VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

NÁVRH A ZAVEDENÍ BEZPEČNOSTNÍCH OPATŘENÍ PRO SPOLEČNOST GEFCO ČESKÁ REPUBLIKA, S.R.O

DESIGN AND IMPLEMENTATION SECURITY MEASURES FOR GEFCO ČESKÁ REPUBLIKA, S.R.O

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — JAKUB VODIČKA
AUTHOR

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

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Vodička Jakub

Manažerská informatika (6209R021)

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

Návrh a zavedení bezpečnostních opatření pro společnost GEFCO ČESKÁ REPUBLIKA, s.r.o

v anglickém jazyce:

Design and Implementation Security Measures for GEFCO ČESKÁ REPUBLIKA, s.r.o

Pokyny pro vypracování:

Úvod
Cíle práce
Analýza současného stavu
Teoretická východiska práce
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Seznam odborné literatury:

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Computer Press, 2004, 192 s. ISBN 978-80-251-0106-1
HORÁK, J. Bezpečnost malých počítačových sítí. GRADA, 2003, 200 s. ISBN 978-80-247-0663-6.
HORÁK, J. a M. KERŠLÁGER. Počítačové sítě pro začínající správce. Computer Press, 2008, 328 s. ISBN 978-80-251-2073-6.
LUDVÍK, M. a B. ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Computer Media, 2008, 98 s. ISBN 978-80-866-8635-3.
NORTHCUTT, S. Bezpečnost počítačových sítí. Computer Press, 2005, 592 s. ISBN 978-80-251-0697-7.
PROSISE, CH. a K. MANDIA. Počítačový útok - detekce, obrana a okamžitá náprava. Computer Press, 2002, 410 s. ISBN 80-722-6682-9.

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

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2014/2015.

L.S.

doc. RNDr. Bedřich Půža, CSc. Ředitel ústavu	doc. Ing. et Ing. Stanislav Škapa, Ph.D. Děkan fakulty

V Brně, dne 28.2.2015

Abstrakt

Bakalářská práce pojednává o problematice bezpečnostních opatření ve společnosti GEFCO ČESKÁ REPUBLIKA, s.r.o. Nastíněno je zde teoretické pozadí, na které navazuje analýza současného stavu, následně návrhy a zavedení bezpečnostních opatření vedoucí ke zlepšení stávající úrovně zabezpečení.

Abstract

Bechelor’s thesis deal with security measure issues in GEFCO CESKA REPUBLIKA, s.r.o. It’s contain theoretical background, which is connected with analysis of current condition. Afterwards design and implementation security steps to improvement current quality of security protection.

Klíčová slova

informace, riziko, hrozba, bezpečnost, bezpečnostní opatření, zabezpečení informací, zabezpečení dat, bezpečnost informačních technologií, počítačová bezpečnost

Keywords

information, risk, threat, security, security arrangement, security of information, security of data, security of information technology, computer security

Bibliografická citace

VODIČKA, J. *Návrh a zavedení bezpečnostních opatření pro společnost GEFCO ČESKÁ REPUBLIKA, s.r.o.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. 57 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že předložená bakalářská práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 31. května 2015

.....

podpis studenta

PODĚKOVÁNÍ

Rád bych poděkoval vedoucímu bakalářské práce Ing. Viktoru Ondrákovi Ph.D. za cenné rady a čas, který mi věnoval. Dále patří velké poděkování kolegům ze společnosti za spolupráci a rodině za podporu a pomoc.

OBSAH

ÚVOD

Můžeme říci, že informace jsou dnes jednou z nejcennějších věcí, se kterou můžeme manipulovat. Dvojnásob toto pravidlo platí pro množství informací, které můžeme jakýmkoliv způsobem spojit s dalším výnosem či zneužitím. Z tohoto důvodu je zcela přirozené a nutné tyto informace co nejvíce chránit před únikem a následným zneužitím. Konkrétně je tím mířeno na informace a data uvnitř podniku. Data mající obchodní, ale také historický, osobní či dlouhodobý charakter. Všechna taková data lze zneužít či jakýmkoliv jiným způsobem poškodit je nebo jejich vlastníka. Dále bude práce zaměřena nejen na hrozby a rizika, které působí zvenčí ale také na ty, které mohou vzniknout uvnitř firmy. Častější a čím dál více rozšířené jsou právě ty, vznikající či působící zevnitř organizace. S tímto jsou často z velké části spojeni zaměstnanci neboli uživatelé, kteří s těmito daty pracují a využívají je. Tito uživatelé představují pro firmu jednu z největších hrozeb. Neopomínám zde proto činnosti spojené se školením uživatelů a právní opatření proti takovýmto potencionálním útočníkům. Následují návrhy, zavedení, či implementace opatření, vedoucí ke zvýšení úrovně zabezpečení dílčích částí informačního systému.

CÍLE PRÁCE

Cílem bakalářské práce je návrh a následné zavedení jednotlivých bezpečnostních opatření pro brněnskou pobočku společnosti GEFCO ČESKÁ REPUBLIKA, s.r.o. Praktickým přínosem je zvýšení celkové úrovně zabezpečení informačních technologií ve společnosti. Popsána zde jsou jak teoretická východiska, tak konkrétní návrhy řešení, případně jejich aplikace. Jako podklad a prostředek pro navrhnutí jednotlivých opatření je analýza dílčích částí informačního systému, podrobná analýza aktiv, hrozeb, rizik a matice zranitelnosti.

1 ANALÝZA SOUČASNÉHO STAVU

V této části práce se zaměřuji na analýzu dílčích částí informačního systému společnosti, dále na analýzu aktiv, rizik a hrozeb. Analýza je v tomto případě nezbytně nutná a poslouží jako podklad pro návrh jednotlivých bezpečnostních opatření, které povedou ke zvýšení celkové úrovně zabezpečení.

1.1 Základní informace o společnosti

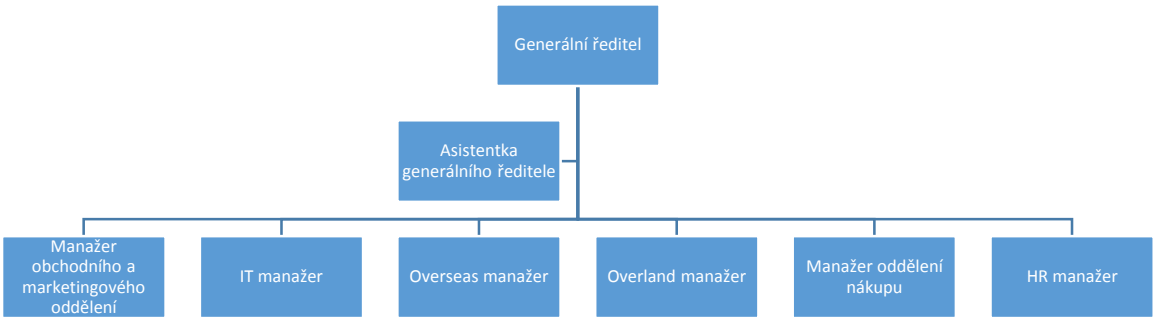
GEFCO ČESKÁ REPUBLIKA, s.r.o. patří mezi jednu z největších logistických společností nejen u nás, ale na celém světě. Nabízí širokou škálu služeb od klasické automobilové nákladní přepravy přes leteckou a námořní až po speciální druhy přeprav vojenských zařízení či vysoce cenných zásilek. GEFCO ČESKÁ REPUBLIKA, s.r.o. patří do skupiny GEFCO GROUP, která sdružuje veškeré pobočky, rozmístěné po celém světě. Po České republice je rozmístěno celkem 6 poboček a to v Praze, kde sídlí vedení společnosti, dále v Říčanech u Prahy, Kolíně, Brně, Ostravě a Otrokovicích. V České republice společnost zaměstnává zhruba 350 zaměstnanců.

Obr. 1 - Mapa poboček v ČR
Zdroj: GEFCO ČR

Organizační struktura

Organizační struktura společnosti, jak je vidět na obrázku níže, je příkladem typické funkční organizační struktury. Lidé jsou zde tedy seskupováni dle funkcí, které zastávají a mají jednoho, jasně daného nadřízeného. V čele společnosti je generální ředitel pro Českou republiku a je jediným nadřízeným všech manažerů příslušných oddělení, kterými jsou např. oddělení financí, marketingu a prodeje, lidských zdrojů či IT oddělení.

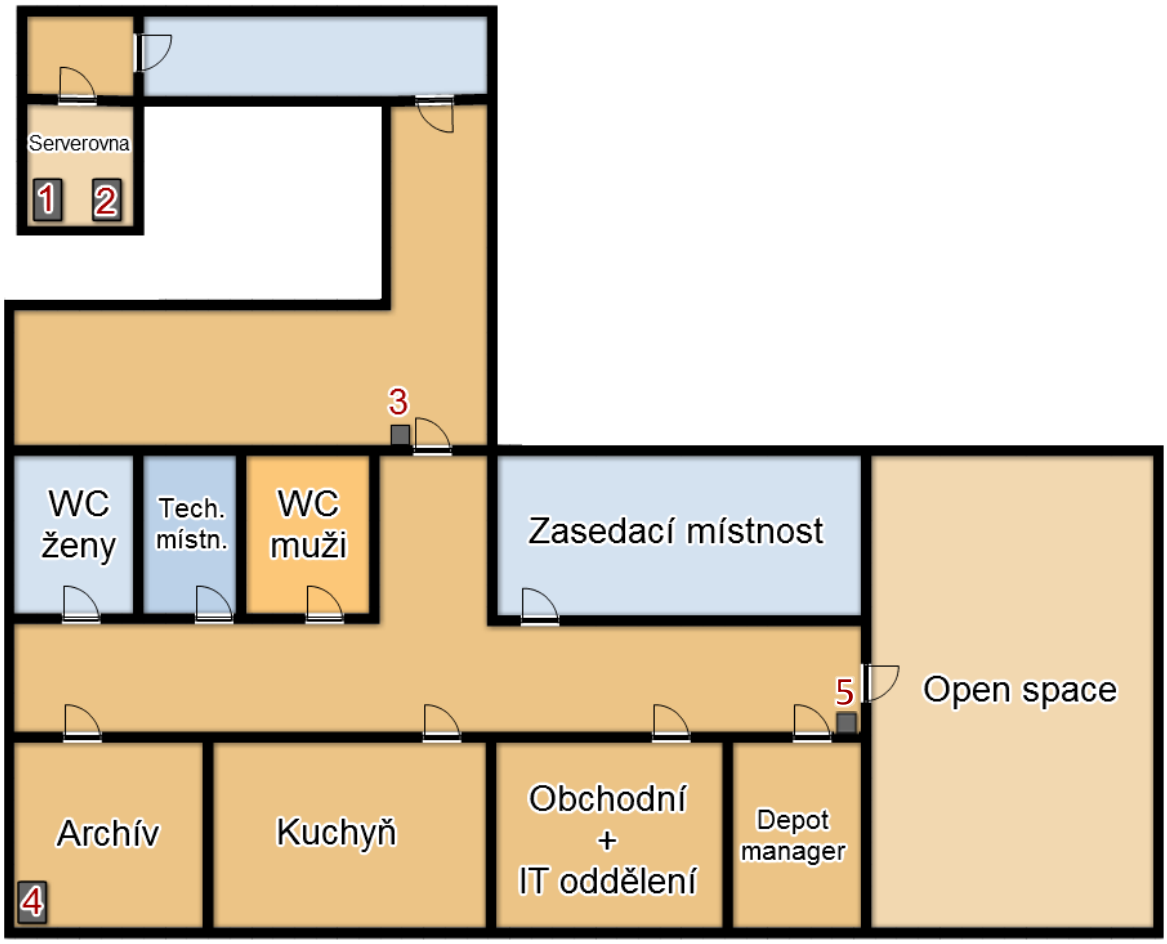
Oblast informační bezpečnosti není přímo začleněna v organizační struktuře. Není zde žádná osoba přímo odpovědná za tuto oblast. Řešení je pouze na korporátní úrovni, kde je jmenován CISO (Chief information security officer). Veškeré informace, změny a nařízení jsou distribuována pomocí lokálního IT oddělení k uživatelům.



Obr. 2 - Organizační struktura managementu společnosti
Zdroj: Vlastní zpracování

Charakteristika analyzované oblasti

Analýza bude prováděna na brněnské pobočce společnosti, a to na adrese Kšírova 255, Brno. Pobočku lze rozdělit na tři základní části, a to na sklad, kanceláře a serverovou místnost. Kancelářské prostory tvoří celkem 3 kanceláře, zasedací místnost, kuchyňka, archív a toalety. Odděleně je umístěna kancelář pro pracovníky skladu. Ta se nachází ve skladovacích prostorech objektu na opačné straně budovy, než jsou kanceláře. Tyto prostory o rozloze zhruba 3000 m^2 slouží k manipulaci se zásilkami či jejich skladování. Serverová místnost je v budově pouze jedna a je mezi společnostmi ELKOV a GEFCO sdílena.



Obr. 3 - Půdorys objektu
Zdroj: Vlastní zpracování

- 1 – umístění všech aktivní prvků (firewall, switche, routery) v rozvaděčové skříni
- 2 - umístění aplikačního a datového serveru v rozvaděčové skříni
- 3 – hlavní vchod do kancelářských prostor
- 4 – umístění NAS (netword attached storage)
- 5 – umístění AP (access pointu)

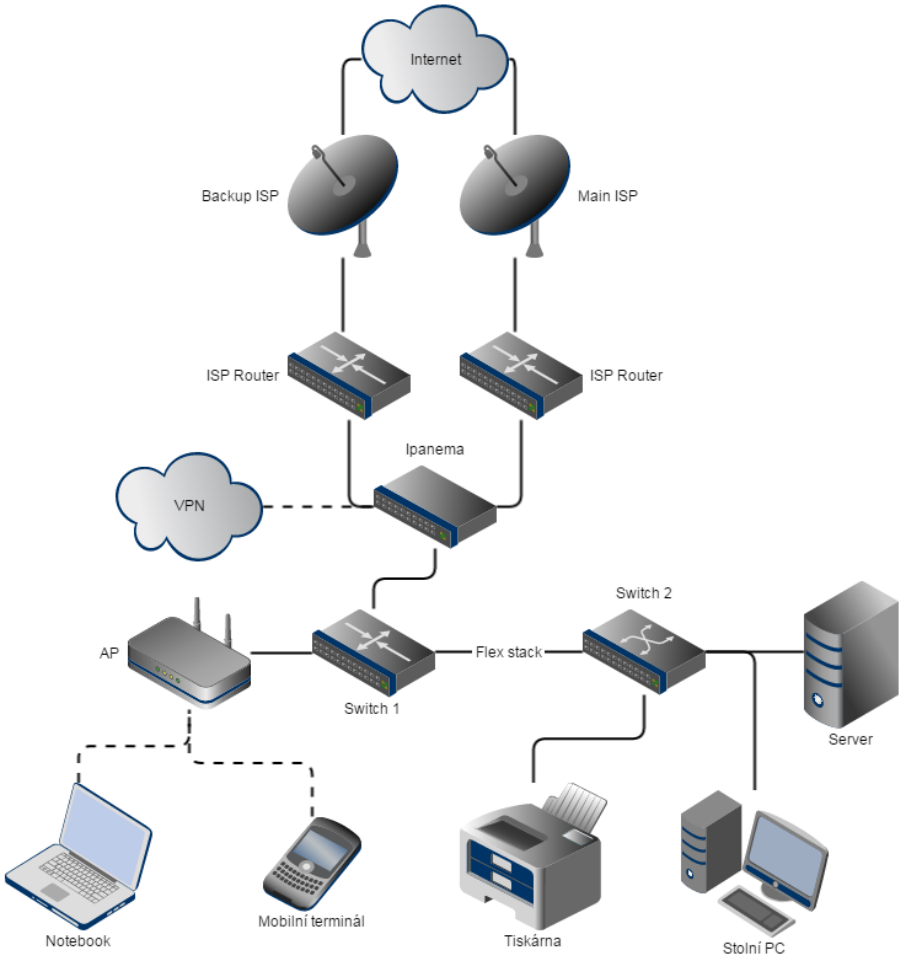
Vstup do kancelářských prostor (na obrázku č. 3) je zabezpečen čtečkou čipových karet, kterou zaměstnanci používají ke vstupu. Vstupní dveře jsou osazeny elektronickým zámkem. V případě návštěvy, lze dveře otevřít vzdáleně, zadáním kódu, za pomoci IP telefonní ústředny. Veškeré ostatní vstupy, včetně vstupu do serverovny, jsou chráněny pouze vstupem na klíč. Momentálně není v kancelářských prostorech instalován žádný zabezpečovací ani kamerový systém. Mimo pracovní dobu je budova chráněna pracovníkem bezpečnostní agentury.

1.2 Počítačová síť

Podkapitola počítačová síť popisuje strukturu sítě, použité technologie v síti, dále způsob přístupu k síti Internet a také síť VPN.

Struktura počítačové sítě

Místní počítačovou síť lze označit jako síť LAN s hvězdicovou topologií. V dnešní době je ovšem těžké definovat rozsah takové sítě. LAN neboli local area network značí počítačovou síť pokrývající menší geografické území, což do modelu jedné pobočky firmy poměrně dobře zapadá. Jedná se o jednu síť typu L3.



Obr. 4 - Struktura počítačové sítě
Zdroj: Vlastní zpracování

Sekce kabeláže

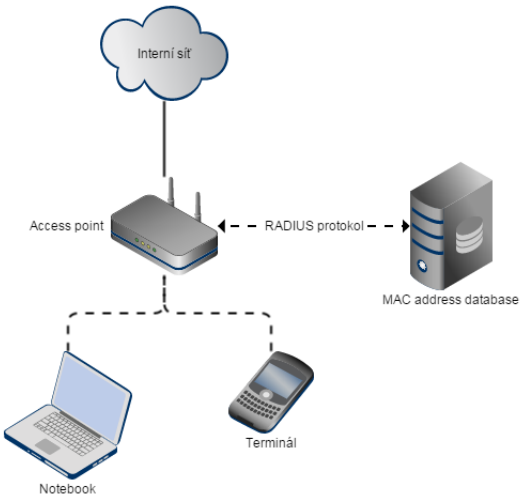
Rozvaděč, umístěný v serverové místnosti, je zabezpečen pomocí klasického rozvaděčového zámku na klíč. Serverová místnost není opatřena žádným zabezpečovacím systémem a vstup zde není monitorován. Přístup je tedy pouze na klíč.

Propojení páteřní sekce s rozvaděčem je realizováno optickým vedením. Horizontální a pracovní sekce obsahuje UTP kabeláž (nestíněnou kroucenou dvojlinku) třídy 5e s PVC pláštěm. Využit je standard přenosů 1000Base-T (Gigabit Ethernet).

Zásuvky v pracovní sekci jsou umístěny v parapetních lištách podél stěn v místnostech a osazeny vždy dvěma konektory RJ-45. Každá zásuvka je očíslována a porty jsou rozlišeny písmeny A, B.

Technologie Wi-Fi

Technologii Wi-Fi využívají pro komunikaci nejen notebooky, ale zejména mobilní terminály Motorola MC7596, MC75A6. Funkční komunikace těchto zařízení v sítí je pro společnost klíčová. Přístupové body jsou značky Cisco. Zařízení jsou již staršího typu, jedná se o Cisco Air-AP1131AG. Využívá se přenosová technologie IEEE 802.11g. Pro zvýšení bezpečnosti je zamezeno vysílání SSID. K zabezpečení Wi-Fi je použit bezpečnostní standard IEEE 802.1x. Při připojení do sítě se provádí autentizace za pomoci RADIUS protokolu, který ověří, zda se fyzická adresa zařízení (MAC adresa) nachází v databázi RADIUS serveru. Tento server je umístěn na centrální pobočce ve



Obr. 5 - Princip bezdrátového připojení
Zdroj: Vlastní zpracování

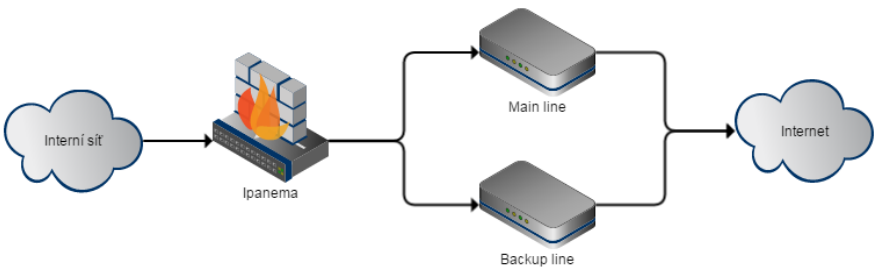
Francii. Pokud ano, zařízení se připojí do interní sítě. Obrázek výše ilustruje princip bezdrátového připojení do sítě.

Síť VPN

Vybraným zaměstnancům je umožněna práce v interní síti i mimo kancelář. Pro přístup do interní sítě je umožněn vzdálený přístup. Tento přístup je realizován pomocí sítě VPN (virtual private network). Klient, který je využit pro toto připojení, se nazývá CheckPoint Endpoint Connect. Využívá se zde bezpečnostní protokol IPsec, pro autentizaci a šifrování. Připojení zajistí pomocí tunelu zabezpečenou šifrovanou komunikaci při využití „nedůvěryhodné“ sítě. Pro navázání komunikace je využita dvoufázová autentizace, kdy se uživatel přihlašuje pomocí uživatelského jména a hesla, navíc je vybaven tokenem SecurID. Bránu VPN tvoří zařízení Check Point UTM-1 Edge N. Uživatel má při tomto vzdáleném připojení přístup k veškerým službám, stejně jako by byl připojen v interní síti společnosti, tzn. na síťové disky, ke korporátním systémům či intranetu.

Přístup k internetu

Bezchybná funkčnost interní sítě, ale také přístupu k internetu, jsou pro chod společnosti klíčové. Pobočka je vybavena jednou hlavní a jednou záložní linkou pro datovou komunikaci a to od různých poskytovatelů. Záložní linka je využívána primárně pro emailovou komunikaci. Ostatní služby spadají pod hlavní linku. Tyto dvě linky sdružuje zařízení zvané ipanema IP engine 05ax. Zařízení podporuje služby Applications



Obr. 6 - Schéma přístupu k internetu
Zdroj: Vlastní zpracování

Visibility pro monitorování a reporting provozu, dále QoS & Control, WAN Optimization, Dynamic WAN Selection a Network Rightsizing. Na základě využití jednotlivých služeb je zajištěno rovnoměrné vytížení linek.

1.3 Hardware

V této kapitole jsou popsána hardwarová zařízení využívaná ve společnosti. Jsou to notebooky, pracovní stanice, mobilní terminály, síťové tiskárny, IP telefony a datová úložiště.

Pracovní stanice

Na pracovních stanicích je instalován operační systém Windows 7 Enterprise. Každý uživatel má vytvořen uživatelský účet v Active Directory a je registrován v doméně. Nastaveny má přístupy a práva pouze do těch složek, se kterými pracuje. Pro přidělení dodatečných práv uživateli je nutné schválení nadřízeným pracovníkem společně s pracovníkem IT, odpovědným za přístupová práva. Antivirová ochrana je zajištěna softwarem Officescan – Endpoint Protection. Software zajišťuje ochranu proti malwaru, rootkitům, cíleným C&C útokům, provádí také skenování složek Microsoft Outlook. Nastaveno je automatické uzamčení pracovní stanice po 5 minutách nečinnosti.

Mobilní terminály

Mobilní terminály plní mezi veškerými zařízeními jednu z nejdůležitějších funkcí. Terminály značky Motorola MC7596, MC75A6 jsou využívány řidiči při přepravě samotných zásilek. Terminály Motorola MC3190 jsou využity pro potřeby skladníků, tzn. při operaci se zásilkami. Tyto terminály disponují jak možností připojení do interní sítě pomocí Wi-Fi, tak i možností připojení přes mobilní GSM síť, což ovšem přináší zpomalení práce se zařízením. Všechna tato zařízení jsou tedy vybavena SIM kartou s datovým tarifem.

Mobilní telefony

Výhoda vybavení zaměstnance firemním telefonem s sebou nese i značné nevýhody, možná až hrozby. Jelikož firma by bez mobilních telefonů v podstatě nemohla fungovat, je nutné veškeré zaměstnance, kteří mobilní telefony k práci potřebují, tímto zařízením vybavit. S přicházející érou tzv. „chytrých“ mobilních telefonů, neboli smartphonů, nechce být firma pozadu, proto se snaží při nákupu takové zařízení volit. A to nejen z důvodu reprezentace, ale také např. pro využití synchronizace a přístupu k účtu Microsoft Exchange. Synchronizace dat v mobilním telefonu s aplikací Outlook je obrovskou výhodou. Bezdrátové připojení mobilních telefonů do interní sítě pomocí Wi-Fi není možné. Připojení mobilních telefonů k počítači či notebooku už firma efektivně eliminovat nedokáže.

IP telefony

Většina stálých, interních zaměstnanců je mimo mobilních telefonů vybavena také pevným stolním telefonem. Tyto pevné linky komunikují pomocí protokolu VoIP (Voice over Internet Protocol) a jsou sdružovány pomocí virtuální ústředny IP centrex do jedné hlasové sítě. Do této telefonní sítě jsou připojeny veškeré pevné linky na všech pobočkách v České republice. Pro tyto IP telefony je v serverovně vyhrazen samostatný přepínač (switch). Velkou výhodou při tomto řešení je možnost využití technologie PoE (Power over Ethernet), tedy napájení telefonů pomocí sítě resp. pomocí technologie Ethernet. Tím je ušetřeno místo v elektrické síti a případný nadbytek kabeláže. Další výhodou je možnost administrace všech telefonů pomocí webového rozhraní, kde je možnost nestavení přesměrování, volání pouze uvnitř podnikové sítě, zakázání vybraných předvoleb či při komunikaci v podnikové síti zobrazit jméno volajícího namísto telefonního čísla. Jako poslední lze zmínit možnost konferenčních hovorů, pro které je zasedací místnost vybavena speciálním konferenčním telefonem Polycom SoundStation2.

Síťové tiskárny

Celkem je na pobočce 7 síťových tiskáren. Všechny tiskárny jsou do sítě připojeny kabelem a mají nastavenu statickou IP adresu. Při běžném tisku je komunikace s tiskárnou realizována lokálním tiskovým serverem. Pokud probíhá tisk z informačního systému INES, je tisk řízen centrálním tiskovým serverem. Pro tento tisk je zde samostatná tiskárna.

Datová úložiště

Na pobočce jsou 2 servery umístěné v serverové místnosti a jedno úložiště typu NAS (network attached storage) umístěné v místnosti nazvané archív. Server Dell T610, s operačním systémem Windows Server 2008 R2 plní roli aplikačního serveru a běží na něm aplikační služby. Například docházkový systém či přepravní software RAAL. Server Dell T420, taktéž s operačním systémem Windows Server 2008 R2 zajišťuje souborové a tiskové služby. Server slouží zejména jako datové úložiště pro pobočku. Datové úložiště typu NAS značky Synology, typ DS211j, plní roli zálohovacích služeb. Je místem pro zálohu uživatelských dat. Datová úložiště umístěná v serverovně jsou ochráněna proti výpadku proudu záložním zdrojem společným pro společnost GEFCO i ELKOV. Jedná se o záložní zdroj APC Smart-UPS 3000VA.

1.4 Software

V následující kapitole je popsán software, který je ve společnosti využíván. Bude popsán jak z pohledu uživatelského, tak i z pohledu administrace a správy. Využití aplikací se liší dle pracovní náplně zaměstnance.

Každá pracovní stanice je předána uživateli plně funkční, s nainstalovaným operačním systémem. Využívaným operačním systémem na všech noteboocích a stolních počítačích je Microsoft Windows 7 verze Enterprise. Společně se systémem je nainstalován základní balíček programů, a to např. balíček Microsoft Office, antivirový software Office Scan Endpoint Protection, doplněk Microsoft Silverlight apod.

Run Advertised Programs

Důležitou součástí každé stanice je ovládací panel Run Advertised Programs. Tato nabídka umožňuje uživatelům dodatečně instalovat programy, které jsou korporátně povoleny a přidány do tohoto seznamu. Uživatel může na stanici instalovat tyto programy bez povolení správce. Nabídka obsahuje programy, které pro svoji práci potřebuje. Jsou to např. Notepad++, Microsoft Skype, Mozzila Firefox, PDF Creator apod. nebo také korporátní aplikace jako jsou NOSTRA, NOMAD či Uniprint. Taktéž je možné zde programy z počítače jednoduše odebrat (odinstalovat). Tyto instalace se obvykle dějí na pozadí. Pokud je nutné instalovat software, neuvedený v tomto seznamu, je nutné s tímto požadavkem kontaktovat oddělení IT. Uživatel nemá přidělena práva pro instalaci dodatečného softwaru.

Informační systémy

V této kapitole jsou popsány informační systémy, které jsou ve společnosti využívány. Jsou to zejména korporátní aplikace a informační systém, vyvinuty či speciálně upraveny pro společnost GEFCO a využívány na pobočkách po celém světě.

INES

INES je francouzský informační systém vyvinutý speciálně pro požadavky společnosti GEFCO. Systém by měl být intuitivní a pokrýt veškeré požadavky na logistické funkce. Je napojen na další systémy, jako jsou SAP, OMS či systém pro řízení tisku GEFPrint. Tento systém zastřešuje veškeré funkce týkající se přepravy, tedy tvorbu objednávek, jejich evidenci a správu. Pro chod společnosti je tento IS klíčový a nelze bez něj efektivně vykonávat práci. Tento software je, jako většina korporátních aplikací, virtualizován. Využívá se formou tenkého klienta. Spouštění se provádí pomocí webového portálu Citrix Web Interface.

CADIS

CADIS je software využívaný zejména v mobilních terminálech pro sběr informací o zásilkách, jejich aktuální poloze, skladování apod. Na stolních počítačích i terminálech je k dispozici tenký klient pro administraci jednotlivých přeprav. Na terminálech pro řidiče a skladníky je instalována optimalizovaná verze pro mobilní PDA zařízení s operačním systémem Windows CE či 6.1.

SAP

SAP je známý a populární informační systém, stavějící na univerzálnosti využití. S tímto systémem je spojena drtivá většina firemních aplikací, zejména pro důvody účetnictví. Ve společnosti je využit zejména pro potřeby financí, evidence majetku a účetnictví, velice málo pak pro evidenci skladování.

1.5 Data

V této kapitole jsou popsána data ve společnosti z hlediska jejich umístění, dostupnosti, způsobu ukládání, zabezpečení, klasifikace apod. Data představují pro firmu jedno z nejcennějších aktiv. Jedná se o data jednotlivých uživatelů, data umístěná na serveru a mezi jedny z nejdůležitějších a zároveň nejproblematičtější patří e-maily, tedy elektronická komunikace a její archivace.

Klasifikace dat

Momentálně neexistuje žádné pravidlo ani směrnice, která by klasifikovala data a nakládání s nimi dle jejich důvěrnosti. Pevně definována je pouze první úroveň stromové struktury složek na síťovém disku. Struktura je tvořena složkami jednotlivých pracovních oddělení. Uživatelé mají automaticky přístup pouze do složky svého oddělení.

Uživatelská data

Každý uživatel potřebuje ke své práci určité množství dat, souborů, se kterými pracuje, ze kterých při práci vychází, čerpá apod. Ty, které využívá pouze dočasně např. pro poznámky, záznamy během dne či pro dočasné úpravy, bývají obvykle uloženy na pevném disku vlastního zařízení. Veškerá ostatní data, výhradně určená pro práci, by uživatelé měli mít uloženy na serveru, v příslušné složce. Tato skutečnost ovšem představuje jeden z velkých problémů vzhledem k pohodlnosti uživatelů, kteří neradi pracují s daty uloženými na serveru z důvodu pomalejší práce s takto uloženými daty. Proto tato doporučení nerespektují a i důležité soubory zůstávají pouze na disku samotného zařízení.

Sdílená data

Velice často se pracuje se soubory, které jsou sdíleny mezi více uživateli. Takové soubory jsou uloženy na jednom z datových úložišť (obvykle souborovém serveru či NAS), dle toho, pod kterou pobočku spadají. Při práci s takto umístěnými daty přichází některá úskalí, jako je např. výrazné zpomalení přístupu k souboru během jeho čtení mezi více uživateli, nebo v jeden okamžik může mít právo daný soubor upravovat pouze jeden uživatel, ostatní z něj mohou pouze číst. Jednoduše se tedy může stát, že si někdo soubor otevře pro úpravy a následně ho zapomene zavřít, v tu chvíli je soubor pro ostatní uživatele dostupný pouze ke čtení, nikoliv pro zápis.

1.6 E-maily

E-mailová komunikace představuje pro chod společnosti jednu z nejdůležitějších funkcí. Většina obchodních informací a jejich detaily jsou obvykle obsaženy v e-mailových zprávách. Proto je jednak důležitá neustálá funkční komunikace tohoto typu a také ukládání a archivace této komunikace. S tím je spojeno vytváření mailových archivů zejména z důvodu limitující velikosti uživatelské mailové schránky.

Využit je poštovní systém Microsoft Exchange. Tento systém umožňuje přístup skrze prostředí Microsoft Outlook, Outlook Web App či mobilní správu Exchange

ActiveSync. Všechny tyto formy přístupu jsou hojně využívány. Na pracovních stanicích je využíván Microsoft Outlook 2007. Komunikace běží na protokolu SMTP. K zabezpečení je využit SSP Microsoft Negotiate s protokolem NTLM. Ověřování pomocí tohoto protokolu probíhá na základě doménového jména, uživatelského jména a hashe uživatelského hesla. Ochrana poštovního systému je také filtrováním komunikace. Využíván je anti-spamový filtr, filtr příloh a firewall s pravidly pro komunikaci přes jednotlivé porty. Velikost zasílané přílohy je omezena na 12MB, velikost emailové schránky je omezena na 550MB.

1.7 Zálohování dat

Jak již bylo zmíněno, data představují pro firmu obvykle velice vysokou hodnotu. Proto je nutné jednak tyto data chránit a opatřit se proti jejich možné ztrátě. Příčiny ztráty dat mohou být různé, např. přírodní katastrofa, porucha hardware či selhání lidského faktoru. Se ztrátou dat mohou být spojeny velké škody. Proti takovým ztrátám se snaží společnost bránit zálohováním a archivací dat.

Zálohování stanic

Zálohování probíhá pomocí integrovaného softwaru ViSave. Task manažer zajišťuje automaticky jednou týdně vyskakovací okno, které uživatele vyzve k zálohování dat. Od uživatele je poté vyžadováno pouze potvrzení, přičemž je upozorněn na případné nedokončené operace v aplikaci MS Outlook, která bude ukončena. Následně se spustí proces zálohování, během kterého jsou nejdříve data zkomprimována a následně přesunuta do složky uživatele na úložišti NAS. Během zálohy nelze pracovat. Průměrná doba zálohy je 20 – 30 minut. Způsob zálohy je pokaždé úplnou (normální) formou, což sebou přináší vysokou časovou náročnost a poměrně velké vytížení sítě při zálohování více stanic zároveň. Nastaveny jsou výjimky ze zálohy pro přípony typu mp3, mp4, avi či wmv.

Pokud uživatel stolního počítače zmešká upozornění na zálohu, objeví se upozornění při příštím přihlášení. Větší problém nastává při zálohování přenosných zařízení, tedy notebooků. Zálohovat je totiž možné pouze při připojení v interní síti. Je

tedy naprosto běžné zmeškat či nemožnost zálohovat, pokud se nacházíte mimo pobočku, což se u těchto uživatelů (např. obchodních zástupců či manažerů) předpokládá. Při úspěšném dokončení zálohy je stará záloha přemazána zálohou novou. Uchovávána je tedy vždy pouze poslední, úspěšně dokončená záloha. Neexistuje ovšem žádná směrnice ani pravidlo, které by nařizovalo uživatelům tuto zálohu provádět.

Zálohování datových úložišť

Veškerá data z uživatelských stanic jsou zálohována na úložiště typu NAS. Toto úložiště je ale potřeba také zálohovat. Na datovém úložišti NAS je využita služba, která umožňuje zálohu úložiště, ta je prováděna vždy jednou za den na jednu pracovní stanici.

Data umístěná na serveru jsou replikována na virtuální server, které je možné pro případ nefunkčnosti fyzického serveru využívat. Dále je prováděna záloha v každodenním intervalu v délce jednoho týdne. Je tedy možné zpětně obnovit a dohledat data v každém dni posledního týdne, poté za každý předchozí týden v délce jednoho měsíce a za každý měsíc jednoho roku.

Plán obnovy

Neexistuje momentálně žádný plán obnovy, který by definoval kroky, jak při nutnosti obnovy postupovat. Veškeré činnosti jsou v případě mimořádné události prováděny operativně. Není definován ani žádný plán nouzového provozu pro případné udržení kritických procesů firmy pro dobu nezbytně nutnou, dokud nedojde ke kompletnímu obnovení systému.

1.8 Analýza aktiv

Pro navrhnutí bezpečnostních opatření je nutné určit aktiva, na která je nutné návrhy zaměřit. U každého aktiva je určena jeho integrita, důvěrnost a dostupnost dle načerpaných informací v podniku. K ohodnocení bude použita škála 1 – 5 (hodnotou 5 jsou označeny nejvíce důležitá aktiva).

Tab. 1 - Velikost dopadu
Zdroj: Vlastní zpracování na základě konzultace se zaměstnanci

Velikost dopadu na organizaci	
Žádný dopad	1
Zanedbatelný dopad	2
Finanční ztráty či potíže	3
Vážné potíže či podstatné finanční ztráty	4
Existenční potíže	5

Tab. 2 - Hodnocení aktiv
Zdroj: Vlastní zpracování na základě pracovněprávního vztahu

Aktivum	**Integrita**	**Důvěrnost**	**Dostupnost**	**Hodnota**
Hardware	4	5	4	**4**
Software pro evidenci přeprav	4	2	4	**3**
Software pro mobilní terminály	4	2	4	**3**
Software pro fakturaci	3	2	2	**2**
Data o zákaznících	3	1	1	**2**
Data o přepravách	2	1	1	**1**
Obchodní data	4	4	3	**4**
Elektronická pošta	4	4	5	**4**
Hlasové služby	4	4	5	**4**

Výše uvedená tabulka představuje způsob ohodnocení aktiv dle celkové velikosti dopadu, při narušení některého z bezpečnostních faktorů, na organizaci. Výsledná hodnota představuje aritmetický průměr ze tří uvedených bezpečnostních faktorů.

1.9 Analýza hrozeb

V následující tabulce jsou zobrazeny pravděpodobnosti výskytu hrozeb ve stupnici 1 – 5. Dále tabulka č. 4 obsahuje výčet hrozeb včetně pravděpodobností jejich výskytu.

Tab. 3 - Pravděpodobnost výskytu hrozby
Zdroj: Vlastní zpracování

Pravděpodobnost výskytu hrozby	
Velmi nízká	1
Nízká	2
Střední	3
Vysoká	4
Velmi vysoká	5

Tab. 4 - Analýza hrozeb
Zdroj: Vlastní zpracování na základě pracovněprávního vztahu

Hrozba	Pravděpodobnost
Přírodní	
Požár	3
Povodeň	1
Technické	
Přerušení dodávky elektřiny	2
Přerušení internetového připojení	3
Selhání HW	2
Ztráta dat	2
Selhání komunikace	2
Lidské	
Krádež	4
Neoprávněný přístup k informacím	3
Neoprávněný přístup do aplikace	2
Zneužití informací	3
Neodborná manipulace	4
Vymazání dat	4
Zapomenutí	4

1.10 Matice zranitelnosti

Hodnota zranitelnosti představuje součet mezi pravděpodobností výskytu hrozby a hodnotou daného aktiva. Spočteny jsou pouze reálně se vyskytující kombinace.

Tab. 5 - Matice zranitelnosti
Zdroj: Vlastní zpracování

Matice zranitelnosti	Pravděpodobnost výskytu	Hardware	Software pro evidenci přeprav	Software pro mobilní terminály	Software pro fakturaci	Data o zákaznících	Data o přepravách	Obchodní data	Elektronická pošta	Hlasové služby
Hodnota aktiva		4	3	3	2	2	1	4	4	4
Požár	3	7				5	4	7		7
Povodeň	1	5				3	2	5		5
Přerušení dodávky elektřiny	2	6	5	5	4	4	3	6	6	6
Přerušení internetového připojení	3		6	6	5		4		7	7
Selhání HW	2	6	5	5	4				6	
Ztráta dat	2		5	5	4	4	3	6	6	6
Selhání komunikace	2		5	5	4		3	6	6	6
Krádež	4	8				6	5	8	8	
Neoprávněný přístup k informacím	3		6	6	5	5	4	7	7	7
Neoprávněný přístup do aplikace	2		5	5	4				6	
Zneužití informací	3		6	6	5	5	4	7	7	7
Neodborná manipulace	4	8	7	7	6					
Vymazání dat	4		7	7	6	6	5	8	8	
Zapomenutí	4	8				6	5	8	8	
SUMA		**48**	**57**	**57**	**47**	**44**	**42**	**68**	**75**	**51**

1.11 Analýza rizik

Hodnota rizika = hodnota aktiva * pravděpodobnost výskytu hrozby * zranitelnost aktiva

Tab. 6 - Analýza rizik
Zdroj: Vlastní zpracování

Analýza rizik	Pravděpodobnost výskytu	Hardware	Software pro evidenci přeprav	Software pro mobilní terminály	Software pro fakturaci	Data o zákaznících	Data o přepravách	Obchodní data	Elektronická pošta	Hlasové služby
Hodnota aktiva		4	3	3	2	2	1	4	4	4
Požár	3	84	0	0	0	30	12	84	0	84
Povodeň	1	20	0	0	0	6	2	20	0	20
Přerušení dodávky elektřiny	2	48	30	30	16	16	6	48	48	48
Přerušení internetového připojení	3	0	54	54	30	0	12	0	84	84
Selhání HW	2	48	30	30	16	0	0	0	48	0
Ztráta dat	2	0	30	30	16	16	6	48	48	48
Selhání komunikace	2	0	30	30	16	0	6	48	48	48
Krádež	4	128	0	0	0	48	20	128	128	0
Neoprávněný přístup k informacím	3	0	54	54	30	30	12	84	84	84
Neoprávněný přístup do aplikace	2	0	30	30	16	0	0	0	48	0
Zneužití informací	3	0	54	54	30	30	12	84	84	84
Neodborná manipulace	4	128	84	84	48	0	0	0	0	0
Vymazání dat	4	0	84	84	48	48	20	128	128	0
Zapomenutí	4	128	0	0	0	48	20	128	128	0
SUMA		**584**	**480**	**480**	**266**	**272**	**128**	**800**	**876**	**500**

Z výše uvedené tabulky je zřejmé, že nejvyšší hodnoty rizik připadají na obchodní data a elektronickou poštu. Vysoká hodnota rizika působí také na hardware.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole budou popsána jednotlivá teoretická východiska, která v práci využiji, nebo jsou pro pochopení dané problematiky stěžejní. Jedná se o teorii potřebnou k alespoň částečnému porozumění problematice zabezpečení dat a informací.

2.1 Informační bezpečnost

Představa o tom, co jsou to obecně data, informace a k čemu slouží je klíčová pro pochopení dané problematiky. Proto budou tyto pojmy včetně dalších s nimi spojenými objasněny a vysvětleny v následujících podkapitolách.

Data

Data by měla představovat kvalitativní nebo kvantitativní reprezentaci skutečnosti. Reprezentaci v takovém formátu, se kterým lze dále operovat, zpracovávat jej či archivovat. Obvykle slouží k dalšímu zpracování lidmi či automatizovanými prostředky. (2, s. 6)

Přenos dat

Digitální komunikace či přenos dat je realizován za pomoci dvoubodového či vícebodového fyzického přenosového prostředí. Tímto prostředím přitom může být bezdrátový přenos, metalický či optický kabel. (1, s. 12)

„Přenos dat na fyzické vrstvě OSI komunikačního modelu je přenos informace vodičem změnou vhodné fyzikální veličiny“ (1, s. 13)

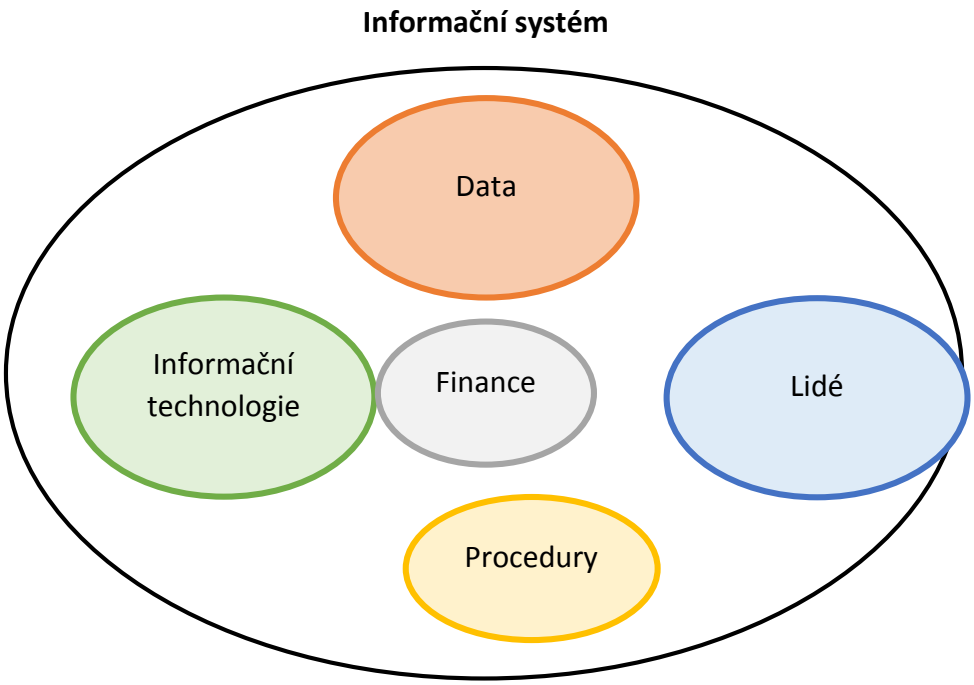
Informace

Informace v oblasti, na kterou se zaměřím lze interpretovat jako data v takovém formátu, který je dostatečně srozumitelný lidem. Takovéto informace mohou být jednak interní, např. informace o chodu podniku, či informace o zaměstnancích nebo budoucích

záměrech. Dále to mohou být informace většího formátu jako např. databáze či větší datové sklady. V neposlední řadě to mohou býti informace dostupné široké veřejnosti. To znamená informace veřejné, ke kterým by měl být volný přístup. (2, s. 7)

Informační systém

Naprosto správná a přesná definice pro informační systém neexistuje, záleží tedy obvykle na úhlu pohledu. Informační systém lze interpretovat jako soubor prvků, mezi kterými existují určité vazby, a zároveň je užíván uživatelem za účelem získání informací. Do takového informačního systému patří technické vybavení (hardware), programové vybavení (software), dále jsou to samotná data či informace a v neposlední řadě všichni uživatelé informačního systému. (2, s. 6)



Obr. 7 - Ilustrační schéma IS
Zdroj: Vlastní zpracování

Bezpečnostní faktory

Základními stavebními kameny pro zabezpečení informací je zajištění tří skutečností. Jako první je to **důvěrnost**. Pokud se budeme bavit o důvěrnosti informací, znamená to, že k informacím bude mít přístup pouze ten, kdo je k tomu oprávněn, jinak

řečeno, komu je přístup dovolen. Dále je to zajištění **dostupnosti** informací. Dostupnost znamená, že informace bude dostupná vždy, pokud to bude zapotřebí. Nedostupnost některých informací může být pro společnosti velice problematická a může způsobit nemalé ztráty. Jako poslední je třeba zajistit **integritu** informací, jinak řečeno celistvost. V praxi to znamená, že informace bude kompletní a nebude nijak pozměněna či modifikována. (2, s. 5)

2.2 Základní pojmy informační bezpečnosti

S bezpečností v organizacích jsou spojeny další důležité pojmy, se kterými se zde můžeme setkat. Vedle pojmů jsou tu i důležité procesy které je vhodné popsat. V neposlední řadě jsou to postupy a metodiky, které se v praxi často aplikují.

Aktivum

Aktivum je jiné vyjádření pro majetek. V informačním systému se jedná jak hmotný, tak nehmotný statek (majetek), který má pro informační systém hodnotu, přičemž tato hodnota může a nemusí být vyčíslitelná. Aktiva tedy nemusí být pouze hardware či software, aktivem mohou být také samotné informace uvnitř informačního systému (data). (1, s. 82)

Hrozba

Hrozba představuje událost nebo akci, která má za následek narušení informací či zdrojů a to buď náhodné či záměrně. Aktivu tedy hrozí modifikace, narušení celistvosti, vyzrazení, nedostupnost či úplná ztráta. Hrozba představuje vždy nějakou újmu či škodu pro společnost. Jinak řečeno, jedná se o prvek působící na bezpečnost systému. (2, s. 17)

Riziko

Velikost rizika určuje úroveň ohrožení aktiva. Jinak řečeno vyjadřuje míru nebezpečí uplatnění hrozby vedoucí k poškození aktiva či vzniku škody. (1, s. 91)

Riziko lze také vyjádřit jako kombinaci hrozby a zranitelnosti s dopadem na aktivum. (1, s. 16)

Zranitelnost

Zranitelnost udává úroveň zabezpečení aktiva. Čím vyšší je jeho zranitelnost, tím vyšší je na takovém místě pravděpodobnost výskytu a vzniku hrozby. Zcela přirozeně se budeme snažit aktiva s vysokou hodnotou a zároveň velkou úrovní zranitelnosti co nejvíce chránit před možnou realizací hrozby nebo alespoň co nejvíce snížit úroveň rizika na přijatelnou úroveň. (2, s. 18)

Bezpečnostní událost

Za bezpečnostní událost považujeme takový stav systému, sítě nebo služby, která značí možné narušení bezpečnosti, bezpečnostní politiky či opatření. (1, s. 17)

Bezpečnostní incident

Událost, které předchází proces naplnění (realizace) hrozby. Bezpečnostní incident je tedy bezprostřední stav po realizaci hrozby. Stav, při kterém je narušena důvěrnost, dostupnost nebo integrita aktiva. V jiném případě to může být také selhání bezpečnostních opatření nebo porušení bezpečnostní politiky. Reálné důvody pro vznik bezpečnostního incidentů můžou být různé. (1, s. 346)

Identifikace aktiv

Identifikace aktiv je jedním ze základních dokumentů pro úspěšnou analýzu rizik. Detailně popisuje aktiva organizace určená k ohodnocení včetně jejich vlastníka. Správné přiřazení vlastníka aktiva je velice důležité vzhledem ke správě a odpovědnosti za dané aktivum.
(1, s. 68)

Ohodnocení aktiv

Ohodnocení aktiv představuje vyjádření hodnoty identifikovaných aktiv. Aktiva mohou být ohodnocena formou peněžní nebo kvalitativními hodnotami. Je zde také popsán postup, jakým se ohodnocení aktiv provádí. Doporučuje se zde vytvoření přehledné, nejlépe barevně odlišené tabulky. Dále je doporučeno provádět toto ohodnocení s majitelem i uživatelem příslušeného aktiva, vzhledem k možnému subjektivnímu ohodnocení. Ohodnocena by měla být veškerá identifikovaná aktiva, tzn., nemělo by existovat takové aktivum, jehož hodnotu neumíme vyčíslit. (1, s. 68)

Identifikace a analýza rizik

Identifikaci a analýzu rizik IS provádíme jednak za účelem nalezení zranitelných míst v informačním systému, dále také z důvodu vytvoření seznamu hrozeb, které na IS působí. Každému takovémuto zranitelnému místu přiřazujeme příslušnou míru rizika. Tuto analýzu vytváříme zejména z důvodu snížení rizik na přijatelnou úroveň či jejich akceptaci. Pravděpodobnost vzniku a existence rizika může být nahodilá, nepravděpodobná, pravděpodobná, velmi pravděpodobná či trvalá. (1, s. 90)

Řízení rizik

Řízení rizik má za cíl identifikovat a kvantifikovat možná rizika a následně vhodným způsobem rozhodnout o způsobu jejich zvládání. Mezi jednu z nejpoužívanějších metod patří snížení rizika. Jedná se o proces navazujících činností, které se opakují. Obvykle patří mezi činnosti identifikace či analýza rizik, vyhodnocení rizik, zvládání rizik resp. jejich zmírnění a monitoring rizik. (1, s. 95)

Zvládání rizik

Možnosti ošetření proti rizikům lze označit jako zvládání rizik. Cílem je navržení opatření ke snížení, podstoupení, vyhnutí se či sdílení rizik. Rizika lze ošetřit čtyřmi způsoby:

- Modifikací rizik,
- Podstoupením rizik,
- Vyhnutím se riziku,
- Sdílením rizik.

(8, s. 41)

Modifikace rizik

Modifikace rizika znamená opatření proti riziku takovým způsobem, aby po přehodnocení rizika po provedeném opatření bylo zbytkové riziko na přijatelné úrovni. Vždy ovšem existují určitá omezení, která je při zavádění těchto opatření, nutno brát v potaz. Mezi taková omezení patří například omezení finanční, technická, provozní, etická, právní či ekologická. (8, s. 42)

2.3 Bezpečnost

Bezpečnost je velice široký pojem. Podkapitoly jsou zaměřeny zejména na oblasti, týkající se analyzovaného podniku. Na úvod je třeba podotknout, že bezpečnost by měl býti opakující se proces, vedoucí k neustálému zlepšování na uspokojivou úroveň, kterou celý proces nekončí, ale plynule pokračuje činnost monitorování.

Síťová bezpečnost

Dnes problém síťové bezpečnosti řeší řada norem resp. doporučení. Síťová bezpečnost se zabývá jednak ochranou vnitřní části sítě a také ochranou perimetru, tzn. propojení vnitřní části sítě s externími sítěmi. Při řešení je opět nutné provádět analýzu možných rizik, provádět návrhy a opatření zvyšující zabezpečení sítě. Mezi dvě základní oblasti hrozeb pro síť patří její uživatelé či lidé obecně a také přírodní vlivy jako např. živelné katastrofy, požáry apod. Tyto hrozby jsou obecně známé. Při řešení v konkrétním subjektu je třeba se zaměřit na reálné hrozby, kterým síť čelí a zabývat se mírou jejich rizika. (1, s. 162)

Aplikační bezpečnost

Jak již napovídá název, aplikační bezpečnost je pojem týkající se bezpečnosti aplikací. Mezi takové aplikace neboli programy řadíme například nainstalované programy přímo na stanici sloužící pro výkon práce, dále to mohou být čím dál více rozšířené webové či internetové aplikace a výjimkou není ani bezpečnost samotných antivirových programů, které by nám, jak by se mohlo na první pohled zdát, měly bezpečnost zvyšovat. Tento typ programů či aplikací nám bezpečnost samozřejmě zvyšuje, ovšem ne bezpečnost aplikační. Nejčastějším problémem, proč vůbec aplikační bezpečnost musíme řešit, jsou totiž chyby v kódu. Takové chyby se objevují i u aplikací, které nám mají počítač chránit. Tyto aplikace, jako např. zmíněné antivirové programy, jsou obvykle spouštěny s vysokými lokálními právy, tudíž získání kontroly nad tímto programem sebou nese i bonus ve formě těchto vysokých lokálních práv. Mezi čím dál více rozšířené patří webové aplikace neboli aplikace spustitelné prostřednictvím internetového prohlížeče, u kterých obvykle není nutná lokální instalace. Takové řešení aplikací je velice populární vzhledem k jednoduchosti distribuce aplikace. Proto je vhodné se na bezpečnost těchto aplikací zaměřit. (1, s. 172)

Přiměřená bezpečnost

Se zvýšením bezpečnosti a implementací některých bezpečnostních opatření mohou být spojeny finanční náklady, které jsou pro společnost neakceptovatelné. Proto je vždy třeba hledat určitý kompromis či rovnovážný bod mezi úrovní bezpečnosti a náklady s tímto spjaty, přičemž je nutné brát v potaz poměr mezi velikostí investic a úsilí vynaložených do zabezpečení IS vzhledem k hodnotě aktiv a míře realizace možných rizik. (1, s. 36)

Bezpečnostní opatření

Bezpečnostní opatření představují kroky, vedoucí ke snížení, podstoupení, či přenesení rizika na jinou osobu. Jedná se o zabezpečení jednotlivých aktiv uvnitř informačního systému. Pro zvýšení úrovně zabezpečení jsou tato opatření klíčová.

Taková opatření by měla vždy vycházet z analýzy aktiv, v opačném případě je možné že kroky, učiněné ke zvýšení zabezpečení, budou neefektivní. (1, s. 347)

2.4 Ochrana dat

Všechny informační systémy využívají ke své funkci určité množství dat. Tyto data mohou být uložena v databázích, souborech, přenášena elektronickou poštou či na papír apod. Všechna tato data je třeba chránit proti třem hlavním druhům nebezpečí, kterými jsou kompromitace tedy důvěrnost dat před vyzrazením, modifikace, zde data chráníme před jejich neoprávněnou změnou a posledním druhem nebezpečí je zničení. (2, s. 47)

Základem úspěchu je rozdělení dat do skupin dle přístupu, z jakého chceme data chránit.

- Ochrana fyzického přístupu k nosičům dat,
- Ochrana logického přístupu k datům,
- Ochrana uložených dat,
- Ochrana dat přenášených po síti,
- Ochrana dat před zničením.

(3, s. 48)

Ochrana fyzického přístupu k nosičům dat

Tato ochrana by měla začít již před vstupem do budovy, kde jsou nosiče dat umístěny, například formou recepce či vrátnice, která kontroluje vstup jednotlivých osob do objektu. Modernějším řešením jsou automatické dveřní systémy na bázi magnetických či čipových karet. Dalším opatřením může být umístění kamerového systému. Další ochranou by měli být uzamykatelné dveře či ještě dokonalejší dveře na čipovou kartu, pro zaznamenávání průchodů do místností jako je serverovna. Poslední ochranou může být uzamykatelná skříň, ve kterých jsou zařízení umístěny, například typu rack. (2, s. 52)

Mezi ochranu fyzického přístupu řadíme i ochranu před přírodními živly jako jsou požár, zemětřesení, povodně a podobné katastrofy. Ochrana proti požáru je již dnes

poměrně běžnou a známou záležitostí. Instalují se požární hlásiče, samo-hasící systémy či nehořlavé skříně. Zde je třeba dávat zvýšenou pozornost, aby nedošlo ke vniknutí hasební látky do zařízení. Proti zemětřesení se lze chránit například umístěním do protiprachových zařízení či zařízení odolných proti mechanickému poškození.

Alespoň základem je upevnění zařízení a skříní proti pádu. Dalším faktorem mohou být teplotní výkyvy, proti kterým se lze poměrně efektivně ochránit instalací ventilace, klimatizace či jiným systémem chlazení. Za poslední ohrožující faktor lze označit vodu, resp. povodně. Nejjednodušším opatřením je umístění zařízení do vyššího patra budovy, kde je riziko vystoupání vody dosti nereálné (např. povodně, při kterých by voda dosahovala 5. patra budovy je dosti utopická). Další ochranou může být izolace těchto místností. Okna ani žádné potrubí v těchto typech místností nejsou nutná. (3, s. 54)

Ochrana logického přístupu k datům

O problematiku logického přístupu k datům se stará zejména operační systém. Zjednodušeně lze říci, že je třeba uživateli povolit přístup pouze tam, kam ho skutečně potřebuje. Stavebním kamenem pro efektivní řízení je identifikace a autentizace. Přičemž proces identifikace spočívá v zjištění identity uživatele (o koho se jedná) a následná autentizace zajistí ověření, zda uživatele je skutečně tím, za koho se vydává. Zjištění může probíhat různými způsoby, mezi základní patří znalosti (uživatelské heslo či kód), vlastnictví (čipová karta či jiný bezpečnostní předmět) nebo unikátní vlastností uživatele, například biometrickou (otisk prstu). Na základě ověření některého z těchto prvků či jejich kombinace je uživateli povolen či nepovolen přístup. (3, s. 57)

Ochrana uložených dat

I přes všechna opatření, která byla výše vyjmenována, je nutné uvažovat, že je zde možnost získat k datům přístup. Data je tedy nutné určitým způsobem ochránit před modifikací či kompromitací. K tomuto poslouží zejména kryptografické metody a nástroje. V tomto kontextu je vhodnější mluvit spíše o šifrování dat. S šifrováním dat ať už pouze těch vybraných či všech souborů na disku přichází ovšem problematika hesel, bez které se při šifrování lze jen těžko obejít a která je často pro řadové uživatele spíše

prvkem, který je neustále obtěžuje. Šifrovat můžeme vybrané soubory, nejjednodušeji i pomocí programů jako je WinRAR či 7-Zip, tento způsob nám ovšem ochrání data pouze před amatéry. Dalším druhem šifrování může být šifrování online, což spočívá v aplikaci, které šifruje data dle pravidel, např. data umístěná v určitě složce či data odeslaná elektronickou poštou apod. (3, s. 58)

Ochrana dat před zničením

I pokud byly podniknuty pro zabezpečení dat ty nejúčinnější kroky a jsme přesvědčeni, že jsou v bezpečí, je zde stále riziko jejich zničení. Důvodem zničení či ztráty dat může být jejich poškození, smazání nebo poškození samotného nosiče těchto dat. Základním ochranným prvkem, kterým lze předejít následným komplikacím, je zálohování. (3, s. 60)

2.5 Zálohování

Zálohování zjednodušeně představuje zálohování funkci, při které jsou data (všechna či pouze zvolená) uložena na jiné médium. V případě ztráty či zničení dat je možné provést obnovu dat z tohoto média. Logicky budou samozřejmě obnovena pouze ty data, které byla na toto médium uložena. Základem je tedy provádění zálohy co nejčastěji a v pravidelných intervalech. Dnes již existuje spousta sofistikovaných řešení, která provádí zálohu automaticky. Uživatel se tedy nemusí touto operací zabývat. Data jsou automaticky zkopírována, uložena, případně zašifrována a připravena pro nutnost obnovy. (3, s. 61)

Zálohování souborů lze provádět těmito třemi způsoby:

- Normální (úplná záloha) – nejjednodušší varianta pro zálohování i obnovu. Zálohována jsou všechna data bez ohledu na datum jejich změny.
- Přírůstková (inkrementální) – zálohovány jsou změněné soubory od poslední normální nebo přírůstkové metody. Tento druh zálohy je značně rychlejší vzhledem k menšímu objemu zálohovaných dat. Pro obnovu dat je ovšem nutné

mít k dispozici jak zálohu normální tak všechny navazující přírůstkové. Proces obnovy dat je zde tedy složitější.

- Rozdílová (diferenční) – tato metoda zálohuje data změněná od poslední normální či přírůstkové zálohy. Rozdíl je při obnově dat, pří které je nutná záloha normální, poslední přírůstková a všechny rozdílové od poslední normální nebo přírůstkové metody.
- Denní – jak již napovídá název, zálohování dat probíhá každý den. Zálohována jsou data, vytvořená či změněná, mající datum úpravy shodný s datem, kdy probíhá záloha.

(1, s. 330)

3 NÁVRHY ŘEŠENÍ

Navrženy jsou jednotlivé bezpečnostní kroky, vycházející z analýzy současného stavu a analýzy rizik, vedoucí ke zvýšení celkové úrovně zabezpečení jak z hlediska fyzického zabezpečení, tak z hlediska logického. Po zpracování analytické části lze říci, že společnost má již poměrně dobře vybudovanou určitou úroveň zabezpečení, zejména na úrovni síťové bezpečnosti. Jsou tu ale určité nedostatky, které se pokusím odstranit nebo alespoň minimalizovat.

Dle výsledků analýzy se zaměřím zejména na **zabezpečení obchodních dat**, **emailovou komunikaci** a **zabezpečení hardwaru**.

3.1 Zabezpečení dat

Tato opatření jsou určena k minimalizaci rizik, působících zejména na obchodní data. Zaměřena jsou na ochranu proti neoprávněnému přístupu, zneužití, změnu či smazání informací.

První oblastí je logický přístup k obchodním datům, a to zejména na místech, která těchto dat obsahují nejvíce a to jsou uživatelské stanice.

Politika hesel

Správné nastavení politiky hesel je první krok k efektivní ochraně proti potencionálním útočníkům. Obtížně se zde ovšem hledá optimální úroveň složitosti pravidla mezi uživatelsky akceptovatelným a nedostatečně složitým či potencionálně napadnutelným. Nastavení podmínek pro politiku hesel je prováděno v systému Active Directory. V tomto systému jsou rovněž evidovány a spravovány veškeré uživatelské účty včetně jejich hesel. Zde lze navrhnout nastavení paměti uživatelského hesla na poslední 4 hesla, dále vynucenou změnu hesla po 6 měsících. Tzn., že se heslo může opakovat pouze jednou za 2 roky. Tato politika se jeví uživatelsky přijatelná vzhledem k její náročnosti na kompromitaci. Častější změna hesla by mohla být kontraproduktivní a vést k zapisování hesel na lístečky či k volbě velice podobných hesel.

Uživatelské účty

Aktuální nastavení uživatelských účtů po třetím zadání špatného uživatelského hesla zajistí uzamčení uživatelského účtu na dobu deseti minut. Pokud se chce uživatel přihlásit ihned, musí kontaktovat administrátora, v tomto případě linku technické podpory, která mu na základě identifikace, pomocí jeho ID, účet ihned odemkne nebo vynutí nové heslo, které uživateli po telefonu bez dalších autentizačních informací sdělí.

Navrhuji zde zpřísnit pravidlo pro resetování hesla, a to na podmínku vyžádat si od uživatele nejen jeho ID (poslední přihlášené ID je zapamatováno a automaticky zobrazeno na přihlašovací obrazovce), ale navíc i jeho jméno a příjmení a dále jméno a příjmení jeho přímého nadřízeného. Všechny tyto informace má linka technické podpory k dispozici. Toto opatření by mělo zabránit stavu, kdy zavolá na linku technické podpory neoprávněná osoba, která se bude vydávat za někoho jiného, než kým skutečně je.

3.2 Fyzická bezpečnost

Jak již vyplynulo z analýzy, na hardware působí vysoká míra rizika. Zejména pro snížení rizika proti krádeži, poškození či neodborné manipulaci, navrhuji zvýšení zabezpečení serverové místnosti společně s vlastním záložním zdrojem napájení.

Za základní stavební kámen a poměrně velkou mezeru v bezpečnosti považuji fyzické zabezpečení a přístup k síťovým zařízením, jako jsou servery, přepínače, směrovače, firewall apod. umístěné v rozvaděčové skříni sdílené serverové místnosti, jelikož lze toto místo považovat za velmi zranitelné.

Zabezpečení serverové místnosti

Za jeden z hlavních problémů z hlediska fyzického zabezpečení považuji sdílení této serverové místnosti mezi společnostmi GEFCO a ELKOV. Částečným snížením potencionální hrozby je fakt, že rozvaděčovou skříň lze momentálně uzamknout. Stále je zde ovšem riziko vstupu neoprávněných osob do místnosti či nemožnost kontroly průchodů. Nemluvě o hrozbách odcizení, poškození apod. Navrhuji proto zabezpečení

této místnosti, směřované k ošetření přístupu pouze oprávněným osobám z obou společností a navíc kontrole průchodů těchto osob. Tato opatření by měla vést ku prospěchu obou společností.

Navrhuji zde umístění čtečky elektromagnetických karet a osazení vstupních dveří elektronickým zámkem. Příslušnou kartou bude možné dveře otevřít bez nutnosti klíče, přístup přitom bude monitorován. Každý průchod bude uložen společně s identifikací karty, datem a časem průchodu. Karty budou distribuovány pouze oprávněným osobám z obou společností na základě předávacího protokolu. Toto opatření vyřeší problém s autorizací přístupu osob do místnosti.

Jako další krok zde navrhuji opatřit obě rozvaděčové skříně hlásiči otevření dveří. Řešením může být jednoduchý magnetický GSM detektor či sofistikované řešení se zařízením Poseidon, které dokáže monitorovat také teplotu v rozvaděčové skříni, výpadek napájení či výpadek spojení s LAN sítí. Je zde nutné zvolit optimální řešení vhledem k pořizovacím nákladům. Na každý přístup do rozvaděčové skříně lze poté upozornit prostřednictvím SMS či e-mailu. Tyto hlásiče budou sloužit jako další úroveň zabezpečení, v případě neoprávněného vstupu do místnosti.

Záložní zdroj energie

Aby nebylo nutné spoléhat se na společný záložní zdroj napájení, navrhuji opatřit rozvaděčovou skříň vlastním záložním zdrojem napájením neboli UPS. Zařízení ochrání nejen proti výpadku napájení, ale také proti podpětí či přepětí. Všechny tyto faktory mohou mít výrazný vliv na funkci zařízení a jejich životnost. Doporučuji nespoléhat na společné zařízení a implementaci vlastního zdroje nepřerušovaného napájení důrazně doporučuji. Tabulka níže demonstruje energetický odběr jednotlivých zařízení, která je nutné zabezpečit záložním zdrojem. Na základě celkového odběru bude navrhnut konkrétní typ záložního zdroje, který doporučuji zakoupit.

Tabulka 7 - Energetický odběr zařízení
Zdroj: Vlastní zpracování

Zařízení	Počet ks	Zátěž
Server Dell PowerEdge T420	1	422 W
Server Dell PowerEdge T610	1	870 W
Cisco SG300-52	1	64 W
Cisco Catalyst 2950-2	3	30 W
Cisco 880 router for PCI DSS	1	30 W
Cisco 1841	1	45 W
NEC US100 Thin Client	1	13 W
Checkpoint UTM-1 Edge	1	12 W
Mediatrix 4102	2	18 W
SUMA		**1504 W**

Na základě celkového odběru 1504 W a požadované minimální době 10 minut pro pokrytí výpadku, navrhuji zakoupit zdroj APC Smart-UPS 2200VA LCD 230V. Tento záložní zdroj, o výstupním výkonu 1980W, bude schopen pokrýt možný výpadek po zhruba 14 minut. Je zde stále prostor pro případná další zařízení vzhledem k 76 % využití. Cena tohoto zařízení je 33 466,- Kč. Pokud během této doby nedojde k obnovení napájení z elektrické sítě, je UPS vybavena síťovou kartou, která umožňuje připojení zdroje do sítě. Pomocí dodávaného softwaru, lze poté jednoduše nakonfigurovat dobu, po které tento software začne servery bezpečně vypínat, čímž zabrání možnému poškození dat. Postup řešení tohoto krizového stavu navrhuji zahrnout do havarijních plánů.

3.3 Bezpečnostní politika

Opatření spadající do oblasti bezpečnostní politiky nejsou opatřeními proti jednotlivým rizikům. Jedná se o nastavení a udržení určité úrovně důvěrnosti, integrity a dostupnosti dat. Tento dokument by měl pokrýt všechny významné oblasti informační bezpečnosti v organizaci.

Dokument obsahující bezpečnostní politiku již existuje. Nejsou zde ovšem zahrnuty veškeré oblasti, které by být zahrnuty měly. Jsou zde pouze pravidla týkající se práce s výpočetní technikou.

Navrhuji rozšíření tohoto dokumentu o následující položky. Jedná o určení bezpečnostních rolí v oblastní informační bezpečnosti, zavedení interního auditu zaměřeného na tuto oblast, vypracování havarijních plánů, které momentálně nejsou definovány. Dále rozšíření vnitropodnikových směrnic o pravidla přístupu a pohybu osob ve firmě, chování a definice uživatelů v interní síti, vytvoření klasifikace dat, pravidla pro práci při vzdáleném připojení do sítě a směrnice upravující využívání vlastních zařízení.

Bezpečnostní role

Jako první krok, který se promítne do nové bezpečnostní politiky, navrhuji jmenování manažera bezpečnosti (anglicky CISO – Chief Information Security Officer). Na tuto pozici navrhuji člověka, který momentálně pracuje na pozici koordinátora korporátních aplikací. V minulosti pracoval tento člověk jako IT koordinátor, tudíž je mu problematika alespoň částečně známa. Počítat je zde ale nutné s náklady na školení. Předpokládá se úzká spolupráce s korporátním CISO, která bude základem pro tuto pozici. V hierarchii bude přímým podřízeným stávajícího generálního manažera, tzn. na stejné pozici jako IT manažer, se kterým se také předpokládá úzká spolupráce. Jeho úkolem a zároveň cílem práce bude analýza a zvýšení stávající úrovně zabezpečení. Tato osoba bude zodpovědná za informační bezpečnost ve společnosti a bezpečnostní politiku, její zavádění a aktualizaci.

Interní audit

Pro ověření efektivity implementovaných opatření navrhuji audit, který bude následovat půl roku po vydání aktualizace dokumentu bezpečnostní politiky. Cílem auditu bude kontrola zavedených opatření, odhalení a ošetření případných nedostatků. Dále navrhuji opakování tohoto auditu vždy jedenkrát za rok.

Havarijní plány

Havarijní plány, jakožto dokumenty, sloužící k podpoře v případě nestandardních až krizových situací, by měli být součástí bezpečnostní dokumentace ve společnosti. Jejich zpracování může být užitečné nejen pro podporu takovýchto situací ale také pro dokumentaci vývoje navrhnutých řešení.

Do těchto plánů navrhuji zařadit následující krizové stavy:

- Živelná pohroma (požár, povodeň, zemětřesení apod.),
- Výpadek elektrické energie,
- Nefunkční připojení k internetu,
- Porucha serveru,
- Obnova ze záloh po havárii.

Do plánů navrhuji obsáhnout kroky, které je nutné v daném pořadí nutné podniknout bezprostředně po zjištění krizové situace, možnosti odstranění akutního nebezpečí, záložní plán pro zajištění funkcionality v případě havárie. Dále také navrhuji ke každému krizovému stavu uvést kontakty či osoby, na které se lze v případě výskytu tohoto stavu obrátit, a osoby, které jsou za řešení konkrétního krizového stavu zodpovědné.

Například pokud nastane výpadek elektrické energie, bude proti němu firma opatřena záložním zdrojem či zdroji, které dle kapacity baterie nahradí po určitý časový úsek napájení z elektrické sítě.

Směrnice

Další z kapitol, na kterou se bude bezpečnostní politika odkazovat, je kapitola bezpečnostních směrnic. Směrnice budou závazné pro všechny interní i externí zaměstnance společnosti, kteří budou s těmito směrnicemi seznámeni a budou povinni tyto směrnice dodržovat. V případě jejich nedodržení lze přistoupit až k disciplinárnímu řízení ve vztahu k závažnosti tohoto přestupku. Navrhuji vytvoření a zahrnutí do bezpečnostní politiky směrnice zaměřené zejména na tyto oblasti:

Přístup osob do firemních prostor

Osoby, které nejsou zaměstnanci, je možné vpustit do kancelářských a skladových prostor pouze pokud je k tomu účelný důvod jako je např. doručení zásilky, pracovní schůzka apod. Osoby, které se budou po budově pohybovat, se zapíší do příslušené knihy návštěv, kde uvedou své jméno, příjmení, datum příchodu a účel návštěvy. Obdrží kartu s nápisem HOST, kterou umístí po celou dobu návštěvy na viditelné místo. Při odchodu bude karta HOST odevzdána a zapsán čas odchodu. Kontrolu a zodpovědnost za správnost těchto kroků bude mít na starosti asistentka vedoucího pobočky.

Chování ve firemní počítačové síti

Zde navrhuji jasně definovat, kdo je uživatelem firemní sítě. Dále využívání firemní sítě pouze pro pracovní účely nebo účely s tímto výkonem přímo spojené. Zákaz otevírání či jinou manipulaci s neznámými soubory či přílohami. Zákaz zasílání důvěrných informací, jako jsou hesla, po firemní síti. Nestandartní chování systému, podezřelé soubory či jen náznaky nestandartních situací budou uživatelé povinni nahlásit na IT oddělení, přičemž za nestandartní chování a situaci lze považovat podezření na únik dat, neoprávněnou modifikaci, vyzrazení důvěrných informací či podezření o útok na některou z částí IS.

Využívání informačních technologií

Zde je nutné uvést, že informační technologie ve firmě slouží zejména pro podporu a vykonávání pracovní činnosti. Na stolní počítače ani notebooky není dovoleno instalovat software, který se nevztahuje k výkonu práce a nebyl schválen IT oddělením, které je jako jediné oprávněno takovýto software instalovat. Každý uživatel smí vyvolat automatickou instalaci pouze u softwaru uvedeného v seznamu Run Advertised Programs. Tento seznam je dostupný všem uživatelům a je zde obsažena většina aplikací a softwaru nutného pro efektivní vykonávání práce na veškerých pracovních pozicích. S výjimkami je nutné kontaktovat IT oddělení. Využívat výpočetní techniku je možné pouze pod přihlášením do svého vlastního firemního účtu tzn., není dovoleno přihlašování do systému profilem jiného zaměstnance.

Klasifikace dat

Ve firmě nyní neexistuje směrnice, která by kategorizovala data, upravovala práci a následné nakládání s nimi. Navrhuji proto klasifikaci dat do kategorií dle významnosti a následné ohodnocení. Vzhledem k faktu že se jedná o firmu poskytující služby, jsou zde data jedním z nejcennějších aktiv. Navrhuji klasifikační schéma zobrazené v tabulce níže.

Tab. 8 – Klasifikační schéma dat
Zdroj: Vlastní zpracování

Charakter dat	Pravidlo
Veřejné	Dostupné i široké veřejnosti bez omezení, vyzrazení nepředstavuje žádné riziko
Interní	Dostupné pouze pro většinu zaměstnanců, vyzrazení může způsobit určité problémy
Citlivé	Dostupné pouze pro vybrané pracovníky, vyzrazení může způsobit rozsáhlé škody

Dle kategorizace a ohodnocení dat bude poté upraveno, jak s daty příslušeného charakteru nakládat, tzn. jak data uchovávat, zálohovat, s kým lze tato data sdílet a na jakých místech. Přičemž veřejná data jsou pro představu data či informace dostupné na internetových stránkách či soubory volně ke stažení. Interní data jsou data, která jsou

firmou vyprodukována, např. statistiky, interní informace pro zaměstnance apod. Za citlivé informace lze považovat informace chráněné zákonem o osobních údajích, to znamená data personálního oddělení nebo také finanční výkazy, údaje o účtech a jiné.

Každý uživatel navrhne klasifikaci svých jednotlivých dat. Nadřízený poté provede kontrolu a schválení této klasifikace a zároveň přebírá zodpovědnost za korektnost. Doporučena je následující klasifikace konkrétních typů dat:

- Veřejná data – vybrané finanční výkazy, veřejně dostupné a publikované informace.
- Interní data – databáze klientů a dodavatelů, data o přepravách, pracovní postupy.
- Citlivá data – ceníky, data o zaměstnancích, strategické informace, know-how.

Vlastní zařízení

Do sítě není dovoleno připojovat žádné zařízení, které není v majetku firmy či není jeho používání schváleno IT oddělením, tedy zařízení vlastní. Taktéž není dovoleno vkládat ani připojovat k PC či notebooku vlastní zařízení jako jsou USB klíče, CD/DVD apod. zařízení. Toto nařízení je nutné dodržovat zejména kvůli ochraně proti infiltraci nežádoucího či škodlivého softwaru a také z důvodu nedovoleného vynášení informací ze společnosti.

Vzdálené připojení

Pokud je to nutné, mohou uživatelé s notebooky využít vzdálené připojení do firemní sítě za pomoci tokenu. Proto je nutné tento token uchovávat co nejvíce v bezpečí, vzhledem k tomu, že jeho ztráta přestavuje společně s vyzrazením hesla poměrně velkou hrozbu pro systém. Ztrátu či odcizení tohoto zařízení je proto nutné v co nejkratším čase nahlásit IT oddělení, která zajistí jeho okamžitou deaktivaci. Při práci přes vzdálené připojení je nutné dodržovat pravidla stejně jako při práci v interní síti.

3.4 Zálohování

Stávající systém zálohování je funkční, má ale značná omezení. Během zálohy např. nelze vykonávat práci, každá záloha je úplnou (normální) formou, uchovávána je pouze poslední záloha přičemž zálohování probíhá jednou týdně. Nyní budou navrženy kroky, vedoucí k efektivnějšímu způsobu zálohování.

Doporučuji ponechat jednou týdně zálohu úplnou (normální), navíc z důvodu každodenní práce se soubory, provádět vždy jednou denně zálohu přírůstkovou.

Zálohování na síťové uložiště se jeví, při počtu zhruba 20 záloh, jako rozumné řešení. Stávající síťové uložiště Synology s jedním pevným diskem o kapacitě 6TB, doporučuji rozšířit o další 3,5“ SATA III, taktéž o kapacitě 6TB. Technologie RAID 1 (zrcadlení) zajistí, při výpadku jednoho z disků, možnost práce s kopií tohoto disku. Nejedná se ovšem o zálohování samotného disku. Toto zálohování bude stále probíhat na jednu pracovní stanici.

Aktuálně využívaný software neumožňuje provádění zálohy na pozadí, navíc umožňuje pouze úplnou formu zálohy. Navrhuji proto zvolení jiného zálohovacího softwaru. Jednou z možností je využití zálohovacího softwaru Cobian Backup od společnosti CobianSoft. Tento software přinese následující výhody:

- Záloha dat může probíhat automaticky a na pozadí,
- Uživatel je informován o záloze pouze v Taskbaru,
- Lze naplánovat rozdílné typy záloh v různých intervalech,
- Software je dostupný bezplatně.

Při správném nakonfigurování tohoto softwaru lze dosáhnout uživatelsky přívětivého a zároveň efektivního způsobu zálohování.

3.5 Vnitropodnikové vzdělávání zaměstnanců

Jelikož je v organizaci implementován management kvality ISO 9001, doporučuji mezi aktuální témata školení zařadit také školení, zaměřená na oblast informačních technologií a informační bezpečnosti.

Navrhuji rozdělení zaměstnanců do skupin dle pracovního zaměření. Rozdělení připadá v úvahu na řadové zaměstnance a vedoucí pracovníky, přičemž náplň a frekvence školení se dle příslušené skupiny liší. Školení doporučuji provádět vlastními silami formou přednášek s praktickými ukázkami dané problematiky. Každé školení bude zakončeno testem pro ověření načerpaných znalostí. Úvodní školení doporučuji u obou skupin zaměřit na oblast informační bezpečnosti.

Školení zaměstnanců - 2x ročně, vlastními silami

Informační bezpečnost:

- Přiblížení problematiky informační bezpečnosti,
- Přínos zaměstnance k této problematice,
- Představení dokumentu bezpečnostní politiky,
- Zdůraznění pravidel a povinností uživatelů (bezpečnostní směrnice),
- Ověření znalostí formou testu.

V případě školení zaměstnanců navrhuji klást důraz na zpětnou vazbu od uživatelů o užitečnosti školení. Dále zjistit návrhy na témata školení ze strany uživatelů.

Školení vedoucích pracovníků - 4x ročně, vlastními silami

Informační bezpečnost:

- Vysvětlení problematiky informační bezpečnosti,
- Význam a přínos této oblasti ve vztahu k zaměstnanci a společnosti,
- Představení dokumentu bezpečnostní politiky,
- Návrhy pro úpravy bezpečnostní politiky,
- Zdůraznění pravidel a povinností uživatelů (bezpečnostní směrnice),

- Kontrola dodržování směrnic,
- Ověření znalostí formou testu.

V případě školení vedoucích pracovníků navrhuji zaměření se na vzájemnou kooperaci. Dále zjistit nedostatky a oblasti, na které by bylo vhodné budoucí školení zaměřit.

Další možná témata školení: bezpečná emailová komunikace, bezpečná práce s internetem, bezpečná práce s aplikacemi, síťová bezpečnost, krizové a havarijní stavy.

3.6 Ekonomické zhodnocení návrhů

V této kapitole budou vyčísleny náklady spojené se zavedením jednotlivých bezpečnostních opatření.

Některá z navrhnutých opatření budou realizována interními zaměstnanci v rámci jejich pracovního výkonu, což přinese částečné finanční úspory.

Orientační náklady na fyzické zabezpečení, které bude realizováno externí firmou na základě výběrového řízení, budou zahrnovat následující položky (bez DPH):

- Zařízení pro čtečku karet (cca 8 500,- Kč)
- Software pro správu karet (cca 3 350,- Kč)
- Docházkové karty (cca 100Kč / ks)
- Instalace hardware + oživení systému (cca 5 000,- Kč)

Náklady spojené s bezpečnostní politikou zahrnují pouze školení Manažera informační bezpečnosti, které včetně zkoušky a certifikátu nabízí externí společnost za cenu 25 000,- Kč bez DPH.

Zálohování přináší jediný skutečný výdaj navíc, kterým je pořízení pevného disku do síťového úložiště. Tento disk, kterým může být Western Digital 6TB, 3,5", SATA III, lze zakoupit za cenu 7 515,- Kč bez DPH.

Tab. 9 - Cenová kalkulace návrhů
Zdroj: Vlastní zpracování

Opatření	Způsob pořízení	Cena v Kč
Zabezpečení dat		
- Politika hesel	Vlastními silami	**-**
- Uživatelské účty	Vlastními silami	**-**
Fyzická bezpečnost		
- Zabezpečení serverové místnosti	Externě – zařízení, software, karty	**16 950,-**
- Záložní zdroj energie	Externě – APC UPS 2200VA	**33 466,-**
Bezpečnostní politika	Vlastními silami	**-**
- Školení informační bezpečnosti	Externě – Manažer inform. bezp.	**25 000,-**
Zálohování		
- Software	Externě – freeware	**-**
- Konfigurace	Vlastními silami	**-**
- Rozšíření síťového úložiště	Externě – Disk 3,5“ SATA III 6TB	**7 515,-**
Vnitropodnikové vzdělávání zaměstnanců	Vlastními silami	**-**
SUMA bez DPH		**82 931,-**
DPH 21%		**17 416,-**
SUMA včetně DPH		**100 347,-**

Celkové náklady na navrhnutá bezpečnostní opatření činí 100 347,- Kč včetně DPH. Vzhledem k množství navržených opatření považuji tuto cenu za velice nízkou a přijatelnou v poměru s velkým přínosem v oblasti informační bezpečnosti a zabezpečení.

ZÁVĚR

Cílem bakalářské práce je navrhnout a zavést jednotlivá bezpečnostní opatření, vedoucí ke zvýšení celkové úrovně zabezpečení. V první části jsem provedl analýzu současného stavu zabezpečení ve společnosti. Jak vyplynulo z analýzy, společnost je závislá zejména na funkční internetové a hlasové komunikaci. Z hlediska bezpečnosti byly odhaleny určité nedostatky různého typu a charakteru.

Dle vlastních zkušeností plynoucích z pracovněprávního vztahu ve společnosti jsem na základě těchto nedostatků navrhl dílčí opatření, která jsou pro společnost, vzhledem k nákladům, realizovatelná.

Oproti původnímu stavu při analýze již společnost není závislá na záložním zdroji napájení. Návrhy přináší také zvýšení zabezpečení uživatelských účtů, a to uživatelsky přívětivou politikou hesel. Fyzický přístup do serverové místnosti je lépe monitorován, navíc je možné dohledat kdo, a kdy do místnosti vstoupil.

Bezpečnostní politika zajišťuje jasné vymezení pravidel nejen pro uživatele. V případě porušení nastavených pravidel je možné vycházet z tohoto dokument a použít jej jako podklad při řešení nestandartních situací.

Nový způsob zálohování považuji za největší ulehčení práce uživatelů a zároveň kompletní zefektivnění celého procesu. Vzhledem k téměř nulové pořizovací ceně za software považuji toto opatření za velmi efektivní a úspěšné.

Vnitropodnikové vzdělávání zaměstnanců v oblasti IT má úspěch zejména, pokud se školení správně uchopí. V takovém případě mohou být pro uživatele velkým přínosem. Vzhledem ke školení vlastními silami, je možné modifikovat školení přímo pro potřeby zaměstnanců a zaměřit se na konkrétní problémy, se kterými se potýkají.

V součtu je navrhnuto relativně velké množství opatření za poměrně nízké pořizovací náklady. Opatření představují pro podnik také značnou konkurenční výhodu.

Pro kontinuální zlepšování do budoucna doporučuji zvážení pořízení kamerového systému do prostor skladu. Dále doporučuji společnosti zavést systém managementu bezpečnosti informací (ISMS) dle ČSN EN 27001 včetně certifikace, což ovšem může znamenat navýšení počtu zaměstnanců.

SEZNAM POUŽITÉ LITERATURY

Knihy:

[1] ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: CERM, 2013. ISBN 9788072048724.

[2] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Brno: Computer Press, 2007. ISBN 978-80-251-1511-4.

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

[4] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005. ISBN 80-868-9838-5.

[5] POŽÁR, Josef. *Základy teorie informační bezpečnosti*. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

[6] POŽÁR, Luboš. *Ochrana dat v informačních systémech*. Praha: Aleš Čeněk, 2005. ISBN 80-716-9479-7.

[7] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí.* Praha: Grada, 2003. ISBN 80-247-0663-6.

[8] ONDRÁK, Viktor. *Management informační bezpečnosti*. Interní výuková podpora FP-VUT.

[9] HORÁK, Jaroslav a Milan KERŠLÁGER. *Počítačové sítě pro začínající správce*. 5. aktualizované vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3176-3.

[10] LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. *Teorie bezpečnosti počítačových sítí*. Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

[11] PROSISE, Chris a Kevin MANDIA. *Počítačový útok: detekce, obrana a okamžitá náprava*. Praha: Computer Press, 2002. ISBN 80-722-6682-9.

Elektronické zdroje:

[12] KOSTIHA, František. *Bezpečnost informací*. Ikaros [online]. 2006, ročník 10, číslo 5 [cit. 2015-05-20]. ISSN 1212-5075. Dostupné z: http://ikaros.cz/node/12087.

[13] BRECHLEROVÁ, Dagmar. *Řešení informační bezpečnosti: 1. část* [online]. [cit. 2015-05-20]. Dostupné z: http://www.systemonline.cz/clanky/reseni-informacni-bezpecnosti-1-cast.htm.

[14] NOVÁK, Luděk a Josef POŽÁR. *ISMS (ISO 2700x): sborník příspěvků z bezpečnostního semináře Policejní akademie a evropského vedení AFCEA konaného dne 22. září 2011 na Policejní akademii České republiky v Praze*. Praha: Policejní akademie České republiky, 2011. ISBN 978-80-7251-356-7.

Normy:

[15] ČSN ISO/IEC 27001 (36 9797). *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. 2. vydání. Praha: Český normalizační institut, 2014, 25 s.

[16] ČSN ISO/IEC 27002 (36 9798). *Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací*. 2. vydání. Praha: Český normalizační institut, 2014, 73 s.

SEZNAM OBRÁZKŮ A TABULEK