Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

KATEDRA INFORMAČNÍCH TECHNOLOGIÍ

Diplomová práce
Zabezpečení IT infrastruktury firem v ČR

Stára František
Vedoucí: Ing. Čestmír Halbich, CSc.

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

František Stára

Informatika

Název práce

Zabezpečení IT infrastruktury firem v ČR

Název anglicky

IT infrastructure security in companies in Czech Republic

Cíle práce

Hlavním cílem je, na základě teoretických východisek a analýzy výchozího stavu nastavit zabezpečení dané firmy.
Vedlejším cílem je stanovení přiměřené IT bezpečnosti. Dílčí cíle jsou: obecně charakterizovat bezpečnost IT, bezpečnostní politiku, standardy, hrozby a rizika, bezpečnostní incidenty, popř. doplnit o praktické zkušenosti.

Metodika

Výchozím bodem metodiky je prostudovat literaturu s problematikou IT bezpečnosti . Dále následuje formulování hypotézy na základě syntézy teoretických poznatků, analýza výchozího stavu zabezpeční firmy a popis vybrané firmy, sumarizace a zhodnocení výchozího stavu zabezpečení, doporučení pro zkvalitnění zabezpečení IT a návrh realizace zlepšení zabezpečení IT.

Doporučený rozsah práce

60-80 stran

Klíčová slova

informační bezpečnost, hrozby, rizika, bezpečnostní incident, lidské zdroje, outsourcing, cloud computing, bezpečnostní politika, standardy, počítačový útok

---

Doporučené zdroje informací

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, a.s., 2004. 190 s. ISBN 80-251-0106-1

ERNST & YOUNG. Průzkum stavu informační bezpečnosti v ČR 2009. Ernst & Young, NBÚ, DSM data security management a Národní bezpečnostní úřad, 2009. 40 s. ISBN 978-80-86813-19-6

HANTANON, R. Linux : praktická bezpečnost. 1. vyd. Praha: Grada Publishing, a.s., 2003. 440s. ISBN: 80-247-0652-0

HARRIS, S., HARPER, A., EAGLE, CH., NESS, J., LESTER, M. Hacking Manuál hackera. 1. vyd. Praha: Grada Publishing, a.s., 2008. 400 s. ISBN 978-80-247-1346-5

NORTHCUTT, S., ZELTSER, L., WINTERS, S., FREDERICK, K., RITCHEY, R. Bezpečnost počítačových sítí. 1. vyd. Brno: CP Books, a.s., 2005. 589 s. ISBN 80-251-0697-6

POUR, J., GÁLA, L., TOMAN, P. Podniková informatika 1. vyd. Praha: Grada Publishing, a.s., 2006. 484 s. ISBN ISBN 80-247-1278-46.

PROCHÁZKA, J., KLIMES, C. Provozujte IT jinak 1. vyd. Praha: Grada Publishing, a.s., 2011. 288 s. ISBN 978-80-247-4137-6

TVRDÍKOVÁ, M. Aplikace moderních informačních technologií v řízení firmy. 1. vyd. Praha: Grada Publishing a.s., 2008. 176 s. ISBN 978-80-247-2728-8

Předběžný termín obhajoby

2015/06 (červen)

Vedoucí práce

Ing. Čestmír Halbich, CSc.

Elektronicky schváleno dne 31. 10. 2014

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 11. 11. 2014

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 17. 03. 2015

Čestné prohlášení

Tímto čestně prohlašuji, že jsem diplomovou práci na téma „*Zabezpečení IT infrastruktury firem v ČR*“ zpracoval samostatně pouze s použitím uvedené literatury, metod a zdrojů.

V Praze dne 17. 3.2015 …….

Poděkování

Rád bych poděkoval Ing. Čestmíru Halbichovi, CSc. za odborné vedení, cenné rady a ochotu při zpracování této diplomové práce.

Zabezpečení IT infrastruktury firem v ČR

Souhrn

Diplomová práce se zabývá problematikou IT bezpečnosti s důrazem na firemní prostředí. V první části jsou vysvětleny pojmy, které je nutné znát pro bližší porozumění oblasti IT bezpečnosti například charakteristika IT bezpečnosti, bezpečnostních nástrojů jako je firewall, antivir, DMZ, charakterizování útočníků a používaných metod pro útok. Pro realizaci praktické části byla použita reálná firma, z které vycházely další části. Nejprve je společnost představena, poté proveden bezpečnostní audit na základě normy ISO 27001. Po definování bezpečnostních hrozeb ohrožující firemní prostředí a aktiv ve firemní infrastruktuře, provedena analýza rizik na základě, které jsou navrhnuty bezpečnostní opatření pro eliminování zjištěných hrozeb. Práci uzavírá finanční kalkulace navrhovaných opatření.

Klíčová slova

Informační bezpečnost, hrozby, rizika, bezpečnostní incident, analýza rizik, bezpečnostní audit, hacker, bezpečnostní politika, standardy, firewall, počítačový útok.

Summary

The diploma thesis deals with the issue of IT security with a focus on company environment. The first part of the thesis explains terms necessary for further understanding of IT security, for example characteristics of IT security, security tools as firewall, anti-virus, DMZ, characterizing of attackers and of the methods used for attacks.

For the following parts of the thesis, a real company was used as an example. The company's introduction is followed by a security audit based on technical norm ISO 27001. After defining security threats threatening in company environment and assets in the company's infrastructure, analysis of risks is made. Security measures for eliminating the detected threats are proposed based on the risk analysis. A financial calculation of proposed measures concludes the whole thesis.

Key words

Information security, threats, risks, security incident, risk analysis, security audit, hacker, security policy, standards, firewall, computer attack.

Obsah

1 Úvod

V dnešní době je pojem bezpečnost informačních technologií stále aktuálnější a ne jen ve firmách. Přece jen v elektronické podobě je dnes uchováno značné množství duševního vlastnictví a jiné cenné informace. Jedná se například o zdravotní záznamy, účetní záznamy, bankovní záznamy, elektronické platební nástroje, patenty či jiné plány nebo strategie podniku. Ztráta nebo vyzrazení dat může způsobit velkou újmu někdy i existenční. Naštěstí riziko si uvědomuje stále více firem a snaží se investovat stále více finančních prostředků do této oblasti, posilovat zabezpečení a implementovat nové technologie.

Množí se případy průmyslové špionáže, kdy je firma okradena o všechna data a ta jsou poté využita proti ní v konkurenčním boji. Velký fenomén mezi útočníky jsou také DDOS útoky, kdy si konkurence zaplatí na hackerském fóru útok na konkrétní firmu a hackeři odstaví například na několik hodin přístup k firemním aplikacím, což může mít za následek zhoršení pověsti firmy, nedodržení SLA a následnou pokutu nebo může maskovat jiný útok, při kterém dojde k odcizení dat. Z hacktivismu se stal cenný business a přitahuje stále více hackerů. Je finančně výhodný i pro firmy, které implementují bezpečnostní prvky či provádí bezpečnostní audity.

Zabezpečení firemní IT infrastruktury nepojednává jen o hrozbách spojených s útoky „zlých“ hackerů, ale zabývá se i hrozbami ze strany zaměstnanců, selhání hardwaru, výpadků proudu či dalších oblastí. Jedná se o velmi komplexní téma, kterým by se měla každá společnost zabývat dříve, než bude pozdě a o svá data přijde.

Práce se zabývá konkrétní firmou, ve které bude zhodnocen aktuální stav zabezpečení a následné návrhy na úpravy do požadovaného stavu, který dokáže eliminovat aktuální hrozby. Nejprve bude firma představena včetně hardwarového a softwarového vybavení. Poté bude provedena analýza zabezpečení. Z analýzy bude vyvozen závěr a definované doporučení pro zkvalitnění zabezpečení ve firmě a eliminování případných hrozeb.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem literární rešerše je definovat IT bezpečnost, popsat jednotlivé hrozby, rizika, bezpečnostní politiky, standardy a bezpečnostní incidenty.

Cílem praktické části je na základě teoretických východisek a analýzy výchozího stavu zhodnotit a doporučit nastavení zabezpečení.

2.2 Metodika

První část práce bude obsahovat teoretické informace. K jejich dosažení bude zapotřebí nastudování a seznámení se s odbornou literaturou a odbornými texty dostupnými na internetu. V první kapitole budou popsány pojmy související se zabezpečením IT infrastruktury: jednotlivé hrozby, rizika, standardy, bezpečnostní politiky a bezpečnostní incidenty.

V druhé části bude představena analyzovaná společnost: obor působení, počet zaměstnanců, IT vybavení a potencionální hrozby. Zabezpečení společnosti bude analyzováno, na základě normy ISO 27001, kdy bude postupováno podle metodických oblastí použité normy. Analýza nebude provedena do takové hloubky, aby sloužila jako podklad pro provedení certifikace. Bude sloužit jako pomocný nástroj pro zaměření se na kritické oblasti informačních systémů.

Následně bude provedena analýza rizik. Vycházející z definovaných hrozeb a aktiv společnosti. Analýza bude monitorovat pravděpodobnost vzniku rizika, kde bude vycházeno z aktuální možnosti aktivace hrozby. Ohodnocení následků bude specifikovat rizika ohodnoceny mírou závažnosti následků. Celková analýza rizik se bude skládat ze součtu ohodnocení následků a pravděpodobnosti vzniku rizika.

Na základě výsledků analýzy rizik a provedeného auditu zabezpečení budou navrženy možné způsoby pro eliminaci definovaných rizik. Součástí návrhu bude konečná finanční kalkulace navrhovaných změn.

3 Teoretická východiska

3.1 Bezpečnost IT

Bezpečnost informačních technologií je rozebírána z důvodu, aby byla zajištěna data firmy pouze pro přístup oprávněných osob, docházelo ke zpracování nefalšovaných údajů, bylo možné zjistit, kdo a jak s daty pracoval, data nebyla vyzrazena a byly vždy dostupná.

3.1.1 Bezpečnostní audit

Bezpečnostní audit řeší, zda jsou dodržována všechna bezpečnostní opatření. Jedná se o pravidelně opakující se proces. Smyslem auditu je posouzení celkového zabezpečení s ohledem na nové technologie a tím i nových bezpečnostních děr. Postupně jsou vyhodnoceny všechny informační systémy a nalezeny nedostatky a mezery, které by mohly mít za následek bezpečnostní incident[1]. Při auditu jsou zkoumány i záznamy vzniklé v předchozím období. Záznamy auditor vyhodnotí a zjistí, zda byl proveden nějaký útok a jakým způsobem. Audit by měl být prováděn nejlépe externí firmou, která je nezávislá a důkladně odkryje aktuální hrozby. Je nutné celý audit zastřešit smlouvou, jelikož auditor přistupuje ke klíčovým informacím a mohl by stejně jako útočník informace zneužít. [1]
Bezpečností audit prověří:

- používaný software z hlediska bezpečnosti sítě
- aktuálnost používaného software
- specifická bezpečnostní rizika, spojená s používaným software
- nejslabší místa zabezpečení
- způsob a četnost zálohování dat
- způsob ukládání a ochrany těchto dat
- správné nastavení systému [2]

3.1.2 Analýza rizik

Analýza rizik je kontinuální proces, v němž jsou analyzovány veškeré hrozby, které mohou nastat v IT infrastruktuře a mohly by ohrozit chod informačního systému. Hrozby jsou pak ohodnoceny pravděpodobností výskytu. Analýza rizik se využívá obzvláště ke zjištění, zda firemní aktiva jsou dostatečně chráněna a zda případná nová implementace bezpečnostního prvku je finančně přiměřená povaze aktiva. Výskyt hrozeb záleží na oblasti

[1] Pojem bezpečnostní incident je vysvětlen na str. 10.

působnosti dané firmy. Například IT bezpečnost ve finančnictví bude čelit jiným hrozbám než IT ve výrobě. Jak již bylo naznačeno, analýza rizik se skládá ze tří hlavních pilířů, aktiva, zranitelná místa a hrozby.[1,3]

Aktiva jsou definována hmotnými i nehmotnými statky, které slouží k provozu informačního systému. Mezi hmotné statky patří hardware (servery, síťové prvky, počítače atd.), nehmotné statky zastupuje software (operační systém, aplikační program atd.) a firemní data (účetní záznamy, seznam klientů atd.). [3]

Každé aktivum v sobě skrývá zranitelné místo. Slabinu, kterou lze zneužít k modifikaci, zcizení anebo smazání dat. Slabina nemusí být nutně využita třetí osobou. Může se jednat i o selhání hardwaru z technických důvodů. Mezi zranitelná místa mohou patřit například: nezabezpečený vstup do budovy, nespolehlivé napájení, krádeže, smrt, špatný návrh softwaru či odposlouchávaní sítě. Zranitelných míst je celá řada a je zapotřebí všechna analyzovat a správně vyhodnotit. [3]

Hrozbu lze chápat jako reálné nebezpečí vycházející ze zranitelného místa. Hrozby jsou ohodnoceny pravděpodobností, se kterou hrozba může nastat ve firemní infrastruktuře. Zdrojem hrozeb mohou být lidé, kteří mohou poškodit či odcizit data. Může se jednat o zaměstnance nebo potencionálního hackera mimo firemní síť. Dále jako hrozbu je možné považovat určité nehody například požár, lidské selhání, výpadek elektrické energie atd. V neposlední řadě je třeba do analýzy rizik zahrnout hrozby jako jsou přírodní katastrofy, zemětřesení, povodně a další živelné pohromy. [1,3]

Výstupem analýzy rizik je souhrn doporučených protiopatření, která vedou ke snížení rizika na nejnižší možnou míru. Při návrhu eliminování hrozby je zásadní otázka cena aktiva. Není racionální implementovat bezpečnostní prvek, který převyšuje cenu chráněného aktiva. U fyzického aktiva jako serveru není vyčíslení problém, složitější je stanovení hodnoty dat. K vyhodnocení ceny dat se používají speciální metodiky, jako například CRAMM, kdy se pokládají otázky, co by se stalo, kdyby… Způsoby realizace bezpečnostní analýzy (analýzy rizik), popisuje např. mezinárodní norma ISO/IEC TR 13335. Standardy IT bezpečnosti, ať už regulační, nebo doporučující, se takřka bez výjimky odvolávají na směrodatné metody analýzy rizik (ISO/IEC IS 27001, NIST a další). [3]

3.1.3 Penetrační testy

Postupem času jsou operační systémy složitější a komplexnější a to i veškerý software používající se v infrastruktuře. Spolu s tímto faktem přicházejí stále častěji

bezpečnostní díry v používaných produktech. Hackeři bezpečnostní díry využívají k proniknutí do systému. Penetrační testy slouží především k preventivnímu otestování bezpečnosti sítě a odolnosti vůči současně známým útokům. Cílem je pak identifikovat možné hrozby a doporučit opatření k odstranění těchto hrozeb. Výsledek testování může sloužit jako podklad pro stanovení priorit v rámci zvyšování bezpečnosti či důkaz bezpečnosti sítě pro certifikace nebo obchodní partnery. Penetrační testy je potřeba provádět pravidelně jelikož databáze známých útoků neustále roste. [4,19]

Testy jsou pak rozděleny na dvě podkategorie: analýza hrozeb z vnějšího prostředí a analýza hrozeb z vnitřního prostředí tedy hrozeb z řad vlastních zaměstnanců. Nelze odhalit všechna zranitelná místa. Testy jsou limitovány přidělenými prostředky, jako je čas, personál a finance. Je potřeba se zaměřit na místa, která jsou pro společnost kritická a představují největší riziko. Ideální je sestavit penetrační test na základě analýzy rizik. [5]

Obsahem penetračního testu by měly být všechny objekty, u nichž hrozí riziko odcizení dat či odcizení hardwaru. Tím jsou myšleny například webové stránky, informace o klientech, emailové schránky, přístupová hesla, uložiště dat či informační systémy. Zvláště důraz by měl být kladen na objekty, s kterými manipulují zákazníci a hrozí riziko úniku klientských údajů a ztráty důvěryhodnosti ze strany klientů. [5]

Testy jsou rozděleny do několika kategorií. Manuální testy jsou vykonávány manuálně, což umožňuje vytvořit specifické podmínky šité na míru testovanému prostředí. Jsou však časově a finančně náročné. Automatizované testy jsou integrovány do nástrojů, které provádí testy automaticky. To zaručuje kratší čas a menší finanční náročnost na testování. Je však nutné naučit se ovládat a rozumět testování. Semiautomatické testy jsou kombinací automatického a manuálního testování. Představují kompromis obou předchozích metod. [5]

Softwarů pro testování existuje několik desítek, které obsahují řadu nástrojů a různé druhy testů. Běžně používaným softwarem je například Back Track Linux, Fedora Security Spin, KATANA, Pentoo nebo Blackbuntu. Některé z výše uvedených lze použít pro otestování bezdrátových sítí nebo webových aplikací. Distribuce lze stáhnout ve formátu LiveCD a spustit jako bootovatelné médium. [5]

3.1.4 Bezpečnostní politika

Jedná se o hlavní pilíř celé organizace z hlediska bezpečnosti. Bezpečnostní politika je písemný dokument schválený vedením společnosti, stanovující metody pro zajištění

bezpečnosti, cíle organizace v oblasti bezpečnosti, definování odpovědnosti, prostředky, časový plán, definice citlivosti informací, zásady pro havarijní plánování atd. Na základě bezpečnostní politiky lze vymáhat dodržování bezpečnostních zásad po zaměstnancích i externích subjektech, které mají za cíl chránit bezpečnost informací v organizaci. Bezpečnostní politiky bývají vytvářeny na základě norem a standardů používaných v bezpečnosti jako je například ISO 27001, přispívající ke zvýšení bezpečnosti. [1,6]

3.1.5 Bezpečnostní incident

Bezpečnostní incident je identifikovaná událost, při níž došlo k narušení pravidel bezpečnostní politiky, selhání protiopatření, anebo nově zjištěná situace ohrožující bezpečnost společnosti. Incidentem je míněna situace, kdy existuje vysoké procento ohrožení bezpečnosti společnosti. Je nutné, aby všichni uživatelé hlásili veškeré bezpečnostní incidenty a ty byly vyřešeny a zapsány. [1]

3.1.6 Bezpečná firma

Pro zajištění správné firemní bezpečnosti je nutné personální zajištění. Osoba, která bude mít firemní bezpečnost na starosti. Pracovník, by měl být členem vedení společnosti, aby mohl vydávat potřebná rozhodnutí a měl potřebnou pravomoc. Pozice definující zmiňované personální zajištění je nazývána CISO (Chief Information Security Officer).

Jeho prvním úkolem by mělo být vypracování platné bezpečnostní politiky, analýzy rizik, bezpečnostního auditu a penetračních testů. Na základě těchto činností by poté měl sestavit strategii pro zlepšování bezpečnosti. [1,7]

Aby firma byla bezpečná, je třeba vytvořit havarijní plán, který bude popisovat postup při bezpečnostním incidentu či přírodní katastrofě. Plány je potřeba testovat, zda jsou aktuální a vůbec reálné. Je potřeba vytvořit směrnice, které vymezují práci s informačním systémem a uživatelé musí být pravidelně školeni. Je nutné definovat pracovní úkony, které souvisí se změnou pracovní pozice ať už s přijetím, propuštěním anebo například povýšením. [7]

3.2 Nástroje pro řízení bezpečnosti

3.2.1 Řízení přístupu

Aby bylo možné uživatele identifikovat v informačním systému, je nutná jejich autentizace. Jedná se o proces, kdy fyzický uživatel se snaží prokázat systému svojí

totožnost. Nejčastější princip ověřování je použití uživatelského jména a hesla. Systém ověří platnost hesla a poté dojde ke vpuštění do systému, pokud je zadané heslo správné. Jedná se o jednoduchý způsob ověřování, který může být snadno napadnutelný. Firma může mít sebelepší bezpečnostní prvky, ale pokud si uživatelé poznamenají například heslo na místo, které je snadno dostupné nebo zvolí jednoduché heslo je veškeré zabezpečení zbytečné.

Jako obranou proti podobné nekázni je zapotřebí definovat firemní politiky, které vynutí složitost, kvalitu hesel a zaručí kázeň uživatelů při manipulaci s hesly. Vhodné je nastavit vynucovací technické prostředky, jež nevyhovující hesla budou odmítat. [1,7]

3.2.2 Fyzické zabezpečení

Celkem podceňovanou oblastí je fyzické zabezpečení serverů či jiných síťových prvků. Krádež, poškození či modifikace těchto zařízení může mít pro firmu fatální následky. Zařízení by měla být přístupná pouze odpovědným osobám, nejlépe v samostatné klimatizované místnosti zabezpečené kódovým zámkem nebo vstupem na čipovou kartu. Pokud se hacker dostane k serveru, umožní mu to nabootovat systém z instalačního média a vytvořit si administrátorský účet. Taktéž může odcizit pevné disky, které by z tohoto důvodu měli být zašifrované. Totéž platí i o šifrování disků v noteboocích, kde může dojít ke zcizení a ukradení dat či hash kódu s hesly. [12]

3.2.3 Kryptografie

Kryptografie je vědní matematický obor, který se zabývá šifrovacími a kódovacími algoritmy. Kryptografie se konkrétně snaží o znepřístupnění obsahu nepovolaným osobám a zpřístupněním pouze osobám, které mají tzv. klíč. Klíč si mezi sebou předávají komunikující strany a slouží k dešifrování zašifrované informace. Šifrou se nazývá konkrétní algoritmus, který pomocí klíče zašifruje informaci. Takový algoritmus může být například DES, RSA nebo AES. Šifrování se využívá k zašifrování harddisků v serverech, noteboocích, mobilních telefonech či při emailové komunikaci v internetovém bankovnictví, uložení hesel a jiných oblastech, kde je nežádoucí, aby k informaci měla přístup nepovolaná osoba nebo, aby byla změněna integrita dat. [1]

Proti-pól kryptografie je kryptoanalýza. Kryptoanalýza se snaží o prolomení šifry bez požadovaného klíče a získání zašifrované informace nebo samotného klíče. Nejčastější způsob prolamování algoritmu je hrubou silou, kdy jsou postupně zkoušeny všechny kombinace klíčů. Z tohoto důvodu čím delší je klíč, tím je zašifrována informace

bezpečnější. Každá šifra je více méně prolomitelná, je to jen otázka času. Některé dnešní šifry nelze v reálném čase ani pomocí nejmodernějších počítačů rozšifrovat. Mezi další způsoby patří například odposlech velkého množství šifrovaných dat a poté odhadnout šifrovací klíč. [7]

3.2.4 Auditní záznamy

Auditování je pojem, který označuje ukládání záznamů o aktivitách, které se v jednotlivém systému udály a podle kterých může správce najít příčinu bezpečnostního incidentu, viníka či sjednat opatření, aby k podobné události nedocházelo. Každý záznam obsahuje informace, jako je čas události, přihlášený uživatel, detailní popis události, kategorizace události či kód chyby. Je důležité zachovat integritu těchto dat a neumožnit přístup neoprávněným osobám. Důležité je záznamy pravidelně kontrolovat a vyhodnocovat. Nejběžnějším nástrojem na sumarizaci auditních záznamů ve Windows Serveru je Event log, zpracovávající veškeré události, které se v operačním systému udály. [1]

Komplexní řešení, které spravuje logy ze všech systémů, vyhodnocuje je a dlouhodobě ukládá, se nazývá SIEM (Security Information and Event Management). Celý proces je automatizován a nastavený dle predeterminovaných událostí. V případě incidentu je správce upozorněn. Takový nástroj nabízí například výrobce HP s produktem ArcSight a nebo se nabízí levnější produkt Nagios od stejnojmenného výrobce. [10]

3.2.5 Antivirová ochrana

Antivirovou ochranu neboli antivir není potřeba dlouze představovat. Jedná se o základní nástroj na identifikaci a odstraňování kybernetických virů a jiných škodlivých programů, které ohrožují bezpečnost uživatele. Připojením koncového zařízení na internet hrozba nákazy prudce roste a použití antivirové ochrany je nutné. Aby antivirová ochrana byla úplná je důležité správně systém nakonfigurovat, pravidelně aktualizovat a nastavit pravidelné kontroly. Antivir vyhodnocuje viry analýzou heuristiky a dokáže identifikovat viry, které ještě nebyly odhaleny. Porovnává soubory na základě signatur řetězce, který jednoznačně identifikuje vir, s databází již zjištěných infekcí nebo dle detekce anomálií. [7]

V podnikovém nasazení je výhodné implementovat řešení, které umožňuje centrální správu pomocí administrátorské konzole. V konzoli lze provádět globální nastavení všech klientských stanic, spravovat aktualizace, spouštět on-demand skenování či mít přehled o

infikovaných stanicích a verzích instalovaných aktualizačních balíčků. Zmiňované funkcionality nabízí řada firem například ESET s rodinou antivirových programů Endpoint a k jejich správě lze použít Remote Administrator Server a Remote Administrator Console. [11]

3.2.6 Antispam

Antispam chrání mail server a stará se o tzv. message hygienu neboli zabraňuje příjmu spamu do doručené pošty či přijmu virů v příloze emailů. Dnešní trend způsobu útoků je cílení přímo na koncového uživatele například pomocí přílohy emailu ukrývající infikovaný pdf soubor či zip soubor. E-mail se tváří, že pochází z důvěryhodného zdroje, ale je podvrhnut útočníkem a obsahuje virus. Primární funkcí antispamu je chránit uživatele před přívalem množící se nevyžádané pošty. Antispam filtruje poštu pomocí řady parametrů a vyhodnocenou poštu na základě konfigurace přesune do klientského spamového koše, serverového spamového koše anebo rovnou vymaže. Filtr lze nastavovat například podle výskytu nežádoucích slov v emailu (kasino, porno) nebo typu souboru v příloze. Antispam obsahuje algoritmus, který hodnotí obsah emailu bodovou stupnicí dle výskytu typických spamových ukazatelů. Administrátor pak nastaví hraniční bodovou hodnotu, co ještě nelze požadovat za spam a co naopak už spam je. [1,18]

Dalším nástrojem, kterým je antispam vybaven, je kontrola odesílatelů oproti blacklistu. Blacklist je seznam nežádoucích adres ze kterých se šíří spam. Blacklist může vytvořit správce lokálně v nastavení antispamu, ale existuje i celá řada centrálních blacklistů. V centrálních blacklistech jsou umístěny zdroje spamů a zablokováno jejich další šíření. Na blacklist se může dostat i důvěryhodná firma v případě, že některý počítač je infikován a útočníci ho používají k šíření spamu. Poté je potřeba infikovanou stanici odhalit, odstranit virus a požádat o odstranění z blacklistu. [1,16,18]

Antispam obsahují v základním provedení již novější mailové servery, jako je MS Exchange 2010 či MS Exchange 2013. Microsoft nabízel i placené řešení s názvem Forefront, které zaniklo a antispam přesunul pouze do svých cloudových služeb. Dalším řešením antispamové ochrany může být ESET Mail Security, dělící se na řešení dle typu mailového serveru. [1,18]

3.2.7 Firewall

Firewall neboli v překladu bezpečnostní brána je buď fyzické síťové zařízení, nebo software, který ochraňuje koncové stanice či servery. Oba dva typy se starají o oddělení vnitřní a vnější sítě a povolení komunikace, která je povolena v konfiguraci firewallu. Brání příjmu nebo odesíláním dat bez vědomí uživatele. Jednotlivé druhy komunikace jsou zajištěny přes povolené porty. Ideální konfigurace firewallu je zakázat všechny komunikační porty a otevřít pouze ty, které jsou opravdu potřebné. [1,16,18]

Softwarový firewall se dělí na dva druhy. Typicky na softwarový firewall chránící perimetr sítě a firewall chránící koncové stanice. Softwarový firewall chránící perimetr sítě je obvykle Linuxová distribuce s funkcionalitou firewallu. Firewall chránící koncové stanice v základním provedení obsahují dnešní novodobé operační systémy jako Windows 7, Windows 8 atd. Aktuálně je moderní uchopit otázku bezpečnosti komplexně a nerozdělovat ji na antivir, antispam a firewall, ale nasadit jedno řešení, které obsahuje všechny potřebné bezpečnostní nástroje. Existuje celá řada end point produktů například lze zmínit ESET End Point Security nebo Symantec End Point Protection. [11,19]

Hardwarový firewall se používá častěji. Jedná se o síťový prvek umístěn na perimetru firemní sítě, tedy na hranici mezi vnitřní a vnější sítí. Funguje podobně jako softwarový firewall. Zajímavá funkce, která rozšiřuje možnosti zabezpečení, je například DMZ. DMZ je akronym pro Demilitarized zone neboli demilitarizovanou zónu. Oblast, kde se nachází aplikace nebo servery, které mají přidělenou veřejnou IP adresu či jsou přístupné z internetu a je zapotřebí je oddělit od vnitřní sítě. [1]

3.2.8 IDS

IDS je akronymem Intrusion Detection System je detekční software pro detekování hrozeb, které se nachází v infrastruktuře. Výhodou IDS je, že detekuje i činnosti, které předchází hackerskému útoku jako je skenování portů. Pomocí IDS lze sledovat i to co se děje uvnitř sítě nejen na perimetru. Prvotní nastavení se zabývá tím, kde má být prováděno sledování. Jedná se o stanovení logického místa, v němž systém bude monitorovat jisté události, například všechna komunikace, která projde skrz firewall. Druhým bodem je nutné určit, co se má sledovat. Jaké události je nutné hlídat, například skenování portů. Poslední bod, který je nutné specifikovat, je co se má stát, nastane-li určitá akce, odeslání emailů či jiná notifikace. Omezení IDS je, že lze pouze monitorovat jedno rozhraní a kontroluje pouze

podmínky, které jsou předem definované. IDS vyžaduje složitější instalaci a konfiguraci kvalifikovanou osobou. [1,22]

IDS systémy se dělí na dva druhy. Network based Intrusion Datection Systém (NIDS) je umístěn v síti a sleduje veškerý provoz. Sleduje příchozí a odchozí komunikaci, ale i vnitřní toky. NIDS je zpravidla umístěn před a za firewallem. NIDS je například Cisco Secure IDS či Snort. Dalším druhem je Host based Intrusion Detected Systém (HIDS). Jedná se o speciální softwarovou aplikaci, která se nainstaluje na server a zde sleduje provoz a změny souborového systému. Důležité je nasadit HIDS na aplikační servery či poštovní servery dostupné z internetu. Příkladem HIDS je Dragon Squire či Intruder Alert.[12]

3.2.9 IPS

IPS neboli Intrusion Prevention System rozšiřuje funkčnost IDS. Spolupracuje s IDS a provádí aktivní obranu proti dokončení útoku. Systém umožňuje ukončit podezřelý útok zprávou o nedosažitelnosti nebo vytvoří přístupový seznam pro blokování IP adres a útočníkovu IP adresu blokuje. IPS přímo pracuje s firewallem, kdy je schopen zasahovat do konfigurace. IPS dokáže blokovat DOS útoky či vytvořit geolokační filtr, kdy preventivně znepřístupní služby pro IP adresy z rizikových zemí, jako je Rusko nebo Čína. V dnešní době se dodává firewall, VPN, IDS a IPS součástí jednoho zařízení nazýváno Unified Threat Management (UTM). To umožní lepší komunikaci mezi zařízeními, lepší správu a ušetří i místo v serverovně. Takové zařízení nabízí například SOPHOS. [12]

3.2.10 Proxy server

Proxy server filtruje obsah komunikace mezi koncovou stanicí a internetem a to na aplikační úrovni. Firewall blokuje komunikaci na úrovni služeb, proxy server detailně prověřuje komunikaci konkrétní služby. Například je schopen kontrolovat obsah komunikace služby http a případnou nekorektní či zakázanou komunikaci zablokovat. Lze získat podrobný přehled komunikace jednotlivých aplikací a zakázat peer to peer komunikaci sloužící pro stahování nelegálního obsahu. Proxy server dokáže skrýt IP adresu koncového uživatele a komunikace mezi firemní sítí a uživatelem působí jako by v síti byl jeden koncový počítač, což svým způsobem anonymizuje uživatele při pohledu z internetu. Další výhodou proxy serveru je, že dříve načtené stránky uchovává v cache paměti a při opětovném požadavku na otevření webové stránky je znovunačtení rychlejší. Nastavení proxy serveru je obdobné jako u firewallu, základem je všechno zablokovat a povolovat

pouze potřebné komunikační kanály. Nevýhodou je, že při filtraci paketů může dojít ke zpomalení provozu. [1]

3.2.11 WLAN

WLAN neboli Wireless LAN zkráceně WIFI se stala běžným prostředkem pro připojení k internetu a je dostupná na každém kroku (kavárny, letiště, hotely, firmy atd.). Každý člověk se chce připojit k internetu svým mobilním telefonem, tabletem či notebookem. S obrovskou rozšířeností tohoto druhu připojení však zůstává otázka, zdali je dostatečně zabezpečené a datový přenos není modifikován anebo odposlouchán. Výchozím bodem bezdrátové sítě je bezdrátový přístupový bod (Wireless Accesss Point, WAP), který slouží k připojení do lokální sítě. WIFI se nyní řídí normou IEEE 802.11n. Jedná se o normu, která upravuje bezdrátový přenos dat ve frekvenčním pásmu 2,4 GHz. Standart umožňuje bezdrátový přenos až 200Mbps a dovoluje nejmodernější způsoby zabezpečení jako je WPA2. WPA2 je nejnovější druh zabezpečení, obsahuje používání kvalitnějšího šifrovacího algoritmu AES. Jako jediný druh zabezpečení ještě nebyl prolomen. [22]

Z hlediska bezpečnosti firemní sítě je nutné se dívat na několik scénářů. Za prvé, kdy se útočník může snažit proniknout do firemní sítě. Nevýhoda WIFI sítě je, že není omezená vzdálenost vysílání a signál může být zachycen i z prostoru nepatřící firmě. Signál lze ještě zesílit pomocí směrové antény nebo zesilovače. Dalším nebezpečím může být, pokud útočník umístí svůj přístupový bod, který bude shodně nakonfigurován s firemním přístupovým bodem a mobilní zařízení se k němu automaticky připojí. Útočník je schopen, následovně sledovat komunikaci. Nebezpečí může být schované i v podobě firemní návštěvy, která požádá o přístup k WIFI. V neposlední řadě je nutné dát pozor, k jakým přístupovým bodům se zaměstnanec se svým mobilním zařízením připojuje, zda jsou dostatečně bezpečná a nemůže docházet ke sledování či jinému zneužití. [22]

Pro eliminování všech výše zmíněných hrozeb je nutné obzvláště správně nakonfigurovat WAP. Ideálně používat nejméně WPA 2 Personal, nejbezpečnější je WPA 2 Enterprise, který využívá k autorizaci uživatelů radius server. Dále skrytí názvu sítě (SSID) a zapnutí kontroly MAC adres. Do sítě se pak připojí pouze povolená zařízení. Použití dostatečně silného a složitého hesla. Přístup do WAP zabezpečit dostatečně silným heslem. WAP fyzicky zabezpečit. Vytvoření SSID pro návštěvy WIFI sítě, která bude oddělena od firemní sítě. Sledovat pirátská SSID. Například pomocí softwaru InSSIDer. Nejdůležitější ze všeho je však stanovení bezpečnostních politik, které pokrývají oblast bezpečnosti WIFI

sítí. Zákaz připojování do neznámých nebo málo zabezpečených sítí, dodržování pravidla, že se síťovými zařízeními smí manipulovat pouze oprávněný zaměstnanec atd. [12]

3.2.12 LAN

Akronym LAN označuje Local Area Network. Jedná se o síť uvnitř místností, budov nebo malých areálů. Zneužití LAN je to pro případného útočníka složitější než průnik do WIFI. Případný útočník se musí nacházet na půdě firmy a musí mít přístup k síti. Pokud splní toto kritérium, je nutné mu znemožnit případný útok. Nejefektivnější je bezpečnostní mechanismy nastavit na aktivních prvcích nebo návrhem sítě. Návrh sítě znamená oddělení sítě pomocí virtuálních sítí tzv. VLAN. Pomocí VLAN lze oddělit mezi sebou jednotlivé uživatele a dát jim přístup ke zdrojům, které nutně potřebují. Servery by měly být umístěné v jedné VLAN a měl by být zamezen k nim přístup osobám ze zasedací místnosti atd. [19]

Další bezpečnostní mechanismus, který by měl být v síti obsažen, je ochrana pomocí povolených MAC adres. Jedná se o bezpečnostní nastavení na switchi, kdy je definováno, jaká MAC adresa může konkrétní zásuvku využívat. Další funkcí může být např. omezení počtu MAC adres na port. Nastavení zamezí tomu, aby útočník nezahltil switch a ten se poté nezačal chovat jako HUB a neposílal komunikaci všem portům namísto pouze portům, mezi kterými probíhá komunikace. [19]

Funkce DHCP Snooping umožňuje povolení přidělení IP adres pouze DHCP serverům, které jsou povoleny. Tato funkce vylučuje možnost, aby některý zaměstnanec či útočník přinesl špatně nakonfigurovaný směrovač a ten přiděloval špatné adresy koncovým zařízením. Společně s funkcí DHCP Snooping je příhodné aktivovat funkci IP Source Guard. Tato funkce slouží pro zaznamenávání přidělených adres DHCP serverem a pokud se v síti objeví IP adresa, která nebyla přidělena DHCP serverem, komunikace je zablokována.

3.2.13 VPN

Akronym VPN znamená Virtual Private Networks v překladu virtuální privátní sítě. VPN umožňuje přístup zaměstnancům do firemní sítě, odkudkoliv například přístup k file serveru ze vzdálené pobočky či k jiným zdrojům, které nejsou přístupné z internetu. Jedná se o šifrované síťové spojení, které ke své činnosti využívá bezpečný komunikační tunel. Komunikace je šifrovaná SSL certifikátem nebo technologií IPSEC, nelze ji tedy odposlouchávat. Použitím této technologie vznikají však jiná bezpečnostní rizika. Pokud klient vytočí VPN spojení, ocitne se daný počítač ve firemní síti a pokud stanice neodpovídá

firemním bezpečnostním standardům či je infikovaná nějakým virem, může dojít k rozšíření infekce do sítě. Z toho důvodu je nutné dostatečně autorizovat připojené počítače a instalovat VPN klienta a certifikát pouze na stanice, které splňují bezpečnostní normy dané firmy. K vytvoření VPN spojení a připojení do lokální sítě slouží VPN koncentrátor. VPN koncentrátor může být hardwarový už jako součást firewallu, nabízí firma Cisco, či softwarový produkt s názvem OPEN VPN. Na stanicích, které se připojují k VPN koncentrátoru, je pak nainstalován klient a nahrán certifikát, pomocí kterého je spojení šifrováno. [12]

3.2.14 Zálohování

Zálohování dat by mělo být základní preventivní opatření před ztrátou dat a nemělo by dojít k jeho podcenění. Většina uživatelů, kteří nezálohují, začnou zálohování brát vážněji po-té, co je postihne ztráta dat. U firemních dat je zálohování nutností dvojnásob. Přijde-li až poté co firma o data, může to způsobit existencionální problémy. Zálohování předchází nejčastěji ztrátě dat vinou selhání hardwaru. Data jsou uložena na hardwaru, který má omezenou životnost a je poruchový, ať už se jedná o plotnový, SSD nebo flash disk či optické medium. Další scénář, kdy zálohování může zachránit data, je vinou softwarového problému jako je nakažení počítačovým virem, který může data zašifrovat a uživatel k nim nemá přístup nebo chybou programu způsobenou aktualizací špatného aktualizačního balíčku. Posledním scénářem může být chyba uživatele. Kdy smaže data nebo provede nechtěnou modifikaci. [22]

Metody zálohování lze rozdělit na tři způsoby. První způsob je kompletní záloha. Jedná se o metodu, kdy dojde k provedení zálohy celého počítače včetně operačního systému. Provedení další zálohy se provede k vytvoření kopie všech dat, kdy kopie není závislá na předchozí. Kompletní záloha dat je účinná metoda. Není potřeba znát předchozí zálohu. Je však datově i časově náročná. Druhým způsobem je inkrementální metoda neboli přírůstková metoda. Provedení zálohování přírůstkovou metodou předchází vytvoření kompletní zálohy. Poté jsou prováděny přírůstkové zálohy souborů, které se změnily oproti původní kompletní záloze. Výhodou metody je zkrácení potřebné doby pro zálohování a není přenášeno takové množství dat oproti předchozí metodě. Nevýhodou je, nutnost vlastnit nejen poslední zálohu, ale i předchozí kompletní zálohu včetně všech přírůstkových záloh v případě obnovy, což je náročné na úložný prostor. Třetí používaná metoda je rozdílová. Opět je vytvořena kompletní záloha, ale místo aby byla provedena změna oproti poslednímu

přírůstku, dojde k vytvoření změny oproti kompletní záloze. Výhodou je, že nedochází k takovému datovému přenosu jako v případě vytvoření kompletní zálohy a při obnově není potřeba předešlé přírůstkové zálohy, což je úspornější na datové uložiště. [19]

Úspěšné zálohování by mělo začít u vytvoření zálohovací strategie. Strategie by měla obsahovat ohodnocení důležitých dat, která chce uživatel nebo firma chránit. Dále stanovení objemu dat, která se budou zálohovat a intervalu, ve kterém se zálohování bude provádět. Často měněné důležité soubory budou zálohovány několikrát denně, méně důležité soubory budou ukládány méně často. Příhodné je nastavit automatické zálohování a celé zálohování automatizovat, aby se o zálohování nemusel uživatel starat, pouze kontrolovat proběhnuté zálohování.

Dalším krokem je zvolit vhodné médium, na které se zálohy budou ukládat. Může být použit NAS server, USB disk, cloudové uložiště nebo magnetické pásky. Pro dosažení optimální rychlosti zálohování, aby celý proces zálohování nezpomaloval běžnou denní práci a médium bylo spolehlivé a cenově dostupné. Záložní kopie by měli být zašifrované a uloženy v jiné lokalitě než je sídlo firmy neboli off-site uložišti jako prevence proti hrozbě živelné katastrofy. Soubory, ke kterým se již delší dobu nepřistupuje, je dobré uložit na archivační médium o dlouhé životnosti nebo případně uložit na NAS zařízení, aby nedocházelo k provádění zálohování těchto dat a byla ušetřena kapacita určena pro zálohování. Vhodné je provádět archivační zálohy v pravidelných cyklech a archivační zálohy umístit off-site pro případ požadavku obnovení dat delší než je časový úsek provádění zálohy například rok zpět atd. [14]

3.2.15 Obnovení

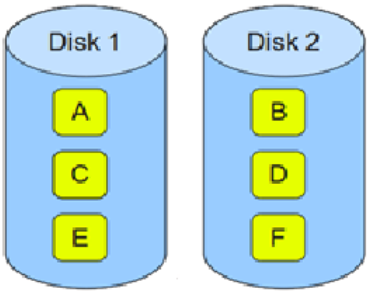
Se zálohováním souvisí obnovení dat ze zálohy. Dojde-li na nejhorší a je potřeba provést obnovení, obvykle je situace provázena stresem. Proto je důležité mít vypracován plán obnovení dat ze zálohy, řídit se tímto postupem a v neposlední řadě provádět pravidelné testování obnovení dat ze zálohy v pravidelných intervalech. Měla by být definovaná časová náročnost obnovy dat, která by měla být schválena od vedení firmy a v případě, že tato doba nevyhovuje, je zapotřebí celý proces zálohování optimalizovat. V případě serverů, je-li využitá virtualizace, je vhodné zálohovat celé virtuální servery, ať už se jedná o virtuální platformu VM WARE nebo HYPER V. Jejich obnova je mnohem rychlejší a není potřeba přeinstalovat aplikace a konfigurovat je. Virtuální servery lze obnovit na jakýkoliv hardware, což je značná výhoda, oproti klasickému zálohování, kdy obnova musí být provedena na

stejný hardware. V případě vytváření zálohovacího plánu je nutné brát v úvahu volbu zvoleného média. Obnova bude jistě pomalejší z cloudového uložiště než z USB disku. Rychlost obnovy bude záviset na provedené kompresi souborů a uložení na jiném objektu, rychlosti získání záložních kopií a záložního hardwaru v případě poruchy.

3.2.16 Ochrana proti HW selhání

Možnost selhání hardwaru může eliminovat nasazení správných ochranných mechanismů. Tyto mechanismy slouží pro případ poškození hardwarových komponentů a jejich nahrazení bez ztráty kontinuity všech procesů. Nejpoužívanější mechanismus proti výpadku hardwaru se nazývá RAID. Jedná se o nastavení pevných disků tak, aby zabezpečily uložená data a v případě poruchy jednoho disku mohl systém nadále vykonávat svoji funkci bez nutnosti obnovy dat. RAID neslouží jako náhrada zálohování, zálohování je nutné provádět i při použití RAID. Nejpoužívanější RAID jsou: RAID 0, RAID 1, RAID 5 a RAID 10.

RAID 0

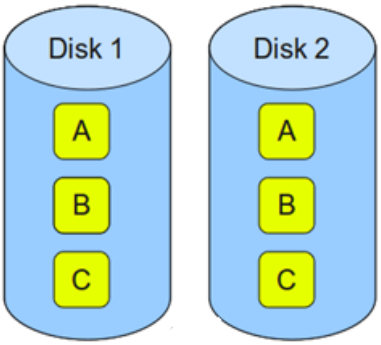


Obrázek 1: Uložení dat v RAID 0

Zdroj: *RAID 0. [online]. [cit. 2015-03-15]. Dostupné z: http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/*

Při použití RAID 0 nedochází ke kontinuální činnosti při výpadku jednoho z disků. Při poruše jednoho z disků jsou veškeré informace ztraceny. Výhodou tohoto zapojení je ale zvýšená kapacita, kterou lze takto dosáhnout. Jedná se o standardní zapojení disků. Nelze použít pro ukládání důležitých dat, pouze pro data, o které může firma přijít.

RAID 1

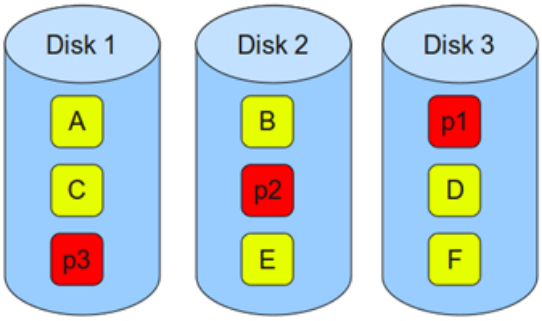


Obrázek 2: Uložení dat v RAID 1

Zdroj: *RAID 1. [online]. [cit. 2015-03-15]. Dostupné z: http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/*

RAID 1 je nejpoužívanější RAID, někdy se používá název zrcadlení. Data jsou uložena na oba disky, na původní i na zrcadlený disk a v případě poruchy jednoho z disků jsou stále uložena na druhém. Po výměně poškozeného disku za nový dojde k překopírování zrcadlených dat na nový disk. Nevýhoda je poloviční kapacita oproti RAID 0. Nutné je použít minimálně dva stejné disky.

RAID 5



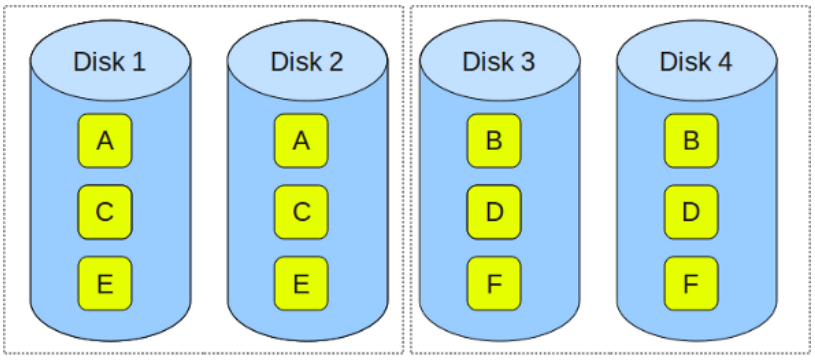
Obrázek 3: Uložení dat v RAID 5

Zdroj: *RAID 5. [online]. [cit. 2015-03-15]. Dostupné z: http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/*

RAID 5 obsahuje minimálně 3 pevné disky. Data jsou uložena pouze jednou, pro případ vyřazení jednoho disku z provozu slouží samo-opravný kód, pomocí kterého lze dopočítat chybějící data. Při poškození dvou disků RAID 5 data neochrání a data jsou

ztracena. Výhodou je zvýšená kapacita a rychlejší čtení. Nevýhodou je pomalejší zápis, při kterém dochází k výpočtu samo-opravného kódu.

RAID 10



Obrázek 4: Uložení dat v RAID 10

Zdroj: *RAID 10. [online]. [cit. 2015-03-15]. Dostupné z: http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/*

Pro použití RAID 10 je nutné použít minimálně 4 pevné disky. RAID 10 je složen ze dvou dvojic disků zapojených do RAID 1 a tyto dvojice zapojeny do RAID 0. Tento způsob je nejvíce efektivní, co se týče kapacity, ochrany před výpadkem, rychlosti čtení i zápisu. Obvykle se používá pro uložení databází. [15]

Další ochranou proti selhání hardwaru může být použití serveru se dvěma zdroji napájení. V případě výpadku jednoho dojde k přepnutí na druhý. Podobnou metodu lze provést pro vyšší síťovou dostupnost, při zapojení dvou síťových karet. Použití dvou síťových karet a správného nakonfigurování je nazýváno NIC teaming. NIC teaming nejenže slouží jako záloha pro výpadek jedné ze síťových karet nebo sítového spoje, ale také zvyšuje síťovou propustnost, kdy jsou pro síťový přenos použity oba síťové adaptéry.

Pro zvýšení dostupnosti je možné zapojit více počítačů do tzv. failover clusteru. Failover cluster funguje tak, že data mezi počítači se replikují a v případě poruchy či plánované údržby je funkce serveru nahrazena činností jiného serveru, který se v clusteru vyskytuje. V případě smazání či jiné chyby je operace provedena na všech serverech a proto je zálohování i v případě použití failover clusteru nutností.

3.3 Útočníci a jejich nástroje

Útočník je osoba, která ohrožuje aktiva. Může se jednat o insidera neboli útočníka uvnitř organizace, nejčastěji zaměstnance anebo se útočník může pohybovat mimo organizaci a využít připojení k internetu jako informační médium pro provedení útoku. Termín útočník není častý, častější je označení hacker. V minulosti označení hacker se používalo pro označení skutečných expertů ve svém oboru, typicky studenti působící na půdě akademie, kteří se později stávali řediteli velkých organizací. Mezi hackery patřil i Bill Gates nebo Mark Zuckenberg. Hackeři z těchto dob jsou označováni jako stará garda. Novodobí hackeři jsou značně problematičtější. Jejich činnost se nepohybuje rozhodně na půdě akademie, ale pohybují se tam, kde za svoji činnost dostanou zaplaceno. Novodobí hackeři se stávají nástroji pro průmyslovou špionáž, krádeže dat, vydírání a další kybernetické zločiny. S tímto vznikají nové pojmy označované jako hacktivismus a kyberterorismus. Hacktivismus je termín určený jako skupinový útok na konkrétní cíl umístěn na počítačové síti. Například mezi hacktivisty patří skupina Anonymous o které je v poslední době hodně slyšet. Kyberterorismus je definován výrokem: „Jde o tzv. neletální (nikoli smrtící) formu teroristické činnosti realizovanou skrze služby, které podporuje a sdílí daná informační či komunikační síť. Sekundárním důsledkem kyberútoku ale může být i fyzická likvidace konkrétního objektu nebo systému, což může vést i ke ztrátám na lidských životech.“ [26]

Pozitivní vliv novodobých hackerů je vznik bezpečnostních záplat, service packů a vytvoření nového trhu s bezpečnostními technologiemi, kterému se v poslední době obzvláště daří.

Hackery v základním dělení lze rozdělit na dva typy hackerů. Na hackery, kteří si své oběti vybírají náhodně anebo cílí na konkrétní subjekt svého útoku. Druhá skupina je nebezpečnější, jelikož se jedná o profesionály, kteří za svoji činnost dostali zaplaceno a nadělají větší škody. Další skupinou jsou etičtí hackeři. Etický hacker je profesionální hacker, který je najat firmou pro provedení hackerského útoku za účelem zjištění bezpečnostních nedostatků ve firmě a jejich následné zlepšení. Certifikaci etických hackerů zastřešuje organizace EC-Council. Crackerem je nazýván útočník, který pronikne do systému za účelem finančního obohacení či pro vlastní zábavu. Jedná se o nejnebezpečnější skupinu, která vytváří nové útoky a objevuje nové bezpečnostní chyby. Útok může být veden od začátečníka, který našel na internetu návod a vůbec nemá znalosti v hackování až po

profesionála, který vytváří nové způsoby útoků. Posledním útočníkem může být zaměstnanec, který zkouší zabezpečení firmy, či se snaží získat chtěné informace. [17,18]

3.3.1 Počítačové hrozby a rizika

První webové hrozby se objevily na internetu již roku 1973. Jejich počet se stále zvyšuje a jsou používány sofistikovanější metody pro provádění útoků. Počítačové hrozby se mohou skrývat prakticky kdekoliv. Ať už na síti, pomocí které se připojujete k internetu, na webových stránkách, v aplikaci v mobilním telefonu nebo ve stolním počítači, WIFI síti, flash disku, emailové komunikaci, v souborech, v chování zaměstnanců atd. Hrozbou může být chyba v bezpečnostním protokolu, v kódu, vir, nízké zabezpečení a cokoliv, co může vést k nežádoucí změně dat. Základní hrozby jsou: únik informací, narušení integrity, potlačení služby, nelegitimní použití a podobně. Z hrozby vyplývá míra pravděpodobnosti neboli riziko uplatnění hrozby. Riziko roste s hodnotou aktiva. Všechny uvedené hrozby jsou definovány jako kybernetická kriminalita neboli kybernalita. Hrozby a s tím spojená rizika je potřeba minimalizovat pomocí ochranných mechanismů, politik, procesů a zajistit tak klidný spánek uživatelům počítačů a jiných mobilních zařízeních. S počítačovou hrozbou je potřeba rozlišovat termín počítačový útok. Počítačový útok je realizovaná počítačová hrozba. [16]

3.3.2 Nástroje útočníků a postup útoku

K provedení útoku používají útočníci celou řadu nástrojů. Útočník musí prvně zvolit, co chce útokem získat, např. změnu dat, krádež dat atd. Po definování účelu útoku obvykle přichází průzkum cíle, jde-li o cílený útok. Průzkum slouží k definování slabých míst a ke správné volbě nástroje, který k útoku bude použit, a formě útoku. Průzkum je označován jako „slídění“. Je to obdobné jako když pachatel trestné činnosti si obhlíží oběť či objekt svého útoku. Hackeři prvně zjistí způsob připojení cíle k internetu, přiřazenou IP adresu, DNS název a veřejné IP adresy. Toto lze realizovat nejjednodušeji pomocí příkazu nslookup. Další informace k realizaci útoku je operační systém, existence IDS či IPS nebo jiných bezpečnostních nástrojů, úroveň fyzického zabezpečení, druh autorizace atd. Případně lze i sledovat zaměstnance a poté je využít k útoku, odcizit laptop, zaslat podvržený email, vydírat atd. Uvedené průzkumné techniky jsou označovány jako pasivní. Mezi aktivní způsoby patří například skenování portů. Skenování portů vypoví útočníkovi, na jakém portu je spuštěná jaká služba, a které porty jsou otevřeny. V případě, že organizace využívá IPS nebo IDS,

skenování portu je vyhodnoceno jako bezpečnostní hrozba a upozorní administrátora. Skenování portů lze provést například pomocí nástroje nmap. Nástrojem fing lze například zjistit všechna zařízení v síti. Po získání informací o cíli je třeba informace vyfiltrovat a sepsat a vybrat, jakou cestou získat přístup do systému. K získání přístupů anebo požadované akce je potřeba využít nějaký z útoků anebo kombinaci útoků pro zmatení oběti. Nové útoky, proti kterým nebyla zatím vydaná ochrana, jsou označovány jako Zero day útoky. Jedná se o nejžádanější útoky na hackerské scéně a je s nimi i obchodováno. Zájem je ze strany útočníků i výrobců softwaru, kde se chyba nachází.

Typy útoků a techniky můžou být:

- Útok na operační systém nejčastěji pomocí známých chyb, které uživatel neaktualizoval anebo pomocí otevřených portů.
- Útok na aplikaci neboli exploit pomocí chyb umístěných v aplikacích jako je JAVA, Flash player, Adobe Acrobat reader nebo jiné.
- Nesprávná konfigurace zapnuté nebezpečné služby jako je FTP, TELNET a nastavení defaultního jména a hesla u síťových zařízení typicky uživatelské jméno admin a heslo admin.
- Útok hrubou silou je spuštění postupného hádání hesel. Čím větší složitost hesla, tím je snížená možnost uhádnutí hesla. Nástrojem pro crackování hesel je například Cain & Abel, který dokáže crackovat hesla do různých míst nebo Aircrack, který crackuje hesla do bezdrátových sítí zabezpečených pomocí WPA nebo WEP.
- Sniffing neboli odposlech se používá pro odposlouchávání provozu na síti a získávání citlivých informací, které po síti tečou, jako jsou hesla a uživatelská jména, pokud je komunikace nezašifrovaná. Pro sniffing se používají sniffery neboli analyzátory packetů, jako je Microsoft Network Monitor nebo Wireshark. Nejčastěji je sniffing používám jako man in the middle, kdy útočník je připojen mezi cílovým a zdrojovým počítačem a komunikace probíhá přes útočníka.
- Přetečení paměťového bufferu - zasílání neúměrného množství instrukcí, se kterými pracuje vyrovnávací paměť a ta vyvolá přetečení bufferu. To způsobí, že systém se začne chovat nestandardně a útočník může vklouznout do systému.
- ARP spoofing nebo ARP poisoning je vydávání útočníka za někoho jiného, útočníkovi pak chodí data určená pro jiný počítač.

- Keylogger - může se jednat o hardwarový anebo softwarový nástroj, který zaznamenává veškeré stisknuté klávesy. V tomto řetězci je pak jednoduché najít požadované informace.
- Cross Site Scripting je technika, kterou útočník ovládne webové stránky nebo aplikace tím, že do nich vloží část Javascriptového kódu. Tím je mu dovoleno vyřadit stránky z provozu, vytvořit si účet či cokoliv jiného.
- SQL injection je metoda podobná Cross Site Scripting s tím rozdílem, že kód je vkládán do SQL databáze.
- Backdoors neboli zadní vrátka jsou většinou umístěna v softwaru a slouží pro obejití autentizace například pro servisní účely, avšak jsou využity pomocí cracknutí jako exploit do aplikace a následného ovládnutí PC.
- Malware je označení pro obecný druh počítačového viru a spadají do něho všechny typy virů.
- Trosjký kůň - jedná se nejčastěji o aplikaci volně šířenou anebo jako warez, v které je umístěn škodlivý software, pomocí kterého je počítač ovládán. Obsahuje obvykle jiné nástroje jako je keyloger, sniffer atd.
- Spyware sleduje uživatele a odesílá informace bez jeho vědomí útočníkovi. Typicky data o navštěvování stránek atd. Bývá součástí freewarů. Může se vyskytovat i na mobilních telefonech.
- Ransomware je vyděračský vir, který po oběti požaduje „výpalné“ za odstranění viru. Jedná se například o policejní vir, kdy vir zablokoval počítač a vyzíval k zaplacení částky. Nejnovější verze ransomwaru uživateli zašifrují data a žádají finanční částku. Po zaplacení uživateli je zaslán klíč, pomocí něhož lze dešifrovat data. Prozatím není lék na druh tohoto viru.
- Rootkit maskuje přítomnost zákeřného malwaru, jako jsou trojské koně, spyware a jiné.
- Červ je specifický malware, který se šíří po síti a infikuje další počítače. Nejen, že se šíří po síti, ale obvykle současně v sobě ukrývá exploit a nebo jinou hrozbu.
- Security software disabler vyřadí z provozu bezpečnostní mechanismy, jako je firewall či antivir.
- DDOS útok - akronym znamená Distributed Denial of Service a v překladu značí odmítnutí služby. Provedením útoku DDOS dochází ke zpomalení až k vyřazení

webové stránky. DDOS útoky mohou mít pouze varovný charakter nebo v rámci nich může dojít k jinému druhu útoku. DDOS útok je prováděn velkým množstvím počítačů označovaných jako bootnet. Do bootnetu mohou být zapojeni i nic netušící uživatelé. Bootnet pak generuje velké množství požadavků na server označovaných například jako Ping-flood, kdy generují žádost o odezvu na příkaz ping a nebo SYN flood, kdy je odesílaná záplava TCP/SYN paketů, či jiné typy DDOS útoků.

- Phishing je podvodná technika, kdy útočník se snaží z oběti vylákat přihlašovací údaje, čísla kreditních karet a podobné. Principem je, že útočník rozešle podvodné emaily s odkazem na podvržené stránky, kde je oběť vyzvána k zadání přihlašovacích údajů například k internet bankingu a podobně.
- Spam je technika, kdy jsou pomocí emailu zasílány nežádoucí reklamní či infikované emaily uživateli.
- Clickjacking je novodobá hrozba, která se rozšířila společně se sociálními sítěmi. Na sociální síť je umístěn odkaz na legitimní stránku, nad tímto odkazem je však umístěno neviditelné tlačítko, které provede skrytou akci například stažení viru.
- Anonymizer slouží útočníkům k zakrytí stop a znemožnění určení odkud útok přišel. Nejznámější je zřejmě anonymizer TOR.
- Reverse ingeneering je metoda, kdy hacker se snaží určit, jak je software nebo jeho část sestrojena a pomocí těchto znalostí zjistit slabiny v systému.

Existuje další celá řada nástrojů a možných útoků. V dnešní době je nejčastější způsob šíření malwaru přímo na koncového klienta. Není nutné pronikat přes firewall, IDP či IPS. Útočník podvrhne uživateli infikovanou webovou stránku nebo zašle email a postačí, aby uživatel otevřel přílohu (PDF či zip) emailu nebo klikl na odkaz a malware infikuje PC. A je-li PC součástí domény pak je jen otázkou času, aby hacker získal práva doménového administrátora a s tím i přístup ke všem firemním datům. Aby hacker nebyl odhalen je nakonec potřeba zamést po sobě stopy. A to vyčištěním logu, systémových registrů a vytvoření backdooru pro případný návrat. [16,17,19]

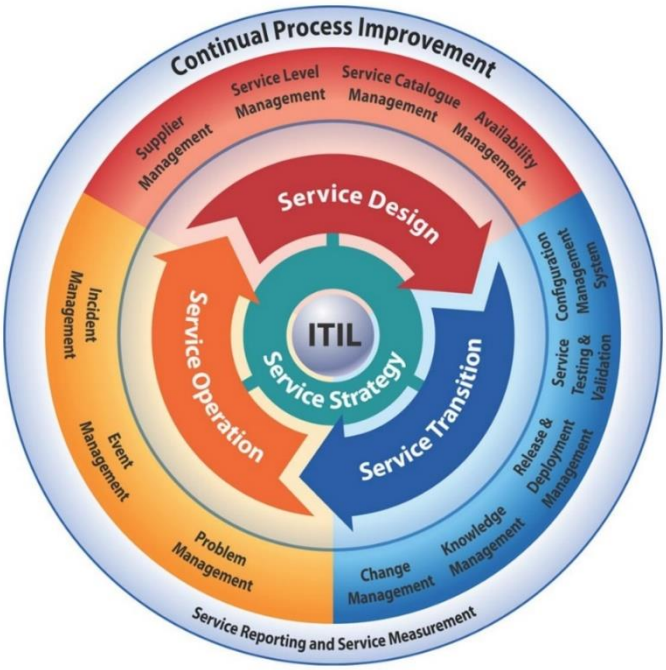
3.4 Certifikace

S přibývajícím počtem počítačových hrozeb na internetu jsou častěji ve firmách zaváděny certifikace na základě mezinárodně uznávaných standardů. Daná certifikace vypovídá, že organizace vlastnící certifikaci odpovídá daným normám a má zavedený

systém řízení bezpečnosti informací neboli ISMS. Aby mohla být zavedená daná norma, je potřeba mít podporu managementu, jinak je zavádění zcela zbytečné.

Organizace ISO v oblasti zabezpečení přináší celou řadu norem. Normy mají samozřejmě i české zastoupení pod hlavičkou ČSN ISO. Jako například norma ČSN ISO/IEC 27001. Norma postihuje široký záběr oblastí bezpečnosti. Obsahuje normy pro jednotlivé oblasti kupříkladu návod, jak pokračovat v činnosti organizace po havárii, řízení přístupů k informačním systémům, jak ve vývoji a údržbě systému, ve fyzické bezpečnosti, personální bezpečnosti, organizování bezpečnosti, správě počítačů, řízení aktiv. Veškerou certifikaci provádí certifikovaná autorita, která vydá společnosti po úspěšném ukončení certifikát potvrzující splnění normy. [19]

ITIL značí IT infrastructure library vytvořenou organizací Central computer and telecommunication agency. ITIL obsahuje dokumenty ve formě návodů neboli "best practices" pro řízení IT služeb. Pokrývá širokou oblast, jako je školení, profesionální kvalifikace, konzultace, softwarové prostředky, výměna zkušeností. ITIL řízení IT služeb rozlišuje tři základní úrovně procesů dle času a možnosti reagovat. Úrovně tvoří strategická, která se týká řízení IT služeb a zahrnuje řízení kvality, bezpečnost a organizační řízení. Dále taktickou úroveň obsahující plánování a kontrolu IT služeb, zajištující splnění požadavků zákazníka. Nakonec výčet úrovní uzavírá operační úroveň, kam spadá podpora IT služeb zajišťující efektivní poskytování IT služeb ze strany servisní organizace. ITIL pomáhá organizacím zefektivnit správu zdrojů a času s větší spolehlivostí. [20]



Obrázek 5: ITIL core

Zdroj: *ITIL: CORE. [online]. [cit. 2015-03-15]. Dostupné z: http://www.systemonline.cz/clanky/vyuziti-metodiky-it-governance-a-itil.htm*

COBIT (Control OBjectives for Information and related Technology) je principiálně podobná ITIL. Také obsahuje soubor "best practices" pro řízení ICT a dosažení strategických cílů organizace díky efektivnímu využití dostupných zdrojů a minimalizaci IT rizik. Rozdíl je, ale v oblasti pro koho je COBIT určen. Cílová skupina je top management a osoby, které provádějí audit. COBIT byl v současné době sloučen do jedné knihy o 213 stránkách, která je rozdělena do 34 procesů začleněných do čtyř hlavních skupin a to plánování a organizace, akvizice a implementace, dodání a podpora, monitorování a vyhodnocování. [21]

4 Praktická část

4.1 Popis firmy

Společnost, pro kterou byla realizována praktická část, si nepřála být jmenována. Z těchto důvodů bude v práci použit fiktivní název společnosti Giga a.s. Firma podniká v oblasti služeb. V současné době společnost zaměstnává kolem 200 zaměstnanců. Uživatelů, využívajících firemní informační prostředky, je však zhruba 75 %. Hlavní sídlo firmy je v Plzni, kde je umístěna majoritní část informačních technologií včetně serverů. Mimo centrálu vlastní další pobočky v Praze a Ostravě. Pobočky jsou připojeny k hlavním serverům pomocí VPN a terminálového serveru. Správa IT infrastruktury je realizovaná vlastními pracovníky plus je outsourcovaná externími zdroji.

4.1.1 Servery

Veškeré servery jsou umístěny v Plzni v sídle společnosti. Na serverech jsou umístěna firemní data, terminálový server, VPN koncentrátor, emailový server, firewall, databázový server a firemní aplikace, kterou používají jak interní zaměstnanci, tak i klienti. Celkově se jedná o 4 fyzické servery a 9 virtuálních serverů. Virtuální servery běží na virtualizační platformě Hyper-V. V tabulce níže jsou uvedeny názvy serverů a jejich funkce.

Tabulka 1: Přehled serverů

Název	Typ	Funkce
CP1	Fyzický	Hyper V hypervizor
CP2	Fyzický	Hyper V hypervizor
CP3	Fyzický	Zálohovací server
CP4	Virtuální	Domain controler, DHCP, DNS
CP5	Virtuální	Domain controler, Poštovní server, DNS
CP6	Virtuální	Terminálový server
CP7	Virtuální	Aplikační server
CP8	Virtuální	Databázový server
CP9	Virtuální	Souborový server
CP10	Virtuální	Aplikační server
CP11	Virtuální	VPN koncentrátor
CP12	Fyzický	Firewall

Zdroj: *Vlastní zpracování*

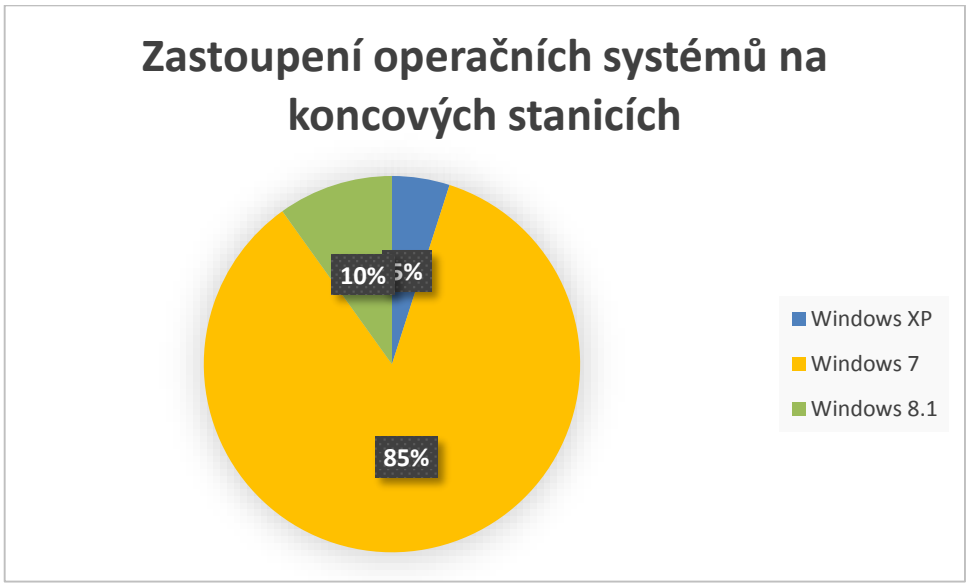
Servery CP1 a CP2 mají dva zdroje napájení pro vysokou dostupnost v případě výpadku jednoho z nich. Servery jsou následně připojeny do záložního zdroje UPS. Jsou v provedení blade a umístěny v racku. Server CP3 zapojen do UPS není. CP12 je zapojen v UPS. CP3 a

CP12 nemají provedení blade, ale jsou umístěny ve společném racku. Všechny servery jsou připojeny k síti přes 1 Gb/s linku, ale pouze jedním síťovým kabelem. Disky ve fyzických serverech nejsou šifrovány. Je na nich nastaven RAID 1, neboli zrcadlení, pro případ poruchy jednoho z disků. Fyzicky jsou umístěny v kanceláři IT, servery nejsou nijak zvlášť klimatizovány. Primárním operačním systémem na serverech je Microsoft Windows Server 2008 R2, na serverech CP10 a CP11, CP12 je nainstalován Linux v distribuci Debian. Přístup na servery pod operačním systémem Windows je umožněn pomocí vzdáleného přístupu pouze pro doménové administrátorské účty, ale je možný z kteréhokoliv počítače. Logy jsou umístěny na jednotlivých serverech a nejsou sumarizovány. Vyhodnocuje je pouze zaměstnanec IT. Servery nejsou zabezpečeny antiviry, pouze na mailovém serveru pro zvýšení message hygieny je nasazen spamový filter.

4.1.2 Koncové stanice

Koncových stanic ve společnosti je téměř 150. Třetinovou část koncových stanic tvoří přenosné notebooky, které jsou přenášeny mezi centrálou, pobočkami a bydlištěm zaměstnanců. Disky notebooků nejsou šifrovány. Průměrné stáří koncových stanic je 3,7 let. Udávané maximální stáří je 4-5 let. Nákup koncových stanic není prováděn centrálně, proto v síti se nachází různorodé značky a typy. Operační systémy zastoupené na koncových stanicích jsou zobrazené v grafu 1. Převážnou část tvoří operační systém Windows 7. V síti se vyskytují počítače, na kterých je nainstalován nepodporovaný operační systém Windows XP. Aktualizace operačního systému a podpůrných programů, jako je Adobe Acrobat Reader, JAVA či Adobe Flash Player, nejsou globálně spravovány ani sledovány. K ochraně koncových stanic je používán ESET Endpoint Antivirus, který zahrnuje pouze antivirus. Rovněž není centrálně spravován, i když tuto možnost produkt nabízí. Při kontrole stanic bylo zjištěno, že někteří uživatelé mají lokální administrátorské účty a že není definováno heslo do BIOS. Koncové stanice na centrále jsou připojeny do domény, stanice mimo centrálu se připojují do sítě přes VPN klienta. Na hlášení závad a veškerých IT požadavků je určen firemní helpdesk.

Graf 1: Přehled operačních systémů na koncových stanicích



Zdroj: *Vlastní zpracování*

4.2 Analýza zabezpečení

Analýza zabezpečení podrobně monitoruje stav zabezpečení firmy dle jednotlivých kategorií a odkrývá bezpečnostní pochybení a hrozby, které firmu ohrožují a měly by být eliminovány.

4.2.1 Bezpečnostní politika

Společnost má definovanou platnou bezpečnostní politiku schválenou vedením společnosti. Bezpečnostní politika pokrývá základní potřebné oblasti od definování bezpečnostních zásad pro zaměstnance i dodavatele a postihy při neplnění příslušných zásad. V bezpečnostní politice chybí podrobný havarijní plán a definovaná politika hesel neodpovídá bezpečnostním požadavkům.

4.2.2 Externí subjekty

Ve firmě působí tři externí subjekty, se kterými má firma odběratelský vztah v oblasti IT. Jedná se o dodavatele mzdového a ekonomického softwaru, dodavatele klientské aplikace a společnost určenou ke konzultacím v oblasti IT infrastruktury. S každým subjektem je podepsaná platná smlouva obsahující doložku o mlčenlivosti. Dodavatel má vstup pouze do oblasti, kde vykonává správu. Bohužel v těchto oblastech nejsou aktivovány záznamy o přístupu. V případě chyby dodavatele společnost není schopná prokázat zavinění

dodavatele. Ve společnosti jsou určeny osoby, které kontrolují dodávané služby. Prováděné kontroly jsou pouze namátkové a nikoliv pravidelné.

4.2.3 Řízení aktiv

Všechna aktiva ve firmě jsou evidována a záznamy pravidelně aktualizovány. Každé aktivum je opatřeno kódem a má určeného vlastníka, který se o aktivum stará a je zodpovědný za případnou ztrátu či poškození zařízení. Převod na vlastníka je formou předávacích protokolů a je zpětně dohledatelný.

4.2.4 Lidské zdroje

V IT oblasti pracují 3 pracovníci na úrovni IT junior, IT administrátor a IT senior. Uživatelé jsou rozděleni do příslušných rolí a na základě přidělené role personálním oddělením je přidělen i odpovídající přístup. Zaměstnanci při nástupu do pracovního poměru jsou proškoleni v používání firemních aplikací, jsou seznámeni s platnými směrnicemi a s postihy plynoucími z nedodržování platných nařízení. Při ukončení pracovně právního vztahu kontaktuje personální oddělení nejprve pracovníka IT a ten zablokuje uživateli přístup do všech systémů. Před ukončením předává svěřená aktiva určenému pracovníkovi. V úvodní dny pracovně právního vztahu zaměstnanec dostane plný přístup do lokální sítě a aplikací. Vhodnější by bylo po určitou dobu nového pracovníka prověřit a až poté mu přidělit přístupové údaje.

4.2.5 Fyzická bezpečnost

Pro vstup do firmy je nutné použít magnetickou kartu a projít turniketem kolem recepční. Zaměstnanci pracují v kancelářích maximálně po pěti osobách. Kanceláře jsou zabezpečeny zámkem. Prostory společnosti jsou zabezpečeny uspokojivě. Nedostatečné je umístění serverů a přenosných médií, které jsou snadno dostupné a zcizitelné. Pro přístup k serverům není využívána žádná dodatečná fyzická kontrola vstupu. Jako bezpečnostní perimetr je využíván turniket, který je společný pro všechny zaměstnance. Případný insider může k serverům bez větších problémů proniknout a napáchat škody. Servery se nachází v místnosti, kde není dostatečná klimatizace a jsou zde umístěny věci, které mohou snadno vzplát.

4.2.6 Bezpečnost zařízení

Servery jsou zapojeny do záložního zdroje UPS. Bohužel do UPS nejsou zapojeny síťové prvky a není připojen ovládací software k UPS, který by umožnil kontrolovat stav UPS a modifikovat nastavení. V blízkosti serveru jsou zásuvky připojeny na dieselový agregát, ale nejsou využity. Kabely jsou uloženy v panelech a je k nim přístup pouze prostřednictvím zásuvky či po odmontování panelu. Zásuvky nejsou nijak blokovány a jsou všechny aktivní pro jakékoliv připojené zařízení. Při vyřazení počítače je vyjmut disk i poškozený, který je evidován a skladován, aby nemohlo dojít ke zneužití dat. Ostatní komponenty jsou ekologicky zlikvidovány. Jiná vyřazená paměťová média jsou taktéž skladována, aby nedošlo ke krádeži dat. V případě potřeby likvidace paměťového média je určena firma pro bezpečnou likvidaci, zajišťující destrukci uložených dat včetně hardwaru v magnetické peci.

4.2.7 Řízení komunikací a řízení provozu

Dokumentace je neúplná. Chybí zdokumentování linuxových serverů CP10, CP11 a CP12. V případě poškození či havárie společnost není schopná obnovit servery do provozu schopného stavu. Obdobný případ nastává u switchů, které nejsou zdokumentovány a chybí přístupové údaje do managementu. Není vypracován plán obnovy pro případ poruchy. Není vypracován časový odhad a případný procesní postup obnovy dat. Testovací prostředí, kde se prvně nasazují nové verze a aktualizace, existuje pouze pro klientskou aplikaci a ekonomicko-účetní software. Zcela chybí testování systémových aplikací, či mzdového softwaru. Zcela chybí pravidelné monitorování systémových zdrojů, volných kapacit a dodatečného přerozdělování zdrojů.

4.2.8 Ochrana proti škodlivým programům a mobilním kódům

Na koncových stanicích vyjma mobilních telefonů je nainstalován antivir od společnosti ESET produkt Endpoint Antivirus. Zmíněný produkt zahrnuje pouze antivir, neobsahuje firewall ani antispam, který by zvyšoval zabezpečení koncových stanic. ESET nabízí centrální správu těchto produktů, ale ve společnosti není centrální správa nainstalována a nejsou vynucovány bezpečnostní politiky. Antivir uživatel může vypnout, není definováno heslo, které by případné modifikaci nastavení zabránilo. Mobilní zařízení nejsou nijak zabezpečena, avšak názory na jejich účinnost jsou prozatím různé. Na mailovém serveru je nainstalováno jiné antispamové řešení než ESET a jeho účinnost je v poslední

době dosti kritizována. File server není zabezpečený žádným antivirovým řešením, což může způsobit hrozbu. Ostatní servery obdobně nejsou chráněny proti případným virovým hrozbám.

4.2.9 Zálohování

Každý den dochází k zálohování celých obrazů všech virtuálních serverů přírůstkovou metodou na připojený NAS server, obrazy se po naplnění vyčleněného datového prostoru smažou. Jsou dostupné pouze zálohy dva dny zpět a nedochází k archivaci například měsíc či rok zpět. Nejsou aktivovány Shadows Copies, které by uchovávaly jednotlivé verze souborů a při smazání souboru je nutné obnovit celý virtuální server z předešlého dne, což je časově náročné a 24 hodinový interval může být nedostatečný. Není definován plán obnovy a nejsou prováděny pravidelné zkoušky obnovy. Nedochází k pravidelnému zálohování transakčních databázových logů či emailového serveru.

4.2.10 Správa bezpečnosti sítě

Plzeňská centrála firmy je připojena k internetu symetrickým, garantovaným připojením podloženým SLA o rychlosti 10Mbps. Firma má pouze jeden přístupový bod a nemá žádné redundantní připojení, které by v případě nedostupnosti sloužilo jako záložní. Vnitřní síť je oddělena od vnější sítě softwarovým firewallem, který je umístěn na serveru CP12 pod Linuxovým operačním systémem. Bohužel k tomuto firewallu neexistuje, žádná dokumentace a při prováděných penetračních testech bylo zjištěno, že operační systém není aktualizován, obsahuje řadu zranitelností a jeho konfigurace není dostatečně bezpečná, jsou povoleny některé porty, které nejsou využívány. V síti se nachází 3 switche. Dva 48 portové pro propojení koncových stanic a jeden 24 portový pro propojení serverů. Oba čtyřiceti osmi portové switche neobsahují dokumentaci a jejich stáří se pohybuje kolem šesti let, což je odhadovaná životnost zařízení. Současně bylo zjištěno, že není zapnutý žádný bezpečnostní mechanismus pro zvýšení bezpečnosti sítě. V síti nejsou vytvořené VLAN, ani není nakonfigurována DMZ či proxy server. V prostorách firmy je WIFI síť, která má dostatečný signál ve všech místech, je zabezpečena používaným standardem WPA2 personal s šifrováním AES a současně je zvoleno dostatečně silné heslo, které však není měněno a je známé mezi zaměstnanci. Pro připojení návštěv je využíváno stejné SSID jako pro zaměstnance. Síť není oddělena od interní sítě a návštěvy mohou přistupovat k firemním datům, či zasahovat do síťového provozu, ať už jeho modifikací či pasivním sledováním. Síť

není zabezpečena proti připojení nových zařízení do interní sítě, ani není aktivní monitorování připojených zařízení. V síti není instalováno žádné IDS či IPS.

Síť na pobočkách v Praze a Ostravě je tvořena pouze WIFI routery Zyxel. Bezdrátová síť je zabezpečena standardy WPA2 Personal s šifrováním AES a je použito dostatečně složité heslo. Routery se nachází v základním nastavení. Připojení od ISP[2] je vyhrazené 5Mbits download i upload. Z důvodu nedostatku volných portů a z častého pohybu zaměstnanců je na pobočkách častěji využíváno bezdrátové připojení.

4.2.11 Monitorování

Ve společnosti nejsou vedeny všechny potřebné systémové záznamy. Není aktivováno zaznamenání hlášení o mazání souborů, přihlášení uživatele nebo o přístupech k datům přihlášených uživatelů přes VPN. Auditní záznamy nejsou nijak agregovány na jedno místo a poté vyhodnoceny pomocí SIEM řešení. Nejsou ani definovány časové intervaly pro procházení logů a co má být monitorováno. Přístup k logům má pouze administrátor. Ve společnosti je veden administrátorský deník, ale je neúplný a ne všichni administrátoři ho využívají.

4.2.12 Řízení přístupů

Společnost má vytvořenou doménu, v rámci které pomocí protokolu LDAP ověřuje svoje zaměstnance a podle přidělených rolí a práv jim je zajištěn přístup k souborům, datům, síťovým zdrojům či do aplikací. Správa uživatelských hesel je řízena pomocí Active directory. Politikami jsou vynucovány zásady pro tvorby hesel, ale hesla neodpovídají doporučeným bezpečnostním požadavkům. Je možné heslo libovolněkrát zadat nesprávně, složitost hesel je definována pro minimální počet šesti znaků bez nutnosti použití nealfanumerických znaků. Politiky vyžadují změnu hesla po době delší jak 90 dnů. Klientská aplikace nemá řízenou autorizaci skrze protokol LDAP a je zapotřebí definovat a spravovat hesla odděleně. Uživatelé si více hesel nepamatují a v lepším případě zatěžují oddělení IT s požadavky na resetování hesel, v horším případě si hesla zapisují na okraje monitorů, i když platná směrnice jim to zakazuje. Firma neprovádí žádné bezpečnostní audity, ve kterých by přezkoumávala přístupová práva jednotlivých uživatelů. Jak bylo výše uvedeno, zřízení i odebrání přístupu je řízeno personálním oddělením.

[2] Internet service provider – poskytovatel internetu

4.2.13 Mobilní zařízení a práce na dálku

V poslední době se ve firemním prostředí rozmohl trend používat chytré mobilní zařízení včetně tabletů, které ne vždy jsou firemní. Mobilní zařízení nejsou spravována BYOD[3] řešením, jejich obsah není šifrován, nejsou vynucovány žádné politiky pro zabezpečení zařízení, není nainstalován antivirový software, ani kontrolovány nebo omezovány instalované aplikace. Může dojít k infikování zařízení infikovanou aplikací a následně odcizení přístupových údajů do domény po zadání jména a hesla do emailového klienta anebo citlivých dat obsažených v zařízení. Práce na dálku je realizována prostřednictvím šifrovaného VPN tunelu, autorizace je realizována protokolem LDAP. Na počítači, ke kterému se uživatel připojuje, je povolen pouze uživatel, kterého administrátor nastaví. VPN klienti jsou instalovány na koncových stanicích, které nespravuje IT oddělení, a mohou obsahovat potencionální hrozby. Hrozba je zmírněna instalací VPN klienta a certifikátu pouze IT oddělením na základě souhlasu nadřízeného.

4.2.14 Zvládání bezpečnostních incidentů

Bezpečnostní incidenty jsou zanášeny do administrátorského deníku a to pouze v podobě, že se daná skutečnost stala. Nejsou vedeny informace o škodách či provedená protiopatření. Není dán přesný postup, jakým způsobem zvládat bezpečnostní incidenty a koho informovat. Uživatelé nejsou povinni nařízením některé směrnice hlásit bezpečnostní slabiny nebo podezřelé výskyty v systémech nebo službách.

4.2.15 Soulad s právními požadavky

Platné směrnice zakazují používání softwaru či dat v rozporu s ochranou duševního vlastnictví. Část uživatelů má na svých koncových stanicích stále administrátorské oprávnění, má nainstalován nelegální software a umístěn nelegální obsah. Momentálně nejsou prováděny pravidelné kontroly koncových stanic, při kterých by docházelo k odhalení těchto skutečností. Nelegální obsah byl objeven i na file serverech, kde také nedochází ke kontrolám přítomnosti audio či video záznamů a následnému vyhodnocení.

4.3 Analýza rizik

Analýza rizik odkrývá konkrétní hrozby, které ohrožují firemní prostředí. Aby bylo možné provést analýzu rizik, je zapotřebí identifikovat všechna aktiva, kterými společnost

[3] Bring Your Own Device – termín označující používání mobilních zařízení ve firemním prostředí

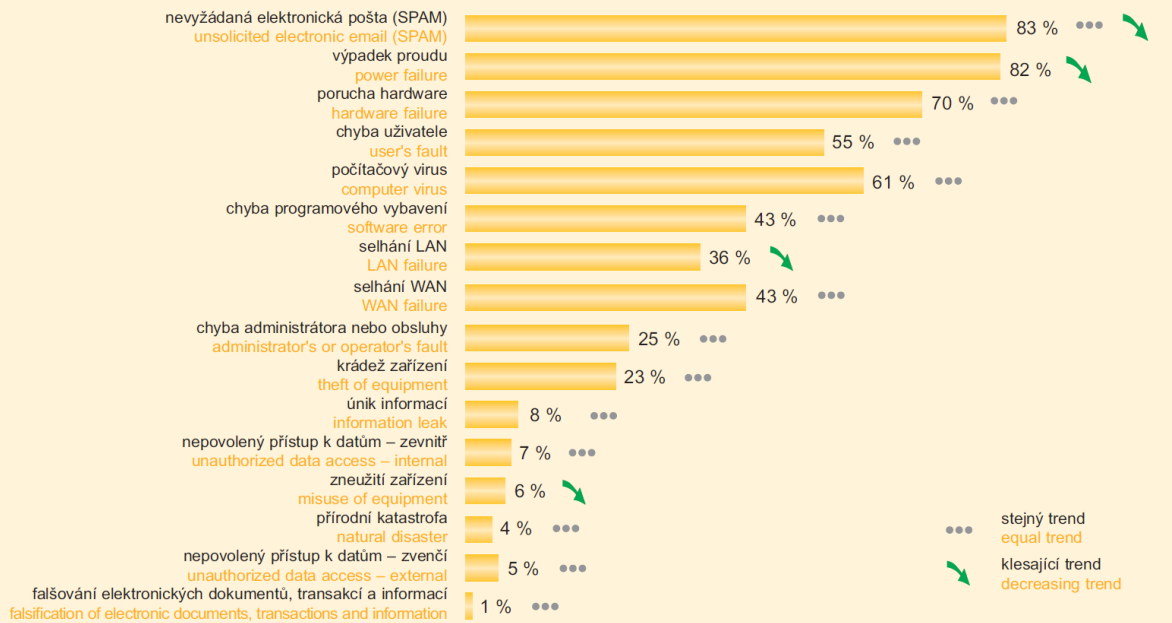
disponuje. Poté určit, která aktiva je zapotřebí ochránit, stanovit seznam hrozeb a jejich dopad na identifikovaná aktiva. Dále určit pravděpodobnost vzniku hrozeb, závažnost dopadu hrozby na konkrétní aktivum a nakonec názor hodnotitelů. Na základě těchto informací vypočítat celkovou hodnotu rizika a nakonec vyvodit závěr, který bude zahrnovat informaci o potencionálních hrozbách a jaká aktiva je zapotřebí chránit.

4.3.1 Identifikace aktiv

Při identifikaci aktiv se používá pět oblastí: hardware, software, data, zaměstnanci a infrastruktura. Při analýze společnosti byly na základě těchto oblastí identifikovány aktiva. Mezi hardware byly zařazeny stolní počítače, notebooky, mobilní telefony, paměťové média, servery, síťové prvky a tiskárny. Do oblasti softwaru byly zahrnuty operační systémy, základní uživatelský software, ekonomický a účetní software, emailový software, mzdový software a klientská aplikace. Do oblasti dat jsou zařazeny tato aktiva SQL databáze, databáze klientského softwaru, mzdové a účetní dokumentace, smlouvy, zálohy dat, business a finanční plány. Oblast zaměstnanců pokrývá administrátora, management a goodwill. Do poslední oblasti tedy infrastruktury, patří serverovna.

4.3.2 Identifikace hrozeb

Po identifikování aktiv je na řadě identifikace hrozeb. Hrozby byly identifikovány na základě Průzkumu stavu informační bezpečnosti v ČR 2009, vydaného ve spolupráci Ernst & Young, NBÚ a DSM. Bohužel novější výzkum nebyl k dispozici. Na základě tohoto průzkumu, ve kterém vychází jako největší nebezpečí hrozby spam, výpadek proudu a porucha hardwaru. Všechny tyto hrozby mohou firmu zasáhnout a je potřeba v analýze s nimi počítat.



Obrázek 6: Výskyt bezpečnostních incidentů za poslední dva roky

Zdroj: *ERNST & YOUNG. Průzkum stavu informační bezpečnosti v ČR 2009. Ernst & Young, NBÚ, DSM data security management a Národní bezpečnostní úřad, 2009. 40 s. ISBN 978-80-86813-19-6*

Výše uvedená rizika jsou pouze nejčastěji se vyskytující incidenty a je potřeba je rozšířit o odposlech komunikace v síti a zkoušení uhádnutí hesel. Existují i další hrozby, ale ty do analýzy z důvodu malého výskytu nebyly zahrnuty.

4.3.3 Pravděpodobnost vzniku rizika

Pravděpodobnost vzniku rizika určuje četnosti, kolikrát se ve firmě daná hrozba vyskytla či jaká je možnost, že se vyskytne. Z tohoto důvodu je dobré vést seznam bezpečnostních incidentů, což firma vede. Jako vodítko sloužil i Průzkum stavu informační bezpečnosti v ČR 2009 uvedený v obrázku 2. Stupnice, z které bylo vycházeno pro ohodnocení pravděpodobnosti výskytu a počet výskytu jednotlivých pravděpodobností vzniků rizika s návazností na jednotlivá aktiva, je uvedena v tabulce 2. Matice jednotlivých rizik, aktiv a ohodnocení možnosti výskytu je uvedena v příloze 1.

Tabulka 2: Stupnice pro ohodnocení pravděpodobnosti vzniku rizika a počet výskytů

Stupeň	Počet	Popis
0	0	Prakticky nemožný výskyt
1	118	Nepravděpodobné
2	126	Méně pravděpodobné
3	56	Pravděpodobné
4	4	Velmi pravděpodobné
5	5	Pravidelný, stále se opakující výskyt

Zdroj: *Vlastní zpracování*

Pravidelně se opakující hrozbou je výskyt spamu, který zatěžuje koncové stanice (stolní PC, notebooky, mobilní telefony), emailový server a práci managementu i administrátora. Téměř každý den firmu zaplavuje množství spamu. Antispamové řešení si mnohými spamy poradí, ale ne se všemi.

Mezi další pravděpodobné hrozby patří výpadek proudu. Servery CP1 a CP2 jsou připojeny přes UPS, v případě krátkodobých výpadků proudu nedojde k ohrožení serverů, většině důležitých aplikací a dat. Výpadek však ohrožuje ostatní fyzické servery, síťové prvky, dostupnost aplikací a práci managementu a administrátora. Porucha HW byla ohodnocena na koncových stanicích jako pravděpodobná, z důvodu neduplikovaných hardwarových prvků. Servery společnosti jsou proti této hrozbě vybaveny. Je použit RAID 1, na hlavních serverech jsou použity záložní zdroje napájení. Z těchto důvodů bylo riziko výskytu na serveru, aplikacích a datech ohodnoceno jako méně pravděpodobné.

Chyba uživatele může pravděpodobně vzniknout v ekonomickém a účetním softwaru. Uživatelé pracující v softwaru mají vysoké oprávnění a vykonávají mnoho operací, při kterých může snadno vzniknout chyba. V klientském softwaru je obdobný případ, s tím rozdílem, že mimo interních zaměstnanců používají systém i klienti, ale ti mají pouze nízká oprávnění a nemohou způsobit vážné dopady. Případy, kdy uživatelé způsobili chyby v aplikaci, byly v minulosti zaznamenány, proto hrozba byla ohodnocena hodnotou pravděpodobná.

Hrozba počítačového viru je ohodnocena jako velmi pravděpodobná. Poslední dobou se ve společnosti množí případy napadení počítačovým virem. Nejčastěji jsou nakažené koncové stanice, do kterých se vir dostane v rámci spamu, prohlížení webového obsahu či nainstalováním infikované aplikace.

Chyba programového vybavení je pravděpodobná u mzdového softwaru, kde nové verze jsou implementovány přímo do ostré verze a často se v ní vyskytují chyby, které se dodatečně upravují.

Selhání LAN bylo ohodnoceno jako pravděpodobné z důvodu stáří switchů. Selhání LAN ohrožuje veškeré aplikace a data. Aplikace využívají výpočetní model klient server.

Selhání WAN je pravděpodobné. Ve společnosti není redundantní WAN připojení a v případě, poslední dobou častějších výpadků ISP jsou firemní aplikace a mailová komunikace nedostupné.

Chyba administrátora je pravděpodobná z hlediska rozsáhlosti sítě a v minulosti se pravidelně opakovaly chyby z důvodů změn v IT infrastruktuře společnosti a nedostatečné počáteční analýze.

Krádeže zařízení a s tím spojená ztráta dat se pravidelně opakují u paměťových médií. Z důvodu velké míry zastoupení v Průzkumu stavu informační bezpečnosti v ČR 2009 byla možnost hrozby vyhodnocena hodnotou pravděpodobná.

Únik informací v podniku zatím nebyl evidován, ale přesto byl označen jako pravděpodobný ze stejného důvodu jako v předchozím případě.

Nepovolaný přístup k datům je označen jako pravděpodobný z hlediska neprováděného auditu přístupu a hrozícího neautonomního přístupu k datům s následkem ohrožení dat, softwaru, práce administrátora, managementu a v konečném důsledku i dobrého jména společnosti.

Hrozba přírodní katastrofy se jeví jako nepravděpodobná z hlediska polohy firemních prostor a to v rámci jak hlavního sídla, tak i poboček. Nejpravděpodobnější přírodní katastrofa je hrozba požáru, ale i ta je zanedbatelná. V případě aktivace této hrozby dojde k postihnutí všech aktiv.

Nepovolaný přístup k datům zvenčí je klasifikován jako nepravděpodobný. Společnost nepoužívá FTP server či jiná datová uložiště prezentovaná směrem do internetu. Muselo by se jednat o cílený útok, kdy by útočník musel překonat bezpečnostní mechanismy společnosti.

Falšování elektronických dokumentů a transakcí je nepravděpodobné. Může zasáhnout falšování mzdových databází, smluv či jiných dat, ale ve firmě podobná situace nebyla zaznamenána a též Průzkum stavu informační bezpečnosti v ČR 2009 hodnotí hrozbu jako málo pravděpodobnou.

Další otázkou je odposlech a modifikace komunikace v síti. Vzhledem k tomu, že síť není monitorována a nejsou blokována všechna neautorizovaná zařízení a někteří uživatelé mají lokální administrátorské účty, je možnost odposlechu sítě pravděpodobná. V ohrožení jsou zvláště data, aplikace a práce zaměstnanců.

Zkoušení hesel jiných zaměstnanců je běžná praktika a její použití je pravděpodobné. Při úspěšném uhodnutí hesla hrozí nebezpečí nesprávné integrity dat a jejich ohrožení.

4.3.4 Ohodnocení následků

Aby bylo možné provést analýzu rizik, je zapotřebí zavést ohodnocení následků, označující jaké následky může způsobit aktivace dané hrozby nejen po finanční stránce, ale i z hlediska chodu společnosti a dalšího fungování. Stupnice, která byla použita v analýze, je zobrazena v tabulce 3 včetně počtu jednotlivých stupňů hrozeb ve vztahu k firemním aktivům. Výsledná matice ohodnocení následku se nachází v příloze 2.

Tabulka 3: Stupnice pro ohodnocení následků a počet výskytů

Stupeň	Počet	Ohodnocení	Popis
0	0	Nejsou vážné	Existuje možnost okamžité nápravy, bez vlivu na chod společnosti.
1	19	Méně vážné	Je potřebné vyčlenit personální zdroje na odstranění vzniklé chyby.
2	101	Vážné	Vyšší finanční ztráty, závažné překážky efektivního chodu společnosti.
3	109	Velmi vážné	Velké finanční ztráty. Mohou být ovlivněné hlavní procesy společnosti, které mohou zapříčinit omezení dodávek služeb.
4	63	Závažné	Kritické problémy, případně zastavení klíčových procesů společnosti. Velmi vysoké finanční ztráty, okamžitý úbytek zákazníků, únik citlivých a osobních údajů, trvalé poškození dobrého jména.
5	4	Existenční problémy	Kritické finanční ztráty, ztráta většiny zákazníků, únik citlivých a osobních údajů, velmi závažné a trvalé poškození dobrého jména společnosti. Existenční potíže.

Zdroj: *Vlastní zpracování*

Hrozba spamu byla klasifikována jako méně závažná. Na odstranění následků je zapotřebí vyčlenit personální zdroje, ale nejedná se o problémy zasahující chod společnosti nebo finančně náročný problém.

Dojde-li k výpadku proudu má to na chod společnosti vážné důsledky. Dostihne společnost zastavení činnosti pracovníků, kteří převážně využívají výpočetní techniku, výpadek proudu bude mít za následek nedostupnost klientské aplikace a spolu s tím utrpí dobré jméno společnosti. V rámci výpadku může firma přijít o důležitá data, která se

nestihnou uložit, či výpadkem dojde k jejich poškození. Výpadek může způsobit poruchu hardwaru.

Při poruše hardwaru na serveru může nastat závažný problém. V případě poruchy například základní desky, je nutné čekat na její dodání. Doba dodání se může pohybovat v jednotkách dnů. Firma nedisponuje náhradním serverem, ani nemá záložní plán obnovy. Situace může být velmi závažná, vyústit může až k existencionálním problémům, kdy například týden nebude dostupná firemní aplikace. Společně s poruchou hardwaru může dojít i k poškození softwaru a dat. V případě poruchy hardwaru koncových zařízení dochází k finanční ztrátě ve výši hodnoty zařízení a softwaru instalovaného na zařízení, k tomu je třeba připočítat personální náročnost, kdy administrátor musí opět zprovoznit nový hardware a k finanční ztrátě dochází rovněž ve výši hodnoty dat umístěných na zařízení.

Chyba uživatele v klientském softwaru či v mzdovém softwaru způsobí velmi vážné problémy. V případě, kdy dojde například k špatnému mzdovému výměru či poškození klientů. Chyba uživatele, který má přístup k business a finančním plánům, může způsobit až závažné problémy, kdy by se firma odchýlila od své strategie a vycházela by z nepravdivých podkladů.

Počítačový virus při napadení serveru, například ve verzi cryptolocker, ohrozí veškerá data, software a tím celý chod společnosti. V případě, že firma nezálohuje, může přijít o všechna data, což může znamenat i její konec. Počítačový virus může zcizit data společnosti a dojít k vyzrazení firemního tajemství.

V případě chyby programového vybavení například bezpečnostní nebo provozní chybě, může být ohrožena dostupnost aplikací a může být způsobena ztráta dat. Chyba v programu může mít dalekosáhlé následky. Proto při chybě programového vybavení vznikají závažné problémy hlavně při poškození mailového klienta, mzdového nebo klientského softwaru.

Selhání LAN bylo klasifikováno jako hrozba způsobující velmi vážné problémy. V případě krátkodobého výpadku lze závadu akceptovat, ale v případě delšího nad jednu hodinu vznikají vážné problémy. Zaměstnancům je znemožněn výkon pracovní činnosti z důvodu použití výpočetního modelu aplikací typu klient server. Při výpadku místní sítě nejsou aplikace přístupné. Nedostupná je klientská aplikace, její běh je zajištěn v některých případech SLA a nedostupnost aplikace znamená pro firmu finanční postih.

Selhání WAN není závažné pro zaměstnance, kteří se připojují v rámci centrální pobočky. Výpadek znamená nedostupnost emailové služby a přístupu na internet, ale dostupnost firemních aplikací je zachována. Velmi vážné problémy však nastávají na straně dostupnosti klientské aplikace. S nedostupností klientské aplikace je spojeno zhoršení image firmy.

Chyba administrátora může mít za následek závažné problémy a může zasáhnout všechny aktiva. Administrátor má přístup do všech aktiv.

Krádež zařízení je závažná v případě, že se jedná o server, serverové disky nebo důležitá data pro chod společnosti. V případě odcizení záloh společnosti nebo harddisků ze serveru může zloděj získat veškeré data a firma se může potýkat se závažnými problémy, pokud pachatel zcizí data i zálohy.

Únik informací může způsobit bezpečnostní závada v aplikaci nebo může vzniknout při neopatrném jednání administrátora. Při úniku informací jsou nejvíce ohrožena data o klientech, smlouvy, business a finanční plány, emailové korespondence a goodwill, který se již těžko může získávat zpět a také je těžké přesvědčit klienty, že daný incident se už nebude opakovat.

Nepovolaný přístup k datům zevnitř může vést ke krádeži či modifikaci dat, například ke změně mzdy, smluv nebo jiných zásahů do dat. Tato změna nemusí být odhalena či až po dlouhé době a může napáchat velké závažné škody.

Přírodní katastrofa zasáhne existenčními problémy celou firmu. V případě požáru může dojít ke zničení veškerého vybavení firmy a firma může přijít o všechna aktiva a není schopná dosahovat svých cílů a poskytovat své služby.

Nepovolaný přístup k datům zvenčí může napáchat stejné škody jako nepovolaný útok zevnitř. Pro případného útočníka je provedení složitější, ale následky mohou být totožné, možná i větší. Útočník, který cílí útok na firmu, má primární cíl poškodit firmu. Nepovolaný přístup k datům zevnitř může vycházet ze zvědavosti a nemusí jít nutně o záměr poškodit firmu, ale takovéto situace jsou výjimečné.

Falšování elektronických dokumentů a transakcí může být následkem některé předešlé hrozby. Jedná se o nebezpečnou činnost z důvodu zjištění modifikace dat bez vědomí uživatelů pozdě či vůbec.

Odposlech nebo modifikace komunikace na síti může být nebezpečná při nešifrovaných přenosech dat či přihlašovacích údajů. V případě, že by došlo k aktivaci hrozby, jsou v ohrožení veškerá data i aplikace.

V případě zkoušení hesel a jejich úspěšného uhádnutí se může jednat až o závažné problémy. V případě uhodnutí hesla doménového administrátora může útočník provádět stejné změny jako administrátor. Může mít kontrolu nad všemi aktivy.

4.3.5 Celkové riziko

Celkové riziko bylo určeno jako součet pravděpodobnosti vzniku rizika a ohodnocení následků. Po umístění aktiv a jednotlivých hrozeb do matice, vyšla finální podoba zobrazena v příloze 3. Pod jednotlivými aktivy je určeno, jaké aktivum je průměrně nejohroženější. Prakticky se jedná o aktiva, která mají ve firmě velkou hodnotu, a jejich chod může narušit nejvíce hrozeb. Nejohroženější aktiva jsou emailový software tedy emailový server, klientská aplikace a její databáze. Jmenovaná aktiva jsou dostupná i z venkovní sítě, proto možnost aktivace hrozby roste.

V tabulce 4 jsou uvedeny jednotlivé hrozby a průměrné riziko propuknutí hrozby s ohledem na způsobené následky na jednotlivých aktivech.

Tabulka 4: Výstupní riziko aktivace hrozby

Hrozby	Riziko hrozby
SPAM	1,30
Výpadek proudu	4,00
Porucha HW	3,96
Chyba uživatele	3,13
Počítačový virus	4,09
Chyba programového vybavení	3,78
Selhání LAN	2,70
Selhání WAN	1,26
Chyba administrátora nebo IT	4,83
Krádež zařízení nebo ztráta	4,70
Únik informací	3,00
Nepovolaný přístup k datům z vnitřní sítě	3,96
Přírodní katastrofa	3,96
Nepovolaný přístup k datům zvenčí	3,61
Falšování elektronických dokumentů a transakcí	1,74
Odposlech a modifikace komunikace v síti	3,91
Zkoušení uhádnutí hesel	4,17

Zdroj: *Vlastní zpracování*

Mezi největší hrozbu patří chyba administrátora nebo IT. Je to z důvodů vysokých oprávnění administrátorů, použití jednoho účtu na správu všech aktiv a z důvodu častého výskytu chyb, které se v poslední době objevovaly při modernizaci IT infrastruktury. Hrozba chyb se prohlubuje neaktivním auditním systémem monitorujícím závady a nedostatečným vedením administrátorského deníku, který může sloužit pro detekci chyby.

Další potencionální hrozba je nebezpečí krádeže či ztráta dat. Zvýšené riziko je způsobené rozšířením notebooků a chytrých mobilních telefonů mezi zaměstnanci a migrace zařízení mezi pobočkami a centrálou. Dalším důvodem je nevyužívání šifrování v mobilních zařízeních, serverech a záložních kopiích.

Zkoušení hesel se řadí na třetí příčku mezi potencionální hrozby. Ve společnosti je zavedena autorizace přes protokol LDAP. Jedná se o bezpečný protokol, ale bohužel není definován počet neplatných pokusů, po kterých by byl účet zablokován. Nedostatečné bezpečnostní opatření dovoluje použití slovníkového útoku pro uhodnutí hesla. Politika tvorby hesel je nedostatečná a útok by mohl být úspěšný. Administrátoři využívají účty přiřazené do skupiny Domain Admins na klientských stanicích a při umístění keyloggeru, nebo odezíráním administrátorského hesla může dojít k jeho získání. Při uhodnutí hesla útočník získá přístup do všech systémů. Bezpečnostní incident, který pravděpodobně vznikl v uhodnutí hesla oběti, se v minulosti ve firmě objevil.

Nákaza počítačovým virem se umístila na čtvrtém místě. Jedná se o aktuální hrozbu a často vyskytovanou v prostředí společnosti. Nejčastěji hrozba se šíří prostřednictvím emailu a jeho následného otevření. Naštěstí útoky počítačovými viry se převážně vyskytují na koncových stanicích, odkud se dále nešíří. Výjimečně byl evidován případ, kdy vir pronikl na server a zašifroval i soubory na serveru. Ve společnosti je použité antivirové řešení, ale bez instalované centrální správy a pouze v základní verzi. Konfigurace antispamového řešení nedopovídá doporučenému nastavení.

Výpadek proudu může potkat firmu a být pro ni dost tragický. UPS jsou zastaralé, zátěž jednotlivých UPS není rozdělena mezi jednotlivé servery a nejsou spravovány ani kontrolovány. V UPS nejsou připojeny síťové prvky a UPS nejsou připojeny do dieselových agregátů.

Možnost poruchy hardwaru je dosti vysoká z důvodu stáří switchů a nedostatečné dokumentace. Další důvod je nevyužití více síťových karet, které by vedlo ke zvýšení síťové dostupnosti a replikaci v případě poruchy jedné komunikační cesty. Nebezpečí hrozí

z důvodu, že firma nevlastní náhradní server či nemá smlouvu s dodavatelskou firmou o jejím zapůjčení.

Riziko nepovolaného přístupu z vnitřní sítě je rovněž vysoké. Ve společnosti není zřízena WIFI síť pro návštěvy a subjekty docházející do firmy. Cizí zařízení se připojují přímo do sítě společnosti. V síti neexistuje monitoring síťových zařízení nebo možnost blokace. Provozní sítě nejsou odděleny pomocí virtuálních sítí. WIFI síť je zabezpečená pouze pomocí WIFI Personal nikoliv Enterprise. Odposlech a modifikace komunikace v síti souvisí s možností nepovolaného přístupu z vnitřní sítě. Naštěstí v poslední době se začíná využívat komunikace skrz šifrované aplikace, u některých aplikací bohužel chybí.

Přírodní katastrofa z hlediska umístění prostor firmy zřejmě nehrozí až na požár, kde situace může nastat. Servery jsou umístěny v kanceláři společně s dalšími skladovanými věcmi, jako jsou papírové šanony, které mohou požár rozšířit. Nebezpečí hrozí zejména neumístěním záloh v jiné lokaci a jejich případné zničení při vzniku přírodní katastrofy. V případě, že by byla aktivována přírodní katastrofa, což je nízká pravděpodobnost, firma by přišla o veškerá aktiva, z tohoto důvodu vyšlo vysoké riziko hrozby.

4.4 Výsledky testů a návrh opatření pro zmírnění následků

Po provedení bezpečnostního auditu ve společnosti bylo identifikováno několik bezpečnostních hrozeb, které je vhodné eliminovat nebo odstranit pomocí některých bezpečnostních opatření. Podle výsledků analýzy rizik, je nejvhodnější se nejprve věnovat oblastem, které pokrývají hrozby s největším rizikem hrozby a mohly by nejvíce ohrozit firemní aktiva.

4.4.1 Zmírnění chyby administrátora

Největší riziko představuje chyba administrátora. Z tohoto důvodu by bylo vhodné zmírnit šanci administrátora IT udělat chybu a zavést monitorovací nástroje, které chyby odstraní. V případě vzniku chyby IT oddělení musí mít možnost monitorovat systém, zjistit závadu včas, zareagovat a zpětně zjistit zdroj chyby a vyhodnotit důsledky. Na základě předchozí rozvahy bude určeno několik úrovní administrátorských účtů pro správu IT ve společnosti, aby došlo k omezení pole působnosti administrátora. Každý administrátor dostane přidělen svůj účet se specifickým rozsahem oprávnění. IT junior bude mít oprávnění pouze lokálního administrátora s možností instalovat a měnit nastavení na koncových stanicích bez možnosti přístupu na server. IT administrátor bude moci vytvářet a modifikovat

konfiguraci v Active directory a MS Exchange. IT senior bude mít účet pro přístup k síťovým prvkům, účet pro úpravy na platformách Windows Server, změny v SQL databázích, rozšířené nastavení, které není přístupné IT administrátorovi a účet pro správu Linuxových serverů. Správce klientského softwaru bude mít přístup pouze do jím spravovaného softwaru a do databáze klientského softwaru. Dodavatel mzdového softwaru bude moci přistupovat do mzdového softwaru a do databáze mzdového softwaru.

Pro monitoring dostupnosti služeb, jako je mailová služba či jiné aplikace běžící na příslušných portech nebo hardwaru využití CPU, disků atd., by bylo vhodné implementovat nástroj Nagios. V případě vzniku problémů s dostupností či s nedostatkem hardwarových zdrojů notifikuje administrátora. Řešení je v core[4] verzi zdarma. Poslední částí je aktivace logování na serveru, aby bylo možné detekovat, kdo změny způsobil. Zapnutím služby User Access Logging, kde je možné sledovat vyvolané změny v serverových rolích a přístupech. Změnou v Group Policy aktivováním audit policy nastavit logování přihlášení, odhlášení a přístupu k souborům a zapnutí auditování na file serveru. V poslední řadě poučit administrátory o nutnosti používat administrátorský deník a jeho používání nařídit směrnicí.

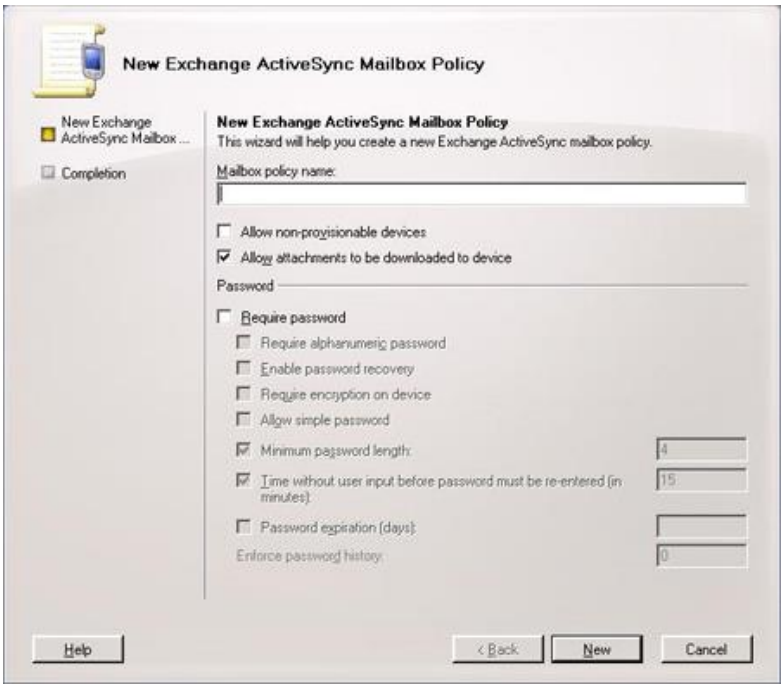
4.4.2 Zmírnění hrozby krádeže

Pro zmírnění hrozby krádeže či ztráty je nejúčinnější zašifrovat obsah a tím zamezit, že se data dostanou do nepovolaných rukou a budou zneužita. Cena hardwaru je v tomto případě minoritní. Nejcennější ohrožená data jsou na serveru, z toho důvodu je nejlepší aktivovat šifrování prvně zde. Fyzické servery běžící pod platformou Windows Server disponují nástrojem bitlocker, který pro zašifrování disků vyhovuje a jeho požívání je zdarma. Pro aktivování šifrování je potřebné doinstalovat feature bitlocker drive encryption a spustit tento prvek. Po spuštění je potřebné zvolit disky k zašifrování a udělat zálohu dešifrovacího klíče. Nejlépe na několik paměťových médií s dlouhou životností např. magnetickou pásku, archivační disky a umístit je do trezoru v jiné budově. Notebooky společnosti mají nainstalovaný Windows 7 a Windows 8, obě platformy obsahují zmíněný šifrovací nástroj bitlocker. K zašifrování disků je potřeba spustit nástroj bitlocker volbou „start“ v operačním systému, dále stisknutím volby ovládací panely a nástroj Bitlocker Drive Ecryption. Zde vybrat příslušný disk k zašifrování a nastavení hesla. Heslo by mělo být jedinečné, dostatečně složité a administrátor by si jej měl zaznamenat. Pokud notebook

[4] Základní verze

vlastní TPM čip[5] je vhodné využití TPM čipu. Klíče pro dešifrování by si měl opět administrátor uložit na média s vysokou životností a vytvořit raději záložní kopii.

Ve firmě není používán žádný software pro správu BYOD zařízení. Implementace řešení BYOD je dosti nákladná. Ve společnosti je využíván software Microsoft Exchange. Microsoft Exchange dovoluje definovat Exchange ActiveSync Mailbox Policies. Na základě této politiky je možné povolovat zařízení, která budou využívat firemní emailový účet, vyžadovat heslo pro zabezpečení telefonu, smazat data v zařízení a další funkcionality aktivní s ohledem na typ mobilního zařízení. Je dobré nastavení aktivovat a chránit firemní mailovou korespondenci a data v mobilním zařízení.



Obrázek 7: Definování nové Exchange ActiveSync Mailbox Policy

Zdroj: *Vlastní zpracování*

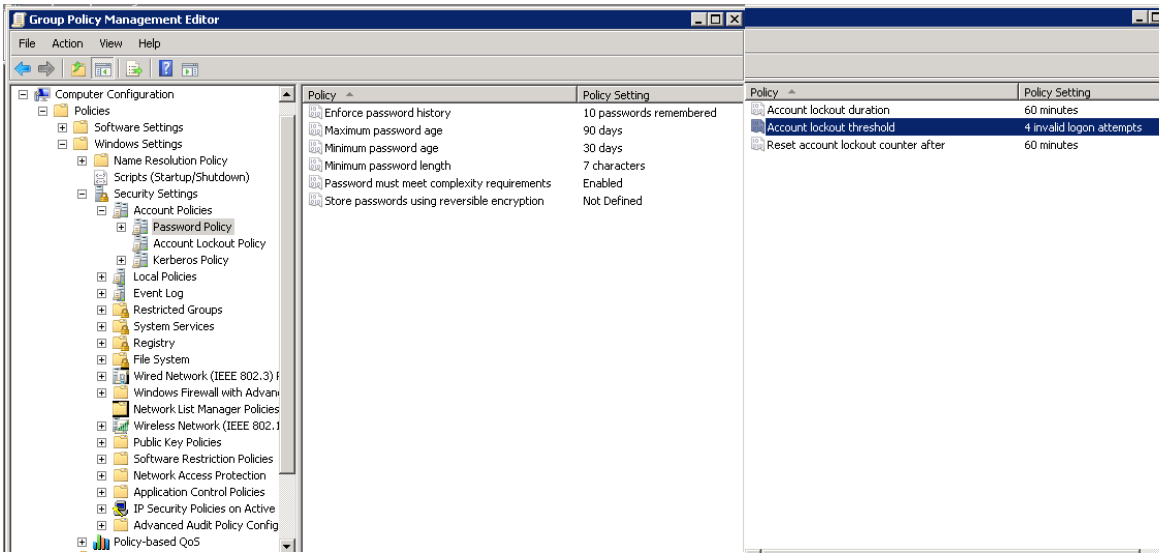
Výrazně je doporučeno přemístit serverovnu do samostatné místnosti se zabezpečeným vstupem chráněným čipovou kartou, vlastní klimatizací a speciálními detektory kouře. Opatření vyžaduje vyšší investici a je na zvážení vedením, zda společnost disponuje vhodnými prostory na zřízení serverovny. Vlastní serverovna nejenže zabrání přístupu nepovolaných osob, ale také hardware bude lépe chlazen a bude prodloužena jeho

[5] Trusted Platform Module – čip vhodný k ukládání kryptografických klíčů

životnost a lépe chráněn proti případnému požáru a eliminaci dalších hrozeb jako třeba banální zakopnutí o kabel.

4.4.3 Zmírnění zkoušení hesel

Pro zabránění zkoušení uživatelských hesel je nejúčinnější vytvořit politiky pro pravidla tvorby hesel, definování složitosti a frekvence změny hesla. Pravidla pro tvorbu hesel jsou obsažena v aktuální směrnici pouze okrajově, je zapotřebí směrnici rozšířit. Aktuálně není zmínka o frekvenci změny hesla po 90-ti dnech, i když je politikami vynucována. Pro splnění podmínky silného hesla je třeba zavést minimální délku hesla sedm znaků, přičemž heslo musí obsahovat alespoň jedno malé, jedno velké písmeno a jeden neabecední znak. Dále zavést, že po čtyřech neplatných pokusech dojde k uzamčení účtu a pro odemčení je nutné kontaktovat administrátora nebo počkat jednu hodinu pro odblokování. Po upřesnění směrnice rozšířit vynucování politik na domain controleru, který slouží k ověřování uživatelských jmen a hesel a donutí uživatele k dodržování směrnice. Jedná se tedy o aktivní vynucování bezpečnostních politik. Základní politiky jsou nastaveny, jen je zapotřebí je zpřísnit. Na platformě Windows Server se definují politiky v nástroji Group Policy Manager. Politiky pro složitost hesel se nachází v Computer settings, Policies, Windows Settings, Security settings a Account Pollicies. Ve volbě Acount Pollicies pod Password Policy je vhodné definovat Enforce password history na hodnotu 10, tj. dobu, za kterou je možné opakovat použitá hesla, Maximum password age na hodnotu 90, tedy maximální stáří hesla, po kterém je nutné si heslo změnit, Minimum password length na hodnotu 7, minimální délka znaků použitých v hesle, Password must meet complexity requirements na hodnotu enable tzn. heslo musí obsahovat nealfanumerické znaky. Pod volbou Account Lockout policy se nachází definování politik pro zablokování účtu při špatných pokusech. Account Lockout duration nastavit na hodnotu 60, což definuje, že zablokování bude trvat jednu hodinu, pokud účet neodemkne administrátor, Account lockout threshold by měl být nastaven na hodnotu 4, aby došlo po čtvrtém špatném zadání hesla k zablokování účtu.



Obrázek 8: Nastavení politiky Password Policy a Account Lockout Policy

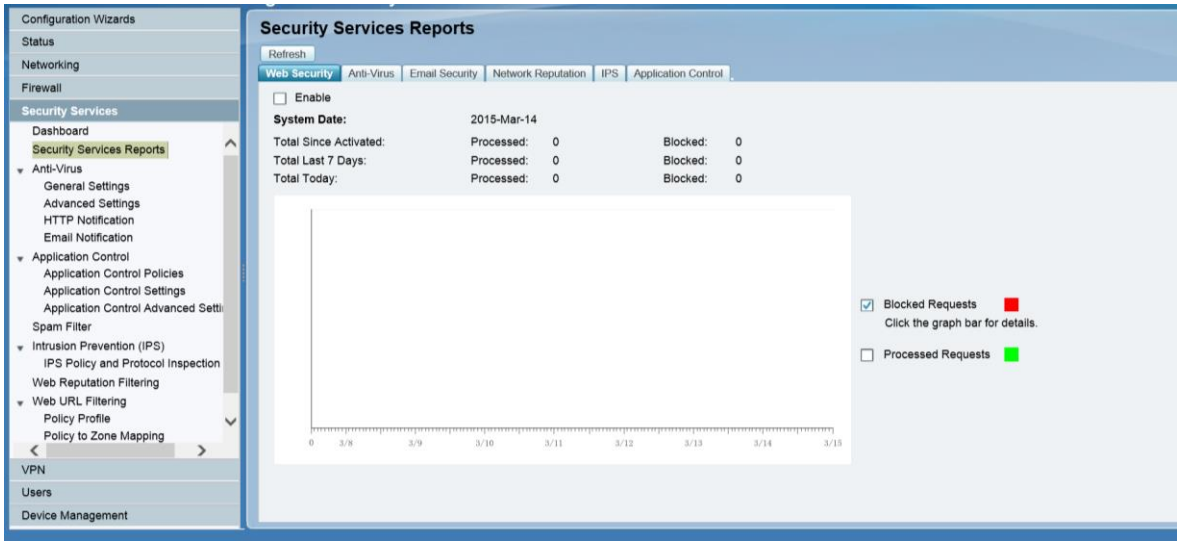
Zdroj: *Vlastní zpracování*

4.4.4 Zmírnění hrozby počítačových virů

Společnost je vybavena základními nástroji na obranu proti virům. Řešení je v dnešní době nedostačující a nedokáže ochránit koncová zařízení na potřebné úrovni. V první řadě je vhodné zabezpečit vstupní perimetr sítě. Nahradit stávající nevyhovující softwarový firewall novým firewallem, který bude spolehlivý a společnost bude schopná jej spravovat a bude mít k němu dostupnou dokumentaci. Z hlediska velikosti společnosti by mohl vyhovovat firewall od společnosti Cisco model ISA 550W. Cisco ISA550W je UTM[6] zařízení, které v sobě obsahuje nejen firewall, ale i řešení pro připojení dvou WAN sítí, vytvoření DMZ zón, VPN koncentrátoru s ochranou SSL i IPsec, IPS, antivirus, kontrolu aplikací, URL filtr, spam filtr, proxy a WIFI access point. Zařízení nabízí mnoho nástrojů pro použití v oblasti zabezpečení. V první řadě implementování firewallu. Implementace firewallu by měla probíhat tak, že všechny porty by měly být zakázané a povolovat pouze ty porty, které jsou potřebné pro komunikaci z vnější sítě, jako jsou porty pro mailovou komunikaci, prohlížení webu a přístup k firemním aplikacím. Po nastavení LAN a WAN parametrů je firewall funkční a může se zapojit do sítě. Zařízení je vybaveno dvěma WAN porty, které mohou být použity pro rozložení zátěže, ale v tomto případě spíše pro vytvoření

[6] Unified threat management – zařízení chránící perimetr sítě, slučující několik nástrojů do jednoho typicky firewall, IPS, VPN a další zařízení.

záložního přístupového bodu pro případ výpadku. V defaultním nastavení jsou všechny zmíněné nástroje vypnuté. Je doporučeno postupem času jednotlivé nástroje zapínat a případně nastavovat dle potřeby, není vhodné aktivovat všechny nástroje najednou z důvodu špatné detekce případné chyby v nastavení. Momentálně klientská aplikace, která je přístupná z vnější sítě, se nachází ve vnitřní síti. Pro eliminaci hrozeb by tento server měl být umístěn v DMZ. Do DMZ lze server umístit připojením UTP kabelu ze serveru do DMZ portu firewallu a ten pak v managementu firewallu přesměrovat na adresu přístupnou z vnější sítě. Tím dojde k oddělení vnitřní sítě a aplikace. V případě prolomení bezpečnosti aplikace útočník nezpůsobí škody na ostatních aktivech. Pro zvýšení zabezpečení proti virovým hrozbám je vhodné aktivovat některé nástroje, kterými UTM zařízení disponuje.



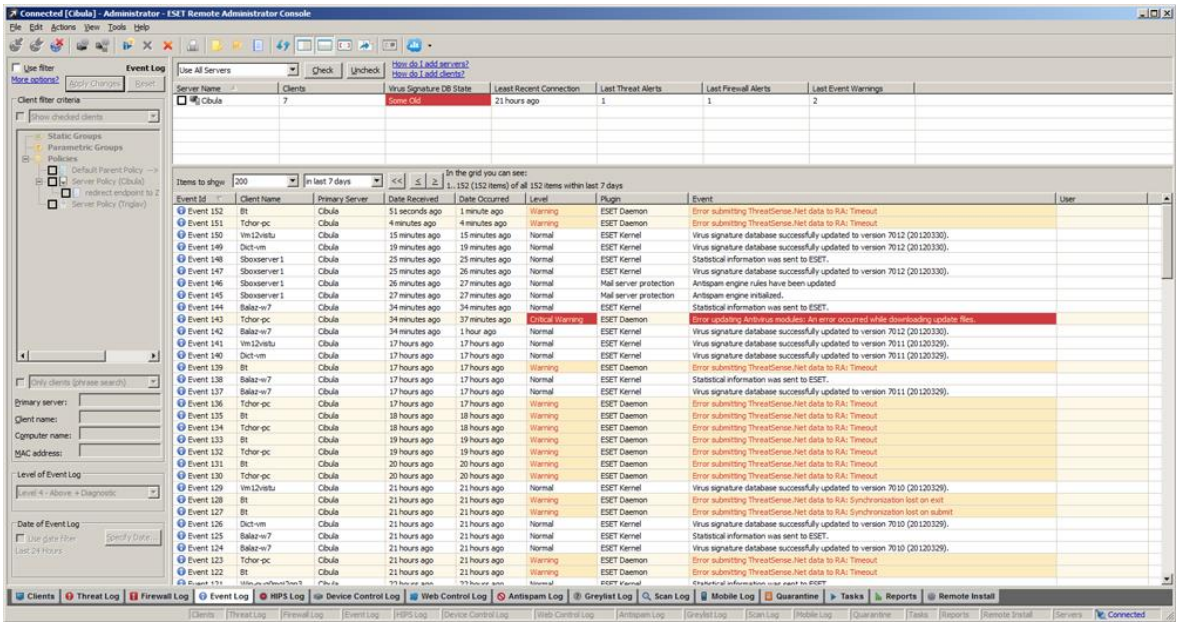
Obrázek 9: Management CISCO ISA550W Security Services

Zdroj: *Vlastní zpracování*

Web Reputation Filtering je nástroj, který hodnotí váhami jednotlivé webové stránky a porovnává je s databází stránek podle toho, zda se na nich vyskytují viry a jiné hrozby, a tím pak přidělí skóre od -10 do +10. Následně podle tohoto skóre považuje stránku za nebezpečnou nebo neškodnou. Pro aktivaci je nutné v modulu Security Services vybrat volbu Web Reputation Filtering a zvolit hodnotu skóre, od kterého bude prováděna blokace. V první řadě bude hodnota nastavena na – 6 a do white listu budou umístěny používané stránky (stránky webových aplikací a partnerů). V případě, že bude docházet k blokování legitimních webových stránek, dojde ke snížení skóre. Další funkcionalita, která bude

aktivována, je Web URL Filtering. Web URL Filtering filtruje webové stránky podle kategorií, do kterých si výrobce firewallů stránky řadí ve spolupráci s mezinárodními organizacemi. Pro začátek bude blokován obsah s pornografií a nelegálním obsahem, kde se nachází nejvíce hrozeb. K nastavení dojde stisknutím nástroje Web URL Filtering. Prvně je zapotřebí definovat politiku a zvolit typ blokovaného obsahu. Politika se následně přiřadí portům připojeným k firewallu a nastaví se port, na kterém probíhá http a https komunikace, nejčastěji se jedná o port 80 a 443. Opět se může zvolit seznam povolených webových stránek. Nástroj Network Reputation ochrání síť před DOS útoky a jinými hackerskými útoky blokováním IP adres, které se vyskytují na aktualizovaném blacklistu. Funkcionalita nemá žádné nastavení, lze ji pouze zapnout nebo vypnout, vhodné je ji zapnout. Jako poslední nástroj bude aktivován IPS. IPS bude monitorovat vnitřní síť, a pokud dojde k podezřelé činnosti, komunikaci zablokuje a informuje administrátora. Po aktivaci je možné nastavit, na jakých portech bude kontrola probíhat a nastavit úroveň nebezpečí. Ta bude nastavena na vysoká.

Další opatření pro zvýšení bezpečnosti je změna antivirového produktu z ESET Endpoint Antivirus na ESET Endpoint Security. Produkt navíc obsahuje firewall a antispam pro zabezpečení koncových stanic. Pro zabezpečení file serverů a mail serverů disponuje nástrojem ESET Mail Security a ESET File Security. ESET řešení umožňuje vzdálenou správu pomocí nástroje ESET Remote Administrator (ERA), kterým lze efektivně spravovat produkty a definovat bezpečnostní politiky. ERA bude nainstalován na CP7. Instalace probíhá jednoduše stylem „další a další“. Pouze je nutné vytvořit administrátorský účet s heslem. Po nainstalování ERA je nutné nainstalovat na počítač IT administrátora a IT seniora ERA konzoli pro práci s ERA. Po instalaci je nutné zadat IP adresu serveru, kde je umístěn ERA, tedy IP adresu serveru CP7. Po přihlášení zvolenými přístupovými údaji je vidět seznam koncových stanic, které lze ovládat, měnit nastavení, spouštět hromadné testy a sbírat bezpečnostní logy.



Obrázek 10: ESET Remote Administrator Console

Zdroj: *ESET: Remote Administrator 5. [online]. [cit. 2015-03-14]. Dostupné z: http://www.eset.com/cz/firmy/produkty/remote-administrator-5/*

V prvé řadě je zapotřebí vložit licenci. Po vložení licence je vhodné definovat defaultní politiku, aby bylo vynucováno základní nastavení antiviru a to pod volbou Tools a Policy manager. Zde je vhodné nastavit heslo pro vstup do nastavení produktu a další nastavení. ESET nabízí konzultaci pro firmy zdarma. Rozhodně je rozumné toto nastavení na základě nabídky konzultovat.

Produkt ESET Endpoint Security (EES) bude nainstalován na všechny koncové stanice a servery mimo file server a mailový server. V nastavení EES bude nastavena vzdálená správa, vyplněný server CP7 pro pohodlnou konfiguraci. Na mailový server bude nainstalován ESET Mail Security, který bude sloužit jako antispam a jeho nastavení zkonzultováno se společností ESET. V případě, že bude velké množství spamu v poštovních schránkách, bude nastavení zpřísněno, či v opačném případě bude zabezpečení sníženo. Na file server bude nainstalován nástroj ESET File Security, který umožňuje chránit data uložená na tomto serveru.

Vedení společnosti bude předložen návrh na instalaci antivirů do mobilních zařízení. Alespoň pro začátek je doporučen Avast, který nabízí verzi zdarma. Z hlediska správy by bylo vhodnější využít verzi od společnosti ESET, ale podle výsledků testů společnosti AV-

test ke konci roku 2014, produkt AVAST Mobile Security 4.0 se umisťuje na předních příčkách.

4.4.5 Zmírnění hrozby výpadku proudu

Ve společnosti jsou nainstalované dvě UPS zařízení, ale není využit jejich potenciál a proti výpadku elektrického proudu brání společnost jen částečně. Prvně by bylo vhodné připojit obě UPS do sítě skrze TCP/IP kabely pro možnost řídit UPS po síti. Výdrž baterií je uváděna výrobcem na 5 let. Skrze management lze zjistit stáří baterie a rozložení připojené zátěže. Z důvodu, že obě UPS jsou identická, mělo by být rozložení zátěže symetrické. Je vhodné nastavit pravidelné self testy, odesílání emailových notifikací administrátorům v případě, že dojde například k výpadku proudu. UPS umožňuje v případě úbytku elektrické energie pod kritickou hodnotu skrze TCP/IP port vypínání serverů. Vypínání lze nastavit aktivování v managementu volbou PowerChute® Network Shutdown Clients, dále definováním doby potřebné pro vypnutí serverů, ideální doba bude 7 minut, a přidáním IP adres serverů CP1, CP2 a CP3. V poslední části na zmíněné servery nainstalovat aplikaci PowerChute Network Shutdown, která umožní zmíněné vypnutí serverů po síti. Dalším krokem ke snížení dopadu výpadku proudu je umístění veškerých serverů a síťových prvků do UPS. Je nutné tedy připojit server CP3, switche a nový firewall do UPS. V objektu se nachází zásuvky připojené na dieslový agregát, který je aktivován a dodává elektrickou energii do sítě v případě výpadku elektrického proudu. Je vhodné UPS připojit do těchto zásuvek a prodloužit výdrž infrastruktury při výpadku proudu.

4.4.6 Zmírnění hrozby poruchy hardwaru

Pro eliminování nebezpečí poruchy hardwaru je vhodné vyměnit dva staré switche, ke kterým není dokumentace a z hlediska stáří hrozí jejich porucha. Vzhledem k použití firewallu od firmy Cisco je vhodné použití switchů od stejného výrobce idealně typ SG500-52P 52-port. Zvolený typ je takzvaně stackable to znamená, že oba dva switche lze ovládat jako jeden a ulehčí tak práci administrátorovi. Po instalaci je nutné zadat nové bezpečné heslo. Po výměně switchů je možné připojit servery pomocí více síťových karet zabezpečit tak vysokou dostupnost a zvýšit propustnost. Po připojení TCP/IP kabelů ze serveru do switche je potřeba nastavit NIC Teaming s využitím protokolu LACP pro agregování síťového provozu do jedné virtuální síťové karty. NIC teaming je potřeba nastavit na switchi pod volbou Port Management, Link Aggregation a LACP. Zde definovat jaké porty je

zapotřebí agregovat. V prostředí Windows Server nástrojem NIC Teaming nadefinovat novým team volbou Task a New Team, zde definovat síťové karty, které se teamu zúčastní a vybrat mód LACP.

Pro eliminaci situace, kdy odejde celý server a společnost nebude mít potřebný hardware, je doporučeno rozšířit stávající smlouvu s poradenskou firmou, která je používána v oblasti IT při vážnějších problémech, o dodatek, který by zahrnul zapůjčení serveru.

4.4.7 Zmírnění hrozby přírodní katastrofa

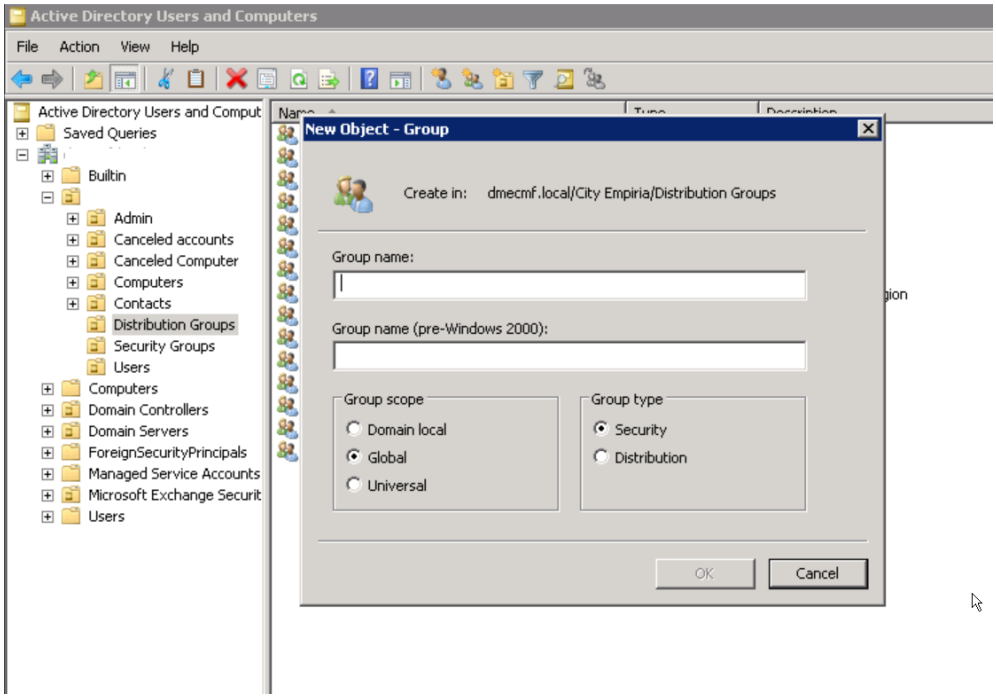
Při propuknutí přírodní katastrofy dojde k postižení všech aktiv a jejich zničení. Společnost musí být schopná obnovit veškerá data, aby mohla pokračovat v provozování činnosti. Z tohoto hlediska je důležité umístit vytvořené záložní kopie mimo objekt. Momentálně v případě katastrofy společnost přijde o všechny data. Vhodné umístění může být v jiné pobočce například v Praze, která je vzdálená cca. hodinu cesty a zaměstnanci cestují mezi těmito lokacemi několikrát denně. Záložní kopie by měly být zašifrované, předávané oproti předávacímu protokolu zvoleným osobám a uložené v trezoru.

4.4.8 Zmírnění hrozby nepovolaného přístup k datům z vnitřní sítě

V případě ochrany vnitřní sítě je vhodné rozsegmentovat vnitřní síť do VLAN oddělení jednotlivých nodů (uzlů) na sítě. VLAN umožňuje konfigurovat povolení či zakázání komunikace mezi sítěmi. Určitě je vhodné, aby se návštěvy nedostaly do vnitřní sítě či zaměstnanci k serverům, kam nemají mít přístup. V případě dané společnosti se jeví jako vhodné použití rozdělení VLAN podle MAC adres. Ve firmě dochází k pohybu zaměstnanců a jen složitě by se dalo definovat VLAN podle portů. VLAN budou vytvořeny na základě organizační struktury firmy. Bude vytvořena VLAN pro IT, kde budou umístěny servery a správci s přístupem ke všem zdrojům. Další VLAN bude pro finanční a mzdové oddělení s přístupem k ekonomickému, účetnímu a mzdovému softwaru, emailovému klientu, file serveru a internetu. Tiskárny budou mít přístup pouze na emailový server pro odesílání naskenovaných dokumentů. Návštěvy budou mít přístup pouze na internet a VLAN ostatní bude umožňovat přístup k firemním aplikacím, datům, internetu a emailu. Konfigurace VLAN a správa MAC adres umožňuje management switchů. Vytvoření VLAN se nachází v sekci VLAN Management pod volbou Creating VLANs, je nutné celou operaci naplánovat a zkonzultovat. Zařízení, které nebudou přiřazena do žádné VLAN se k síti nepřipojí. I tak je vhodné v pravidelných intervalech kontrolovat aktuální zařízení v síti.

Součástí vybraného firewallu je i wireless access point. Ten nahradí stávající WIFI řešení. Bezpečné je vytvoření bezdrátové sítě se zabezpečením WPA 2 Enterprise ověřované Radius serverem. Vyhovující je i WPA 2 personal, které bude implementováno. Šifrování bude nastaveno AES. Z hlediska bezpečnosti budou vytvořeny dvě SSID, jedno pro návštěvy, kterému bude přiřazena VLAN určena pro návštěvy a druhá pro zaměstnance. Konfigurace wireless adaptéru se nachází v managementu firewallu v modulu Wireless pod volbou Basic Settings.

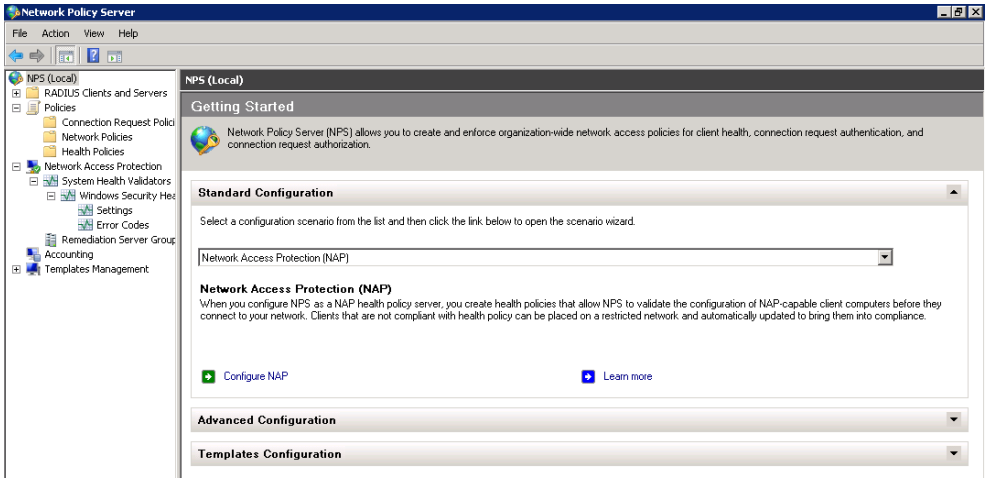
Základem pro to, aby zaměstnanci přistupovali v rámci vnitřní sítě pouze tam, kam mají povolený přístup, spočívá ve správně definovaném přístupu k jednotlivým zdrojům. Definice se provádí na úrovni NTFS oprávnění nad jednotlivými soubory či složkami. Pro jednodušší správu je ke každé složce nadefinováno nastavení s jednotlivými oprávněními a ta jsou pak umístěna do security groups. Jednotlivé security groups jsou poté agregovány do distribution groups, ke kterým je přiděleno členství jednotlivým uživatelům. Správa uživatelů a jednotlivých skupin se provádí na doménovém řadiči pomocí nástroje Active directory users and computers. Ve společnosti se používají pouze distribution groups. Pro jednodušší správu Microsoft doporučuje používat i security groups. Pro řízení přístupu zaměstnanců pouze tam, kam by měli mít přístup, by mělo být ošetřeno správným přiřazení do jednotlivých skupin a nastavení oprávnění na úrovni jednotlivých souborů či složek. Nastavení na obou stranách by mělo být pravidelně kontrolováno pracovníky IT. K tomu však momentálně nedochází. Kontrola by měla být vynucována příslušnou směrnicí a směrnice by měla v ideálním případě nařizovat kontrolu v půlročním intervalu. Pouze takto bude ošetřeno, že zaměstnanec se nedostane k souborům, ke kterým už nemá mít dávno přístup.



Obrázek 11: Active directory Distribution Groups & Security Groups

Zdroj: *Vlastní zpracování*

V rámci bezpečnosti vnitřní sítě se firma potýká s jedním nebezpečným jevem. Do sítě se připojí zařízení, které nemá nainstalované nejnovější aktualizace, nemá antivirus či zapnutý firewall a může být infikované a může tak nákazu rozšířit do celé sítě. Nebezpečí se týká hlavně koncových stanic připojujících se přes VPN. Aby administrátoři mohli vynucovat zabezpečení, je nutné nainstalovat nástroj Microsoft Network Access Protection (NAP). NAP je součástí řešení Windows Server a není zapotřebí platit další poplatky. Instalace se provede spuštěním server manageru a stisknutím tlačítka Add Roles and Features. Pod volbou rolí vybrat Network Policy and Access Services a stisknutím tlačítka instalovat. Konfigurování NAPu se provádí pomocí konzole Network policy server.



Obrázek 12: Konzole nástroje Network Policy Server

Zdroj: *Vlastní zpracování*

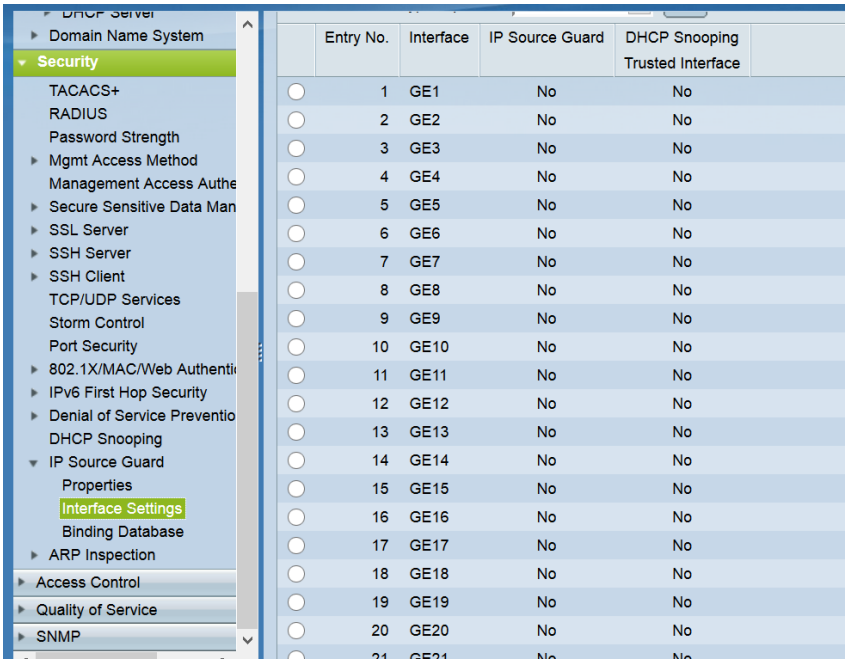
Po zapnutí konzole je nutné stisknout tlačítko Configure NAP. V případě této firemní sítě budou vynucovány restrikce prostřednictvím DHCP server. Proto v otevřeném okně bude zvoleno pod volbou Network connection method hodnota Dynamic Host configuration protocol (DHCP) a pokračováním volbou další. V dalším zobrazeném okně volbou add je zapotřebí zadat IP adresu DHCP serveru a stisknout next. Nastavení bude platné pro všechny DHCP rozsahy, všechny koncové stanice a ostatní hodnoty zůstanou defaultní, proto další okna zůstanou prázdná a je možné pokračovat stisknutím tlačítka next až konec konfigurace se provede stisknutím tlačítka finish. Dále je zapotřebí definovat jaké nastavení bude NAP vynucovat. To se provede v nástroji NPS volbou Network Access Protection - System Health Validators – Windows Security Health Validator – Settings. V prostředí firmy bude vynucováno, aby byl nainstalován antivirus, zapnutý firewall a automatické aktualizace. Pokud koncová stanice stanovené podmínky nesplní, nezíská přístup k firemním zdrojům. K dokončení nastavení je nutné na DHCP serveru v konzoly DHCP kliknutím na volbu IPv4 pravým tlačítkem a vyvoláním volby Properties a pod záložkou Network Access protection stisknout tlačítko Enable on all scopes. V poslední řadě je nutné otevřít nástroj Group Policy Managment (GPM), který je umístěn na doménovém kontroleru. V GPM managementu stisknout pravé tlačítko na Default domain policy a stisknout edit. V nově otevřeném okně pod volbou Computer Configuration – Policies – Security Setings – Network Access Protection – Enforce Client a aktivovat volbu DHCP Quarantine Enforcement Client. Dále v Computer Configuration – Policies – Security Setings – Systém Services nastavit, službu

Network Access Protection Agent na Automatic. Jako poslední je nutné aktivovat Computer Configuration – Policies – Administrative Templates – Windows Components – Security Center a zde se nachází politika s názvem Turn On Security Center. Tím to nastavením je síť zabezpečena proti koncovým stanicím, které nesplňují definované bezpečnostní požadavky.

4.4.9 Zmírnění hrozby odposlechu a modifikace komunikace v síti

Jako poslední část v rámci eliminace definovaných hrozeb je nutné zabezpečit firemní síť proti odposlechu a modifikaci komunikace. Používání VLAN možnost zneužití vnitřní sítě dosti eliminuje, ale stále může dojít k modifikaci komunikace v rámci jedné VLAN. Z tohoto důvodu většina komunikace proudící sítí obzvláště obsahující přihlašovací údajě by měla být šifrovaná. Ve firemní infrastruktuře většina aplikací obsahují šifrovaný SSL certifikát až na klientskou aplikaci. Zde je zapotřebí kontaktovat dodavatele aplikace a zadat mu zabezpečení aplikace TLS certifikátem vydaným certifikační autoritou. U ostatních používaných aplikací provést audit, zda používají nejnovější certifikáty a nejlépe SSL certifikáty nahradit TLS certifikátem.

Pro zvýšení zabezpečení je vhodné aktivovat bezpečnostní prvky na úrovni switche. Nové Cisco switche podporují funkci DHCP Snooping. DHCP snooping umožňuje povolit odesílání packetů DHCP offer pouze z legitimních DHCP serverů a zasílání packetů, pouze cílovým klientům, kteří získali IP adresu z definováného DHCP serveru. To znamená, že v případě, kdy v síti bude umístěn například cizí router se zapnutým DHCP, bude komunikace blokována. Lze ještě zapnout IP Source Guard a v případě, že v síti se bude nalézat zařízení, kterému DHCP server nepřidělil IP adresu, rovněž komunikace bude zablokována. Funkce DHCP Snooping se aktivuje v konzoli switche. V modulu Security – DHCP Snooping / Relay pod volbou Properties. Zde je nejprve nutné aktivovat funkcionalitu volbou enabled, dále v Interface settings definování VLAN, na kterých bude DHCP Snooping aktivován. Ve firemním prostředí bude aktivován na všech VLAN. Pod volbou DHCP Snooping Trusted Interfaces je třeba zvolit port, na kterém je umístěn DHCP server. IP Source Guard se aktivuje taktéž v modulu Security a IP Source Guard a volbou Enabled.



Obrázek 13: Cisco SG500 management konzole

Zdroj: *Vlastní zpracování*

ESET Endpoint Security obsahuje ochranu proti sniffingovým nástrojů a jiným síťovým útokům jako je ARP poisoning atd. V případě detekce hrozby varuje uživatele a administrátora nástrojem ERA. I tak by IT administrátoři měli občas skenovat síť například pomocí nástroje promqry, zda se v síti nenachází sniffer a nebo používat nástroj fing, zda v síti není neznámé zařízení.

4.4.10 Další navrhované prvky pro zvýšení zabezpečení:

- Nástroj pro monitoring síťového provozu pro přehled o trafficu dle jednotlivých zařízení například Katalyzer či NTOP.
- Implementace Radius Serveru a zlepšení zabezpečení WIFI sítě na WPA2 Enterprise. Zamezení zjištění použité verze OS.
- Implementace nástroje Microsoft File Server Resource pro zamezení ukládání nelegálního obsahu a možnosti hlášení například při nahrání mp3 souboru na souborový server.
- Správa a distribuce aktualizací skrze Microsoft WSUS.
- Implementace Proxy serveru k možnosti zvýšení zabezpečení.
- Přidat sekundární DHCP server.

- Aktivování VSS na souborovém serveru.
- Definovat ACL pro přístup k síťovým prvkům.

4.5 Cenová kalkulace navržených změn

Ekonomické náklady navrhovaných změn byly v co největší míře eliminovány a většinu navrhovaných změn je schopné zajistit vlastní IT oddělení. V případě práce IT oddělení je v přehledu definována pouze přibližná časová náročnost pro dodatečné vyčíslení ceny zabezpečení včetně práce IT pracovníků. V kalkulacích nejsou zahrnuty náklady na přestěhování serverovny. Jednotlivé navrhované změny a jejich pracnost je uvedena v tabulce 5.

Tabulka 5: Časová náročnost navrhovaných změn

Činnost	Úroveň IT	Časová náročnost
Přenastavení admin účtů	IT administrator	2 hod.
Nagios	IT senior	40 hod.
Bitlocker servery	IT administrator	2 hod.
Bitlocker notebooky	IT Junior	20 hod.
Definování Exchange ActiveSync Mailbox Policies	IT administrator	1 hod.
Změna politiky hesel	IT administrator	1 hod.
Instalace a nastavení Cisco ISA 550W		
Instalace a základní nastavení	IT senior	4 hod.
URLF, DMZ, IPS	IT senior	3 hod.
VPN	IT senior	4 hod.
WIFI	IT senior	4 hod.
Instalace a nastavení ESET		
ESET Mail Security	IT senior	4 hod.
ESET File Server	IT senior	3 hod.
ESET Endpoint Security servery	IT administrator	3 hod.
ESET Endpoint Security koncové stanice	IT Junior	40 hod.
ESET ERA	IT administrator	5 hod.
Překonfigurování UPS	IT senior	2 hod.
Instalace a nastavení 2x Cisco SG500-52P		
Instalace a základní nastavení	IT senior	16 hod.
VLAN	IT senior	10 hod.
NIC Teaming	IT senior	4 hod.
DHCP Snooping	IT senior	3 hod.
NTFS audit	IT administrator	8 hod.
Instalace a nastavení NAP	IT administrator	5 hod.

Zdroj: *Vlastní zpracování*

Celková časová náročnost na jednotlivé IT pracovníky je uvedena v tabulce 6.

Tabulka 6: Pracnost navrhovaných změn celkem

IT pracovník	Časová náročnost
IT Junior	60 hod.
IT administrator	27 hod.
IT senior	97 hod.
Celkem	**184 hod.**

Zdroj: *Vlastní zpracování*

Finanční náklady na snížení bezpečnostních rizik mimo práce interních IT pracovníků jsou uvedeny v tabulce 7. Z hlediska personálních nákladů záleží na společnosti, jestli má volné kapacity v řadách svých zaměstnanců anebo navržené implementace bude realizovat externí firmou. V případě outsourcingu veškerých implementací je přibližná částka vyčíslena v tabulce 7 při běžných tržních cenách uvedených bez DPH.

Tabulka 7: Kalkulace nákladů za práci při realizaci externí firmou

IT pracovník	Hodinová sazba	Celková cena
IT Junior	500 Kč	30 000 Kč
IT administrator	1 100 Kč	29 700 Kč
IT senior	1 500 Kč	145 500 Kč
Celkem		**205 200 Kč**

Zdroj: *Vlastní zpracování*

Náklady na navržené bezpečnostní prvky jsou určeny v tabulce 8. Ceny jsou uvedeny bez DPH.

Tabulka 8: Finanční náklady na zmírnění bezpečnostních rizik

Položka	Množství	Cena bez DPH
ESET EES	160x	131 680 Kč
Cisco ISA 550W	1x	17 000 Kč
Cisco SG500-52P	2x	90 000 Kč
TLS certifikát	1x	8 100 Kč
TLS certifikát práce	4 hod.	6 000 Kč
Celkem		**244 550 Kč**

Zdroj: *Vlastní zpracování*

Od nákladů pro reálnou hodnotu investice do zabezpečení je nutné odečíst 92 000 Kč. Tato částka tvoří roční paušální náklad do stávajícího antivirového řešení. Při změně antivirového řešení náklad odpadne. Ideální doba pro změnu antiviru bude před vypršením stávající licence pro eliminaci nákladů. V případě, že firma využije outsouricngu a po odečtení nákladů na nastávající antivirové řešení je hodnota investice k realizování navrhovaných změn 357 750 Kč.

5 Závěr

Bezpečnost informačních systémů je důležitou otázkou, kterou by se měla zabývat každá firma od malých až po velké firmy. Velikost finančních prostředků vynakládaných na bezpečnost by měla být přímo úměrná povaze a hodnotě chráněných aktiv. Je nevhodné implementovat bezpečnostní mechanismy, u kterých cena převyšuje hodnotu chráněných aktiv. Na druhou stranu nelze praktikovat názor, že této firmy se problémy netýkají a není třeba implementovat potřebné zabezpečení. Pro úspěšné řízení bezpečnosti ve společnosti je nutné mít podporu vedení pro vydávání bezpečnostních norem, vynucovaných restrikcí a schvalování nákupu nových bezpečnostních nástrojů.

Vedlejším cílem práce bylo definovat pojmy, které jsou používány v oblasti IT bezpečnosti. V praktické části jsou vysvětleny pojmy IT bezpečnost, popsání jednotlivých hrozeb, rizik, bezpečnostní politiky, standardů, bezpečnostních incidentů a dalších termínů, které pomohou lépe pochopit a porozumět dané problematice.

Hlavním cílem praktické části bylo na základě teoretických východisek a analýzy výchozího stavu zhodnotit a doporučit nastavení zabezpečení. Nejprve byla představena analyzovaná společnost včetně přiblížení, jakým disponuje IT vybavením. Poté byl proveden bezpečnostní audit, který vycházel z metodiky normy ISO 27001. Provedený audit byl zjednodušen a v případě rozhodnutí společnosti pro provedení certifikace ISO 27001 je nutné provést bezpečnostní audit více podrobně. Zde byl audit použit pro přiblížení aktuálního stavu, jako návod pro metodický postup a definování kritických oblastí.

Po provedení bezpečnostního auditu a přiblížení společnosti byla provedena analýza rizik. Analýza rizik určuje kritická aktiva umístěna ve společnosti a dává je do vztahu s aktuálními hrozbami, které mohou aktiva postihnout. Mezi nejkritičtější hrozby se řadí chyba administrátora, krádež nebo ztráta zařízení, zkoušení uhádnutí hesel a počítačový virus. Tedy hrozby hrozí spíše z vnitřního prostředí a je potřeba je ošetřit. Mezi nejohroženější aktiva patří emailový server a klientská aplikace.

Na základě analýzy rizik a zjištění bezpečnostních nedostatků v provedeném bezpečnostním auditu byly navrženy způsoby jak hrozby eliminovat a lépe zabezpečit aktiva. Zlepšení bylo navrženo pro všechny kritické hrozby. Jedná se například o zakoupení nového firewallu, switche implementování nového antivirového řešení. Zlepšení pro oblasti, které nejsou takovou mírou ohroženy, byly navrženy jen bodově. Aplikováním navrhovaného zlepšení dojde k odstranění některých zmiňovaných hrozeb v provedeném

auditu. Například dojde k odstranění kritických serverů, které pracují na linuxové platformě a obsahují řadu bezpečnostních chyb a nejsou dostatečně spravovány. Jedná se o servery CP12 a CP11, server CP10 je zapotřebí aktualizovat případně nahradit serverem s platformou MS Windows. Pro správný chod IT, je zapotřebí definovat pravidelné činnosti administrátorů a evidování v administrátorském deníku.

V závěru práce je souhrn časové náročnosti uvedených prací pracovníky IT a cen použitých technologií. Souhrn je k dispozici vedení společnosti pro dodatečné vyčíslení celkových nákladů na implementované bezpečnostní mechanismy. Pro práci nebyla získána informace o hodnotě práce jednotlivých IT pracovníků z toho důvodu, je vyčíslena pouze časová náročnost. Ceny použitých technologií jsou uvedeny bez DPH. Náklad na implementaci produktu ESET je vysoký, ale pro vypovídající hodnotu jako změny oproti stávajícímu řešení, je nutné od tohoto nákladu odečíst náklady na stávající řešení.

Cíle práce byly dosaženy. Práce může být použita jako podklad vedení společnosti pro schválení navrhovaných změn a jako podklad pro IT manažera, který získá určitý návod jak navrhované změny v infrastruktuře provést, časovou náročnost pro vytváření plánu implementace a ohrožená aktiva a seznam nedostatků.

6 Seznamy

6.1 Seznam použitých zdrojů

1) KUCHAŘ, Miloš. Bezpečná síť: jak zajistíte bezpečnost vaší sítě. 1. vyd. Praha: Grada, 1999, 91 s. ISBN 80-716-9886-5.

2) LOCKHART, Andrew. *Bezpečnost sítí na maximum*. Vyd. 1. Překlad Jiří Veselský. Brno: CP Books, 2005, 276 s. ISBN 8025108058.

3) IT Security: Analýza rizik. [online]. [cit. 2015-03-19]. Dostupné z: http://www.it-security.cz/sluzby/analy-rizik.html

4) IT Security: Penetrační testy. [online]. [cit. 2015-03-19]. Dostupné z: http://www.it-security.cz/sluzby/penetracni-testy.html

5) SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.

6) AEC: Bezpečnostní politika organizace. [online]. [cit. 2015-03-19]. Dostupné z: http://www.aec.cz/cz/sluzby/bezpecnostni-politika-organizace

7) DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Brno: Computer Press, a.s., 2004. 190 s. ISBN 80-251-0106-1

8) System Online: Analýza rizik IT bezpečnosti. [online]. [cit. 2015-03-19]. Dostupné z: http://www.systemonline.cz/it-security/analyza-rizik-it-bezpecnosti.htm

9) ERNST & YOUNG. Průzkum stavu informační bezpečnosti v ČR 2009. Ernst & Young, NBÚ, DSM data security management a Národní bezpečnostní úřad, 2009. 40 s. ISBN 978-80-86813-19-6

10) AEC: SIEM. [online]. [cit. 2015-03-19]. Dostupné z: http://www.aec.cz/cz/produkty/siem

11) ESET. [online]. [cit. 2015-03-19]. Dostupné z: http://www.eset.com

12) NORTHCUTT, S., ZELTSER, L., WINTERS, S., FREDERICK, K., RITCHEY, R. Bezpečnost počítačových sítí. 1. vyd. Brno: CP Books, a.s.,2005.589s.ISBN 80-251-0697-6

13) Svět sítí: Zabezpečení lokálních datových sítí proti neoprávněným uživatelům. [online]. [cit. 2015-03-19]. Dostupné z: http://www.svetsiti.cz/rubrika.asp?rid=17&tid=285

14) Tech Ihned: Vše, co potřebujete vědět o zálohování. [online]. [cit. 2015-03-19]. Dostupné z: http://tech.ihned.cz/c1-59066300-zalohovani-dat-navod-1-dil

15) The Geek Stuff: RAID 0, RAID 1, RAID 5, RAID 10 Explained with Diagrams. [online]. [cit. 2015-03-19]. Dostupné z: http://www.thegeekstuff.com/2010/08/raid-levels-tutorial/

16) Hacking - manuál hackera Allen Harper, Shon Harris, Chris Eagle, Jonathan Ness, Michael Lester

17) JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha: Grada, 2007, 284 s. Hacking. ISBN 9788024715612.

18) Anonymous. Maximální bezpečnost. Svazek 1. Praha: Soft Press, 2004, 433 s. ISBN 80-86497-65-8

19) THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. Cisco systems. ISBN 8025104176.

20) System Online: Využití metodiky IT governance a ITIL. [online]. [cit. 2015-03-19]. Dostupné z: http://www.systemonline.cz/clanky/vyuziti-metodiky-it-governance-a-itil.htm

21) Clever and smart: COBIT tajemství zbavený. [online]. [cit. 2015-03-19]. Dostupné z: http://www.cleverandsmart.cz/cobit-tajemstvi-zbaveny/

22) ENDORF, Carl F, Eugene SCHULTZ a Jim MELLANDER. *Detekce a prevence počítačového útoku*. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 8024710358.

23) CISCO: Cisco Small Business ISA500. [online]. [cit. 2015-03-19]. Dostupné z: http://www.cisco.com/c/en/us/products/collateral/security/small-business-isa500-series-integrated-security-appliances/data_sheet_c78-717565.html

24) AV-test: The best antivirus software for Android. [online]. [cit. 2015-03-19]. Dostupné z: http://www.av-test.org/en/antivirus/mobile-devices/

25) Svět sítí: Virtuální lokální sítě VLAN. [online]. [cit. 2015-03-19]. Dostupné z: http://www.svetsiti.cz/rubrika.asp?rid=17&tid=237

26) Business IT: Kybernetická kriminalita. [online]. [cit. 2015-03-19]. Dostupné z: http://www.businessit.cz/cz/kyberneticka-kriminalita-iii-hacktivismus-a-kyberterorismus.php

27) HARRIS, S., HARPER, A., EAGLE, CH., NESS, J., LESTER, M. Hacking Manuál hackera. 1. vyd. Praha: Grada Publishing, a.s., 2008. 400 s. ISBN 978-80-247-1346-5

28) CISCO: Cisco SG500-52P. [online]. [cit. 2015-03-19]. Dostupné z: http://www.cisco.com/c/en/us/support/switches/sg500-52p-52-port-gigabit-poe-stackable-managed-switch/model.html

29) Microsoft Technet: Architektura NAP. [online]. [cit. 2015-03-19]. Dostupné z: https://technet.microsoft.com/cs-cz/library/cc753550%28v=ws.10%29.aspx

30) ČSN ISO/IEC 27001. *ČESKÁ TECHNICKÁ NORMA: Informační technologie - Bezpečnost techniky - Systémy managementu bezpečnosti informací - Požadavky*. Říjen 2006. Praha: Český normalizační institut, 2006.

6.2 Seznam obrázků:

6.3 Seznam tabulek:

6.4 Seznam příloh

Příloha 1: Analýza rizik pravděpodobnost vzniku rizika

Hrozby	Aktiva	Hardware	Stolní PC	Notebooky	Mobilní telefony	Paměťové média	Servery	Síťové prvky	Tiskárny	Software	Operační systémy	Základní SW	Ekonomický a účetní SW	Emailový SW	Mzdový SW	Klientská aplikace	Data	SQL databáze	db klientského SW	mzdové a účetní	smlouvy	zálohy dat	Business a finanční plány	Zaměstnanci	Administrátor	Management	Goodwill	Infrastruktura	Serverovna
SPAM			4	4	4	0	3	0	0					4		3									2	4			
Výpadek proudu			2				2	2	2		2	2	2	2	2	2		2	2	2	1	1	1		1	1	2		2
Porucha HW			2	2	2	2	2	2	2		2	1	1	1	1	1		1	1	1	1	1	1		1	1	1		1
Chyba uživatele			2	2	2	2			1		2	2	3	2	2	3		2	3	3	2								
Počítačový virus			3	3	2	3	2				3	1	1	1	1	1		1	1	1	1	1	1		2	2	1		
Chyba programového vybavení			1	1	1		2	1			2	2	1	1	1	2		2	2	2					1	1	1		
Selhání LAN							1	2					2	2	2	2		2	2	2	1	2	1		1	1	2		2
Selhání WAN							1	2						2		2									1	1	2		
Chyba administrátora nebo IT			3	3	2	3	2	2	2		3	3	2	2	2	3		2	2	2	1	2	2		2	2	2		2
Krádež zařízení nebo ztráta			1	3	3	4	2	1			2	2	1	1	1	2		2	2	1	2	3	3		2	3	2		
Únik informací													1	3	2	3		2	3	2	3	3	3			2	3		
Nepovolaný přístup k datům ze vnitř							2				2	2	2	2	1	2		3	3	3	3	3	3		2	2	1		
Přírodní katastrofa			1	1	1	1	1	1	1		1	1	1	1	1	1		1	1	1	1	1	1		1	1	1		1
Nepovolaný přístup k datům zvenčí							1				2	2	2	2	1	2		2	2	1	3	2	3		2	2	1		
Falšování elektronických dokumentů a transakcí																					2	2	2		1	1	1		
Odposlech a modifikace komunikace v síti						3	3	2			3	2	2	3	2	3		1	1	2	3	1	2		2	2			
Zkoušení uhádnutí hesel			3	3	2	1	2	1			2		2	2	3	3		1	1	2	3	1	3		3	2			

Příloha 2: Analýza rizik ohodnocení následků

Hrozby	Aktiva	Hardware	Stolní PC	Notebooky	Mobilní telefony	Paměťové média	Servery	Síťové prvky	Tiskárny	Software	Operační systémy	Základní SW	Ekonomický a účetní SW	Emailový SW	Mzdový SW	Klientská aplikace	Data	SQL databáze	db klientského SW	mzdové a účetní	smlouvy	zálohy dat	Business a finanční plány	Zaměstnanci	Administrátor	Management	Goodwill	Infrastruktura	Serverovna
SPAM			1	1	1		1																		1	1			
Výpadek proudu			3	2			3	3	1		3	3	3	3	3	3		3	3	3	3	3	3		2	2	3		2
Porucha HW			2	2	2	2	4	3	2		3	2	3	4	3	3		3	3	3	2	2	2		2	2	2		4
Chyba uživatele			2	2	2	2			2		2	2	2	1	2	3		2	3	3	2		4				3		
Počítačový virus			2	2	1	1	4				3	2	3	4	3	4		4	4	3	4	3	4		4	3	4		
Chyba programového vybavení			2	2	2	3	3	3	1		3	2	3	4	4	4		4	4	4	4	2	3		2	2	2		
Selhání LAN							1	1					2	3	2	3		2	3	3	3	3	2		2	2	3		
Selhání WAN							1	2						2		3		2	3						1	1	3		
Chyba administrátora nebo IT			2	2	2	2	4	3	2		3	2	3	4	3	3		3	3	3	2	2	2		2	2	2		4
Krádež zařízení nebo ztráta			2	2	2	3	4	3	3		3	2	4	4	3	3		3	4	3	2	4	2		2	3	4		
Únik informací													1	4	2	3		4	4	3	4	3	4			3	4		
Nepovolaný přístup k datům ze vnitř							3				3	2	3	4	4	4		4	4	4	4	4	4		2	3	3		
Přírodní katastrofa			2	2	2	2	5	3	2		3	2	3	5	3	5		4	3	3	2	2	2		2	2	5		4
Nepovolaný přístup k datům zvenčí							3				3	2	3	4	3	4		4	4	3	4	4	4		2	3	3		
Falšování elektronických dokumentů a transakcí													3	3	3	3				4	4	2	4		1	1	3		
Odposlech a modifikace komunikace v síti						3	3	2			3	2	3	3	2	3		4	4	3	4	4	4		2	2	2		
Zkoušení uhádnutí hesel			2	2	2	2	4	3	2		3	2	3	4	3	3		3	3	3	2	2	2		2	2	2		

Příloha 3: Analýza rizik výsledná tabulka

Hrozby	Aktiva	Hardware	Stolní PC	Notebooky	Mobilní telefony	Paměťové	Servery	Síťové prvky	Tiskárny	Software	Operační	Základní SW	Ekonomický a	Emailový SW	Mzdový SW	Klientská	Data	SQL databáze	db klientského	mzdové a účetní	smlouvy	zálohy dat	Business a	Zaměstnanci	Administrátor	Management	Goodwill	Infrastruktura	Serverovna	Riziko hrozby
SPAM			4	4	4	0	3	0	0		0	0	0	4	0	3		0	0	0	0	0	0		3	5	0		0	**1,30**
Výpadek proudu			5	2	0	0	5	5	3		5	5	5	5	5	5		5	5	5	4	4	4		3	3	5		4	**4,00**
Porucha HW			4	4	4	4	6	5	4		5	3	4	5	4	4		4	4	4	3	3	3		3	3	3		5	**3,96**
Chyba uživatele			4	4	4	4	0	0	3		4	4	5	3	4	6		4	6	6	4	0	4		0	0	3		0	**3,13**
Počítačový virus			5	5	3	4	6	0	0		6	3	4	5	4	5		5	5	4	5	4	5		6	5	5		0	**4,09**
Chyba programového vybavení			3	3	3	3	5	4	1		5	4	4	5	5	6		6	6	6	4	2	3		3	3	3		0	**3,78**
Selhání LAN			0	0	0	0	2	3	0		0	0	4	5	4	5		4	5	5	4	5	3		3	3	5		2	**2,70**
Selhání WAN			0	0	0	0	2	4	0		0	0	0	4	0	5		2	3	0	0	0	0		2	2	5		0	**1,26**
Chyba administrátora nebo IT			5	5	4	5	6	5	4		6	5	5	6	5	6		5	5	5	3	4	4		4	4	4		6	**4,83**
Krádež zařízení nebo ztráta			3	5	5	7	6	4	3		5	4	5	5	4	5		5	6	4	4	7	5		4	6	6		0	**4,70**
Únik informací			0	0	0	0	0	0	0		0	0	2	7	4	6		6	7	5	7	6	7		0	5	7		0	**3,00**
Nepovolaný přístup k datům ze vnitř			0	0	0	0	5	0	0		5	4	5	6	5	6		7	7	7	7	7	7		4	5	4		0	**3,96**
Přírodní katastrofa			3	3	3	3	6	4	3		4	3	4	6	4	6		5	4	4	3	3	3		3	3	6		5	**3,96**
Nepovolaný přístup k datům zvenčí			0	0	0	0	4	0	0		5	4	5	6	4	6		6	6	4	7	6	7		4	5	4		0	**3,61**
Falšování elektronických dokumentů a transakcí			0	0	0	0	0	0	0		0	0	3	3	3	3		0	0	4	6	4	6		2	2	4		0	**1,74**
Odposlech a modifikace komunikace v síti			0	0	0	6	6	4	0		6	4	5	6	4	6		5	5	5	7	5	6		4	4	2		0	**3,91**
Zkoušení uhádnutí hesel			5	5	4	3	6	4	2		5	2	5	6	6	6		4	4	5	5	3	5		5	4	2		0	**4,17**
Rizikové aktiva			**2**	**2**	**2**	**2**	**4**	**2**	**1**		**4**	**3**	**4**	**5**	**4**	**5**		**4**	**5**	**4**	**4**	**4**	**4**		**3**	**4**	**4**		**1**	