response.

Are all moveable media (eg: floppy disks, CDs, etc) scanned for viruses before any data or programs are copied/executed from or to them ?

Yes

☐

Only If From External Source

☐

No

☐

Question 8 - Completion is OPTIONAL, and more than one response may be selected.

Please identify approximately how many virus incidents have there been in the last 12 months. Once all selections have been made, press OK.

In The Immediate Area:

In The Organisation, If Known: