Analýza bezpečnosti dat ve firmě

An analysis of data security in a company

Filip Hasík

Bakalářská práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Filip HASÍK**
Osobní číslo:	**A09178**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Analýza bezpečnosti dat ve firmě**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Nastudujte možnosti zabezpečení dat v malých a středně velkých firmách. Využijte doporučenou literaturu a především odborné časopisy.**
3. **Proveďte analýzu bezpečnosti dat ve firmě Technodat ve Zlíně.**
4. **Navrhněte vhodná opatření pro zkvalitnění bezpečnostních opatření.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno: Computer Press, 2004, 190 s. ISBN 80-251-0106-1.**
2. **JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.**
3. **JAŠEK, Roman. Ochrana znalostí a dat v podnikových informačních systémech. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-731-8095-2.**
4. **JAŠEK, Roman. Proces implementace poznatků informační bezpečnosti do informační bezpečnosti podniku a vysokoškolské výuky. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2005. Habilitační práce.**
5. **KLÍMA, Vlastimil. Archivy publikací o kryptologii a počítačové bezpečnosti [online]. 1993-2011[cit. 2012-02-06]. Dostupné z: http://cryptography.hyperlink.cz/**
6. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-807-3186-319.**
7. **Crypto-world [online časopis]. 1999-2012 [cit. 2012-02-06]. ISSN 1801-2140. Dostupné z: http://cryptoworld.info/index2.php**

Vedoucí bakalářské práce: **Ing. Bronislav Chramcov, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání bakalářské práce: **24. února 2012**

Termín odevzdání bakalářské práce: **25. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

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

ABSTRAKT

Cílem práce bylo vytvořit literární rešerši na dané téma. Problém se týká bezpečnosti dat v malých a středně velkých firmách. V práci byl objasněn pojem bezpečnostní politika a bylo pojednáno o důležitosti zavedení bezpečnostní politiky ve firmě. Analýzou bezpečnosti jsem zjistil konkrétní problémy, na které je potřeba se zaměřit. Na základě specifických poznatků jsem vyhodnotil stávající situaci ve firmě a navrhl opatření ke zlepšení stavu. Práce byla vytvořena na základě informací z odborné literatury, vlastních zkušeností získaných realizací analýzy současného stavu a internetu.

Klíčová slova:

bezpečnost, bezpečnostní politika, bezpečnostní analýza, analýza rizik, počítačová síť

ABSTRACT

The main goal of this thesis was to create literary researches for given topic. The problem was directed to data security in small and medium companies. I tried to clarify the term security policy. The thesis has dealt with importance of introducing security policy in the company. Analysis of security found out specific problems that need to be aimed. I evaluated the current situation of a company on the basis of specific knowledge and suggest measures for improvement. The bachelor was created with information from specialized literature, own experience gain by realization an analysis the current state and the internet.

Keywords:

security, security policy, security analysis, risk analysis, computer network

Poděkování

Na tomto místě bych chtěl poděkovat svému vedoucímu bakalářské práce Ing. Bc. Bronislavu Chramcovovi, Ph.D. za odborné vedení, poskytnuté konzultace a čas nutný při tvorbě bakalářské práce.

Také bych chtěl poděkovat správci sítě ve firmě Technodat, panu Ivo Machačovi, za poskytnuté informace a čas při spolupráci, a za mnoho podnětných připomínek při informačních schůzkách.

V neposlední řadě patří můj vděk všem, kteří mne při této práci i celém studiu podporovali.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Neustále narůstá množství dat a vzhledem k postupné digitalizaci všech součástí firemních záležitostí je potřeba mít data neustále pod kontrolou a dokonale zajistit bezpečnost těchto dat.

K zajištění dokonalé bezpečnosti je potřeba vypracovat detailní soupis pravidel chování s citlivými daty. Prvotní proces určování a sepisování těchto pravidel může být náročný a zdlouhavý, ale samotné dodržování těchto pravidel už nijak složité není. Chce to pouze určitou znalost dané bezpečnostní politiky a trpělivost tato pravidla dodržovat.

Je však velice náročné provádět kontroly dodržování bezpečnosti. V tomto směru většinou převládá lidská lenost a neochota dodržovat něco, co není běžnou náplní práce, a tudíž nemá vliv na výsledek naší aktivity.

Pro zavedení a dodržování pravidel je důležité vytvořit celistvou bezpečnostní politiku firmy. Všechny dokumenty by měly mít určitý řád a být pohromadě. Obsahem jsou principy, standardy a zásady pro dodržování bezpečnosti. Samostatná bezpečnostní politika je důvěrný dokument a tudíž nesmí být veřejně k dispozici. Přístup by měly mít pouze osoby odpovídající za bezpečnost. Ti se poté musí postarat o to, aby ostatní zaměstnanci byli o bezpečnostních zásadách podrobně a pravidelně proškoleni.

Základním prvkem bezpečnostní politiky je vytvoření všech možných analýz - ať už jde o analýzu prostředí nebo analýzu rizik. Při vytváření různých pravidel je potřeba, abychom dané prostředí nejdříve dokonale poznali. Musíme si vytvořit úplnou představu, co všechno vůbec budeme chránit, teprve pak můžeme začít přemýšlet nad tím, jak to ochránit. Právě k tomu nám analýzy slouží.

Cílem práce je kompletní analýza bezpečnosti dat ve firmě Technodat, zpracování bezpečnostní politiky, zhodnocení současného stavu a případné navržení nových pravidel.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA FIRMY

Základním dokumentem každé společnosti z hlediska počítačové bezpečnosti je bezpečnostní politika. Dokument by měl být v psané formě. Základními otázkami při vytváření bezpečnostní politiky je co, proč a jak to chceme chránit. Poté nás bude ještě zajímat, jak ověříme, že je to opravdu chráněno a co budeme dělat, když se něco pokazí.

Bezpečnostní politika podniku by měla obsahovat:

- program informační bezpečnosti podniku s vyjádřenými cíli podniku v oblasti informační bezpečnosti,
- odpovědnost za naplňování bezpečnostní politiky podniku,
- prostředky k jejich naplňování,
- časové období pro jejich naplňování,
- hlavní zásady jejich naplňování,
- zásady koordinace informační, majetkové a osobní bezpečnosti podniku.[1]

Podniky potom musí tyto zásady dále rozpracovat např. do:

- specifikace platných oprávnění a jiných předpisů,
- specifikaci bezpečnostních požadavků podniku,
- metoda a způsoby ochrany informací a informačního systému v oblasti fyzické, organizační, softwarové atd.,
- způsoby a postupy řešení,
- zásady řešení bezpečnostních incidentů,
- metody a způsoby koordinace informační bezpečnosti s majetkovou a osobní bezpečností podniku.[1]

1.1 Analýza rizik

Při sestavování bezpečnostní politiky musí být nejprve provedena analýza rizik. Analýzou zjistíme co, a proti čemu budeme chránit.

- identifikace aktiv - v první fázi zjistíme, jaká aktiva se v systému vyskytují. Jednotlivá aktiva by měla být oceněna.
- identifikace hrozeb - v závislosti na prostředí, ve kterém bude systém nasazen, identifikujeme hrozby, které mu hrozí.

- vlastní analýza rizik - konkrétním aktivům přiřadíme konkrétní hrozby. Po provedení tohoto kroku by mělo být jasné, kterým aktivům hrozí zanedbatelné hrozby a která je třeba chránit.[2]

1.2 Navržení vhodné ochrany

Pomocí analýzy rizik zjistíme, jakou hodnotu mají aktiva v informačním systému. Odhadneme také pravděpodobnost hrozeb, proti kterým se budeme chránit. Tato hodnota je přímo úměrná finanční hodnotě chráněných aktiv. Ochrana by měla být navrhována pro každou dvojici aktivum - hrozba. Každý bezpečnostní prostředek má však širší možnost využití, proto je potřeba s tím počítat a využít všech kombinací ochran.

Základní pravidlo při navrhování ochrany je jednoduché: náklady na zavedení ochrany nesmí převýšit cenu chráněných aktiv.[2]

1.3 Havarijní plány

Při běžném provozu bychom měli být připraveni na většinu možných nebezpečí - odhalí nám je analýza rizik a podle toho navrhneme ochranná opatření. Může však nastat jakákoliv nepředvídatelná situace, bezpečnostní opatření mohou selhat.

Takový stav nazýváme jako krizový stav systému. I na takové stavy však musíme být připraveni. Je potřeba jednat rychle a uvážlivě, abychom co nejvíce předešli ztrátám. V případě havárie musí být co nejrychleji obnovena činnost důležitých částí informačního systému a poškozená data.

1.3.1 Základní části havarijního plánu

- odstranění akutního nebezpečí - základní opatření závislé na druhu katastrofy,
- obnovení důležitých částí systému - výměna poškozených hardwarových součástí, instalace nových verzí programového vybavení, konfigurace systému,
- obnovení poškozených dat - využijeme záložních kopií. Obnoví se poslední nepoškozená verze dat a uživatelům je třeba vysvětlit, o která data při obnově přišli. Systém by již měl být zpřístupněn alespoň do lokální sítě. Je potřeba systém dokonale ošetřit a zabezpečit před povolením přístupu do internetu.

- zavedení příslušných protiopatření - využijeme havárie a ponaučíme se z chyb, které se vyskytly. Snažíme se jim předejít a vytvořit nová preventivní opatření.[2]

1.4 Údržba bezpečnostní politiky

Po zavedení nových opatření je možné systém zprovoznit v plném rozsahu. Je ale potřeba zvýšené kontroly, která nám může odhalit nedokonalost těchto opatření. Po úpravě je nutné aktualizovat dokument bezpečnostní politiky.

Kontrola a aktualizace bezpečnostní politiky by měly být prováděny pravidelně, ne jen při krizových a jiných výjimečných stavech. Dokument by měl být průběžné doplňován při změnách v informačním systému. Pravidelnou kontrolou také zjistíme, zda ochrana nebyla odstraněna, ať omylem, nebo záměrně.

2 POČÍTAČOVÁ SÍŤ

V dnešní době internetu a digitalizace je počítačová síť základním prvkem fungování všech firem. Už žádná společnost se neobejde bez zpracování dat v počítačích a málokterá prosperující firma bez své stránky na internetu.

Proto je v každé firmě vybudována počítačová síť, která zahrnuje veškeré počítače, síťová zařízení a další prvky pohromadě a dodržuje pevně daná pravidla.

2.1 Síťová zařízení

Pod pojmem síťová zařízení zahrnujeme veškeré zařízení a prvky připojené do počítačové sítě, které mezi sebou realizují výměnu informací. Rozdělujeme je na aktivní a pasivní prvky

2.1.1 Aktivní prvky

Slouží ke vzájemnému propojování počítačových sítí a k připojování koncových zařízení do sítě. Jsou to taková zařízení, která aktivně působí na přenášené signály - obnovují, zesilují, případně upravují. Mezi nejčastěji používané patří opakovač (repeater), převodník (transceiver), rozbočovač (hub), most (bridge), přepínač (switch), směrovač (router), brána (gateway). [3]

2.1.2 Pasivní prvky

Pasivní prvky jsou média, kterými se šíří signál. Základní dělení prvků:

- metalické kabely - přenos elektrických signálů klasickým měděným vodičem,
- optické kabely - přenos světelných paprsků, v nichž jsou zakódována data,
- bezdrátový přenos vzduchem - přenos dat v bezdrátových sítích pomocí elektromagnetických vln.[3]

2.2 Rozdělení počítačových sítí

Počítačové sítě bývají zpravidla rozdělovány na privátní a veřejné, jejichž definice a vymezení bylo přesně dáno. V důsledku vizualizace se však rozdíly částečně smazávají a začínají se prosazovat virtuální privátní sítě, které jsou vytvářeny v rámci sítí veřejných.[4]

2.2.1 Privátní síť

Síť, která slouží jednomu konkrétnímu subjektu (např. firmě, podniku, organizaci). Příkladem privátních sítí jsou lokální sítě LAN. Ty prakticky vždy slouží potřebám jediného subjektu, který je současně i jejich vlastníkem. U většiny lokálních sítí je jejich provozovatel současně i majitelem přenosových cest, které jeho síť používá.

2.2.2 Veřejné datové sítě

Pokud vlastník privátní sítě nevyužívá část nebo celou dostupnou přenosovou kapacitu své sítě, může ji poskytovat k využití jinému subjektu, na komerční bázi. Uživatelé pak využívají služeb veřejné datové sítě, aby jejím prostřednictvím komunikovaly s jinými subjekty, také připojenými k veřejné datové síti, aby prostřednictvím veřejné datové sítě propojovaly mezi sebou své dílčí lokální sítě.

2.2.3 Virtuální privátní sítě

Tato síť slouží k propojení několika počítačů prostřednictvím veřejné počítačové sítě. Provozovatel veřejné sítě pro svého zákazníka vyčlení část sítě a nakonfiguruje ji tak, aby se chovala jako zcela samostatná síť, kterou má zákazník jen pro sebe. Tím dosáhneme toho, že počítače spolu mohou komunikovat stejně jako v jedné soukromé síti. Komunikace pomocí VPN je šifrována.

3 INFORMAČNÍ SYSTÉMY

Informační systém je soubor technického (hardware) a programového (software) vybavení, záznamových médií, dat a personálu, který organizace používá ke správě svých informací. [5]

Systém uchovává všechna data týkající se firmy a poskytuje nám přesně ty informace, které potřebujeme. Mnoho firem se v rámci úspor snaží místo informačních systémů zavádět data pouze do vlastních vytvořených tabulek. S vývojem firmy a stoupajícím množstvím důležitých informací je však logické a žádoucí, aby byla data pohromadě a přehledně uložená na jednom místě, v jednom systému.[6]

Mezi základní a nejvíce využívané informační systémy patří účetní (ekonomické) systémy. Právě ve financích musí být vždy určitý řád. A vzhledem k modularitě současných účetních systémů je pro firmy již téměř nezbytné je využívat. Kromě samotného účetnictví nabízejí zpravidla i moduly pro správu objednávek, skladu, mezd.

3.1 Základní okruhy funkčnosti IS

Následující okruhy jsou nejčastěji zpracovávané v informačních systémech:

- Zaměstnanci - nábor, docházkový systém, výkazy práce, mzdy, zaměstnanecké výhody, školení, sledování výdajů zaměstnance, hodnocení zaměstnanců,…
- Dodavatelé a nákup - přehled nákupů a dodavatelů, přehled komunikace, sdílení dokumentů s dodavateli, hodnocení nabídek, hodnocení dodavatelů, objednávky,…
- Logistika - doprava, sklady,…
- Výroba - tvorba prognóz, plánování, správa technických, kalkulace, sledování průběhu výroby, řízení jakosti, údržba výrobních kapacit,…
- Projekty - projektová dokumentace, řízení projektů, sledování vytížení/volné kapacity zdrojů, sledování postupu projektu, finanční řízení projektu, řízení rizik,…
- Prodej - distribuční systém, maloobchod, propagace, e-shop, mobilní prodej, prodejní dokumenty, cenové kalkulace/slevy, rezervace, přehled nabídek,…
- Marketing - segmentace trhu, marketingové akce (a analýza akcí), direct mailing, podpora tvorby katalogů produktů, sledování konkurence, analýza příležitostí,…

- Zákazníci - analýza chování zákazníků, získávání zákazníků, podpora marketingu, správa odpovídajících dokumentů, kontaktní centrum, servis,…
- Účetnictví - vnitropodnikové, daňové, faktury, celní deklarace, DPH, Intrastat, cizí měny, přístup k internet bankingu, tisk platebních poukázek,…
- Majetek - krátkodobý a dlouhodobý, umístění a inventarizace majetku, analýzy,…
- Správa dokumentů - příjem a archivace dokumentů, vyhledávání, správa oficiálních šablon dokumentů,…
- Správa IT - správa událostí, správa konfigurací, řešení problémů, řízení změn,…
- Specifické požadavky různých odvětví podnikání.[6]

4 OCHRANA DAT

Vzhledem k neustálému zvyšování objemu dat a neustále se zvyšující počítačové kriminalitě je nutné data chránit. Abychom zajistili dostatečnou ochranu dat před odposlechem případně před krádeží, měli bychom je šifrovat. Šifrování neboli kryptografie je nauka o metodách utajení smyslu zpráv tím, že je převedeme do nečitelné podoby. Takto zašifrované zprávy lze číst pouze se speciální znalostí. Šifrování nám umožní dostatečnou a vlastně jedinou ochranu dat i přesto, že nám data budou odcizena. Šifrovací algoritmy dělíme na symetrické, nesymetrické a hashovaní funkce.

4.1 Symetrické šifry

Jde o šifry používající stejný šifrovací klíč jak pro zašifrování, tak pro dešifrování.[5] Tato výhoda jediného klíče pro všechny úkony se zpracovávanými daty se projevuje i vyšší rychlostí práce počítače při šifrování. Výhoda na jedné straně je ale nevýhodou na straně druhé, neboť v okamžiku prozrazení jsou odkryta všechna takto zašifrovaná data. V praxi se symetrické šifry využívají především pro zašifrování zálohovaných dat.

Mezi nejznámější a nejpoužívanější symetrické šifry patří DES, TripleDES, IDEA, BlowFish, CAST.

4.2 Asymetrické šifry

Při asymetrickém šifrování jsou použity dva klíče. Jeden, veřejný klíč pro zašifrování zprávy (je veřejně přístupný) a druhý pro dešifrování, soukromý klíč. Soukromý klíč je tajný, a proto musí být pečlivě střežen a chráněn. Při generování klíče pomocí speciálního počítačového programu přitom ve skutečnosti jde o jeden klíč, který se v následném kroku rozdělí na dvě části, vzájemně neodvoditelné. Soukromý a veřejný klíč spolu tvoří klíčový pár.[5]

Zásadní pokrok asymetrických šifer je v tom, že již není potřeba skrývat algoritmus a postup při šifrování. Asymetrické šifrování je totiž založeno na dokonalosti matematických funkcí, které je možné vypočítat pouze jedním směrem. Vypočítat z výsledku zpětně původní hodnoty je vzhledem k současnému výkonu počítačů nemožné.

Nevýhodou nesymetrického šifrování je pouze rychlost, která je oproti symetrickému šifrování velmi pomalá. Proto se s výhodou využívá kombinace obou možností, kdy se daný text zašifruje symetricky a heslo asymetricky.

K zástupcům asymetrické kryptografie řadíme RSA, Diffie-Hellman, DSS a moderní eliptické kryptosystémy.

4.3 Hash algoritmy

Vedle šifrování symetrickým a asymetrickým klíčem existuje ještě jedna oblast šifrování, kde potřebujeme informaci pouze zašifrovat, ale už nikdy dešifrovat. V takových případech používáme hashovaní algoritmy.[5] Příkladem je uložení hesel v operačním systému. Ze zadaného textu se pomocí hash algoritmu provede minimální otisk, který je při stejném zadaném textu vždy stejný. Tímto postupem dosáhneme, že systém nemusí znát heslo uživatele, ale stačí znát jeho zašifrovanou hodnotu.

Úkolem hashovacích algoritmů je jednoznačně identifikovat celistvost a stejný obsah textu. Podmínky pro silnou hashovaní funkci:

- jednosměrnost - nesmí být možné z hodnoty hash odvodit původní zprávu,
- bezkoliznost - nesmí být možné dostat na dvě různé výchozí zprávy tutéž hodnotu hash.

Mezi nejčastěji používané bezpečnostní hashovací funkce patří MD2, MD5 a NIST.

4.4 Nástroje na šifrování

4.4.1 Pretty Good Privacy

PGP představuje komplexní nástroj, který je schopen vysoce efektivně zabezpečit ochranu komunikovaných dat mezi uživateli internetu. V současnosti je PGP jeden z nejrozšířenějších a nejbezpečnějších prostředků pro šifrování elektronické pošty a pro ověřování digitálních podpisů. Digitální podpisy slouží k ověření integrity a autenticity přijímaných dokumentů (souborů).

PGP pracuje se symetrickými i asymetrickými šifrovacími algoritmy, např. CAST, AES, TripleDES, IDEA, TwoFish, a lze tedy říci, že patří mezi kryptograficky silné prostředky. Je dostupný pro všechny platformy operačních systémů.[5]

4.4.2 TrueCrypt

Velmi známý program pro šifrování dat, který je volně šiřitelný, se nazývá TrueCrypt. TrueCrypt je velmi variabilní, umožňuje šifrovat jednotlivé složky a soubory, ale také celé diskové oddíly (včetně systémového). Výhodou je také to, že jej není třeba instalovat, proto jej můžeme přenášet například na flash disku.

Program také využívá kombinaci několika šifer, mezi nejznámější patří AES, TwoFish, Serpent.

II. PRAKTICKÁ ČÁST

5 FIRMA TECHNODAT

Pro vytvoření bezpečnostní analýzy jsem vybral firmu Technodat. Správce sítě byl velmi ochotný a poskytl mi veškeré údaje o firmě a o zpracování bezpečnostní politiky.

Firma Technodat, CAE-systémy, s.r.o., byla založena roku 1992 ve Zlíně jako sesterská společnost rakouské firmy Technodat, Technische Datenverarbeitung GmbH.[7] Od této firmy byl v první etapě činnosti přebírán sortiment nabízených systémů a značná část potřebného technického know-how. Postupně docházelo k osamostatňování obchodních aktivit a k rozšiřování firmy. V současné době je Technodat ryze českou, finančně zcela stabilní a úspěšnou firmou.

Firma je systémovým integrátorem komplexního řešení počítačové podpory technické přípravy výroby pro průmyslové podniky, projekční a inženýrské kanceláře a dodavatelem řešení pro digitální archivaci a zálohování i pro jiné typy organizací.

Řešení zahrnuje jednak softwarové produkty, které svojí kvalitou garantují vložené investice zákazníků, ale také analýzu potřeb uživatele a projekt nasazení systému, dodávku a instalaci hardware a síťového řešení, školení a technickou podporu uživatele po celou dobu používání. Firma Technodat má vytvořeno dostatečné technické i obchodní zázemí a působí samostatně v teritoriu České republiky a Slovenska.

Partnerskými firmami jsou společnosti Dassault Systemes, Aucotec, Carat GmbH.

V současné době má firma Technodat 6 poboček. Kromě 5 českých, včetně hlavního sídla ve Zlíně, má také zastoupení na Slovensku. V práci budu analyzovat stav zabezpečení dat ve Zlínské budově a propojení s ostatními pobočkami.

5.1 Organizační struktura

Firma je rozdělena do čtyř částí, které však spolu úzce souvisí a spolupracují. Každé oddělení má svého vedoucího a všichni jsou podřízeni jedinému majiteli. Tyto oddělení dále postupně rozeberu.

5.1.1 Technodat CAE-systémy, s.r.o.

Firma zabývající se prodejem a implementací 3D PLM řešení. PLM je zkratka pro správu životního cyklu výrobku (Product Lifecycle Management), což je informační platforma,

která v sobě zahrnuje technické, výrobní i marketingové údaje o daném výrobku. Nabízené 3D PLM řešení je postaveno na produktech a řešení společnosti Dassault Systemes. Firma nabízí specializované softwarové produkty Catia, Enovia, Delmia, Simulia, 3Dvia, DraftSight.[7]

5.1.2 Technodat Elektro, s.r.o.

Společnost Technodat Elektro se zabývá podporou zpracování a správy elektro-dokumentace v oblastech automatizace, petrochemie, energetiky, kolejové dopravy, instalace budov apod. Na tato CAD a CAE řešení má opět specializované softwarové systémy Engineering Base, Elcad, Aucoplan, Ruplan, Spac.[7]

5.1.3 Technodat Engineering, s.r.o.

Tato skupina je převážně orientována na koncové uživatele, kteří mají na starost obsluhu a správu zařízení a to jak většího (rozvodny, elektrárny, teplárny), tak i menšího charakteru (ČOV, pracovní linky). Cílem je pomoci těmto uživatelům s elektro dokumentací. Při zpracovávání předpisů jsou aplikovány aktuální normy.[7]

5.1.4 Technodat Develop spol. s.r.o.

Firma založená roku 1995 je členem skupiny firem Technodat. Zabývá se vývojem software pro skupinu firem Technodat a pro zahraniční i české zákazníky. Vyvíjí také vlastní produkty - CRM systémy CRMfree a CRMplus a docházkový systém RAC. Firma poskytuje a zajišťuje komplexní podporu software pro podporu prodeje nábytku CARAT.[7]

Firma Technodat Develop sídlí ve vedlejší budově.

6 PRVKY POČÍTAČOVÉ SÍŤĚ

V této kapitole budou popsány všechny prvky počítačové sítě ve firmě Technodat. Vysvětlím, k jakým potřebám zařízení slouží, kde jsou uchovávána data, kdo a jak k jednotlivým zařízením může přistupovat, jakým způsobem je rozčleněna síť.

6.1 Pracovní stanice

V počítačové síti Zlínské pobočky je 55 pracovních stanic a 6 serverů. Část sítě je postavena na 1 Gbit/s a část na 100 Mbit/s Ethernet. Pracovní stanice jsou z velké části notebooky, pouze několik kusů jsou počítačové sestavy. Tyto jsou převážně využívány jako grafické pracovní stanice. Vzhledem k tomu, že budu o pracovních stanicích mluvit často obecně, budu pro zjednodušení používat slovo počítač pro notebooky i pro desktopy. Firma nakupuje hardware výhradně od firmy DELL především díky bezproblémovému servisu, který probíhá přímo v sídle firmy.

Na většině počítačů je nainstalován nejnovější operační systém Windows 7. Pouze na několika posledních kusech je systém Windows XP, ale správci provádějí pravidelnou údržbu a operační systém i další důležité programy aktualizují na novější verze. Proti virům a jiným škodlivým programům je na počítačích antivir Microsoft Security Essentials. V programu jsou nastaveny automatické aktualizace. Dále je využíváno programů z balíčku Microsoft Office.

Další instalace programů není příliš omezena. Vzhledem k tomu, že hodně zaměstnanců pracuje ve vývoji a často potřebuje instalovat nový software, jsou na počítačích povolena nejen uživatelská, ale i administrátorská práva. Ve firmě je vypracován dokument, který uživatelům říká, jaký software mohou instalovat a kam mají přístup.

Zaměstnanci potřebují přístup k firemním aplikacím, na kterých je prováděn vývoj a zkoušení. Všechny aplikace, na které má firma licence, jsou nainstalovány na aplikačním serveru. Je však důležité přístup omezit. Vzhledem k tomu, že na serverech jsou všechna citlivá data firmy, bez omezení by mohla být některá použita k nekalým účelům. Přístup k jednotlivým aplikacím je zajištěn přes doménový kontroler.

6.2 Doménový kontroler

Kontroler je zaveden na počítači s operačním systémem Windows Server. Na tomto počítači je prováděna centrální správa účtů. Správce tak může definovat jednotlivé uživatelské účty a všichni uživatelé, kteří jsou v lokální síti, mají přiřazena určitá práva přístupu k firemním aplikacím a souborům.

6.3 Virtual Private Network

Propojení mezi pobočkami zajišťuje virtuální privátní síť. Všechny pobočky jsou napojeny do VPN pomocí routerboardů Mikrotik.

Pro bezpečný a bezproblémový přístup do sítě VPN je na počítačích nainstalován program OpenVPN. Tento software je volně šiřitelný a umožňuje ověření navazovaného spojení pomocí přihlašovacího jména a hesla, případně pomocí digitálního certifikátu. Pro šifrování komunikace jsou využívány knihovny OpenSSL, které používají mnoho různých kryptografických algoritmů - hashovaní funkce, symetrické a asymetrické šifry.

6.4 Vzdálený přístup

Pro zaměstnance je také umožněn vzdálený přístup do firemní sítě pomocí OpenVPN stejným principem, jakým jsou propojeny jednotlivé pobočky mezi sebou. Přihlašování probíhá pomocí certifikátu, uživatelského jména a hesla.

6.5 Aktivní prvky

6.5.1 Mikrotik routerboard

Je to univerzální zařízení umožňující síťovou komunikaci. Routerboard je počítačová základní deska, kterou je možné rozšířit pomocí doplňujících prvků. Podle jednotlivých doplňků lze routerboard používat jako přístupový bod, bridge, router a další podobné síťové prvky. V základním vybavení obsahují procesor a integrovanou operační paměť. Podle různých typů jsou dále vybaveny integrovanou síťovou kartou, USB porty, LAN porty, Wi-Fi modulem, anténami a nespočetně dalšími doplňky. S routerboardy Mikrotik je dodáván linuxový operační systém RouterOS. Další výhodou routerboardu je, že umožňuje

funkci PoE, tedy napájení přes ethernetový kabel. Nepotřebuje tedy zapojení do elektrické sítě, tím ulehčuje jeho umístění a šetří nám další kabely.[8]

6.5.1.1 Mikrotik RB493AH

Zlínská pobočka používá Mikrotik RB493AH. Tento routerboard je velmi výkonný a v poměru cena/výkon patří k těm nejlepším. Je osazen 680 MHz síťovým procesorem Atheros a má 128 MB DDR RAM paměti. Zařízení má plnou podporu IPv6 a pro sdílení internetu má devět RJ45 LAN portů a také Wi-Fi modul. Routerboard je využíván také jako hardwarový firewall. Firewall filtruje síťový provoz a tím dokáže zabránit napadení počítačového systému hackerem nebo různými druhy červů. Dále je zařízení využíváno jako gateway (brána), což je síťový uzel, který může spojovat dvě sítě s různými protokoly. Brána nám například umožní autentizaci neznámého počítače, který se do sítě přihlásí poprvé. Po úspěšném ověření brána odblokuje přístup počítače do sítě.[8]

6.5.2 Switch

Z routerboardu je internet dále veden do switchů, ze kterých je dále veden po celé firmě. Switch je aktivní síťový prvek, který propojuje jednotlivé části sítě. Ve zlínské síti jsou čtyři switche Netgear, které umožňují rychlost až 1 Gbit/s a jeden switch 3Com, který pracuje rychlostí 100 Mbit/s.

6.5.3 Bridge

Bridge neboli most rozděluje síť na dvě kolizní domény. Umožní nám z pracovních stanic v jakékoliv síti přistupovat na zdroje v jiné síti. Bridge odděluje provoz různých částí sítě a zmenšuje tak zatížení sítě.

6.5.4 Bezdrátové AP

Připojení počítačů do sítě je možné jak kabelem, tak bezdrátovým připojením přes Wi-Fi. V budově jsou dva přístupové body se stejným SSID. Klienti se automaticky připojí vždy na AP se silnějším signálem. Oba přístupové body jsou připojeny do bridge s lokální sítí a jsou jim přiděleny IP adresy dle stejných pravidel, jako při připojení přes kabel do LAN. Autentifikace do bezdrátové sítě probíhá zadáním hesla. Síť je šifrována pomocí WPA-PSK/TKIP.

6.6 Servery

Ve firmě je šest serverů. Vzhledem k tomu, že byly pořizovány postupně, je každý server od jiného výrobce. Některé servery jsou fyzické a některé pouze virtuální - s nainstalovaným serverovým operačním systémem na běžném počítači.

6.6.1 DNS server

Server sloužící k řízení sítě. Jmenný neboli DNS server slouží k překladu doménových jmen na IP adresy. Server využívá technologii DHCP pro automatickou konfiguraci počítačů a jiných zařízení připojených do počítačové sítě. Pomocí DHCP protokolu je počítačům přidělována IP adresa a maska sítě.

Při přihlášení uživatele do sítě je proces ověřování založen na kontrole MAC adresy a poté proběhne automatická kontrola dle prvních 4 znaků názvu počítače. Každý počítač, server a aktivní prvek v síti má svůj přesně daný název kvůli jednoduššímu ověření a přiřazení do správné skupiny.

Pokud se přihlásí do sítě neregistrovaný počítač, je mu přidělena veřejná IP adresa. Veřejné adresy se udělují pouze na určitou dobu a umožňují přístup na internet, nikoliv do lokální sítě. Vzhledem k tomu, že na tomto serveru musí být zaregistrována všechna zařízení, která jsou připojena do sítě, slouží nám také jako kontrolní seznam, kolik a jaká zařízení jsou v sítí aktivně využívána.

DNS server je linuxový server na operačním systému Debian 6.0.

6.6.2 E-mailové (poštovní) servery

Ve firmě jsou dva poštovní servery, přičemž každý má svou úlohu.

První, opět linuxový, server slouží pro přijímání a odesílání pošty. Na tomto serveru je nainstalován antispam a antivir, které zajišťují bezpečnou komunikaci. Filtrují poštu a dále přeposílají pouze zkontrolované bezpečné zprávy.

Na první linuxový server je připojen druhý e-mailový server, který už pracuje pouze s filtrovanou komunikací a není zahlcen například spamy. Na tomto serveru je nainstalován software Microsoft Exchange, který umožňuje spolupráci s programem Microsoft Outlook a tak dovede synchronizovat události z kalendáře a další úkony. Zároveň je využíván jako

File server pro sdílení souborů. Umožňuje tak připojeným uživatelům přístup k uloženým souborům, správcům nabídne výhody centralizované správy, jednoduché údržby a sdílení dat.

6.6.3 Aplikační server

Na aplikačním serveru běží několik softwarových aplikací, které jsou určeny především pro testování, jak pro vývojáře, tak pro zákazníky. Nainstalován je software pro PLM, dále programy Enovia SmarTeam, Enovia V6 a další.

Server je používán také jako databázový. Je zde nainstalován systém řízení báze dat Oracle, který má velmi pokročilé možnosti zpracování dat. Oracle Database, jak zní oficiální název produktu, podporuje standardní databázový jazyk SQL, ale také vlastní jazyk PL/SQL, který rozšiřuje základní možnosti jazyka SQL, podporuje objektové databáze a XML hierarchické databáze.

6.6.4 Ekonomický server

Ekonomické a účetní aktivity zajišťuje systém Money S3. Data na tomto serveru jsou pro firmu velmi důležitá, proto je ekonomický server jediný, který využívá šifrování dat. Přístup do tohoto systému mají pouze 3 lidé ve firmě.

6.6.5 Server - telefonní ústředna

Poslední server je využíván pro telefonii. Komunikace pomocí telefonu probíhá v celé firmě přes VOIP technologii. Software pro zajištění telefonních hovorů je nainstalován na tomto serveru.

6.6.5.1 Voice over Internet Protocol

Volání přes internetový protokol je technologie, která umožňuje přenos digitalizovaného hlasu přes pakety prostřednictvím počítačové sítě. Přenos je zajišťován rodinou protokolů UDP, TCP a IP. Při volání přes internet je nutné zajištění QoS, tzv. kvality služby.

6.6.5.2 Quality of Service

QoS zajišťuje řízení datových toků v telekomunikačních a počítačových sítích s přepínáním paketů. Protokoly vyhradí přenosovou kapacitu, aby nedošlo ke snížení kvality síťových služeb při zahlcení sítě. Abychom dosáhli bezproblémové komunikace, můžeme například prohlásit provoz při telefonování za prioritní před ostatními nebo rozdělit provoz do kategorií podle nastavených parametrů. QoS nám tak poskytuje garantovanou kvalitu, a zajistí, aby nedocházelo ke ztrátovosti a zpoždění. V lokálních sítích je většinou telefonie bezproblémová, proto jsou tyto pravidla většinou potřeba až při volání ven z naší sítě.[9]

6.6.6 Záložní zdroj UPS

Všechny servery jsou zálohovány proti výpadku proudu UPS záložním zdrojem. UPS je zařízení, které nám zajistí dodávku elektřiny pro citlivá zařízení, která nesmějí být vypnuta neočekávaně. Zařízení funguje jako akumulátor, pokud elektřina funguje, udržuje plnou kapacitu své baterie. V okamžiku přerušení dodávky elektřiny zajišťuje napájení připojených zařízení buď do obnovení primárního zdroje napětí, nebo do svého vybití. Doba, po kterou UPS udrží servery v chodu ve firmě Technodat je 15 minut.

6.6.7 Umístění serverů

Servery jsou spolu s rozvaděčem umístěny v jedné místnosti, která však není speciálně upravená pro potřeby serverů. Místnost je uzamčena, klíč si však může vypůjčit kdokoliv a přístup není omezen.

Problém může být i v nejednotnosti serverového vybavení. Pro bezproblémové fungování by mělo být zajištěno odebírání hardwaru pouze od jednoho výrobce, pravidelná údržba a obměna zařízení.

6.6.8 Šifrování dat na serverech

Velkým problémem je, že data na serverech a nejsou nijak šifrována. Jedinou částí, kde je využíváno šifrování, je ekonomický software na serveru. Je tak možné, že data budou odposlechnuta a zneužita. Vzhledem k tomu, že na serverech jsou uloženy všechny citlivé informace o firmě, o zaměstnancích, ale také o zákaznících a zakázkách, je tento stav alarmující.

6.6.9 Zálohování dat

Všechna data na serverech jsou zálohována. Data jsou zálohována každý den inkrementální metodou.

U inkrementální, neboli přírůstkové, metody se nejprve vytvoří plná záloha všech dat a poté se již zálohuje pouze přírůstek dat od poslední zálohy. Tato metoda je tak nejméně náročná na místo na disku. Nevýhodou však je, že pokud ztratíme některou část přírůstkové zálohy, ztratíme tak všechny další. Zálohy na sebe totiž navazují, a při ztrátě jedné nebude možné číst všechny další.

Tento problém je vyřešen vytvářením kopií všech záloh na jiné úložné zařízení ve druhé budově.

6.6.10 Budoucnost

V souvislosti s nedostatky spojenými s fyzickým a logickým zabezpečením dat však již je vypracován plán na novou serverovnu, která by měla být postavena do konce kalendářního roku v nově vznikající budově. Místnost již bude vytvořena zcela dle potřeb pro uchovávání dat, bude zakoupeno nové vybavení a je plánováno také zabezpečení přístupu do serverovny, především omezení přístupu pouze určitým lidem a důsledné proškolení těchto osob.

7 INFORMAČNÍ SYSTÉMY

Většina dat je zaznamenávána pomocí informačních systémů. Proto jsou pro firmu tolik důležité a proto je také důležité používat kvalitní systémy, které se firmě přizpůsobí přesně podle jejich požadavků. Ve firmě Technodat jsou využívány velmi známé a kvalitní informační systémy pro ekonomické potřeby a pro e-mailovou komunikaci. Docházkový systém a systém pro styk se zákazníkem jsou dokonce vyvíjeny přímo pro firmu Technodat, tudíž je možné do nich integrovat jakékoliv specifické požadavky. Systémy jsou tak firmě plně přizpůsobeny.

7.1 Money S3

Účetní program Money S3 patří k nejrozšířenějším ekonomickým systémům pro malé a střední firmy v České i Slovenské republice. Software nabízí podvojné účetnictví i daňovou evidenci, adresář, fakturaci, informace ze skladů, objednávky i mzdy. Je možné jej rozšířit o další užitečné doplňky a moduly, například kniha jízd a cestovní náhrady a spoustu dalších.

Vzhledem k enormně důležitým ekonomickým údajům firmy Technodat v rámci konkurenčního zpravodajství jsou data v tomto systému šifrována.

7.2 Microsoft Exchange

Softwarový produkt sloužící pro zasílání e-mailových zpráv, spolupráci a sdílení zdrojů. Tento program do jisté míry omezuje rizika znehodnocení a úniku citlivých dat. Komunikace je automaticky zabezpečena a citlivé údaje bez autorizace neopustí firmu.

Výhodou softwaru od firmy Microsoft je jeho snadné propojení s ostatními produkty téhož výrobce. Právě toho je ve firmě Technodat využíváno. Propojení s programem Microsoft Outlook nám umožní synchronizaci všech kontaktů, ale také dalších údajů a úkolů v kalendáři. Pomocí svého účtu v Outlooku také mohou zaměstnanci přistupovat k souborům, které jsou na e-mailovém serveru k dispozici.

7.3 CRMplus

Profesionální CRM systém, který vyvíjí firma Technodat Develop. Customer relationship management je databázová technologie, která umožňuje a zjednodušuje lidem pracujícím

v marketingu a obchodě administraci aktivit, které jsou spojené s péčí o zákazníky - shromažďování, zpracování a využití informací o zákaznících firmy.[7]

CRM systém vyvíjen přímo pro potřeby firmy Technodat, umožňuje spolupráci s účetním systémem Money S3 a rychlý import dat z tohoto systému.

7.4 Docházkový systém RAC

Docházkový systém je opět plně vyvíjen firmou Technodat Develop, tudíž plně odpovídá potřebám a požadavkům firmy Technodat. Systém má spoustu funkcí, především umožňuje spravovat údaje o zaměstnancích a jejich docházce, v přehledné aplikaci si můžeme okamžitě zobrazit pohyb zaměstnanců, kdykoliv si můžeme zobrazit historii docházky, případně můžeme nastavit automatické generování měsíčních výkazů.

Je založen na architektuře klient-server. Systém je složen ze 4 modulů, kde 2 moduly běží na klientu a 2 na serveru. Aplikace na jednotlivých modulech jsou pojmenovány: RAC Reports, která je hlavní aplikací a zajišťuje správu měsíčních výkazů, zakládání do evidence a další, dále RAC Scanner sleduje a umožňuje zadávání a hlídání docházky, RAC WebScan provádí webovou kontrolu a umožňuje zadávání docházky přes web a poslední RAC Daemon zajišťuje vyčítání dat z terminálu.[7]

Systém je vytvořen na technologiích Delphi, MS SQL Server, MS ADO.

Čtečka docházkového systému je nainstalována v prvním patře budovy. Příchod a odchod je zaznamenáván pomocí čipů, tzv. touch memory. Všechna data jsou uložena do databáze a je možné si je kdykoliv prohlédnout.

8 ANALÝZA BEZPEČNOSTI DAT

Provedením bezpečnostní analýzy a následného návrhu řešení vytvoříme pravidla pro bezpečnostní politiku, které je nutné dodržovat. Abychom mohli provádět následná školení zaměstnanců a dalších osob, kterých se tato pravidla dotýkají, potřebujeme je mít zdokumentovaná. Proto veškeré činnosti, které v rámci analýzy provádíme, musíme postupně zapisovat a následně z nich vytvořit funkční bezpečnostní politiku. Právě vytvoření kvalitní bezpečnostní politiky je naším cílem.

8.1 Identifikace aktiv

Identifikace spočívá ve vytvoření soupisu všech aktiv ležících uvnitř hranice analýzy rizik. Hranice je pomyslná čára, která odděluje aktiva, která budou patřit do analýzy rizik, od ostatních. Uvnitř hranice budou ležet jednotlivá aktiva, ze kterých je systém složen, budovy, ve kterých jsou tato aktiva umístěna, a budovy, kde jsou zařízení, na kterých je provoz informačního systému závislý (rozvaděče nebo náhradní zdroje elektrické energie). [10]

V každé firmě je nejvíce chráněnou částí serverovna. Tam jsou totiž všechna důležitá a citlivá data společnosti. Chránit je však třeba všechna zařízení v síti, protože jak praví známé přísloví: řetěz je tak silný jako jeho nejslabší článek. Pokud by tedy nebyl některý článek v počítačové síti zabezpečen, znehodnotilo by to celý bezpečnostní systém. Proto do identifikace aktiv zahrneme veškerá zařízení, software a informace z celé počítačové sítě firmy.

V následující tabulce jsou zahrnuta veškerá aktiva a je jim přiřazena hodnota podle velikosti škod, které by nastaly v případě jejich znehodnocení. Hodnoty jsou od 1 do 5, přičemž 1 je přiřazena aktivům, u kterých by vznikly minimální škody a 5 pro aktiva s největším dopadem na řádné fungování firmy. Při vytváření jsem vycházel z poznatků získaných při praktickém provádění analýzy, ze zkušeností uživatelů podobných zařízení a z obecných vědomostí získaných při studiu.

Identifikace	Hodnota
HW	
Servery	5
Počítače	3
SW	
Informační systémy	3
Operační systém	1
Firemní aplikace	2
Data	
E-maily	3
Databáze	5
Firemní data	4

Tabulka 1: Identifikace aktiv

8.2 Identifikace hrozeb

Nedílnou součástí analýzy rizik je identifikace všech hrozeb, které mohou nastat při běžném provozu. S hrozícími nebezpečími musíme počítat téměř na každém kroku, u každého zařízení. Hrozby mohou být nehody, ale také cílené útoky. Mezi nejčastější nehody patří selhání hardwaru a softwaru, neúmyslná modifikace nastavení, ale také povodeň a jiné živelné katastrofy. Nesmíme opomenout ani možnost krádeží nebo interních útoků, například od nespokojených zaměstnanců.

Největší nebezpečí však mohou přijít z internetu. Programy, které jsou vytvořeny proto, aby škodily, nám mohou připravit hodně nepříjemností. Taková nebezpečí se dělí na ta, která hrozí připojeným počítačům a datům na nich uložených, a která hrozí přenášeným datům. Oba typy hrozeb jsou závažné a je nutné se proti nim účelně bránit.

V tabulce 2 je soupis různých typů hrozeb, které mohou nastat. Možnost, že se daná hrozba stane, je reprezentována číselnou hodnotou. Podobně jako v předchozí tabulce nám číslo 1 udává nejméně pravděpodobnou možnost, že daná situace nastane, číslo 5 naopak nejvíce pravděpodobnou. Opět jsem vycházel především z vlastních znalostí a ze zkušeností uživatelů počítačových zařízení. Jednotlivé hrozby jsou v dalších kapitolách postupně rozebrány. Vysvětleny jsou především jejich škodlivé účinky a opatření k zabránění vzniku takových situací.

Identifikace	Hodnota
Odposlech a zpronevěra dat	4
Útoky proti zařízením v síti	5
Živelné katastrofy	1
Selhání HW	2
Selhání SW	2
Krádež	3
Neúmyslná modifikace	5

Tabulka 2: Identifikace hrozeb

8.2.1 Penetrační testy

Při určování hrozeb, které mohou nastat, je vhodné vytvořit určitý podklad, ze kterého vycházíme a který průběžně upravujeme a doplňujeme. Pro vytvoření podkladu je ideální provést penetrační testy. Testy by měly být pevnou součástí bezpečnostní analýzy.

Penetrační test nám otestuje reálný stav bezpečnosti naší počítačové sítě. Zaměřuje se na možnost úniku informací, nabourání sítě pachatelem a čtení nebo modifikaci našich dat. Testy simulují útoky na naši síť a zaznamenají všechny bezpečnostní trhliny. Pomocí výsledku můžeme dále přistupovat k zabezpečení systému a preventivním opatřením před podobnými škodlivými útoky.

Na penetrační testy existuje několik specializovaných internetových stránek. Je důležité vybrat si takové, které jsou ověřené a u kterých nehrozí žádná další bezpečnostní rizika. Ideální je vybírat takové, které vyvíjí, nebo které svým jménem podporují, známé a ověřené firmy poskytující softwarové řešení pro ochranu dat, např. antivirové programy.

Musíme rozlišovat použití testů na soukromých nebo na firemních počítačích. Pro firemní účely jsou potřeba zcela jiné podmínky a pravidla. Většina penetračních testů, které jsou nabízeny zdarma, jsou proto především na domácí použití, případně u firemních zařízení je obsah testu omezen pouze na základní funkce.

8.2.1.1 Výsledek testu

Pro testování jsem využil stránek www.paranoia.cz , které nabízejí online test speciálně pro firemní zařízení - EVA Free. Služba Paranoia.cz je provozována společností ESET - divizí ESET Services. Tento test je prováděn na vyžádání a výsledek můžeme mít do 24

hodin od zadání příkazu. Jelikož je poskytován zdarma, obsahuje pouze základní testování. Firma má v nabídce také další placené varianty testů, které poskytují podrobnější a pravidelné testování s přesným popisem zranitelností a návrhem opatření.

V testu jsme zjistili dva závažné problém. Jedním bylo špatné nastavení DNS serveru a umožnění použití serveru pro distribuované útoky. Útočník by tak byl schopný nabourat se na náš server a použít jej pro cílený útok na třetí objekt, případně by mohl zahltit náš server rekurzivními dotazy.

Vzhledem k závažnosti hrozby a v současné době poměrně oblíbenému typu útoku je nutné tuto hrozbu řešit okamžitě a důsledně. Především musí být více omezen přístup na DNS server z veřejné sítě a rekonfigurace pravidel přístupu a odpovídání dotazů, které jsou základním prvkem pro zahlcení serveru pomocí distribuovaných útoků.

Druhý problém se objevil při provádění testu na trojské koně. Test byl proveden na možnost přístupu trojských koňů do internetu přes otevřené porty. Testováno bylo 30 portů a většina přístup odmítla. Pouze jeden port byl otevřen, tudíž by mohl být škodlivými programy zneužit například pro vytvoření přístupu útočníkovi nebo pro odesílání citlivých informací.

Otevřenost portů se ovládá pomocí firewallu. Proto je nutné zkontrolovat a upravit nastavená pravidla pro síťový provoz.

8.2.2 Odposlech a změna dat

Odeslaná data přes internet je velmi jednoduché odposlechnout nebo dokonce modifikovat. Přístup k datům může získat spousta lidí - od technika, který provádí údržbu počítačů, po hackera, kterému se podaří získat kontrolu nad počítači, routery a jinými síťovými zařízeními.

Největší bezpečnostní nevýhodou digitálních dat je jejich snadná možnost kopírování. Nikdy totiž nezjistíme, kolikrát byl dokument zkopírován předtím, než dorazil k cílenému adresátovi. Velmi jednoduché je také modifikovat posílaná data.

Musíme počítat s tím, že největší výhoda internetu je zároveň jeho největší nevýhodou. Počítačová síť je otevřena pro jakéhokoliv uživatele. Tím je snadné zaslat komukoliv určitá data během okamžiku. Bohužel tato otevřenost umožňuje právě odposlechnutí zasílaných dat.

Jedinou možností, jak zajistit bezpečný přenos dat a znemožnit modifikaci, je jejich šifrování. Právě šifrování dat je slabým článkem zabezpečení ve firmě Technodat. Šifrování je použito pouze na ekonomické údaje.

8.2.3 Útoky na zařízení připojená do sítě

Všechny počítače, které jsou připojeny k počítačové síti, jsou snadným terčem útočníků. Pro hackery není žádný počítač nezajímavý. Útočník náhodně provádí útoky na různé počítače a testuje, zda nejsou některé porty otevřené. Jakmile narazí na nějakou bezpečnostní trhlinu, okamžitě ji zkusí využít a pokusí se získat alespoň částečnou kontrolu nad počítačem. Pokud útočník získá přístup k počítači, je už pro něj jednoduché získat data. Takto ovládané počítače jsou ovšem využívány i jinak. Nejlepší ochranou je instalace a správné nastavení firewallu.

Pro absolutní ochranu je vhodné použít hardwarový firewall. Tento je ve firmě Technodat nastaven v routerboardu tak, abychom mohli bezpečně přistupovat z lokální sítě do veřejného internetu. Softwarové firewally jsou nainstalovány a používány na všech počítačích i serverech. Pravidla pro povolování připojení je však potřeba upravit, protože penetrační test ukázal, že jsou v nastavení skulinky, které by mohl případný útočník zneužít.

8.2.4 Typy útoků

Útočníci dokáží využít i té nejmenší chyby v nastavení a přes otevřené porty v protokolech nám mohou velmi škodit. Zde uvádím dva nejčastější a mezi útočníky nejoblíbenější útoky na síťová zařízení.

8.2.4.1 Útoky DoS a DDoS

Pokud útočník získá kontrolu nad větším množstvím počítačů, může je využít pro distribuované útoky například k zahlcení serveru. Servery nebo počítače jsou zahlceny velkým množstvím dotazů a nestíhají tak reagovat na regulérní dotazy jiných uživatelů. Takové útoky se nazývají DoS a DDoS.

DoS znamená Denial of Service, neboli odepření služby. Takový útok je prováděn pouze z jednoho počítače. Většina serverů i počítačů si však již s takovým útokem dokáže poradit.

Mnohem nebezpečnější a výkonnější variantou je distribuovaný útok - DDoS. Ten je již prováděn z velkého množství počítačů. Tyto útoky se objevují ve větší míře v poslední době a můžeme vidět, že málokterý server jim dokáže odolat.

8.2.4.2 Man-in-the-middle

Další velmi známý útok. Útočník se stane prostředníkem v komunikaci mezi dvěma subjekty. Zachytává tak veškerou komunikaci. Kromě odposlechnutí dat však může snadno i měnit obsah zpráv. Pokud je odposlouchávána veškerá komunikace, nepomůže nám ani šifrování. Při posílání šifrovacího klíče jej získá útočník a nahradí ho svým vlastním. Uživatelé tak sice vidí, že komunikují šifrovaně, pachatel však komunikaci může lehce dešifrovat.[11]

Abychom takovému útoku zabránili, je nutné všechna odesílaná data šifrovat. Pro výměnu šifrovacích klíčů ale musíme použít jiný komunikační kanál. Šifrovací klíč také můžeme opatřit digitálním podpisem, který byl ověřen certifikační autoritou a zajišťuje tak integritu dat a identitu odesílatele. Tak budeme mít jistotu, že daný klíč nikdo nezmění a že se za nás nebude vydávat nikdo jiný.

8.2.5 Škodlivé programy

Největší výhodou škodlivých programů je, že se mohou šířit automaticky, bez další podpory útočníka. Jsou uloženy ve zdrojových kódech programů, a proto si je většinou uživatel nainstaluje nevědomky sám. Abychom tomu zamezili, musíme používat pravidelně aktualizovaný antivirový program a také správně nastavený firewall.

V tomto ohledu je firma Technodat opět na velice dobré úrovni. Antivirový program je zakoupen a nainstalován na všech počítačích. Při penetračním testu zaměřeném speciálně na trojské koně byly téměř všechny žádosti o instalaci odmítnuty. Pouze jeden port vykazoval aktivitu a možnost vytvoření přístupu pro škodlivé programy. Řešením tohoto problému je oprava nastavení ve firewallu. Antivirový program fungoval v pořádku.

8.2.5.1 Trojský kůň

Trojský kůň je samostatný program nebo část programu se škodlivou funkcí. Touto funkcí může být sledování a odposlouchávání přístupových údajů k účtům, získání údajů o uživateli

při surfování na internetu a následné umožnění zasílání spamu. Trojský kůň může také obsahovat síťovou službu, která umožní útočníkovi nepozorovaně vstoupit do naší sítě a získat přístup do systému. Takových škodlivých funkcí je nespočetně, právě proto jsou tyto programy velice nebezpečné.

8.2.5.2 Počítačový vir

Virus je v počítačové terminologii program, který se dokáže šířit, aniž by o tom uživatel věděl, ale pouze v rámci počítače, do kterého byl instalován. Počítačové viry opět mohou mít mnoho účelů. Některé jsou pouze obtěžující, ale jsou i takové, které mohou cíleně mazat soubory na disku.

8.2.5.3 Počítačový červ

Červ je velmi podobný škodlivý program jako virus, často s ním bývá nesprávně zaměňován. Rozdíl mezi nimi je v tom, že červ se umí automaticky šířit počítačovou sítí na jiné počítače. Program infikuje systém a převezme kontrolu nad síťovou komunikací. Tak se může bezproblémově rozesílat skrze internet. Stejně jako jiné škodlivé programy může mazat programy v počítači, omezit samotnou činnost počítače, získávat osobní data a vytvářet bezpečnostní trhliny pro šíření dalších škodlivých programů.

8.3 Stanovení hodnoty aktiv a jejich zranitelnosti

Hodnota aktiv se stanovuje na základě velikosti škody, která by nastala při zničení aktiva. Vychází se z jeho pořizovací ceny. Pokud je však aktivum nezbytné pro další chod informačního systému, jeho hodnota se může zvyšovat.

Ke všem aktivům se přiřadí všechny hrozby a vytvoří se tak dvojice, které nám ukazují zranitelnost aktiv. Ke každé dvojici musíme najít vhodné bezpečnostní řešení. Pokud možno nacházíme taková řešení, která dokáží zneškodnit co nejvíce hrozeb.

Nejdříve určíme úroveň hrozby k aktivu a úroveň zranitelnosti aktiva k této hrozbě. To je zobrazeno v následující tabulce, která vychází z předchozích dvou tabulek. Soupis aktiv jsem spojil se soupisem hrozeb a jednoduchým výpočtem mi vzešly výsledky, ze kterých jasně vidíme, kterých situací bychom se měli obávat nejvíce a kterých nejméně. Stupnice opět začíná na čísle 1 pro nejmenší hodnotu zranitelnosti, a může nabrat maximální hodnoty

25. Podle Dané hodnoty bychom se měli soustředit na následná bezpečnostní opatření. Je jasné, že největší zranitelnost hrozí firemním datům. Měli bychom tedy co nejvíce omezit přístup, aby nedošlo k neoprávněnému přístupu. Ztráta takových dat by měla největší dopad na další fungování firmy. Naopak hrozba živelné katastrofy vzhledem k umístění budovy není příliš pravděpodobná.

Hrozby:	**Identifikace**	Servery	Počítače	Informační systémy	Operační systém	Firemní aplikace	E-maily	Databáze	Firemní data
Aktiva:	**Hodnota**	5	3	3	1	2	3	5	4
Identifikace	**Hodnota**								
Odposlech a zpronevěra dat	4	20	12	12	4	8	12	20	16
Útoky proti zařízením v síti	5	25	15	15	5	10	15	25	20
Živelné katastrofy	1	5	3				3	5	4
Selhání HW	2	10	6						
Selhání SW	2			6	2	4			
Krádež	3	15	9			6	9	15	12
Neúmyslná modifikace	5	25	15	15	5	10	15	25	20

Tabulka 3: Stanovení zranitelnosti aktiv

9 NÁVRH OPATŘENÍ

Po stanovení všech aktiv a hrozeb je nutné vytvořit soubor preventivních opatření. Cena zavedení opatření by neměla přesáhnout hodnotu následků po havárii. Přitom však musí být provedena tak, aby byla účinná.

Je důležité si uvědomit, že cena při odstraňování škod může být až několikanásobně vyšší než proaktivní opatření. Proto by se nemuselo vyplatit odmítání bezpečnostní politiky a výdajů za taková pravidla. Jako podřízený zaměstnanec samozřejmě nemůžeme jít proti rozhodnutí ředitele a něco provádět na „vlastní pěst“. Už proto, že by nám vynaložené prostředky nejspíše nikdo nevrátil, ale také bychom se při takovém počínání mohli s firmou rychle rozloučit.

Na vedení firmy proto musíme pravidelně apelovat a vysvětlit jim, že veškerá prevence sice není životně důležitá, ale velice kladně ovlivní další náklady za odstranění škod a obnovení dalšího provozu.

Při vytváření návrhu řešení vycházíme ze všech předchozích poznatků, z analýzy rizik a předchozích útoků a havárií. Dalším prvkem je výsledek penetračního testu, provedeného nejlépe na více počítačích v lokální síti.

9.1 Ochrana proti nehodám

Abychom co nejvíce předešli ztrátám dat kvůli selhání HW a SW, je nutná pravidelná kontrola a obnova všech zařízení. Samozřejmostí je používání legálního softwaru. Pokud to programy umožňují, nastavíme jejich automatické aktualizování.

Při živelných katastrofách nám pomůže jedině pravidelné zálohování a zrcadlení dat na více místech. Občas je také nutné zálohy zkontrolovat, zda všechno probíhá v pořádku. S těmito pravidly jsou správci seznámeni. Záloha je prováděna každý den. Zálohy jsou navíc kopírovány na druhé datové úložiště, tudíž je zajištěna kontinuita dat při jakémkoliv, i dvojitém výpadku v síti. Toto řešení je pro firmy v kategorii malé a střední, do které firma Technodat patří, dostatečné. Proto není potřeba na takovém provedení nic měnit.

Také ostatní opatření jsou ve firmě správně plněny, proto ochranu proti nehodám zavedenou ve firmě Technodat považují za ideální.

9.2 Ochrana proti vnějším útokům

Internetoví útočníci neustále nacházejí další a další bezpečnostní trhliny, proto není nikdy stoprocentně možné preventivně se bránit. Je však nutné to útočníkům alespoň co nejvíce znepříjemnit.

Před škodlivými programy nám pomáhá chránit počítač brána firewall. Je důležité ji správně nastavit a povolovat pouze takové služby, u kterých si jsme stoprocentně jistí, že neobsahují škodlivý kód. V žádném případě tomu nesmí být naopak, že všechny služby povolíme a poté podle identifikovaných hrozeb jednotlivé relace zakazujeme. Tento postup musí být důrazně zakázán, protože nikdy nejsme schopni předem určit všechny problémy, které mohou nastat. A řešit problémy až poté, co nastanou, zcela vyvrací celou logiku vytváření bezpečnostních preventivních opatření.

Dále musí být v počítači nainstalován antivirový software. Je dobré jej vybírat podle předchozích nezávislých testů, abychom si mohli porovnat jejich účinnost. Vzhledem k tomu, že nové hrozby vznikají neustále, je potřeba mít pro co nejúčinnější ochranu zapnuté automatické aktualizace virové databáze. Přestože je vždy možné, že náš systém napadne zcela nový vir, antivirové společnosti se snaží reakční dobu neustále snižovat a některé dokáží vytvořit záplatu na nové hrozby již do dvou hodin od první detekce.

Abychom zabránili možnosti odposlechu a modifikace dat, je nutné používat šifrování dat. Toto pravidlo platí u serverů dvojnásob. Právě na servery míří většina cílených útoků, protože tam je nejvíce informací, citlivých dat a celé know-how firmy.

V šifrování dat ve firmě Technodat vidím jeden z největších problémů. Většina dat tímto způsobem není chráněna vůbec. Proto důrazně doporučuji zavést šifrování dat na všech serverech. Tím bude zabezpečena většina firemních dat, jak databáze z informačních systémů, tak data vytvořená zaměstnanci při práci.

Na linuxových operačních systémech je již možnost šifrování implementována a provádí se pouze zadáním správného příkazu. Pokud používáme operační systémy Windows, je vhodným řešením použití speciálních programů a nástrojů. Mezi nejznámější patří výše uvedené nástroje PGP a TrueCrypt. Pomocí těchto programů je možné šifrovat e-mailovou komunikaci, jednotlivé soubory a složky, ale i celé disky.

9.3 Ochrana proti interním útokům

Nespokojený zaměstnanec může být pro firmu velice nebezpečný. Má totiž téměř neomezený přístup do všech firemních prostor a k firemním aplikacím a datům. Proto je velmi těžké se takové hrozbě chránit. Na pracovišti by tak měla být neustále přátelská atmosféra a vedení by mělo se zaměstnanci vést pravidelné debaty o pracovních podmínkách a úkolech, zbytečně zaměstnance nepřetěžovat a nevystavovat je stresovým situacím.

Provádíme také pravidelná školení zaměstnanců a seznámíme je se správným používáním všech zařízení, dále se základními bezpečnostními pravidly jako používání bezpečného hesla, odhlašování při odchodu z pracoviště, znalost postupu při kritických bezpečnostních situacích. Měli by také být seznámení se všemi druhy hrozících útoků, především o technikách sociálního inženýrství, které je mířeno především na neznalé osoby.

S nedostatečným zpracováním bezpečnostní politiky ve firmě Technodat souvisí nedostatečné školení zaměstnanců. Proto je cílem zpracovat všechna pravidla a vytvořit potřebnou dokumentaci.

9.4 Ochrana proti krádežím

I přes zabezpečený vchod do firmy se může ve firmě vyskytnout zloděj. Proto by měl být chráněn vstup i do dalších důležitých místností, především do serverovny. Místnost se servery by měla být ve všech ohledech výjimečná. Musí se brát ohled na to, že to je nejdůležitější místnost ve firmě a vniknutí nepovolaných osob by mohlo mít pro firmu fatální následky. A to jak z hlediska konkurenční politiky, tak z hlediska kontinuity provozu firmy.

Před krádežemi musíme zajistit i přenosné počítače, nejlépe zámkem na klíč. Všechna firemní zařízení by také měla být opatřena evidenčním číslem a pravidelně by se měla provádět inventura veškerého majetku. U většiny místností by se mohly nainstalovat čtečky karet pro přístup pouze oprávněným osobám. Jednoduše bychom tak mohli vést evidenci přístupů.

9.5 Ochrana serverů

V plánu je výstavba kompletně nové serverovny. Proto je důležité dát si záležet na zavedení správných pravidel hned při vytváření. Jako nejdůležitější bych doporučil uzamčení

serverovny a zavedení pravidel pro vstup do této místnosti. Vstup by měl být povolen jen několika osobám, které skutečně potřebují mít přístup, především správcům sítě. Toho bychom mohli dosáhnout zavedením čteček a čipových karet, které by nám umožnily snadnou identifikaci pro přístup, a bylo by také možné podle záznamů uložených v databázi jednoduše kontrolovat, kdo a kdy do místnosti vstoupil.

V serverové místnosti by měly být navrženy vhodné podmínky. Především by měla být zajištěna stálá teplota a vlhkost, které nám mohou zaručit delší životnost počítačových součástek. Ventilační systém by měl také vhodně filtrovat vzduch, aby zajistil bezprašné prostředí.

Abychom zabránili požárům, měly by být instalovány detektory kouře a ohně, po ruce by měly být plynové hasicí přístroje. Pro dokonalou ochranu před požáry bývá instalováno stabilní hasicí zařízení. Takové zařízení je vedeno v trubkách po celé serverovně, pro hašení se používají speciální tlakové lahve s hasicím plynem. Nevýhodou jsou velké skladovací prostory pro tlakové lahve a především velké náklady na zřízení i další provoz. Vhodné je položit nehořlavou podlahu.

Musí být zajištěna záloha elektrického zdroje při výpadku elektrického proudu. Toto už je ve firmě správně zavedeno a je zajištěn chod na záložní zdroj minimálně 15 minut pro bezpečné ukončení všech aplikací a souborů. S výhodou bývá instalováno duplicitní připojení do počítačové sítě, aby bylo zabráněno výpadkům celé sítě při poruše jedné části.

9.6 Bezpečnostní politika

Bezpečnost dat ve firmě Technodat je na dobré úrovni. Nedostatek je však ve zpracování pravidel počítačové bezpečnosti. Ve firmě sice existuje dokument, který shrnuje základní pravidla chování při práci s počítačem a při práci v lokální síti, je však velmi stručný. Proto považuji za vhodné vytvoření kompletní dokumentace.

Správce sítě samozřejmě ví, jak se o zařízení starat a co dělat při různých krizových situacích. Ze zákonů schválnosti však víme, že k nestandardním situacím dojde vždy v nejméně vhodnou dobu. Pokud například správce sítě právě není k dispozici, musí za něj zaskočit jiný kolega, který však nemá dané zkušenosti. Ten tedy využije zpracované bezpečnostní politiky a postupuje dle sepsaných zásad.

Komplexní bezpečnostní politika by měla zahrnovat přesný popis hardwarových a softwarových součástí používaných ve firmě. V soupisu hrozeb, které mohou nastat, by měl být alespoň stručný popis řešení při odstraňování následků. V dokumentaci také musí být jasně stanoveno, který uživatel má přístup do které části sítě. Tato pravidla jsou uložena na serverech a přístup je tak automaticky kontrolován, sepsání je nutné pro kontrolu správného nastavení nebo při obnovení nastavení po havárii.

Se základními bezpečnostními pravidly musí být seznámení všichni zaměstnanci firmy. Každý uživatel by měl vědět, ke kterým počítačům má přístup a které aplikace smí používat. Abychom docílili bezpečného přístupu do lokální sítě, je nutné určit základní pravidla i pro vytváření uživatelských hesel. Pro opravdu bezpečné přihlašování musí být dodrženy podmínky:

- délka hesla alespoň 14 znaků
- kombinace velkých a malých písmen, čísel a speciálních znaků
- pro každé zařízení jiné heslo
- pravidelná a častá změna hesla - alespoň jednou za půl roku
- nesdělovat heslo jiným osobám
- nepsat heslo na zařízení, na papírek v blízkosti zařízení
- heslo nesmí mít přímou souvislost s danou osobou (jméno, příjmení, přezdívka,…)

9.6.1 Problémy při zavádění bezpečnostní politiky

Velmi častým jevem při zavedení jakýchkoliv pravidel je vytváření kompromisů. Pravidla, která se nám nelíbí, nebo která komplikují naši práci, raději vypustíme, než abychom je dodržovali. Taková situace je zcela nepřípustná. Při vyskytnutí problému je nutné ho ihned řešit, ne jej ignorovat. Pokud nebude prováděna pravidelná kontrola dodržování daných pravidel, nikdy nedocílíme kvalitního řešení a všechna předchozí práce při vytváření bezpečnostní politiky a výdaje s ní spojené budou naprosto zbytečné.

Ve spojení s předchozím problémem musíme však myslet na to, aby pravidla byla vytvořena tak, aby nekomplikovala naši práci příliš. Těžko můžeme být spokojení s dokonalým zabezpečením dat, když dodržování bezpečnosti pro nás bude znamenat drastickou ztrátu

efektivity práce. V takovém případě by politika ztrácela smysl, protože by se změnil objem zabezpečovaných hodnot a daná pravidla by byla zbytečná.

Proto je dobré při vytváření spolupracovat s co největším počtem lidí, kterých se to bude dotýkat. Formou dotazníků získáme dostatečný přehled a vytvoříme si lepší vstupní podmínky pro přijetí zaměstnanci.

Ke špatnému přijetí může dojít i při náročném a rozsáhlém provedení politiky. Cílem dokumentu musí být jasný a srozumitelný výstup pravidel pro snadné pochopení a pro jejich snadnou implementaci do provozu. Zaměstnanci těžko budou dodržovat něco, co jim ani dostatečně nevysvětlíme. Tomu předejdeme také důsledným školením zaměstnanců.

Dokument samozřejmě není veřejně přístupný, protože pro případného útočníka by to byl jednoduchý návod na proniknutí ke všem aktivům naší společnosti. Pro zaměstnance musí být obsah osvětlen právě podrobným a především pravidelným školením. Podcenění informování všech zaměstnanců pak může vytvořenou bezpečnostní politiku zcela degradovat.

Posledním prvkem kvalitní bezpečnostní politiky je aktualizace a provádění pravidelných kontrol zavedených pravidel. Nesmíme brát daná pravidla jako neměnná. S vývojem firmy se neustále mění situace v počítačové síti, proto musí být postupně rozvíjena i bezpečnostní pravidla. Musíme reagovat na nová zařízení v síti, ale také na nové hrozby a další problémy, které nastanou, nebo je pravděpodobné, že nastat mohou.

ZÁVĚR

Firma Technodat je na tom v zabezpečení dat velmi dobře. O síť se starají vlastní správci, což je podle mého mínění ideální řešení. Pokud si na provedení bezpečnostních opatření najmeme externí firmu, nemáme o řešení tak dobrý přehled, jako při zpracování vlastními zaměstnanci. Navíc se firmě musí svěřit všechny citlivé informace, což je v jisté míře také velké riziko.

Na všech počítačích je nainstalován firewall a antivirový program, správně nakonfigurován a nastaven pro automatické aktualizace. Také operační systém je zakoupen vždy v nejnovější stabilní verzi.

Správci sítě, kteří jsou za bezpečnost dat odpovědní, nemají vypracovanou bezpečnostní politiku, tudíž nemají zpracována všechna rizika, která hrozí. K zabezpečení přistupují postupně, vždy se zaměří na jednu oblast a zajistí opravení nedostatků. V případě jakéhokoliv problému jsou flexibilní a ihned tento problém řeší.

Bezpečnost dat musí být na dobré úrovni z toho důvodu, že zlínská pobočka je propojena pomocí VPN s ostatními pobočkami firmy Technodat, jak v České republice, tak na Slovensku. Při nedostatečném zabezpečení by se případná hrozba mohla šířit po celé síti a způsobit velké problémy. Firma by se tak mohla stát nedůvěryhodnou a ztratit svou pozici nejen na českém trhu. Vzhledem k tomu, že firma spolupracuje i s několika zahraničními firmami a je dodavatelem známých firem Škoda auto nebo Honeywell, mohla by být ztráta důvěryhodnosti zcela zásadní.

Největší bezpečnostní trhlinou je zabezpečení serverů. Místnost se servery není klimatizována a není speciálně vytvořena pro ideální podmínky. Dveře do serverovny jsou sice zamčeny, klíče si však může vypůjčit kdokoliv a neprobíhá žádná kontrola a evidence. Data na serverech kromě ekonomického softwaru nejsou šifrována, je tak možný jejich odposlech. Správci však o těchto problémech vědí, proto již je naplánována nová serverovna, která bude splňovat všechna bezpečnostní pravidla. Místnost bude v nové budově, která se staví v sousedství.

ZÁVĚR V ANGLIČTINĚ

The Technodat Company has very good realized data security. There are company network administrators and it is optimal solution. We can hire an external company for implementation security precautions but we have not got good survey of the solution as in the processing of its own employees. The company has known any sensitive information so it could be also a big risk.

All computers have installed firewall and antivirus software, right configured and set for an automatic update. Operating system is also purchased in the newest stabile version.

Network administrators who are responsible for data security do not have a security policy therefore do not processed all the risks that threaten. They approaching to security successively and always focused to one area and ensure correct deficiencies. In case of any problem they are flexible and immediately solve this issue.

Data security must be in advanced level because the Zlín branch is connected to other branches of Technodat in the Czech Republic and Slovakia via VPN. Without adequate security there could be the potential threat which could spread throughout the network and cause major problems. The company could become untrustworthy and lose its position on the Czech market. The company cooperates with several foreign companies and is a supplier of well known companies Škoda auto and Honeywell so a loss of credibility could be crucial.

The biggest security hole is server security. The server room is not air-conditioned and is not specially made for ideal conditions. Door to the room is locked indeed. But the key could be borrowed by anybody without checking and registering. The data on servers is not encrypted so there is possible interception. The only one encrypted is economic software. However administrators know about these problems and planned the new data center which will meet all security rules. The room is going to be in the new building in the neighborhood.

SEZNAM POUŽITÉ LITERATURY

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

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

[3] PETERKA, Jiří. Aktivní síťové prvky - co jsou a k čemu slouží. *Computerworld*: *Ucelený informační zdroj pro IT profesionály*. Praha: IDG Czech, a.s, 1994, č. 38. ISSN 1210-9924. Dostupné z: http://www.earchiv.cz/a94/a438c500.php3

[4] PETERKA, Jiří. Privátní vs. veřejné sítě. *Chip-week*: *Počítačový týdeník*. Praha: Vogel Publishing, 1996, č. 17. ISSN 1211-1007. Dostupné z: http://www.earchiv.cz/a96/a617k150.php3

[5] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 80-731-8095-2.

[6] Lehký úvod do problematiky podnikových informačních systémů. *BusinessIT.cz* [online]. 2011, č. 10 [cit. 2012-05-20]. ISSN 1805-0522. Dostupné z: http://www.businessit.cz/cz/podnikovy-informacni-system-uvod-moduly-funkce-nasazeni-vyber.php

[7] *TECHNODAT, CAE - systémy, s.r.o.* [online]. 1992-2012 [cit. 2012-04-12]. Dostupné z: http://www.technodat.cz

[8] *MikroTik* [online]. 2007-2012 [cit. 2012-04-12]. Dostupné z: http://www.mikrotik.cz

[9] HON, Petr. Jak funguje řízení datových toků s QoS. *Connect!*: *odborný měsíčník pro komunikace, počítačové sítě a otevřené systémy* [online]. 2012, č. 1 [cit. 2012-04-12]. ISSN 1211-3085. Dostupné z: http://connect.zive.cz/clanky/jak-funguje-rizeni-datovych-toku-s-qos/sc-320-a-161738

[10] JAŠEK, Roman. *Proces implementace poznatků informační bezpečnosti do informační bezpečnosti podniku a vysokoškolské výuky*. Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 2005. Habilitační práce.

[11] HASSELL, Jonathan. Wireless Attacks and Penetration Testing. *SecurityFocus* [online]. 2010 [cit. 2012-05-12]. Dostupné z: http://www.securityfocus.com/infocus/1783

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access point
DDR	Double data rate
DHCP	Dynamic host configuration protocol
DDoS	Distributed denial of service
DoS	Denial of service
DNS	Domain name server
HW	Hardware
IP	Internet protocol
IT	Information technology
LAN	Local area network
MAC	Media access control
PoE	Power over ethernet
PGP	Pretty good privacy
QoS	Quality of service
RAM	Random access memory
SQL	Structured query language
SSID	Service set identifier
SW	Software
UPS	Uninterruptible power source (supply)
VOIP	Voice over internet protocol
VPN	Virtual private network
Wi-Fi	Wireless fidelity

SEZNAM TABULEK