Návrh zabezpečení informačního systému městského úřadu

Bc. Jan Števko

Diplomová práce
2014

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2013/2014

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan Ševko**
Osobní číslo:	**A12352**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh zabezpečení informačního systému městského úřadu**
Téma anglicky:	**A Proposal for the Security of a Municipality's Information System**

Zásady pro vypracování:

1. **Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.**
2. **Analyzujte současný stav zabezpečení informačního systému městského úřadu.**
3. **Na základě výsledků analýzy navrhněte vhodný způsob zabezpečení informačního systému městského úřadu.**
4. **Realizujte a ověřte navržená opatření.**
5. **Proveďte vyhodnocení celého projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman: Ochrana znalostí a dat v podnikových informačních systémech. Zlín : Univerzita Tomáše Bati ve Zlíně, 2002. 115 s. ISBN 80-7318-095-2.**
2. **DOSTÁLEK, Libor. Velký průvodce protokoly TCP/IP: bezpečnost. Vyd. 1. Praha: Computer Press, 2001, xvi, 565 s. ISBN 807226513x.**
3. **MALANÍK, David: Význam fyzického zabezpečení IT systémů. Security Revue září 2010. ISSN 1336-9717.**
4. **NORTHCUTT, Stephen, et al. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.**
5. **THOMAS, M. : Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno : CP Books, 2005. 338 s. ISBN 80-251-0417-6.**
6. **DOSEDĚL, Tomáš: Počítačová bezpečnost a ochrana dat. Vyd. 1. Brno : Computer Press, 2004. ix, 190 s. ISBN 80-251-0106-1.**

Vedoucí diplomové práce:	**doc. Ing. Jiří Gajdošík, CSc.** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**7. února 2014**
Termín odevzdání diplomové práce:	**27. května 2014**

Ve Zlíně dne 7. února 2014

prof. Ing. Vladimír Vašek, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně ……

podpis diplomanta

ABSTRAKT

Účelem této diplomové práce je zabezpečení informačního systému městského úřadu pomocí vhodně zvolených metod, postupů a zařízení. Práce se skládá ze dvou hlavních částí. První část pojednává o současných trendech v zabezpečení informačních systémů a jejich využití. Druhá část se zabývá popisem současného stavu informačního systému městského úřadu, po němž následuje analýza současného stavu a navržení vhodných kroků k navýšení bezpečnosti IS. Na základě požadavků jsou potom vybraná opatření implementována a ověřena.

Klíčová slova: firewall, IPS, VPN, aktualizace, zálohování

ABSTRACT

The purpose of this diploma work is the proposal for the security of a municipality´s information system by suitable chosen methods, procedures and device. The thesis is composed of two parts. The first part deals with contemporary trends in security of information systems and their utilizing. The second part deals with the description of contemporary state of a municipality´s information system. Then follow the analysis of contemporary state and a proposal of suitable steps for the increase of security of the information system. According to the requirements selected arrangements are inserted and proved.

Keywords: firewall, IPS, VPN, updates, backup

Tímto bych chtěl poděkovat vedoucímu diplomové práce panu doc. Ing. Jiřímu Gajdošíkovi, CSc. za odborné vedení při tvorbě této diplomové práce.

Rád bych také poděkoval své rodině za trpělivost při tvorbě této práce.

Motto:

Systém je absolutně bezpečný pouze v případě, že je:

- vypnut
- odpojen
- zaplombován v titanovém kontejneru
- zalit v betonovém bunkru
- zaplaven nervovým plynem
- hlídán přeplacenými strážemi

Ovšem ani zde jeden nikdy neví…

Gene Spafford - Director Computer Operations, Audit, and Security Technology (COAST), Purdue University

OBSAH

ÚVOD

Zabezpečení informačních systémů v podnikovém prostředí bývá stále ještě mnohokrát jeho opomíjenou součástí. Společnosti mnohdy nevidí důvod pro vynakládání finančních částek na zvýšení bezpečnosti informačního systému, dokud nenastane situace, která může ohrozit chod samostatné organizace. Přitom mnohá opatření mohou být nastavena i bez významných nákladů. Hlavním cílem mé práce je seznámit čtenáře s celkovým náhledem na bezpečnost informačního systému, identifikaci hrozeb a jejich možného řešení.

Teoretická část je zaměřena na obeznámení čtenáře se současným stavem bezpečnostní problematiky. Ukáže mu, jak komplexně nahlížet na bezpečnost informačního systému. Pomůže mu zjistit, jakými postupy lze rozpoznat aktuální stav bezpečnosti, navrhnout příslušná opatření a jakými dokumenty či postupy ji nadále v budoucnu udržovat v potřebném stavu. Nakonec je seznámen se základními hrozbami pro informační systém a s problematikou řešení fyzické, datové a personální bezpečnosti.

Praktická část této práce je provedena na informačním systému vybraného městského úřadu. Na počátku je popsán vývoj systému během posledních letech až do současnosti. Následně je provedena bezpečnostní analýza současného stavu. Na základě této analýzy jsou navržena vhodná bezpečnostní opatření k posílení zabezpečení, která jsou potom realizována. Závěrem jsou realizovaná opatření zhodnocena a je nastíněn další možný budoucí rozvoj problematiky posílení bezpečnosti informačního systému.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ SYSTÉM

Informační systém (IS) je soubor technického (hardware) a programového (software) vybavení, záznamových medií, dat a personálu, který organizace používá ke správě svých informací [1]. V informačních technologiích zastupují:

- technické vybavení – hardwarové komponenty, síť, kabely, zdroje atd.,
- programové vybavení – operační systémy, aplikační programové vybavení,
- záznamová média – tiskárny, pásky, DVD atd.,
- data – soubory a databáze, vstupní a výstupní data apod.,
- personál – uživatelé, správci systému, obsluha.

1.1 Informační systém veřejné správy

Informační systémy veřejné správy jsou souborem informačních systémů, které slouží pro výkon veřejné správy. Veřejnou správu je možno charakterizovat jako správu veřejných záležitostí, která sleduje naplňování veřejných cílů a je prováděna ve veřejném zájmu. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.

ISVS mohou být v případě obcí kupříkladu

- evidence uložených pokut (správních sankcí) podle § 58 a 59 zákona č. 128/2000 Sb., o obcích,
- evidence plátců místních poplatků podle zákona č. 565/1990 Sb., o místních poplatcích,
- evidence obyvatel.

Správcem ISVS je orgán veřejné správy, pakliže neurčí jinak zvláštní zákon. Správce ISVS ovšem nemusí být jeho provozovatelem. Zákon upravuje povinnosti správců ISVS. Zavádí pro orgány veřejné moci povinnost vytváření a vydávání informační koncepce a provozní dokumentace, jím spravovaných ISVS. Dokumenty potom uplatňují v praxi a pravidelně vyhodnocují jejich dodržování. Provozní informační systémy nemusí být obsahem informační koncepce. Provozním informačním systémem je informační systém zajišťující in-

formační činnosti nutné pro vnitřní provoz příslušného orgánu, například účetnictví, správu majetku, a nesouvisející bezprostředně s výkonem veřejné správy [6]. Doporučuje se ovšem, aby orgán veřejné správy uvedl do informační koncepce všechny informační systémy, kterých je správcem, tedy ISVS i provozní. Obsah a struktura informační koncepce jsou určeny prováděcími právními předpisy [7]. Povinnosti provozovatele již tak přesně zákon nedefinuje, hlavně mu klade za povinnost zajišťovat ochranu a bezpečnost informací v rámci provozovaného ISVS.

Zároveň zákon klade za úkol zajištění atestace dlouhodobého řízení ISVS (dlouhodobé cíle v oblasti řízení kvality a dlouhodobé cíle v oblasti řízení bezpečnosti) a prokázání plnění povinností ohledně vytváření a vydávání informační koncepce a provozní dokumentace, a jejich uplatňování v praxi a vyhodnocování jejich dodržování.

Povinnost zajištění atestace informační koncepce informačních systémů veřejné správy se nevztahuje na obce, které vykonávají přenesenou působnost pouze v základním rozsahu. I tyto obce se však nezbavují jako správci ISVS povinnosti vytvářet a kontrolovat informační koncepci a provozní dokumentaci.

Mimoto musí dle zákona o ISVS orgán veřejné správy:

- zpřístupňovat ministerstvu v elektronické podobě, ve formě a s technickými náležitostmi stanovenými prováděcím právním předpisem, bez zbytečného odkladu informace o jimi spravovaném informačním systému a jím poskytovaných službách a používaných datových prvcích, a to za účelem uveřejnění v informačním systému
- postupovat při uveřejňování informací způsobem umožňujícím dálkový přístup tak, aby byly informace související s výkonem veřejné správy uveřejňovány ve formě, která umožňuje, aby se s těmito informacemi v nezbytném rozsahu mohly seznámit i osoby se zdravotním postižením. Formu uveřejnění informací stanoví prováděcí právní předpis
- uplatňovat opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy [6].

2 BEZPEČNOST

Pojem bezpečnost má široké pole působnosti. Obecně se dá říci, že za bezpečného považujeme toho, kdo není vystaven nebezpečí, popřípadě poskytuje ochranu před nebezpečím, nebo je nezpochybnitelný, důvěryhodný, spolehlivý.

2.1 Informační bezpečnost

Informační bezpečnost chápeme jako ochranu informací ve všech jejich formách a po celý jejich životní cyklus - tedy během jejich vzniku, zpracování, ukládání, přenosu a likvidace prostřednictvím technických, fyzických a organizačních opatření, jejichž cílem je zabránit ztrátě důvěrnosti, integrity a dostupnosti.

Základním cílem je ochrana a eliminace hrozeb včetně jejich dopadů.

Hrozbami jsou například:

- kompromitace,
- nedovolená modifikace (změna hodnot),
- destrukce části, nebo celého informačního systému,
- zneužití citlivých informací,
- použití klamných dat, ze kterých budou odvozeny chybné výsledky a závěry,
- špatná interpretace hodnot,
- neoprávněný přístup k hmotným (hardware) i nehmotným (data, informace) hodnotám,
- únik informací (kopie, krádež, odvození požadovaných údajů ze získaných zdrojů dedukcí) [1].

2.2 Identifikace možných hrozeb a následků

Chceme-li zlepšit nebo zjistit bezpečnostní stav IS, je potřeba, abychom rozpoznali, na které oblasti se orientovat či jak daný bezpečnostní problém odstranit. Toto zjistíme, jestliže systém podrobíme analýze.

Můžeme volit např.:

- jednodušší bezpečnostní analýzu, která nám pomůže nalézt nedostatky současného systému a nalezne nejvhodnější opatření pro jejich řešení,
- či komplikovanější analýzu rizik, která by měla poskytnout odpověď na otázky, jaká aktiva organizace má, jak jsou pro ni důležitá, jakých působením hrozeb je organizace vystavena, jak hodně jsou její aktiva vzhledem k těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije určitou zranitelnost a jaký dopad (odhad ztrát) by to na společnost mohlo mít.

Výstupem analýzy je zpráva, která zahrnuje souhrn identifikovaných nedostatků a návrh doporučení na jejich odstranění, který je dále využitelný při plánování následujících kroků budování informační bezpečnosti organizace.

2.3 Bezpečnostní postupy a opatření

Na základě analýzy rizik určíme, která rizika budeme nuceni přijmout a jejich dopady řešit pomocí havarijních plánů a plánů obnovy.

Havarijní plán IS by měl pokrývat oblasti napadení viry, hackery, selhání prostředí (výpadek elektřiny, klimatizace, selhání hardwaru), působení přírodních katastrof apod. V havarijním plánu musí být určeny role a odpovědnosti zaměstnanců (kdo, kdy plán aktivuje, jakou má v něm roli atd.), popis postupů, aby prvotní i druhotné následky havárie byly minimalizovány.

Plán obnovy je dokument, který obsahuje postupy pro zajištění nouzového provozu po havárii a činnosti vedoucí k plnohodnotné obnově provozu tak, aby dopad havárie byl na chod organizace minimální.

Je vhodné pravidelně ověřovat funkčnost těchto plánů, abychom například nezjistili, že zálohy sice máme, ale jsou nefunkční.

2.4 Bezpečnostní politika

Jestliže jsme provedli analýzu rizik, rozhodli jsme se s největší pravděpodobností vytvořit dokument pro celkové řešení informační bezpečnosti – bezpečnostní politika IS.

Bezpečnostní politika jako soubor norem, požadavků a pravidel, které vymezují přístup organizace k zajištění důvěrnosti, integrity a dostupnosti informací, je klíčovým dokumentem, ve kterém vedení organizace deklaruje své cíle v této oblasti. Schválením tohoto dokumentu management organizace zároveň deklaruje svoje odhodlání řešit problematiku bezpečnosti svého informačního systému [9].

Zpracování bezpečnostní politiky a provedení analýzy rizik je přímo vyžadováno legislativou České republiky pro informační systémy veřejné správy daného správce mající vazbu na jiný informační systém veřejné správy spravovaného odlišným správcem.

Pokud je zpracována a schválena bezpečnostní politika organizace (jsou vytčeny konkrétní a měřitelné cíle v oblasti bezpečnosti) a zpracována analýza rizik (vím, co je třeba chránit a proti čemu), je možno zpracovat bezpečnostní projekt, který představuje výběr konkrétních bezpečnostních opatření k eliminaci hrozeb, plán jejich implementace a zdroje (finanční, časové, lidské, materiálové,…) nutné k realizaci bezpečnostního projektu [9].

V každém případě by se mělo jednat o dokument písemný, ústní verze mají nemilý sklon k modifikaci, ať již úmyslné či neúmyslné. Bezpečnostní politika by měla najít odpovědi na několik základních otázek:

- co chceme chránit,
- proč to chceme chránit,
- jak to chceme chránit,
- jak se ověří, že je to opravdu chráněno,
- co se bude dělat, když se něco pokazí.

Bezpečnostní politika se řadí k základním dokumentům, které definují strategii informační bezpečnosti a základní pravidla v organizaci.

3 HROZBY PRO INFORMAČNÍ SYSTÉM

Tato kapitola se zabývá popisem nejčastěji se vyskytujících hrozeb pro informační systém.

3.1 Viry a jiné aplikace (červi, trojské koně atd.)

Virus je program, který se šíří tím, že vytváří kopie sama sebe, aniž by uživatel o tom věděl. K šíření většinou využívá soubory ostatních aplikací. Virus se přenáší při přenosu těchto souborů na jiné zařízení. Činnosti virů mohou být různé otravné efekty (zvukové, obracení obrazovky atd.) až po destrukční akce (mazání dat, formátování disku atd.).

Červi se na rozdíl od virů šíří sami bez potřeby přenosu hostitele. Jejich šíření pomocí sítí je pak velice rychlé a dopad potom daleko rozsáhlejší.

Trojské koně jsou programy, které mimo své primární funkce vykonávají i jinou bez vědomí uživatele. Mezi tyto jejich záškodnické funkce spadá odesílání různých souborů pryč z počítače, sledovat znaky zadané na klávesnici, vytvořit spamový server či otvírat síťovou komunikaci (porty) pro vzdálený přístup útočníka.

Spyware jsou programy, které mimo svou standardní funkci, vykonávají i posílání důvěrných informací o počítači či uživateli na vzdálené servery.

Spamy a hoaxy jsou poplašné, obtěžující či obchodně zaměřené zprávy. Často mívají za úkol získat od lidí citlivé informace či peníze. Podružných dopadem jejich hromadného šíření je i zatěžovaní internetových linek a emailových serverů.

3.2 Hackeři a crackeři

Výkladový slovník výpočetní techniky a komunikací praví, že hacker je „osoba zabývající se hakováním", což je „nestandardní použití systému či aplikace, při němž uživatel uplatňuje neobvyklé a nekomentované funkce systému a může využít některých jeho jinak nepřístupných schopností."

Slovo „hacker" je dnes chápáno značně rozsáhle. Ustálilo se na označení schopného programátora, jehož chytré řešení problému je dobrým „hackem". Proces řešení je obvykle označován jako „hacking". Hackeři jsou odborně velmi zdatní uživatelé internetu, kteří dokáží překonat mnohé nástrahy a využít nejrůznější mezery a skulinky k provedení něčeho, co „není zcela standardní". Důležitá je přitom jejich motivace a podstata jejich „nestan-

dardních" činů. Klasický hacker nemusí mít skutečně zlé úmysly, spíše mu jde o to, aby si ověřil svou odbornou zdatnost, aby ukázal, co umí. V novinářské praxi se obvykle pojmem „hacker" označuje ten, kdo se pokouší vlámat do počítačového nebo síťového systému násilím, ilegálně, a nějak ho poškodit nebo zneužít. Výstižnější je však používat v takových případech pojem „cracker", „crack" a „cracking".

Je zřejmé, že úspěšným crackerem může být i dobrý hacker. Ale vůbec není pravda, že každý hacker musí být nutně crackerem. V praxi ale toto jemné rozlišení není bráno příliš v úvahu a termínem „hacker" je nepříliš správně označován i „cracker", neboli i ten, kdo má skutečně zlé úmysly [14].

Motivací crackerova útoku může být více důvodů:

- Přerušení komunikace
- Odposlech dat
- Záměna dat
- Zfalšování dat

3.3 Uživatelé

Útočníky ve vnitropodnikové síti mohou být samotní zaměstnanci organizace nebo lidé zvenčí, kteří nějakým způsobem proniknou k prostředkům IT infrastruktury. V případě zaměstnanců se může jednat o neopatrného zaměstnance, který svojí nezodpovědnou činností vpustí do svého počítače škodlivý kód útočníka zvenčí, zlomyslného zaměstnance, který se snaží získat citlivé informace nebo si zvýšit úroveň oprávnění v některém klíčovém systému a v neposlední řadě obdoba „internetového vandala“ – zaměstnance, který se při ukončení pracovního poměru pokusí o smazání či odcizení dat nebo o zhroucení klíčového systému, případně zanechání zadních vrátek pro další činnost vně firmy.

Mimo klasické uživatele je nutno počítat do této oblasti i administrátory. Ti si můžou do systému buď úmyslně vytvořit nějaká zadní vrátka nebo svou neodbornou správou či nevhodným nastavením umožnit napadení systému.

3.4 Přírodní katastrofy

Přírodní katastrofy jsou zemětřesení, tsunami, sněhová kalamita, povodně, sopečná činnost, požáry a sesuv půdy atd. Tyto hrozby jsou mnohdy těžko předvídatelné, proto je prevence obtížná a je zapotřebí řešit spíše minimalizaci jejich dopadů. Již při návrhu IS je potřeba přihlížet například na vhodné umístění jednotlivých částí mimo oblast působnosti jednotlivých přírodních katastrof, na instalaci technických opatření jako požární signalizace, záplavová čidla atd. pro včasnou detekci hrozby.

4 FYZICKÁ BEZPEČNOST

Velmi často zanedbávanou oblastí v oblasti bezpečnosti bývá zajištění fyzické bezpečnosti. Přitom bezpečnost systému by měl být rozumný souhrn všech opatření, jelikož bezpečnost celku je zpravidla dána mírou bezpečnosti jeho nejslabší části.

Fyzická bezpečnost se zaobírá zabezpečením kritických prostor organizace, aby nedocházelo k nepovolanému přístupu do těchto oblastí, neoprávněnému užívání, poškození či újmě. Prvky fyzické bezpečnosti je potřeba aplikovat dle důležitosti jednotlivých zařízení na základě identifikace hrozeb.

4.1 Fyzický přístup

Pro fyzický přístup k prvkům důležité infrastruktury by mělo platit:

Přístup do serveroven a dalších místností se speciálním určením pro umístění komponent IS podléhá vysokému zabezpečení. Přístup je povolen pouze oprávněným osobám.

Další omezení jsou vztažena na zaměstnance údržby, úklidových služeb a nekvalifikovaného personálu. Omezení lze chápat jako zamezení samostatného vstupu do kritických prostor souvisejících s provozem IS.

Těmito kritickými prostory jsou chápány především:

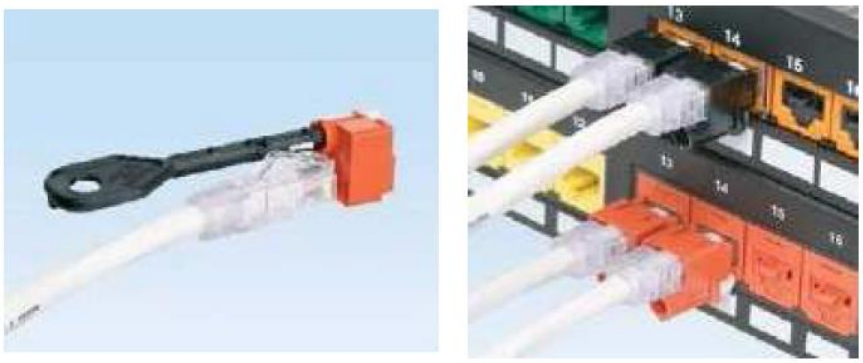
- Serverovny
- Datová úložiště
- Prostory s klíčovými prvky IT infrastruktury (tj. routery, switche apod.)
- Pracoviště správců IT systému

Cílem je zamezení rizik vzniku kritických událostí při neodborné manipulaci s IT komponentami IS nebo cílené činnosti s úmyslem poškození.

Vstup do těchto prostor je možný pouze s kvalifikovanou osobou.[3]

Do fyzické bezpečnosti můžeme zařadit i fyzickou bezpečnost počítačové sítě, kdy například pro nevyužité síťové zásuvky ve veřejných místnostech lze využít prvky pro blokování portů (Obr. 1) a pro osazené zásuvky prvky pro uzamčení síťové kabeláže (Obr. 2).

Obr. 1: Prvky pro blokování zásuvek RJ45 [8]



Obr. 2: Zámky pro blokování RJ45 kabelů [8]

Pro zvýšení odolnosti celého systému je vhodné separování zálohovacího zařízení od zálohovaných zařízení do jiné zabezpečené lokality. Nejlepší je umístit ho do jiné budovy, jestliže to nejde, tak přinejmenším do jiné místnosti.

Zcela opomíjenou oblastí fyzické bezpečnosti bývají činnosti spojené s likvidací zařízení s citlivými informacemi, kdy před opuštěním organizace by měly být z likvidovaného zařízení tyto informace zaručeně odstraněny.

4.2 Živelné pohromy

Další z opatření, na které potřeba pamatovat, je již při navrhování IS brát zřetel na ochranu před živelnými pohromami jako jsou záplavy, požár, bouřka, ale dá se sem i zařadit horko či extrémní mráz. Místnosti s citlivou infrastrukturou by od počátku měly být mimo záplavové zóny. V těchto citlivých oblastech s důležitou infrastrukturou je též vhodné zajistit ochranu zařízení před selháním napájení (záložní zdroje, motorgenerátor) či zajištění stabilní teploty (klimatizace). Pro případ požáru je příhodné mít tyto místnosti separované do

více lokalit, zvláště žádoucí je to pro umístnění zálohovacích zařízení. Je také potřeba dbát na ochranu před přepětím vzniklým například při bouřce, kdy může přijít jak po vysokonapěťové kabeláži tak po nízkonapěťové. V exponovaných místech je vhodné řešit ochranu samotných budov jímači blesků.

Jsou i další přírodní katastrofy jako lavina, zemětřesení, sopečná erupce atd., které se ale u nás víceméně nevyskytují. Pakliže je IS systém umístěn v lokalitě, kde je pravděpodobnost jejich výskytu, je potřeba pamatovat i na ně.

5 DATOVÁ BEZPEČNOST

Základem datové bezpečnosti je zajistit důvěryhodnost, integritu a dostupnost dat IS. Máme tím na mysli zpřístupnění dat výhradně oprávněným osobám, zabezpečení poskytovaných dat před modifikací během přenosu než dorazí na místo určení a zajištění jejich co nejvyšší dostupnosti (data, která v potřebný okamžik nejsou dostupná, jakoby nebyla). Pro zajištění těchto požadavků můžeme využít některé z níže popsaných technologií.

5.1 Fyzické a logické členění sítě

Pro větší bezpečnost jednotlivých segmentů sítí (hlasová, administrativní, uživatelská síť apod.) je rozumnější je buď fyzicky oddělit samostatnými síťovými prvky či na logické úrovni pomocí síťových prvků podporujících standard IEEE 802.1Q. Standard IEEE 802.1Q dává do hlavičky ethernetového rámce 32bitovou položku, která definuje virtuální síť (VLAN) a umožňuje tak rozčlenit fyzickou síť na více logických podsítí.

Toto rozdělení na více segmentů sítí mimo jiné přináší odlehčení zátěže na síti (omezení všesměrového vysílání atd.) a zároveň zvýšení bezpečnosti, když například na administrativní rozhraní jednotlivých síťových zařízení mají přístup jen uživatelé z počítačů zařazených do dané podsítě.

5.2 Firewall

Firewall je speciální síťové zařízení, které je umístěné mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení (např. typicky mezi internetovým připojením a vnitřní zabezpečenou sítí), a slouží k řízení a zabezpečování síťového provozu. Neustále tedy sleduje veškerou komunikaci procházející skrze něj, přičemž podle nastavených pravidel zakazuje, odmítá či povoluje daný provoz.

První z používaných filtrů na firewallech byly paketové filtry. Jejich princip spočívá v pravidlech z jaké adresy a portu může být paket doručen na jakou adresu a port. Výhodou je jejich rychlost, nevýhodou nízká úroveň kontroly procházejících spojení, jako absence kontroly stavu připojení či zda daným portem protéká komunikace na daném protokolu.

Stavové filtry mají oproti paketovým filtrům rozšířenou funkčnost o ukládání informace o povolených spojeních, na základě nichž pak mohou rozhodnout, zda další komunikace náleží do již povoleného existujícího spojení.

Dalšími rozšířeními funkčnosti firewallu může být implementace funkcí proxy, IDS, IPS atd.

5.3 DMZ (Demilitarized Zone)

Demilitarizovaná zóna se nejčastěji používá k vyčlenění serverů, které mají být dostupné z Internetu a jsou tím více exponované vůči útokům, do separované sítě a izolují se tak od systémů určených výhradně pro potřeby interních uživatelů dané společnosti. Do DMZ se často umisťují mailové servery, DNS (Domain Name System) servery a webové servery. Zvlášť u webových serverů bývá komplikované zajištění všech programových kódů umístěných na serveru vůči všem zranitelnostem, takže je vhodné jejich izolace do DMZ.

5.4 NAT (Network Address Translation) / PAT (Port Address Translation)

Překlad síťových adres převádí adresy jedné sítě na adresy druhé sítě. Používají se hlavně překlady 1:1 nebo 1:N, označovaný jako PAT (Port Address Translation). Mechanismus PAT umožnuje schovat celou počítačovou síť za jednu veřejnou IP adresu. NAT pomáhal oddálit vyčerpání omezeného rozsahu veřejných IP adres IPv4. NAT nemá ambice nahradit firewall, pomáhá ovšem zesílit bezpečnost počítačové sítě za ním připojené, jelikož potencionální útočník nevidí strukturu dané sítě a nemůže se rovnou připojit na konkrétní počítač.

5.5 IDS (Intrusion Detection System)/ IPS (Intrusion Prevetion System)

Systém detekce síťového narušení (IDS) se snaží na základě odhalení anomálií neboli odchylek od standardního chování či na základě detekce signatur (vzorů) neboli řetězců neoprávněného jednání odhalit nepatřičnou komunikaci v počítačové síti. Hlavním cílem je tedy identifikace útoku a jiných bezpečnostních incidentů.

Systém prevence síťového narušení (IPS) oproti IDS přidává navíc funkcionalitu zabránění nebo přerušení útoku či škodlivého jednání. Často je označován jako nástavba IDS. IPS

používá k detekci nevhodného chování obdobné techniky jako IDS. V současnosti již mnohdy bývá součástí funkcí firewallu.

5.6 Proxy

Proxy je program, který pracuje na aplikační úrovni. Skládá se ze dvou částí. Na jedné straně pracuje jako server a na druhé straně jako klient. Serverová část proxy přijímá požadavky od klientů a předává je klientské části proxy, která jménem klientů předává požadavky cílovému serveru [2].

Proxy se používá hlavně pro tyto funkce:

Filtrace – proxy totiž vidí až do aplikačního protokolu a může na základě toho filtrovat obsah, zakazovat a povolovat přístup tj. sledovat, zdali někdo nepřistupuje na nepatřičné stránky, či nevynáší informace z informace z vnitřní sítě.

Cache – umožňuje zrychlení odpovědi na dotaz, kdy již jednou zpracovaný dotaz udržuje v paměti či na disku a v případě opakovaného požadavku na něj, odpoví proxy. Zároveň tím pomáhají snížit síťový provoz na odchozí lince do internetu.

5.7 VPN (Virtual Private Network)

Síť VPN (Virtual Private Network) je chráněná relace při komunikaci v síti, vytvořená nad nechráněnými kanály, jako je Internet. Pod zkratkou VPN označujeme často zařízení na obvodu sítě, která umožňují činnost takovéto chráněné (šifrované) relace [4].

Virtuální privátní sítě jsou čím dál více oblíbené, jelikož umožnují levně a bezpečně propojit vzdálené pobočky firem. Samozřejmě tomu také nahrává rozvoj dostupnosti vysokorychlostního internetu. Dříve si pro tento účel firmy pronajímaly soukromé linky (okruhy), což ale bylo podstatně finančně náročnější.

Další možností je bezpečně připojit mobilního zaměstnance prakticky odkudkoliv do vnitřní sítě firmy a tím mu zpřístupnit například interní IS firmy.

5.8 Autentizace a autorizace

Autentizace je v informatice ověření identity uživatele služeb nebo původce zprávy. Používají se tyto základní metody pro zjištění identity:

- podle toho, co uživatel zná (zná správnou kombinaci uživatelského označení a hesla nebo PIN),
- podle toho, co uživatel má (nějaký technický prostředek, který uživatel vlastní – hardwarový klíč, smart card, privátní klíč apod.),
- podle toho, čím uživatel je (uživatel má biometrické vlastnosti, které lze prověřit – otisk prstu, snímek oční duhovky či sítnice apod.),
- podle toho, co uživatel umí (umí správně odpovědět na náhodně vygenerovaný kontrolní dotaz) [12].

Autorizace většinou navazuje na autentizaci a rozumí se jí ověření přístupových oprávnění uživatele vstupujícího do IS a řízení, zdali může provádět dané operace.

5.9 Antiviry a antispamy

Antivirovým programem označujeme počítačový software, který slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiného škodlivého softwaru (malware). K zajištění těchto funkcionalit může využívat více technik jako:

- kontrolu integrity, zdali modifikace souborů či adresářů neindikuje napadení virem,
- prohlížení otvíraných či na disku umístěných souborů na odpovídající sekvenci kódu příslušící viru v databázi,
- vyhledávaní viru pomocí analýzy podezřelého chování a projevů, které mohou značit infekci.

Antispamový program slouží ke snaze odhalit nevyžádanou poštu. Rozdíl mezi vyžádanou a nevyžádanou poštou může být někdy zcela nicotný. Proto je potřeba být v této oblasti velice obezřetný. K detekci se většinou využívá:

- antispamových databází,
- hledání různých příznaků potenciálně značících spam, na základě nichž sestaví bodové ohodnocení emailu a podle nastavených bodových mezí případně mail označí jako spam,
- učením od uživatelů.

Jak antivirový program tak antispamový je potřeba pravidelně aktualizovat o nové databáze, aby dosahovaly co nejvyšší účinnosti odhalení. Nikdy nám ovšem nezaručí stoprocentní ochranu.

5.10 Zálohování a archivace

Při zálohování vzniká kopie zdrojových dat (záloha), která bývá zpravidla uložena na jiné datové úložiště, než se nacházejí zdrojová data. Důraz je kladen na rychlou dostupnost těchto záloh pro případ obnovy dat. Nejčastěji jsou v současnosti na jejich uložení využívána disková pole. Zálohy jsou využívány v případě, kdy dojde ke ztrátě či poškození dat, abychom byli schopni plně obnovit funkční stav, který existoval krátce před vznikem poruchy.

Archivace je proces přesouvání již neaktuálních dat na média, kde bude zajištěna jejich dlouhodobá spolehlivost a vysoká trvanlivost, pro jejich případné pozdější využití. Není potřeba zajišťovat tak rychlou dostupnost dat, jako v případě záloh. Ideálním médiem splňující tyto požadavky jsou například datové pásky.

5.11 Šifrování a elektronický podpis

Pro zajištění důvěryhodnosti dat při jejich uložení a přenosu je důležité používat šifrování. Šifrováním se snažíme utajit obsah zprávy před nepovolanými třetími osobami. Využívá se například při komunikaci s portály bank (https), poštovními servery (imaps, pop3s, smtps) nebo při ukládání dat na úložiště (TrueCrypt, BitLocker atd.). Šifry se v základu dělí na symetrické a asymetrické. Symetrické využívají k šifrování a dešifrování stejný klíč, jsou rychlejší, ale je potřeba zajistit utajený přenos klíče protistraně. Naproti tomu asymetrická šifra je postavena na využívání dvou klíčů tzv. veřejného a soukromého. Veřejným klíčem, který může být volně uveřejněn, se šifruje a soukromým se zašifrovaná zpráva dešifruje. Odpadá tedy nutnost zabezpečené výměny klíčů.

Integritu dat nám může zajistit například elektronický podpis při podepisování mailů či elektronických dokumentů. Jednak jím prokazujeme, že jsme dokument vytvořili právě my, nebo lze detekovat, zdali zprávu někdo během přenosu nemodifikoval.

5.12 Aktualizace

Důležité je také udržovat aplikace a systémy aktualizované, aby neměly dostupné všeobecně známé zranitelnosti, chyby a měly dostupné nejnovější bezpečnostní prvky, aby útočník neměl ulehčenou roli při pokusu o napadení systému. Ve větších organizacích je vhodné mít centrální správu aktualizací, aby administrátoři měli přehled, jaké záplaty má konkrétní stanice či server, a případně dle toho přijali bezpečnostní opatření. Při instalaci aktualizací je potřeba postupovat obezřetně, zvlášť pokud organizace má nějaké specifické aplikace, u nichž by po instalaci aktualizace mohla nastat nějaká nekompatibilita či nefunkčnost. Proto je užitečné instalovat aktualizace na vzorové stanici či nekritickém serveru a až potom nasazovat na zbývající zařízení.

5.13 DLP (Data Loss Prevention)

Systém prevence ztráty dat se používá k detekci neoprávněného užití či předávání důvěrných informací. Systém identifikuje, monitoruje a blokuje vybrané datové toky, aby minimalizoval riziko úniku dat, jak vědomého tak neúmyslného. Samozřejmě jako každý systém nezajistí stoprocentní bezpečnost těchto dat, jelikož nezabrání například opsání těchto dat či jejich ofocení. Tímto selháním lidského faktoru, by se měla zabývat personální bezpečnost.

6 PERSONÁLNÍ BEZPEČNOST

Personální bezpečnost je jednou z neméně důležitých položek celkové bezpečnosti IS. Personální bezpečnost začíná již při vhodném výběru zaměstnanců a dodavatelů, čímž si můžeme rapidně snížit pravděpodobnost vnitřního útoku. Interní uživatel má většinou znalosti o vnitřním uspořádání a bezpečnosti systému, které případný vnější útočník nemůže tak jednoduše získat. Má totiž pravidelný kontakt se systémem a ví, kde jsou jeho silné a slabé stránky.

Proto je potřeba zaměstnance při nástupu na pracoviště dokonale obeznámit s interními směrnicemi a nařízeními a potom pravidelně proškolovat, zvyšovat jejich kvalifikaci a bezpečnostní povědomí, proč jsou taková bezpečnostní opatření aplikována a je potřeba je dodržovat. Zcela běžně se totiž ve větších firmách stává, že když se člověk po telefonu představí jako správce, uživatel mu bez okolků sdělí například heslo či jiné údaje pro provedení útoku. Nebo si třeba hesla píšou do stolních kalendářů, kde je každý hned objeví. Velkým problémem bývá i nasazování nových bezpečnostních opatření do stávajícího systému, kdy jsou uživatelé nuceni dodržovat nová pravidla omezující jejich dosavadní zvyklosti v práci s IS. Proto je potřeba před každým novým opatřením uživatele s ním detailně seznámit. Je ovšem potřeba i prověřovat, zdali zaměstnanci aplikovaná bezpečnostní opatření dodržují.

Současně by zaměstnanci měli být motivováni k loajálnosti k zaměstnavateli mzdou, dobrými vztahy na pracovišti a podobně. Není nic horšího než mít na pracovišti zaměstnance, který je s ostatními ve sporu či je zneuznaný nebo propuštěný. Pak jsou mnohdy všechna bezpečností opatření k ničemu a je třeba rozumnější ponechat zaměstnance do konce výpovědní lhůty doma a nepovolit mu přístup na pracoviště. Bohužel někdy bývá velký problém vybrat vhodného kandidáta na obsazení pracovní pozice, jelikož na současném pracovním trhu se mnohdy těžce hledá patřičně kvalifikovaná osoba.

II. PRAKTICKÁ ČÁST

7 ANALÝZA SOUČASNÉHO STAVU

Praktická část diplomové práce bude provedena na jednom blíže nespecifikovaném městském úřadu.

7.1 Představení městského úřadu

Postavení a působnost Městského úřadu (MěÚ) upravuje zákon č. 128/2000Sb., o obcích, ve znění pozdějších předpisů (dále jen zákon o obcích), a zvláštní zákony. MěÚ plní úkoly v samostatné a přenesené působnosti. MěÚ je pověřeným obecním úřadem a rozsah státní správy vykonávané MěÚ je dán vyhláškou MV č.388/2002 Sb., o stanovení správních obvodů obcí s pověřeným obecním úřadem a správních obvodů obcí s rozšířenou působností, podle § 3 zákona č. 314/2002 Sb., o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností, správní obvody obcí s pověřeným obecním úřadem.

Správní obvod města s pověřeným městským úřadem je vymezen dle § 7 vyhlášky č. 388/2002 Sb., územím obcí. Městský úřad tvoří starosta, místostarosta, tajemnice městského úřadu a zaměstnanci města, zařazení do městského úřadu (dále jen zaměstnanci), kterých je v současnosti 25.

Správa informačního systému je zajišťována pro zaměstnance MěÚ, 9 městských strážníků (interní uživatelé) a některých jeho částí i pro příspěvkové organizace města (základní školy, kulturní středisko, mateřská škola, …), kterým je poskytováno i internetové připojení.

Informační systém městského úřadu poskytuje interním uživatelům všechny podpůrné prostředky pro výkon státní správy (matrika, ohlašovna, stavební úřad atd.), samosprávy a provozních věcí. Příspěvkovým organizacím a organizacím s majetkovou účastí města je poskytován poštovní server a server pro hostování webových stránek. Veřejnosti umožňuje získávat aktuální informace na stránkách města s úřední deskou.

Správa informačního systému musí být vykonávána dle zákona č. 365/2000 Sb., o informačních systémech veřejné správy, který stanovuje práva a povinnosti správců informačních systémů veřejné správy (ISVS) a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy.

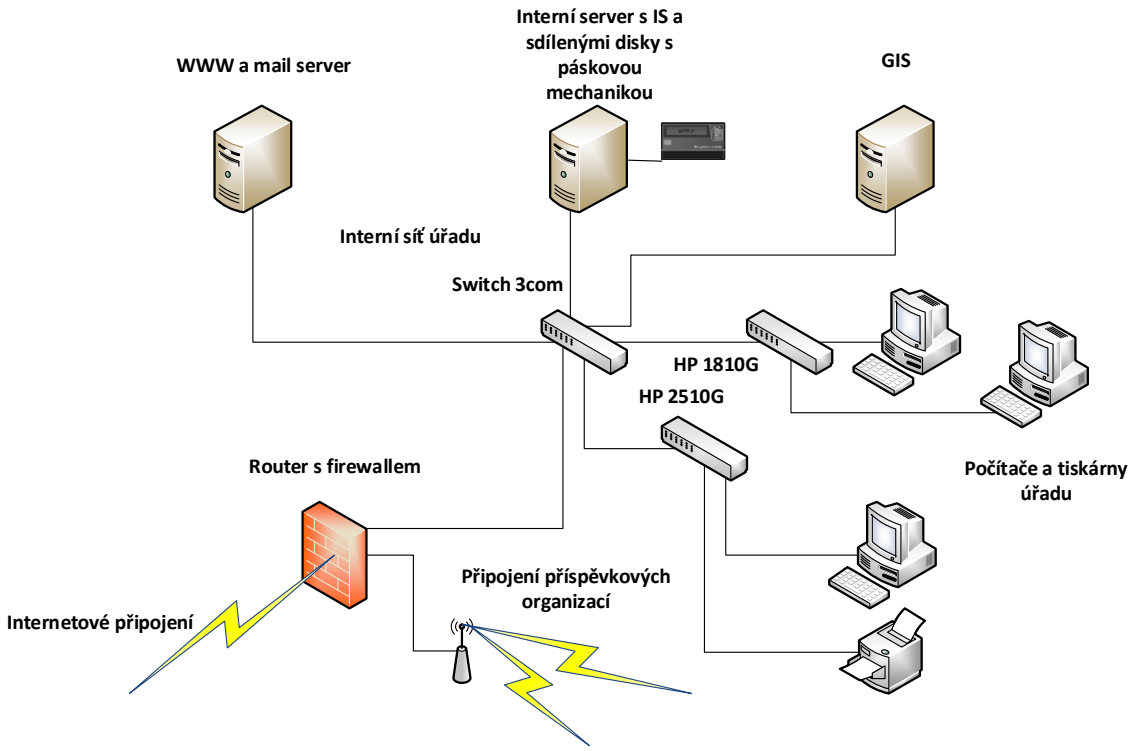
V praktické části práce se zaměřím na oblasti dle aktuálních požadavků úřadu, což jsou: zajištění vnitřní sítě před vnějším a vnitřním útokem, bezpečnost dat IS, bezpečnost klientských stanic.

Z důvodu zajištění bezpečnosti informačního systému, budou některé níže uvedené informace uvedeny jinak, než budou reálně implementované.

7.2 Vývoj stavu informačního systému

Informační systém na městském úřadu byl postupně budovaný již od devadesátých let minulého století. Do správy jsem tento systém převzal koncem roku 2010. Okamžitě jsem začal zjišťovat stav a funkčnost daného prostředí. Zjistil jsem, že stav není zcela vyhovující.

Síť byla postavena na třech serverech, čtvrtý server byl připraven pro plánované zprovoznění doménového řadiče, propojených přepínači (switchy) 3com 4500 50-Port (48x 10/100 + 2xSFP 1000), HP ProCurve 1810G-24 (24x 10/100/1000 + 2xSFP) a HP ProCurve (2510G-24 24x 10/100/1000 + 4xSFP). Její topologie je schematicky zobrazena na obrázku(Obr.2).



Obr. 3: Síťová topologie MěÚ v roce 2010

První server sloužil jako webový a poštovní server pro MěÚ a příspěvkové organizace města. Byl provozovaný na platformě FreeBSD na serveru IBM BladeCenter HS22 2x Xeon E5504, 14GB RAM a 2x 73 GB SAS HDD. Po konzultaci s dodavatelem, který server uváděl do provozu, jsem zjistil, že server není nijak zálohovaný, jediná ochrana jeho

dat spočívala v ochraně diskového prostoru RAID 1(Mirror) z výše uvedených dvou disků. Díky diskové kapacitě server sloužil spíše jen pro předávání mailů. Dalším překvapením bylo nepoužívání, mimo ssh, šifrovaných protokolů. Na server byl proto pro protokoly POP3, SMTP, IMAP a FTP nastaven přístup striktně na IP adresy příspěvkových organizací a vnitřních počítačů radnice. Webové rozhraní emailového serveru, bylo povolováno jen určitou dobu např. pobytu dané osoby na dovolené. Po praktické demonstraci jednoduchého odchycení hesla na protokolu http, bylo jeho využívání okamžitě zakázáno.

Druhý server, který byl pro úřad nejdůležitější, běžel na platformě Red Hat Linux na serveru IBM XSeries226 Intel Xeon 3,2 GHz, 8GB RAM a 4x74GB SCSI HDD. Na něm byly provozovány hlavní IS městského úřadu Radnice VERA (většina agend úřadu) s databází Informix, mzdový IS Orsoft RADNICE, intranetové webové stránky a sdílené síťové disky. Tento server byl chráněný raidem i úplnou zálohou uživatelských dat a dat informačních systémů každý pracovní den v noci, se zkopírováním této zálohy na pásku LTO 2 v něm umístěnou, která měla být každý den měněna.

Třetí server, na kterém běžel GIS (Geografický informační systém), bylo obyčejné PC Intel Core 2 Duo E6300 1,86GHz, 2x 512MB RAM 533MHz, 2x 200GB HDD opět chráněné jen ochranou proti selhání disku RAID 1.

Čtvrtý ještě do provozu neuvedený server byl identický server IBM BladeCenter HS22. Zbývající obslužné aplikace jako centrální správa antiviru, monitoring zaměstnanců byly umístěné na PC správce počítačové sítě.

Tento zjištěný stav byl vyhodnocen jako ne zcela vyhovující jelikož:

- První server kromě výpadku disku nebyl nijak zajištěn. V případě jakéhokoliv jiného selhání či napadení úřad o data neodmyslitelně přijde. U poštovního serveru to nebylo ještě tak ožehavé, jelikož uživatelé si všechnu poštu stahují k sobě a na serveru se drží jen několik dní zpátky dle nastavení konkrétního emailového klienta. V případě výpadku by byl server nedostupný a příchozí poštu by přijímal po dobu výpadku záložní server u poskytovatele internetového připojení. Horší je to ale u webových stránek. Tyto stránky by měly být trvale dostupné kvůli umístění úřední desky úřadu a dlouhodobý výpadek by byl proto nežádoucí. Jejich rekonstrukce by byla též velice problematická. Server nebyl pravidelně aktualizovaný a nepoužíval šifrované protokoly, proto byl jednodušeji napadnutelný. Tuto hypotézu potvrdil in-

ternetový útok na zranitelnost jedné z webových aplikací. Naštěstí v tu dobu byl již připravovaný přechod na nový server, takže data jen několik dní stará byla nakopírována v testovacím prostředí a stránky byly v řádu hodin obnoveny.

- Data na druhém serveru jsou díky kopírování na pásku dostatečně chráněná. Jediný větší problém je lidský faktor vstupující do zálohování v potřebě výměně pásky. Pakliže nemohla být páska v řádném intervalu vyměněna například z důvodu absence informatika či opomenutí, vznikal v systému uložení záloh na pásky nepořádek. Dalším problémem v případě rozsáhlejší havárie je nutnost asistence dodavatele informační systému při instalaci či obnově dat, čím by vzniknul velký časový prostoj. Také by bylo vhodné zálohovat po všechny dny v týdnu, ne jen pracovní, kvůli novému 24 hodinovému provozu městské policie.
- Třetí server nebyl výkonnostně zcela vhodný pro provozování GISu a byl zcela nechráněný proti selhání lidského faktoru např. odmazání či nechtěnou editaci dat. Zásadní rozdíl by ale byl oproti ostatním serverům v ceně obnovy. Geografická data jsou velice drahá, některá byla dodána na zakázku jen pro úřad a vše by tedy bylo závislé jak na vstřícnosti jednotlivých dodavatelů, kteří data v minulosti dodali, pakliže je ještě u sebe budou mít, tak na výrobci geografického informačního systému.

Problém všech serverů je také v závislosti obnovy dat na dodavatelích (nutnost zprovoznění jejich technikem) v případě totálního selhání hardwaru i na dodávce nového. Nezálohování dvou severů bylo zřejmě způsobeno nedostatkem prostředků pro zálohování takového množství dat.

Otázkou bylo i technické zajištění serverové místnosti. Servery, datový rozvaděč, záložní zdroj a další technické zázemí jsou sice umístěny v jedné místnosti, od které by měly mít klíč pouze pověřené osoby. Časem ale vyplynulo napovrch, že existuje ještě generální klíč. Samotná serverovna není střežena samotným poplachovým zabezpečovacím zařízením (PZS). PZS je střežen celý objekt radnice, po jeho opuštění zaměstnanci a také spisovna samostatně kódovatelnou smyčkou. Neplánovaně se ukázal problém s klimatizací, která neuměla obnovit svůj provoz po výpadku elektrického proudu a chladit za mrazivého počasí.

Aby úřad nemusel mít takové obavy o svá data, vystavovat se případně problémům s neplněním zákonných povinností, měl svá data trvale dostupná a nebyl tak závislý na benevolentnosti dodavatelů, bylo rozhodnuto, že se bude potřeba zaměřit na síťovou bezpečnost, zajištění co nejrychlejší obnovy provozu v případě jakéhokoliv ohrožení infrastruktury IS s ohledem i na ekonomičnost daných opatření.

V první řadě byla provedena úprava serverového prostředí. Jako centrální úložiště pro všechny servery bylo pořízeno diskové pole EMC VNXe 3100 12x 600GB SAS HDD, které je vysoce odolné vůči selhání díky redundantnosti jeho řadiče i zdroje. Diskové pole je uvnitř rozděleno na dvě části, jedna je chráněna RAID 10 a druhá RAID 5. Pro obě části je jeden společný hot-spare disk. Pole je k serverům připojeno přes iSCSI redundantní síťovou trasou. S ohledem na zajištění vícecestného připojení mezi diskovým polem a servery v síti SAN, pro zamezení vzniku nekonzistentnosti dat při výpadku trasy, byl přikoupen přepínač Cisco SG300-52 (52x10/100/1000 + 4xSFP) a pro zajištění větší propustnosti v interní síti úřadu byl vyměněn přepínač 3com za Cisco SG500-52 (52x 10/100/1000 + 4xSFP). Jediným slabým místem diskového pole je problém jeho celkového selhání. Ochranu by zajistilo druhé pole, na které by se toto pole replikovalo, ale jeho pořízení bylo vyhodnoceno jako nerentabilní.

V dalším kroku byl přikoupen jeden použitý server HP ProLiant DL380 G6 2x Xeon E5530 2,4GHz, 24GB RAM, 2x146 GB SAS HDD RAID 1, na který byla nainstalována virtualizační platforma VMware. Tato platforma byla zvolena s ohledem nutnosti podpory linuxových operačních systémů. Díky postupnému přesunu fyzických serverů do virtuálního prostředí mohla být tato platforma nainstalována i na dva současné servery IBM BladeCenter HS22, kterým byla navíc přikoupena operační paměť. Tato změna zaručuje v případě hardwarového selhání některého serveru rychlé obnovení služeb na jiném serveru. V případě zálohování kompletních virtuálních serverů nebude úřad již tak závislý na službách dodavatelů v případě havárie.

Každý migrovaný IS byl pokud možno nově nainstalovaný na samostatný operační systém, aby v případě havárie vyvolané některým z nich nebyla ovlivněna funkčnost ostatních IS. Nainstalovány byly dva doménové řadiče na Windows Server 2008 R2 a vůči nim spuštěno ověřování nového mailového serveru Kerio Connect na operačním systému CentOS. Uživatelé mají ve výchozím nastavení dostupnou schránku o 1GB, kterou není problém v případě potřeby navýšit. Server již vynucuje využití šifrovaných protokolů a umožnuje syn-

chronizaci mobilních zařízení pomocí ActiveSync. Lze tedy využívat jeho služby odkudkoliv z internetu. Také webový server byl přesunut na další samostatný virtuální server opět běžícím na CentOS. GIS byl též převeden do virtuálního prostředí na serverový operační systém Windows Server. K němu byl na server pořízen právní systém Codexis. Na další Windows Server byly přesunuty aplikace pro monitoring zaměstnanců a centrální správu a aktualizaci antiviru.

Nyní se rozhodovalo, kam a jak toto celé prostředí zálohovat. Fyzická kapacita diskového pole díky zvoleným raidovým polím a jeho rozdělení může při maximálním zaplnění přesáhnout 3TB. Kam takovou kapacitu bezpečně zálohovat a držet například 14 dní záloh zpětně?

Po diskuzi nad problémem bylo stanoveno, že zálohovat se budou, pokud to lze, kompletní virtuální stroje pro rychlejší obnovu a větší nezávislost na dodavatelích. Zařízení by v případě nouze mělo být schopné krátkodobě zastoupit hlavní diskové pole při dostačujících výkonových parametrech, eventuálně by, v krajní nouzi, mohlo hostovat některé virtuální stroje. Zálohování by mělo probíhat automaticky, bez nutnosti spoléhání na lidský faktor.

Při sondování trhu bylo zjištěno, že zařízení umožňující zálohovat takovou kapacitu nejsou zrovna nejlevnější a mnohdy jsou jednoúčelová. Proto bylo rozhodnuto vystavět si zařízení svépomocí. Byly zakoupeny enterprise komponenty: serverová deska Intel S1400FP s 4 síťovými kartami, s podporou TPM (Trusted Platform Module) a vzdálené správy, 6 jádrový procesor Intel Xeon E5-2420, 24 GB ECC RAM, řadič Adaptec RAID 51645 s Battery Backup Unit (BBU), 13 kusů 2 TB disků WD RE4 RAID EDITON a věžová počítačová skříň s hotplug diskovými rámečky.

Nad disky bylo po sestavení serveru vybudováno z 12 disků RAID 6 pole a 13. disk slouží jako hot-spare disk. Reálná kapacita pole lehce přesahuje 18 TB. Řadič pravidelně kontroluje konzistenci diskového pole a v případě nějakého problému zasílá mail administrátorovi.

S ohledem na případné využití serveru při havárii byl zvolen jako podkladový operační systém Windows Server 2012 s Hyper-V. Od této verze již také Windows Server umí deduplikaci dat nad souborovým systémem. Celý diskový prostor je díky podpoře TPM šifrován BitLockerem, takže v případě krádeže disku jsou data pro zloděje nečitelná. Windows

Server umí poskytovat služby iSCSI target. Windows platforma byla zvolena i s ohledem na to, kdyby se serverem musel někdo nouzově manipulovat bez přítomnosti informatika.

Virtualizační platforma je bohužel ve verzi VMware Essentials, takže neobsahuje interní podporu zálohování VMware Data Recovery (v poslední verzi vSphere Data Protection). Rozšíření licence by ovšem bylo podstatně finančně náročnější než nákup některého ze zálohovacích programů. Jako vhodné řešení byl vybrán program Veeam Backup & Replication, jelikož není závislý na typu hypervisoru – podporuje jak VMware tak Hyper-V. Obsahuje i další užitečné funkce. Deduplikuje data už na úrovni jednotlivých záloh a rovnou je komprimuje. Umí vypublikovat zálohu virtuálního stroje rovnou do hypervisoru a uvést do chodu a až následně dle potřeby jeho úložiště přesunout ze zálohovacího diskového pole na hlavní diskové pole (v případě podpory virtualizační platformou i za provozu), což značně urychluje obnovu služeb. Zálohy probíhají ze snapshotů (otisků) virtuálních strojů, takže jsou rychlé a neomezují tak činnost serverů. Jen je potřeba ověřit, zdali shapshoty všechny aplikace podporují. Problém bývá u databází či aplikací, kde probíhá na pozadí synchronizace dat. Mimoto umí ze zálohy virtuálního strojů obnovit data na úrovni souborů. Od aktuální hlavní verze (číslo 7) zálohuje již i na pásku či do cloudu. Ve vyšší verzi může například automaticky ověřovat obnovitelnost každé zálohy.

Nyní přišlo na řadu nastavení samotného zálohování. Virtuální stroj s hlavním informačním systémem Radnice VERA je zálohován každý den před půlnocí úplnou zálohou. Po dobu vytváření otisku musí být na pár minut pozastavena databáze běžící na serveru, kvůli konzistentnosti dat. Všechny ostatní virtuální servery, mimo doménových řadičů, jsou zálohovány v pátek večer úplnou zálohou a po zbývající dny v týdnu inkrementální. Doménové řadiče nemohou být zálohovány snapshoty, kvůli replikaci dat probíhající na pozadí mezi nimi. Při případné obnově by totiž mohla vzniknout nekonzistentnost v datech řadičů. Zálohy snapshoty podporuje až Windows Server 2012 s nejnovějšími verzemi virtuálním platforem. Doménové řadiče jsou proto zabezpečeny vytvořením System State zálohy, která je následně skriptem zkopírována do sdílené složky na zálohovacím serveru. Zálohy dobíhajících služeb (IS Orsoft Radnice, souborový server Samba) na starém serveru, jsou mimo kopie na pásce duplikovány ještě do složky na zálohovacím serveru. Všechno nyní probíhá automaticky bez zásahu administrátora, který je jen maily informován, s jakým výsledek zálohy proběhly. Časově jsou zálohy rozloženy od 23 hod do 2 hod, aby byla lépe rozložena zátěž na počítačovou síť a disková pole.

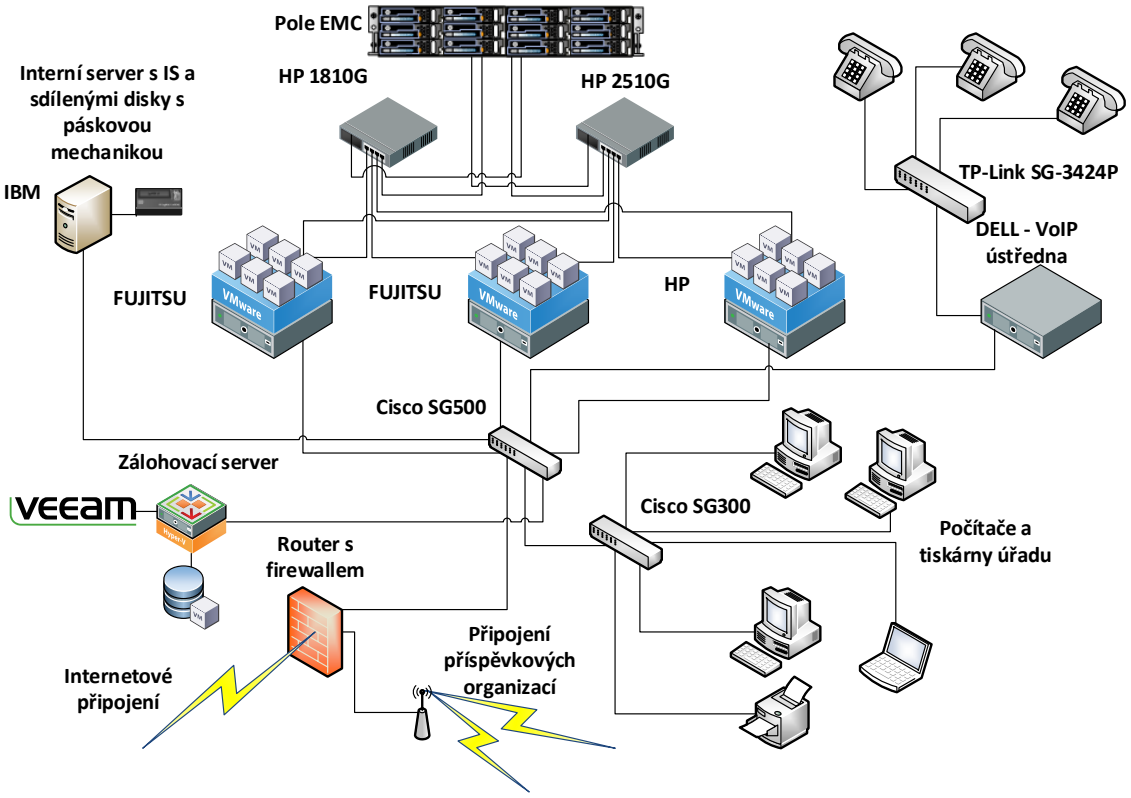
Z důvodů poruch na stávající telefonní ústředně Alcatel a jejich nemožnosti odstranění, byl uskutečněn přechod na VoIP (Voice over IP) ústřednu Asterisk dodanou firmou Daktela na serveru DELL, kdy pro VoIP telefony byl doplněn samostatný PoE (Power over Ethernet) switch TP-Link TL-SG3424P (24x 10/100/1000 PoE + 2xSPF). Infrastruktura vniřní VoIP sítě je tedy momentálně zcela hardwarově oddělená.

Pořízena byla taká druhá UPS (Uninterruptible power supply), aby každý zdroj v serveru či diskovém poli, byl zálohován z jiné UPS a tím zároveň napájen z jiné fáze. V serverovně přibyla druhá klimatizace s pamětí posledního stavu a chlazení i při nižších teplotách. Dveře do serverovny byly osazeny bezpečnostním kováním a novým zámkem, od kterého již mají klíč pouze pověřené osoby.

Aktuálně nejnovější významnou změnou byla v lednu roku 2014 výměna obou serverů IBM BladeCenter HS22, u nichž se v minulosti objevily poruchy, za dva nové servery Fujistu RX300 S8 Intel Xeon E6-2650v2 2,6 GHz, 64 GB RAM, 6x 300GB 15K SAS HDD, 8x 1Gbit ethernet a integrovaným hypervisorem VMware vSphere.

Posledními zachovanými servery jsou pozůstatky na serveru IBM XSeries 226 s IS Orsoft RADNICE, intranetem a sdílenými disky. Hlavní IS Radnice VERA je již přesunutý na samostatném virtuálním serveru. Topologie sítě na počátku roku 2014 je zobrazena na obrázku (Obr. 4).

Samotné funkční uspořádání vnitřní počítačové sítě se za celou dobu nijak významně nezměnilo. Síť je rozdělená do několika síťových subnetů, které jsou proroutovány směrovačem MikroTik RouterBoard RB433GL (routerem) umístněným ve věži radnice. Router ovšem obhospodařuje i bezdrátové spoje s příspěvkovými organizacemi, které tak prakticky vidí do vnitřní počítačové sítě, a příchozí bezdrátový internetový spoj s kapacitou 20/20 Mbit/s. V síti nejsou použité žádné virtuální sítě, mimo trasy mezi diskovým polem a servery. Všechna síťová zařízení, mimo routeru, jsou umístěné za NATem. Prostupy z internetu do vnitřní sítě skrze firewall na routeru, jsou striktně, mimo šifrované protokoly poštovního a webového serveru, povolovány na IP adresu tvůrce připojení. Městský úřad má momentálně k dispozici blok 14 veřejných IP adres, za kterými je skrytých 30 stolních počítačů, 12 notebooků, 14 síťových tiskáren, všechny servery MěÚ a další desítky síťových zařízení příspěvkových organizací. Počítače úřadu běží na operačních systémech Windows Vista a 7. Mají nastavenou pravidelnou aktualizaci ze serverů Microsoft Update a využívají centrálně spravovaný antivirus AVG AntiVirus Business Edition.



Obr. 4: Síťová topologie MěÚ v lednu roku 2014

Ověřování uživatelů do jednotlivých IS je prováděno separátně v každém IS. Doménové řadiče jsou momentálně propojené jen s mailovým serverem a serverem s právním IS Codexis.

7.3 Bezpečnostní analýza

7.3.1 Fyzická bezpečnost

Fyzická bezpečnost IS městského úřadu je až určité výjimky nastavená správně. Serverovna je mimo zátopovou oblast, přístup do ní je zajištěn pouze oprávněným osobám, teplota je udržována na optimální teplotě pomocí redundantních klimatizací a vnitřní elektrické rozvody jsou chráněné vůči selhání a přepětí. Těmi výjimkami jsou:

- umístění zálohovacího serveru ve stejné místnosti jako zbytek síťové infrastruktury, což by v případě např. požáru či krádeže znamenalo i ztrátu zálohovaných dat. Tento problém by se vyřešil dislokací serveru do jiné lokality.
- nezajištění síťové kabeláže z věže radnice MěÚ proti přepětí. Antény bezdrátových spojů jsou sice kryté proti přímému zásahu blesku, ale není tím řešen dopad nepří-

mého úderu blesku neboli atmosférického přepětí. Všechny ostatní vyčleněné rozvody (napájecí síť atd.) jsou chráněné proti přepětí. Problém by odstranilo nasazení přepěťové ochrany na strukturovanou kabeláž přívodu z věže.

7.3.2 Datová bezpečnost

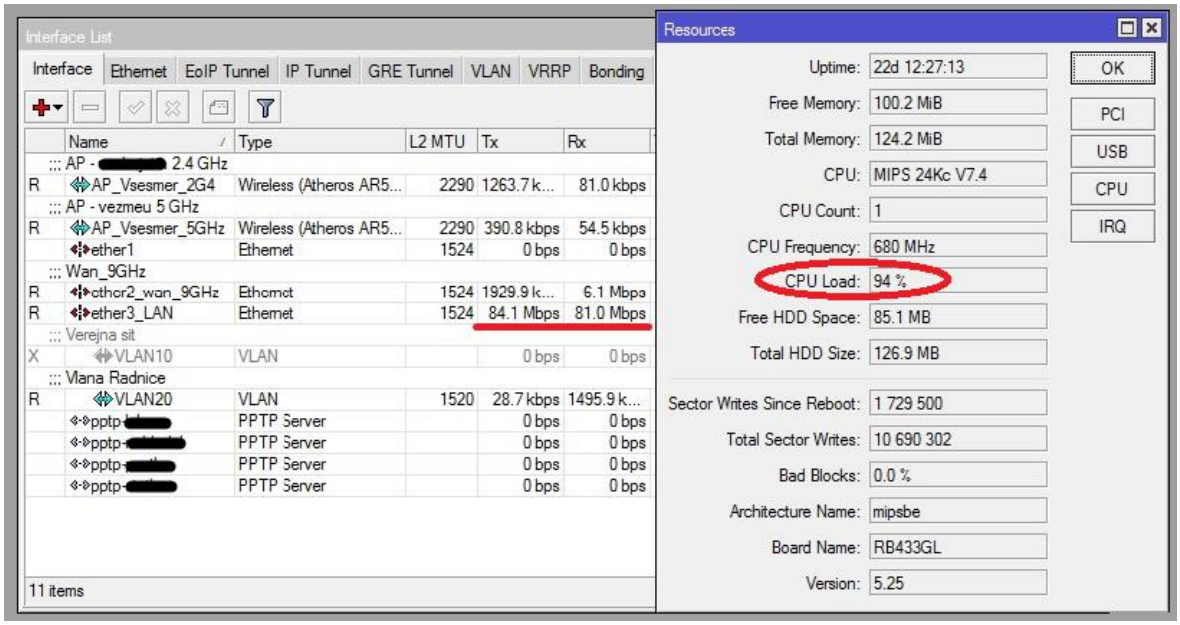
Velkými neduhy ovšem trpí datová bezpečnost. Městský úřad má v současnosti sice všechny servery zálohovány 14 dní zpětně na šifrovaném úložišti, servery dimenzované, že v případě výpadku některého z nich ho ostatní zastoupí, centrálně spravovaný antivirový program a síť chráněnou firewallem, ale i v tomto řešení se najde ještě několik podstatných nedostatků.

Jedním z hlavních z bezpečnostních problémů městského informačního systému je sdílení routeru s příspěvkovými organizacemi města, což umožnuje prakticky přístup z jejich počítačů do vnitřní sítě úřadu. Poněvadž síťová zařízení si ve svých sítích příspěvkové organizace spravují svépomocí či pomocí externích dodavatelů nelze asi zjistit, jaké riziko od nich hrozí. Útok či infiltrace vnitřní sítě MěÚ nemusí ovšem přijít přímo od nich. Jelikož organizace jsou připojené bezdrátovými spoji (5GHz a 2,4GHz) a potom tedy stačí, aby někdo zkušený napadnul tyto spoje. Nedostatkem je také výkon samotného routeru. Router byl dimenzovaný pouze na řízení internetového provozu v řádu desítek Mbit a ne na správu interní gigabitové sítě. Při větším provozu tento router zcela nestíhá (Obr. 5) a třeba telefonní spojení přes VoIP se potom stává naprosto nepoužitelné. Ideálním řešením tohoto problému by bylo oddělení interní počítačové sítě městského úřadu od sdíleného routeru a vyčleněním tohoto routeru jen pro řízení vnějších sítí.

Dalším rizikem je umístění serverů vystavených do internetu (webový server a mailový server) v síti městského úřadu. Pokud by na některý z nich někdo podniknul takový útok, že by získal nad serverem nadvládu, měl by opět zbytek sítě přímo na dlani. Nabízejícím se východiskem je umístění těchto serverů do samostatné chráněné sítě.

Problémové je ovšem i členění vnitřní počítačové sítě MěÚ, jelikož je omezená pouze na jednu podsíť, do které jsou zapojena všechna síťová zařízení městského úřadu. To je ovšem velice rizikové, jelikož jsou v tomto případě všem dostupná i administrativní rozhraní všech kritických zařízení jakou jsou diskové pole, páteřní switche apod. Navíc by po nasazení nového switche sítě sloužícího jak pro zařízení vnitřní sítě tak VoIP sítě, docháze-

lo ke kolizi DHCP (Dynamic Host Configuration Protocol) serverů těchto sítí. Rozumné by bylo rozdělení sítě do více samostatných oddělených sítí.



Obr. 5: Zátěž internetového routeru

Pamatovat by se mělo i na vstup cizího síťového zařízení do interní sítě MěÚ. V současnosti jsou zapojeny jen používané síťové zásuvky, volné jsou nezapojené. Lze ale samozřejmě místo připojeného zařízení připojit cizí zařízení. Mělo by se implementovat opatření omezující přístup jen zařízení městského úřadu.

Data městského úřadu jsou, jak bylo zmíněno výše, zálohována 14 dní zpětně na šifrovaném úložišti. Není ale dořešena totální ztráta dat zálohovacího serveru, ať už havárií, útokem či selháním prostředků. Zálohování momentálně rovněž neřeší objevenou ztrátu či poškození dat starší než 14 dní. Vhodným opatřením by bylo prodloužení období uchování záloh a archivace starších záloh po rozumně delší dobu na jiném zařízení.

Nedostatkem je též decentralizovaná aktualizace stanic a serverů. Stanice mají mnohdy rozdílně nainstalované aktualizace operačního systému a Office, což nejednou způsobilo nekompatibilitu s nově instalovanými či na novější verzi povýšenými ostatními aplikacemi. Doporučením je nasazení centralizované správy a distribuce aktualizací.

Současný firewall má trvale otevřené některé porty pro vzdálený přístup zaměstnanců k jejich počítačům. Některé tyto porty nejsou dokonce ani omezené na žádnou IP adresu. Toto nastavení dává útočníkovi volnou ruku k pokusům o prolomení účtů na daných počítačích a následně k možné infiltraci interní počítačové sítě. Ideálním řešením tohoto nedo-

statku by bylo nasazení VPN, která zamezí všeobecnému přímému přístupu k těmto počítačům, ale zároveň umožní vybraným osobám připojit se k nim zabezpečeným připojením.

7.3.3 Personální bezpečnost

Na personální bezpečnost je na úřadě dbáno již od počátku přijímacího procesu nového zaměstnance. Již před přijímacím řízením je prováděna analýza rukopisu uchazeče, během pohovoru je prověřována jeho počítačová gramotnost a pokud to pozice vyžaduje, je uchazeč podroben psychologickému testu. Zaměstnanci jsou během pracovního procesu obeznamováni s důvody aplikací nových opatření. Je snaha je i motivovat pro co nejlepší pracovní výsledky. Všechna tato opatření ovšem nezabrání například nepovolenému vynesení důležitých dokumentů pomocí počítačové sítě. Práce na počítačích je sice monitorována, s čímž jsou zaměstnanci seznámeni dle vnitřní směrnice, a tak by se původce vynesení dal s největší pravděpodobností dohledat, ale to by už bylo pozdě. Všechny informace mají totiž svou cenu a je pak čistě na zaměstnanci, zdali podstoupí toto riziko. Řešením je instalace zařízení na ochranu před ztrátou dat.

8 NÁVRH VHODNÉHO ŘEŠENÍ

Na základě bezpečnostní analýzy byla navržena následující opatření.

8.1 Fyzická bezpečnost

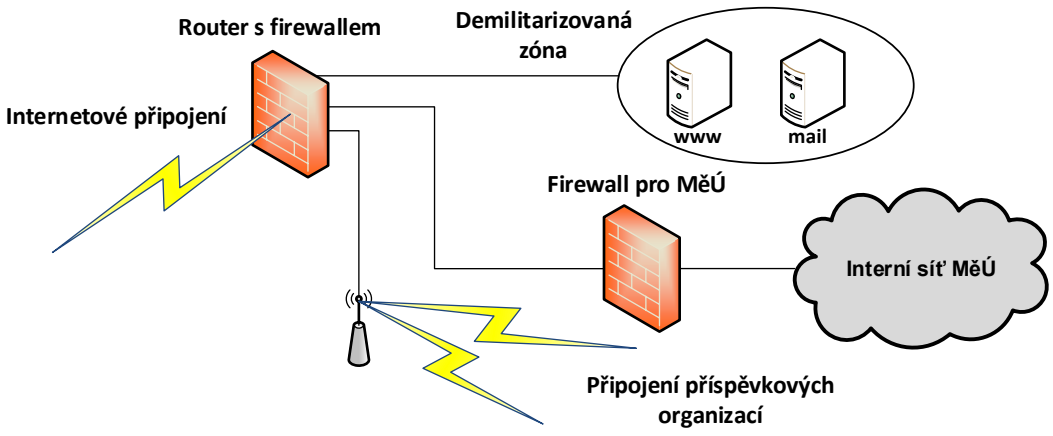
Pro ochranu proti přepětí bylo vybráno zařízení APC ProtectNet PNET1GB filtrující na všech vodičích strukturované 1Gbit kabeláže a zároveň umožňující propuštění PoE.

Pro zvýšení bezpečnosti zálohovaných dat byl navržen přesun zálohovacího serveru i jednoho záložního zdroje ze serverovny do místnosti spisovny. Do spisovny je striktně vymezený přístup určitých osob a je zabezpečena poplachovým zabezpečovacím zařízením.

8.2 Datová bezpečnost

8.2.1 Oddělení sítí - nasazení IPS

Pro oddělení interní sítě městského úřadu od zbývajících sítí se jeví nejúčelnější implementování druhého firewallu určeného čistě pro ochranu sítě úřadu, zároveň s tím bude vytvořena demilitarizovaná zóna pro webový a mailový server (Obr. 6).



Obr. 6: Umístění firewallu pro MěÚ a vytvoření DMZ

Rozumné by bylo nasazení nějakého chytřejšího zařízení jako IPS, které bude monitorovat aktivity na síti a případně blokovat nekalé činnosti.

Pro tyto účely bylo vybráno hardwarové zařízení FortiGate 90D od firmy Fortinet s funkčním rozšířením UTM Bundle. Společnost Fortinet celosvětově představuje jednoho z předních výrobců zařízení pro zabezpečení sítě. Zařízení FortiGate mohou být nasazena

jak v hardwarové podobě, tak ve virtuální. Hardwarová zařízení mají ale výhodu speciálních akceleračních ASIC (Application-specific integrated circuit) procesorů, které urychlují schopnosti firewallových systémů. Virtuální stroje se spoléhají čistě na surový procesorový výkon. Rozšíření UTM Bundle obsahuje služby – Antivirus, IPS, filtrování webového obsahu, DLP a Antispam. Standardními funkcemi Fortigate jsou firewall, VPN brána, řízení provozu (Traffic Shaping). Zařízení lze rozdělit až na 10 virtuálních strojů a každý z nich přidělit například pro jinou organizaci atd. Výhodou zařízení firmy Fortinet je, že nejsou licencována na počty uživatelů. Rozdíl mezi jednotlivými modely FortiGate je většinou jen ve výpočetním výkonu každého zařízení a tím dané propustnosti (Obr. 7). Model FortiGate 90D byl vybrán s ohledem na kapacitu stávajícího internetového připojení s rezervou pro jeho případný rozvoj do budoucna.

FortiGate
Network Security Platform - *Top Selling Models Matrix

	FG/FWF-30D	FG/FWF-60C	FG/FWF-60D	FG/FWF-90D	FG-100D	FG-200D	FG-240D	FG-280D-POE	FG-300C	FG-600C
Firewall Throughput (1518/512/64 byte UDP)	800 / 800 / 800 Mbps	1 / 1 / 1 Gbps	1.5 / 1.5 / 1.5 Gbps	3.5 / 3.5 /3.5 Gbps	2500 / 1000 / 200 Mbps	3 / 3 / 3 Gbps	4 / 4 / 4 Gbps	4 / 4 / 4 Gbps	8 / 8 / 8 Gbps	16 / 16 /16 Gbps
Firewall Latency	8 µs	4 µs	4 µs	4 µs	37 µs	2 µs	6 µs	2 µs	2 µs	7 µs
Concurrent Sessions	200,000	400,000	500,000	1.5 Mil	3 Mil	1.4 Mil	3.2 Mil	3.2 Mil	2 Mil	3 Mil
New Sessions/Sec	3,500	3,000	4,000	4,000	22,000	77,000	77,000	77,000	50,000	70,000
Firewall Policies	5,000	5,000	5,000	5,000	10,000	10,000	10,000	10,000	10,000	10,000
IPSec VPN Throughput	350 Mbps	70 Mbps	1 Gbps	1 Gbps	450 Mbps	1.3 Gbps	1.3 Gbps	1.3 Gbps	4.5 Gbps	8 Gbps
Max G/W to G/W IPSEC Tunnels	20	50	200	200	2,000	2,000	2,000	2,000	2,000	2,000
Max Client to G/W IPSEC Tunnels	250	500	500	1,000	5,000	5,000	5,000	5,000	10,000	50,000
SSL VPN Throughput	25 Mbps	19 Mbps	30 Mbps	35 Mbps	300 Mbps	400 Mbps	400 Mbps	400 Mbps	200 Mbps	1 Gbps
Recommended SSL VPN Users	80	100	100	200	300	300	300	300	500	5,000
IPS Throughput	150 Mbps	135 Mbps	200 Mbps	275 Mbps	950 Mbps	1.7 Gbps	2.1 Gbps	2.1 Gbps	1.4 Gbps	4 Gbps
Antivirus Throughput (Proxy-Based/ Flow-Based)	30 / 40 Mbps	20 / 40 Mbps	35 / 50 Mbps	35 / 65 Mbps	300 / 700 Mbps	600 / 1,100 Mbps	600 / 1,100 Mbps	600 / 1,100 Mbps	200 / 550 Mbps	1.3 / 2.8 Gbps
Max FortiAPs (Total / Tunnel)	2 / 2	10 / 5	10 / 5	32 / 16	64 / 32	64 / 32	64 / 32	64 / 32	512 / 256	1024 / 512
Max FortiTokens	20	100	100	100	1,000	1,000	1,000	1,000	1,000	1,000
Max Registered FortClient	10	200	200	200	2,000	2,000	2,000	2,000	2,000	2,000
Virtual Domains (Default/Max)	-	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10	10 / 10
Interfaces (FE, GE ports)	5x GE RJ45	8x GE RJ45	10x GE RJ45	16x GE RJ45	20x GE RJ45, 2x Shared Port Pairs (100D only)	18x GE RJ45, 2x GE SFP	42x GE RJ45, 2x GE SFP	54x GE RJ45, 32x PoE GE RJ45, 4x GE SFP	10x GE RJ45	18x GE RJ45, 4x Shared Port Pairs, 2x Bypass Pairs
Interfaces (Others)	FWF - a/b/g/n	FWF - a/b/g/n	FWF - a/b/g/n	FWF - a/b/g/n	-	-	-		-	-
Local Storage	-	-	-	32 GB	32 GB	16 GB	32 GB	64 GB	32 GB	64 GB
Power Supplies	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Ext RPS	Single AC Power Supply, opt. Dual PS or Ext RPS
Form Factor	Desktop	Desktop	Desktop	Desktop	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 1 RU	Rack Mount, 2 RU	Rack Mount, 1 RU	Rack Mount, 1 RU
Variants	WiFi, POE	WiFi, Anal.Modem, Wifi+Ana. Modem, LENC, SFP, POE, ADSL	WiFi, POE, LENC	WiFi, POE, LENC	LENC, High port density, High port density + POE	LENC	-	-	DC, LENC	DC, LENC

Obr. 7: Přehled vybraných zařízení FortiGate[11]

8.2.2 VLAN (Virtual Local Area Network)

Jelikož všechny přepínače používané úřadem podporují standard IEEE 802.1Q, jeví se jako nejlepší řešení rozdělení vnitřní sítě na několik samostatných virtuálních sítí (VLAN).

Navrhované rozdělení je:

- VLAN10 bude sloužit pro vyvedení síťové komunikace zóny DMZ ze serverovny až k prvnímu routeru.
- VLAN20 je určená pro všechny zaměstnanecké počítače, tiskárny a servery s vnitřními informačními systémy.
- VLAN30 má za úkol propojit administrativní rozhraní klíčových zařízení s PC správce počítačové sítě. Tato síť nebude vůbec připojena do internetu.
- VLAN40 bude síť vyčleněná jen pro zařízení VoIP telefonní sítě.

8.2.3 Port security

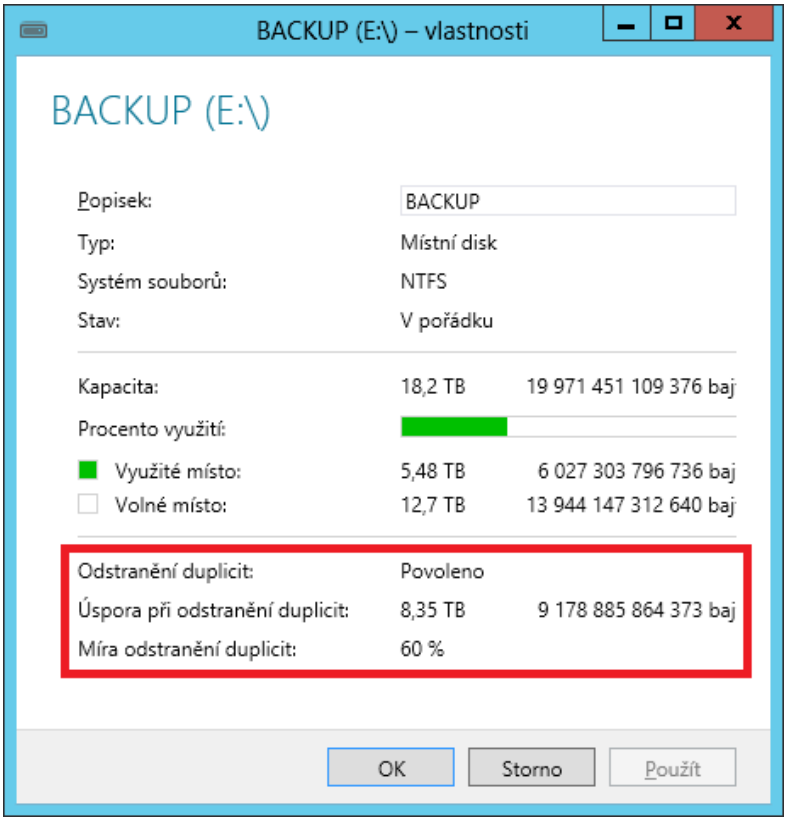
Ideálním řešením zamezení vstupu do sítě cizího zařízení by bylo využití autorizace dle standardu IEEE 802.1X, ověřovaného vůči doménovému řadiči například proti doménovým účtům počítačů. Bohužel přibližně polovina z počítačů, kvůli nějakému historickému zásahu do systému, špatně komunikuje s doménovými řadiči, takže je do jejich reinstalace nelze k nim připojit, proto je toto řešení momentálně nevyužitelné.

Jako náhradu této autorizace se jeví účelné využít funkcionality switchů nazvanou Port security. Tato funkcionalita kontroluje, zdali packety na daném portu přicházejí z povolené MAC (Media Access Control) adresy. Pokud se na port připojí jiné zařízení, bude mu zamezena komunikace v síti. Samozřejmě to má nevýhodu, že pokud si útočník naklonuje na své síťové zařízení povolenou MAC adresu, bude do sítě vpuštěn. S tím ovšem musí předem počítat.

8.2.4 Zálohování a archivace

Nadále bude prodlouženo, díky výrazné úspoře místa na zálohovacím serveru zajištěné deduplikací (Obr. 8), časové rozmezí ukládaných záloh ze 14 dní na 28 dní.

Pro zajištění archivace bude pořízena LTO (Linear Tape-Open) 6 pásková mechanika, na kterou budou jednou za 4 týdny archivovány zálohy. Páska bude následně uložena do ohnivzdorného trezoru úřadu.



Obr. 8: Příklad úspory dat deduplikací

8.2.5 Centrální správa aktualizací počítačů

Přímo nabízejícím se řešením centrální správy aktualizací je využití stávajících Windows Serverů a implementace role WSUS (Windows Server Update Services) na jednom z nich. Jelikož stanice nejsou v doméně, bude u nich nutné provést změnu nastavení aktualizačního serveru pomocí úpravy registrů. Mimo získaného přehledu o aktualizacích, jejich kontrole atd. ušetříme i datové pásmo internetové přípojky, jelikož se z internetu data aktualizací budou stahovat jen jednou na aktualizační server a ne pro každou stanici a server zvlášť.

8.2.6 VPN

Pro implementaci VPN opět využijeme zařízení FortiGate 90D. Jako ideální se jeví nasazení SSL VPN s webovým portálem. Toto řešení zajistí zabezpečený přístup bez nutnosti instalace dalších aplikací na klientské zařízení. Všechny potřebné funkce může poskytovat portál VPN včetně například RDP klienta, pokud není na klientském zařízení nainstalován.

8.3 Personální bezpečnost

8.3.1 DLP

Proti vynesení důležitých informací je ideální využít funkcionality nasazené FortiGate 90D Data Leak Prevetion, což je prakticky trochu jinak pojmenovaná Data Loss Prevention. Pomocí nasazených sensorů mohou být potom v síťové komunikaci vyhledávány zprávy či soubory dle zadaných kritérií a následně tato komunikace logována, blokována či umístěna do karantény.

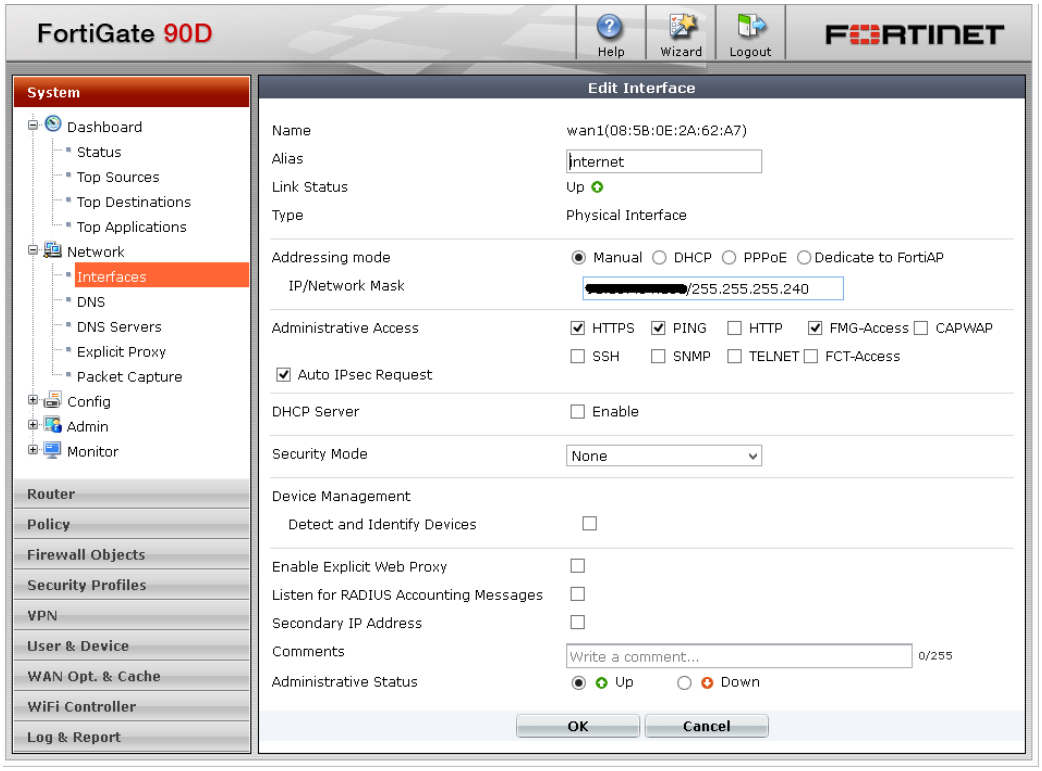
9 REALIZACE A OVĚŘENÍ REALIZOVANÝCH OPATŘENÍ

V této sekci si předvedeme vzorová nastavení jednotlivých zařízení, pro jejich nasazení dle navržených opatření.

9.1 Nasazení IPS

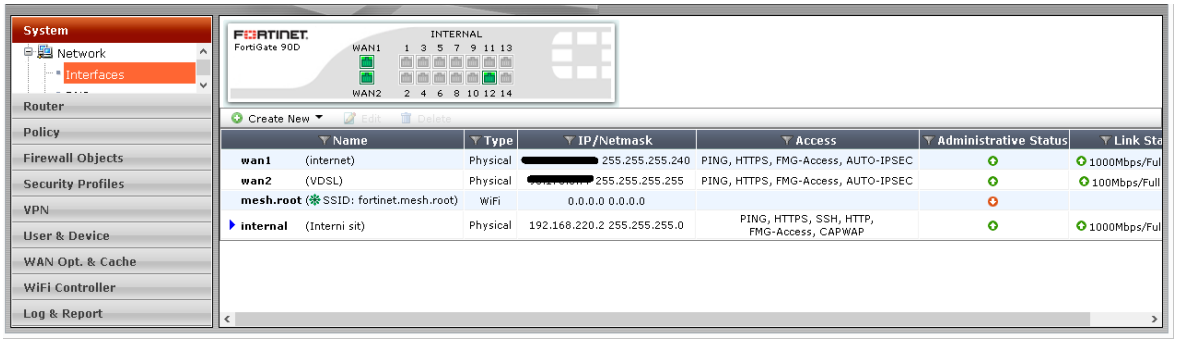
Předvedeme si vzorové nastavení FortiGate pro připojení vnitřní sítě do internetu a nastavením IPS. Konfiguraci budeme provádět skrze webové rozhraní zařízení.

První co musíme udělat je nakonfigurovat vnější a vnitřní rozhraní pro propojení sítí (Obr. 9). Nastavíme, jaké přístupy budou na těchto rozhraních povolené a či bude využito DHCP serveru. V sekci DNS vyplníme, které servery bude zařízení používat.

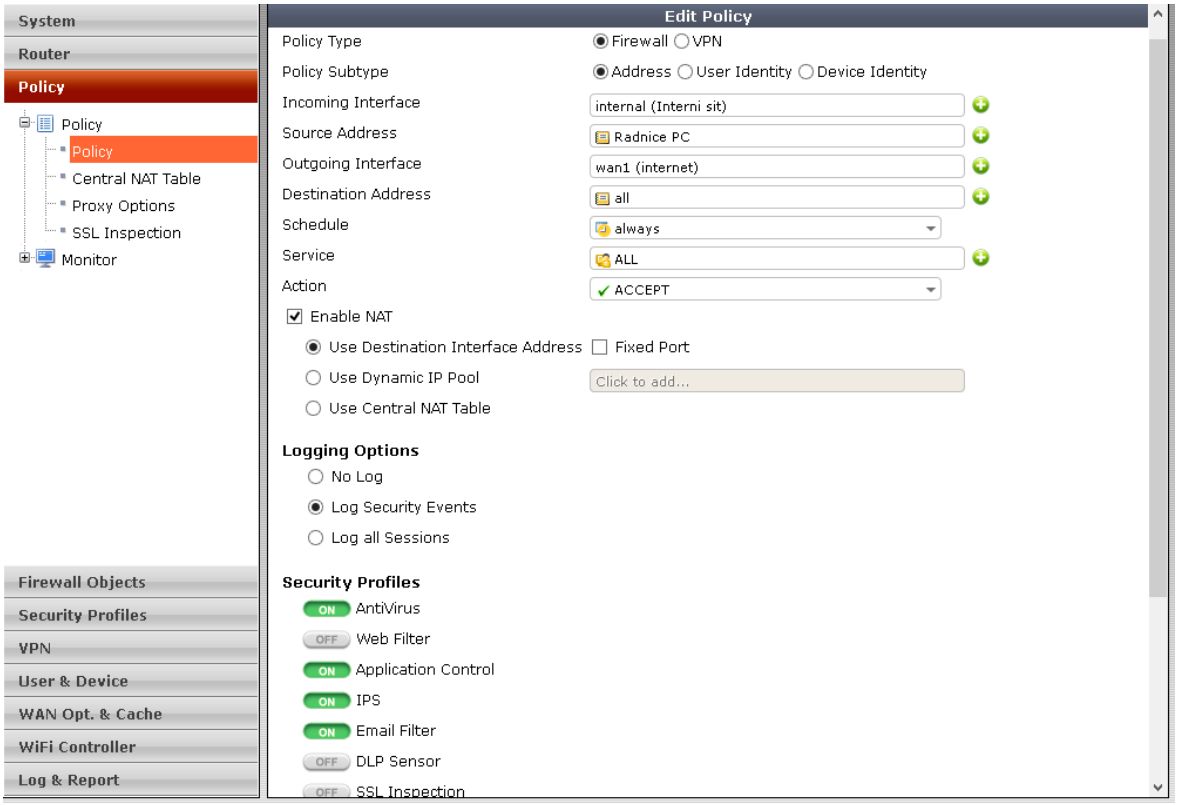


Obr. 9: Nastavení rozhraní

Tímto sice máme nastavena rozhraní (Obr. 10), ale nemáme určeno, co se mezi nimi má dít. Abychom se dostali do internetu, je potřeba v sekci Policy povolit odchozí komunikaci pro vybraná zařízení na vnitřním rozhraní. Povolena bude do internetové sítě komunikace pro všechna zařízení interní sítě (Obr. 11) s tím, že na ni bude aplikován NAT. Přenášená data budou kontrolována antivirem, IPS, antispamem atd. Všechna ostatní komunikace (z internetu a jiných rozhraní) je ve výchozím stavu zakázána.

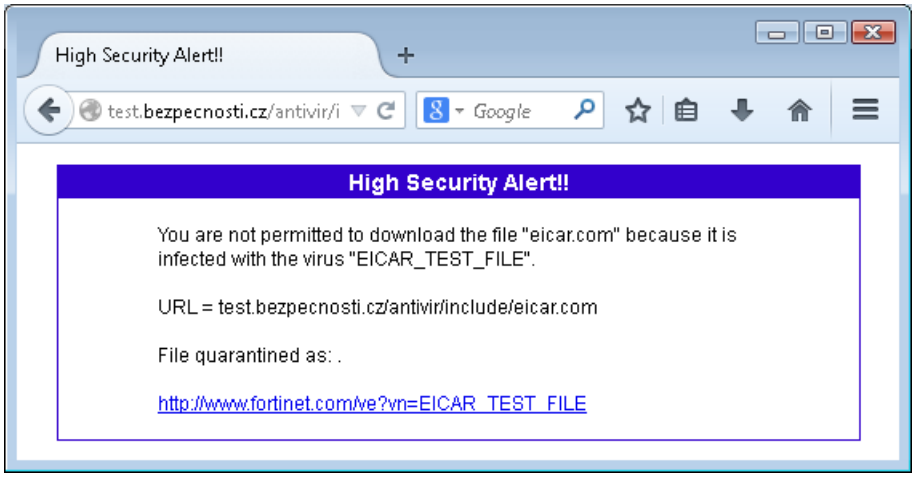


Obr. 10: Nakonfigurovaná rozhraní



Obr. 11: Povolení připojení vnitřní sítě do internetu

Naše síť je teď připojená do internetu a z něj k nám nikdo nesmí. Nyní ověříme funkčnost například antiviru nad naší komunikací. Pokusíme se stáhnout soubor eicar.com z internetové stránky http://test.bezpecnosti.cz/antivir/. FortiGate komunikaci zablokoval (Obr. 12), soubor neměl šanci dostat se na stanici a antivir stanice tedy vůbec nezareagoval.



Obr. 12: Blokování viru IPS

9.2 VLAN

Konfigurace VLAN v síti provedeme následujícím způsobem. Přihlásíme se na konzoli switche a vytvoříme jednotlivé virtuální sítě.

SG500-52#configure terminal - vstup do konfiguračního režimu

SG500-52(config)# vlan database - vstup do konfigurace VLAN

SG500-52(config-vlan)#vlan 10,20,30,40 - vytvoření VLAN 10,20,30,40

SG500-52(config-vlan)#exit - odchod z konfigurace VLAN

Bližší nastavení konkrétní virtuální sítě provedeme například takto:

SG500-52 (config)# interface vlan 20 - vybereme VLAN, jestliže VLAN nebyla předtím vytvořena, vytvoří se.

SG500-52 (config-if)# ip address 192.168.220.150 255.255.255.0 – IP adresa switche v dané virtuální síti

SG500-52 (config-if)# name Zamestnanci – název (popis) virtuální sítě

SG500-52(config-vlan)#exit

Konfigurace portu pro zaměstnanecké počítače a tiskárny spočívá v přiřazení portu do virtuální sítě a vypnutí značkování.

SG500-52#configure terminal - vstup do konfiguračního režimu

SG500-52(config)#interface range GE 1/1/43-44 – vybrání rozsahu konfigurovaných portů

SG500-52(config-if-range)#switchport mode access – přepnutí do neznačkovaného režimu

SG500-52(config-if-range)#switchport access vlan 20 – přiřazení do VLAN číslo 20

SG500-52(config-vlan)#exit

Stejně může přiřadit porty s VoIP telefony do VLAN 40.

Porty pro servery, spoje mezi switchy a pro počítač správce sítě budeme konfigurovat jako trunk. Jako trunk prohlašujeme port, který je přiřazen do více VLAN.

SG500-52#configure terminal - vstup do konfiguračního režimu

SG500-52 (config)# interface gi1/1/1 - vstup do konfigurace portu

SG500-52 (config-if)# switchport mode trunk - nastavení portu jako trunk

SG500-52 (config-if)# switchport trunk allowed vlan add 10,20,30 – přidaní VLAN do trunku

SG500-52 (config-if)# switchport trunk native vlan 1 – určení VLAN do které bude přesměrována neznačkovaná komunikace

Jakmile máme všechny porty nastavené, skončíme s konfigurací a nezapomeneme konfiguraci uložit, jinak by po restartu switche zmizela.

SG500-52(config-if)#end

SG500-52#copy running-config startup-config

9.3 Port security

Nyní si ukážeme, jak nakonfigurujeme port security pro koncová zařízení tak, aby si switch pro daný port pamatoval poslední připojené zařízení a další již nedovolil připojit. Pro porty na kterých jsou připojené servery, port security nastavovat nebudeme, jelikož bychom s každým novým virtuálním serverem či přidanou síťovou kartou museli měnit konfiguraci switchů. Mimoto servery mohou i migrovat mezi svými hostiteli.

Po přihlášení do konzole switche se přepneme do konfiguračního režimu.

SG500-52#configure terminal - vstup do konfiguračního režimu

Vybereme port, který hodlám konfigurovat, můžeme využít i range pokud chceme konfigurovat stejně více portů.

SG500-52(config)#interface GE 1/1/44

Zadáme počet MAC adres, které si switch bude pamatovat pro daný port jako povelené.

SG500-52(config-if)#port security max 1

Nastavíme mód učení MAC adres nebo jejich možného statického zadání.

SG500-52(config-if)#port security mode max-addresses

Určíme, co se stane, když se připojí nepovolené zařízení. Námi vybraný mód komunikaci s jinou než naučenou MAC adresou zahodí a následně trvale vypne daný port.

SG500-52(config-if)#port security discard-shutdown

Ukončíme práci v konfiguračním režimu a uložíme konfiguraci.

SG500-52(config-if)#end

SG500-52#copy running-config startup-config

Nyní si ověříme, zdali je konfigurace port security na správně nastavená.

SG500-52#show port security GE 1/1/44

Port status Learning Action Maximum Trap Frequency

--- --- --- --- --- --- ---

gi1/1/44 Enabled Max-Addresses Discard, Shutdown 1 Disabled -

Je vidět, že konfigurace je taková, jakou jsme nastavili.

Prakticky ověříme, zdali konfigurace funguje tak, jak má. Výpis aktuálního stavu daného portu:

SG500-52#show interfaces status GigabitEthernet 1/1/44

Flow Link Back Mdix

Port Type Duplex Speed Neg ctrl State Pressure Mode

--- --- --- --- --- --- --- --- ---

gi1/1/44 1G-Copper Full 1000 Enabled Off Up Disabled Off

Původní síťové zařízení z portu odpojíme a připojíme jiné. Switch inicializuje port.

24-May-2014 18:32:09 %LINK-I-Up: gi1/1/44

Zjistí, že zařízení na portu nevyhovuje port security a následně port vypne.

24-May-2014 18:32:26 %LINK-W-PORT_SUSPENDED: Port gi1/1/44 suspended by port-security

24-May-2014 18:32:26 %LINK-W-Down: gi1/1/44

Z výpisu stavu daného portu switche vypátráme, že port byl vypnut systémem.

SG500-52#show interfaces status GigabitEthernet 1/1/44

Port	*Type*	*Duplex*	*Speed*	*Neg*	*Flow ctrl*	*Link State*	*Back Pressure*	*Mdix Mode*
gi1/1/44	*1G-Copper*	--	--	--	--	*Down**	--	--

**: The interface was suspended by the system.*

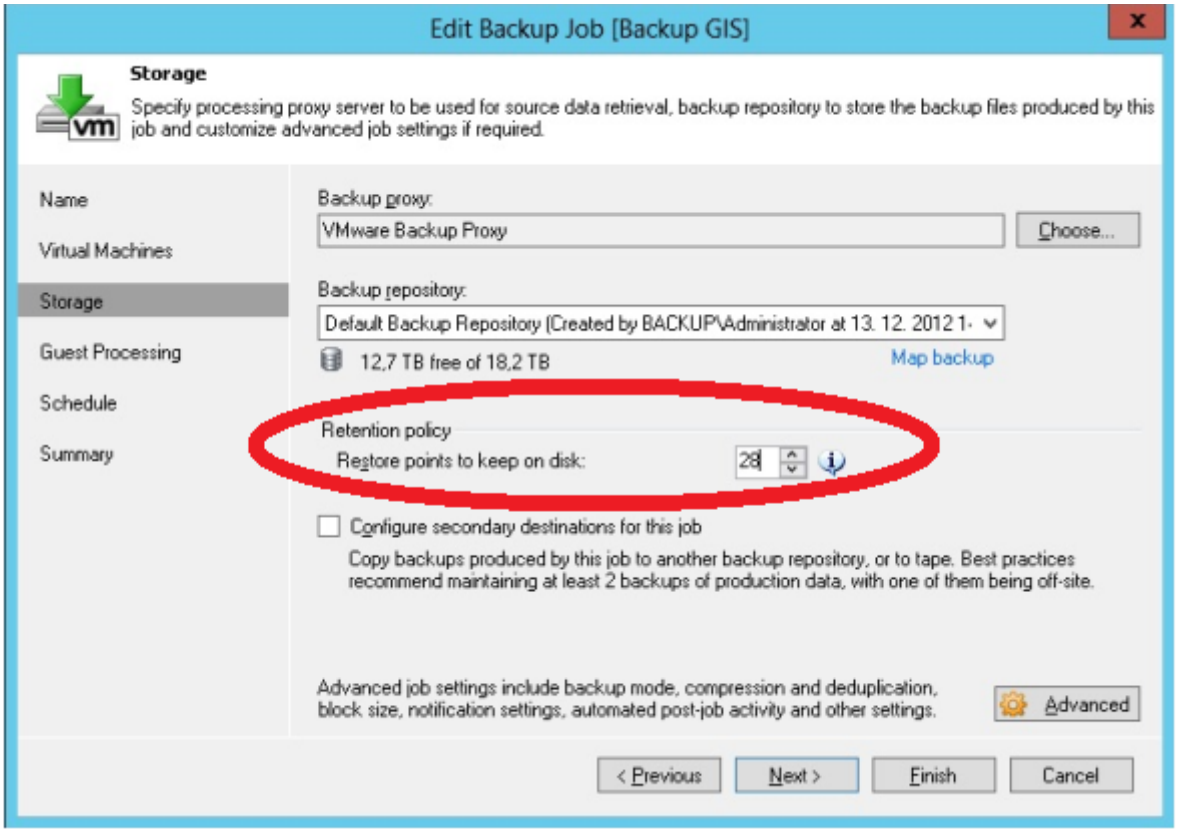
Tímto jsme ověřili, že naše nastavení funguje přesně, jak jsme chtěli.

9.4 Zálohování a archivace

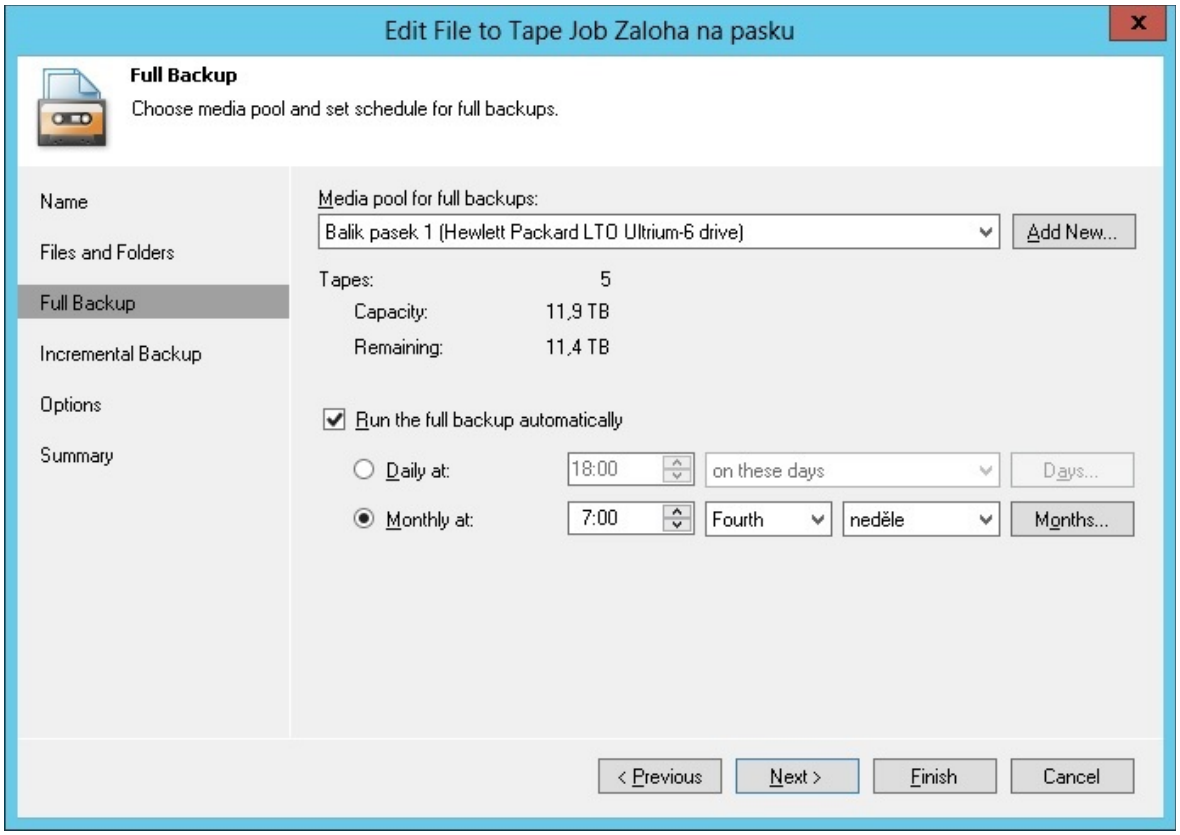
Pro zvýšení fyzické bezpečnosti byl zálohovací server fyzicky přesunut dle navrženého opatření do spisovny úřadu. Následně na něm byly upraveny zálohovací úlohy o prodloužení zachování záloh na disku na 28 dní (Obr. 13).

Nově pořízená externí pásková mechanika HP LTO Ultrium-6 byla připojena k řadiči serveru. Potom byla nastavena úloha pro archivaci záloh každou čtvrtou neděli v měsíci v 7 hodin ráno (Obr. 14). Pro začátek byl na archivaci vyčleněn balík pěti LTO6 pásek. Uzná-li se to jako opodstatněné, bude jejich počet navýšen. Momentálně vychází přibližně množství jedné archivace na jednu celou pásku, to znamená zajištění objemu archívu záloh za posledních pět měsíců.

Neplánovaně byla ověřena účelnost archivace záloh, když se zjistil poškozený pasport geografického informačního systému, který neměl u sebe ani dodavatel. Vypadalo to, že několikatýdenní práce přijde nazmar. S velkým štěstím se zjistilo, že několik dní před poškozením dat (více než dva měsíce zpátky) byla prověřována funkčnost dodané páskové mechaniky a na jednu pásku byly nahrány aktuální zálohy serverů. Data byla tedy nakonec úspěšně obnovena.



Obr. 13: Prodloužení zachování záloh na disku na 28 dní



Obr. 14: Archivace záloh na pásku

9.5 Centrální správa aktualizací počítačů

Nejdříve musíme na Windows Serveru nainstalovat novou roli Windows Update Server Services. Průvodce nás vybídne, jestliže na serveru není nainstalován, i k instalaci webového serveru IIS (Internet Information Services). Potom se zeptá na adresář pro ukládání stažených aktualizací a vyzve nás k volbě databáze. Nám bude stačit výchozí volba Internal Database. Zobrazí nám souhrn zvolené konfigurace a nyní ho můžeme nechat vše nainstalovat.

Po instalaci se spustí průvodce s prvotní konfigurací. Zeptá se, z kterého serveru chceme stahovat aktualizace, což většinou bude přímo ze serveru Microsoft Update, ale lze jej provést ve větším firemním prostředí z jiného WSUS serveru. Potom bude chtít vědět případnou konfiguraci proxy pro připojení do internetu a provede synchronizaci dostupných aktualizací. Po synchronizaci nás průvodce nechá zvolit, jaké jazykové verze aktualizací (v našem případě anglické a české), pro které produkty (MS Office, MS Windows Server, Exchange, Bing, Windows Vista atd.), které druhy aktualizací (kritické, doporučené, ovladače, service packy atd.) chceme instalovat. Průvodce se nakonec zeptá, zdali synchronizaci chceme nadále provádět ručně nebo chceme naplánovat každodenní automatickou synchronizaci. Po dokončení průvodce máme server nainstalovaný a zkonfigurovaný.

Nyní je k němu potřeba připojit počítače a servery. Jelikož počítače nejsou v doméně, jejich připojení k aktualizačnímu serveru bude provedeno pomocí následující úpravy hodnot v registrech.

Úprava registrů:

Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]

"WUServer"="http://192.168.110.212" *- IP adresa aktualizačního serveru*

"WUStatusServer"="192.168.110.212" *- IP adresa aktualizačního serveru*

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]

"NoAutoUpdate"=dword:00000000 *0: Automatické aktualizace jsou povoleny*

1: Automatické aktualizace jsou zakázány.

"AUOptions"=dword:00000004 *4: automaticky stahovat a plánovat instalaci.*

"ScheduledInstallDay"=dword:00000000 *- den v týdnu – 0 každý*

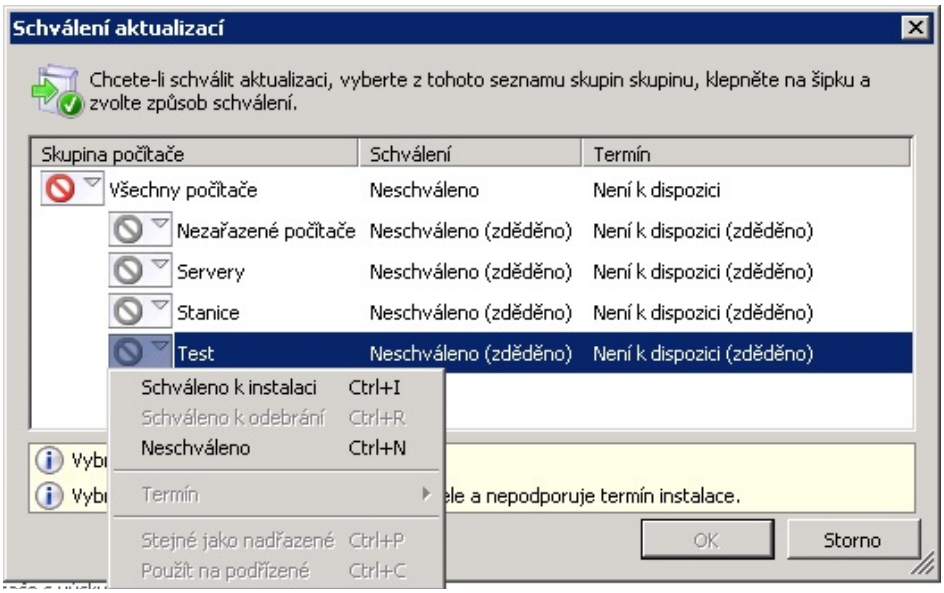
"ScheduledInstallTime"=dword:00000008 *- v kolik hodin instalovat aktualizace*

"UseWUServer"=dword:00000001 *- nastavení WSUS místo Windows Update*

"RescheduleWaitTime"=dword:00000015 *-*

"NoAutoRebootWithLoggedOnUsers"=dword:00000001 - zakázání restartu, když je uživatel přihlášen

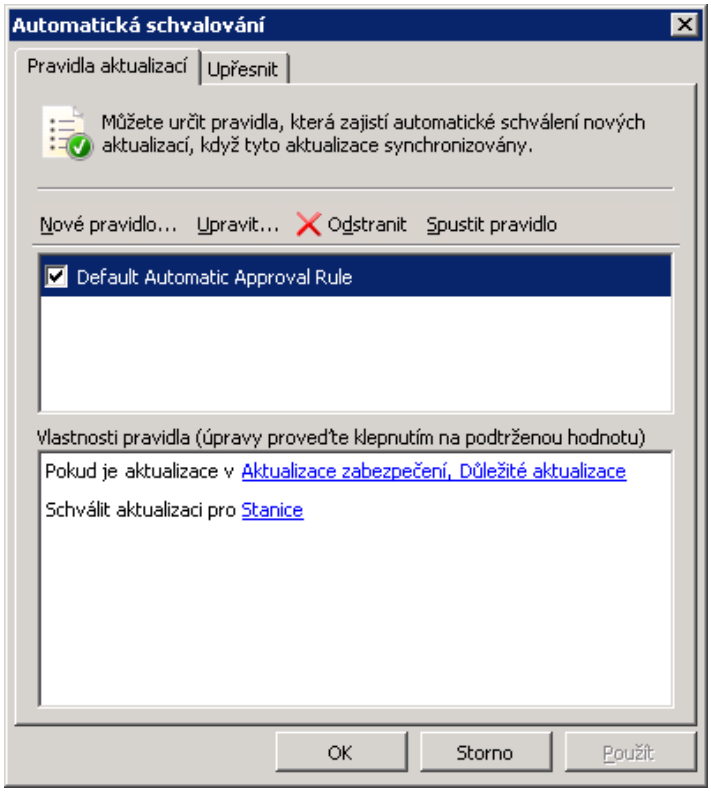
Po připojení stanic k serveru je vhodné je rozumně rozčlenit do skupin, jelikož schvalování aktualizací se provádí dle skupin (Obr. 15).



Obr. 15: Schvalování aktualizací

Nyní nám již jen zbývá schválit aktualizace, které chceme instalovat, a zařízení se budou samy aktualizovat. Schvalování je vhodné provádět pravidelně po každém vydání aktualizací nebo lze nastavit pravidla pro automatické schvalování aktualizací (Obr. 16).

Pro administrátora by bylo ještě záhodno provést nastavení zasílání pravidelných reportů o stavu instalace aktualizací, aby jejich stav nemusel sám kontrolovat na serveru.



Obr. 16: Automatické schvalování aktualizací

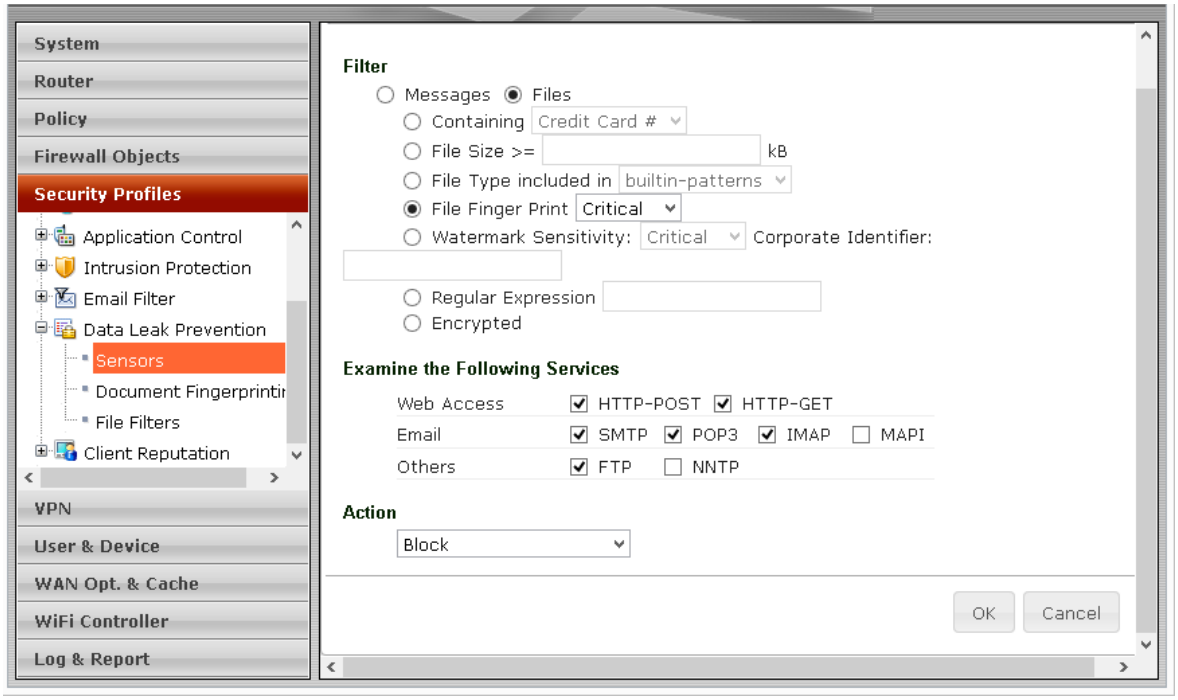
9.6 Přepětí

Zařízení APC ProtectNet PNET1GB bylo připojeno na síťový kabel vedoucí z věže radnice a jeho zemnící kabel byl připevněn k ochrannému vodiči uzemňující rack a další zařízení.

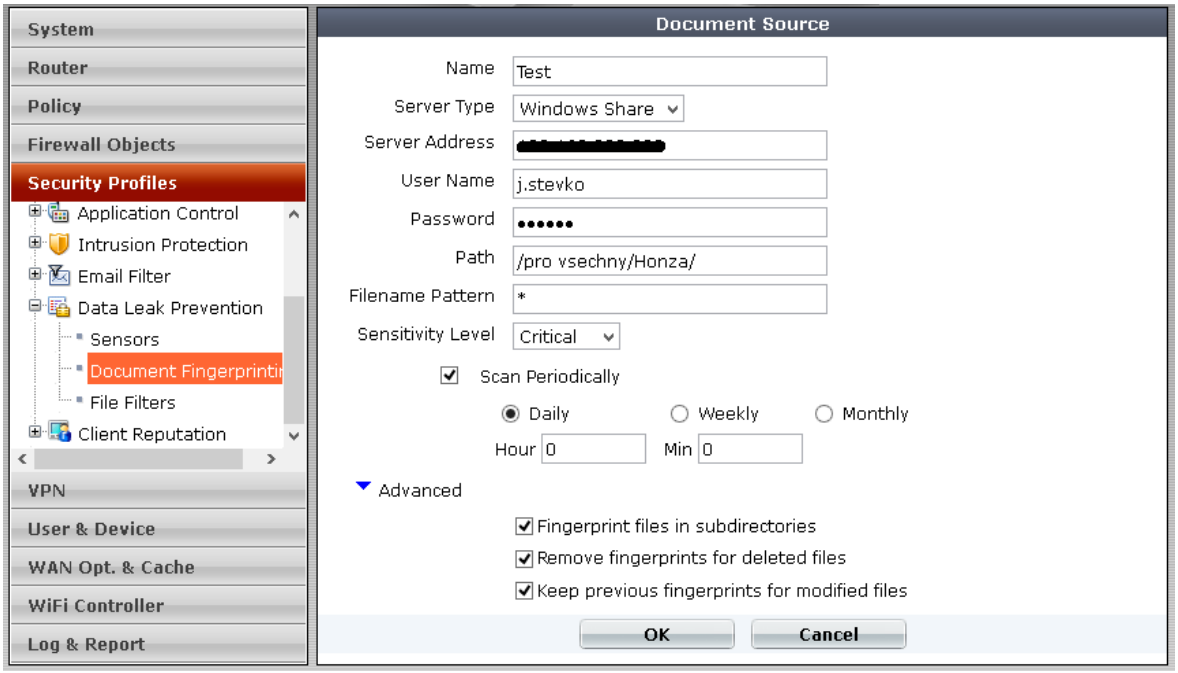
9.7 DLP

Pro ochranu interních dokumentů zprovozníme bezpečnostní funkcionalitu FortiGate Data Leak Prevention. Nejdříve si vytvoříme sensor (Obr. 17), který bude ve vybrané komunikaci hledat otisky souborů. Následně nastavíme, z čeho si bude zařízení otisky vytvářet. My je budeme vytvářet z dokumentů ve sdílené složce na síťovém disku (Obr. 18).

Aby sensor fungoval, je potřeba na některém pravidlu v sekci Policy povolit využití DLP senzoru. My jsme ho povolili na pravidle pro odchozí komunikaci (Obr. 11). Zároveň s ním jsme aktivovali SSL Inspection, abychom byli schopni najít nepovolenou komunikaci i v šifrovaném přenosu.

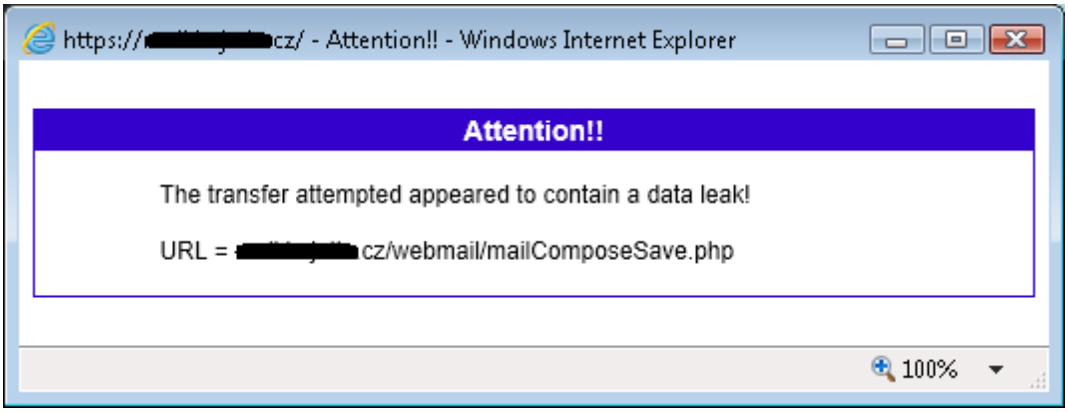


Obr. 17: Vytvoření DLP senzoru



Obr. 18: Vytvoření otisků souborů

Jestliže se nyní pokusíme vynést soubor přes šifrované webové rozhraní mailové serveru, pokus skončí varováním (Obr. 19).



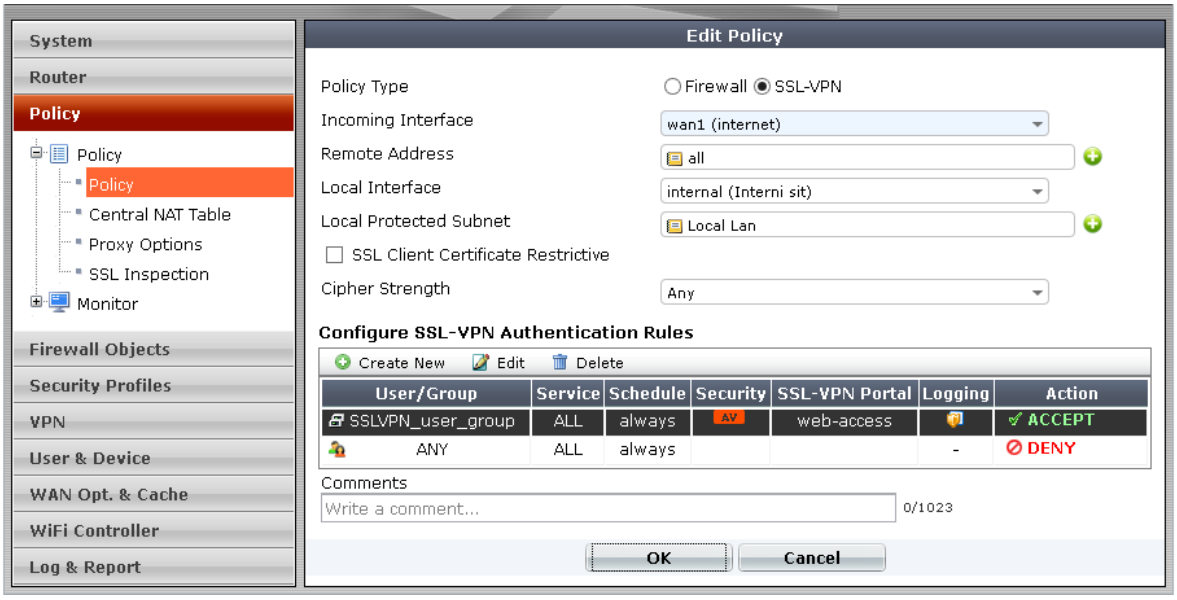
Obr. 19: Zablokování vynesení interního dokumentu

9.8 VPN

Pro zabezpečený přístup do interní sítě úřadu implementujeme na zařízení FortiGate 90D.

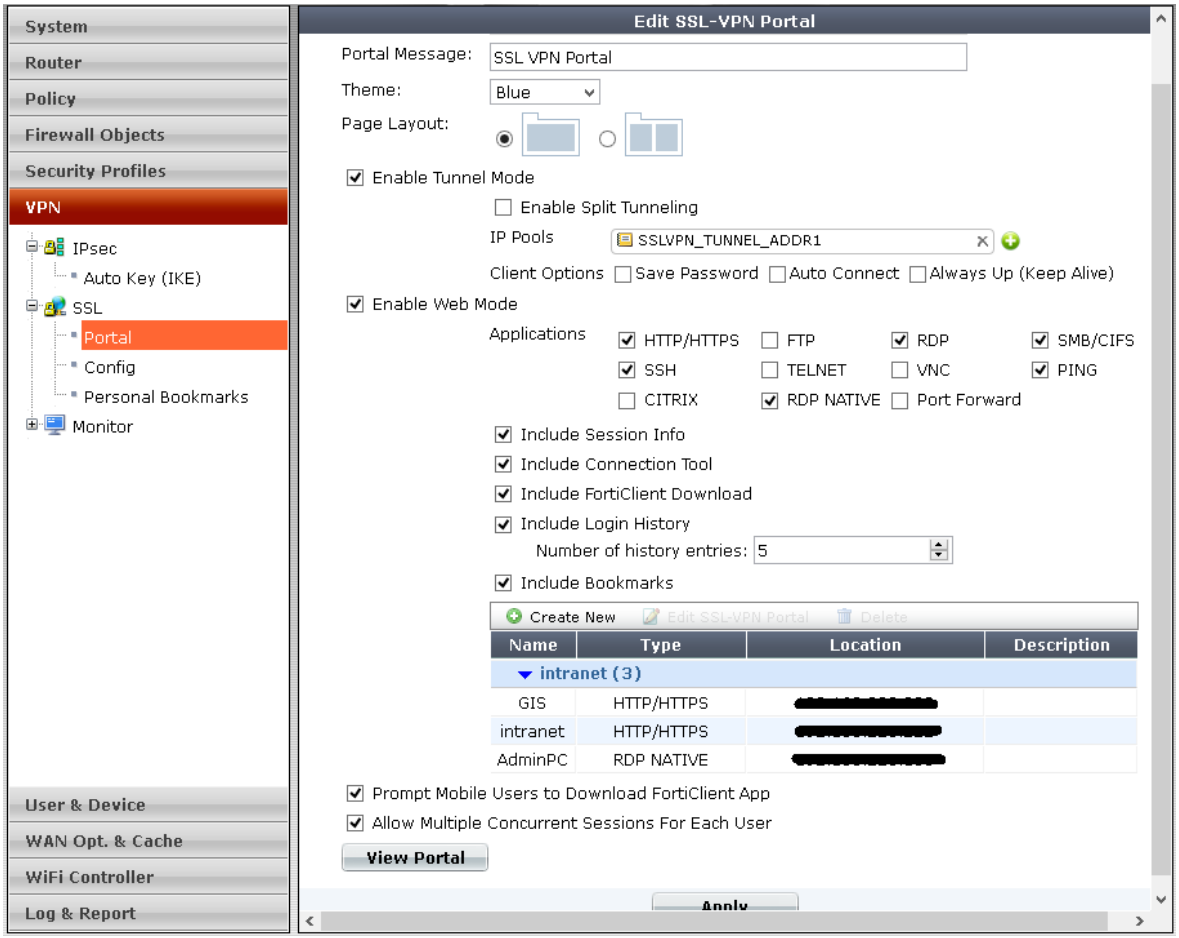
Nejdříve si v sekci Users & Device vytvoříme uživatele, kterým chceme umožnit přístup a přiřadíme je do skupiny vytvořené pro VPN. Potom si v sekci Firewall Objects – Address vytvoříme IP rozsah přidělený pro využívání VPN.

Nyní přistoupíme k definici pravidla k sekci Policy - Policy pro povolení přístupu skrze SSL VPN do interní sítě (Obr. 20). Můžeme zde také nastavit, které senzory budou na tato připojení aplikovány.



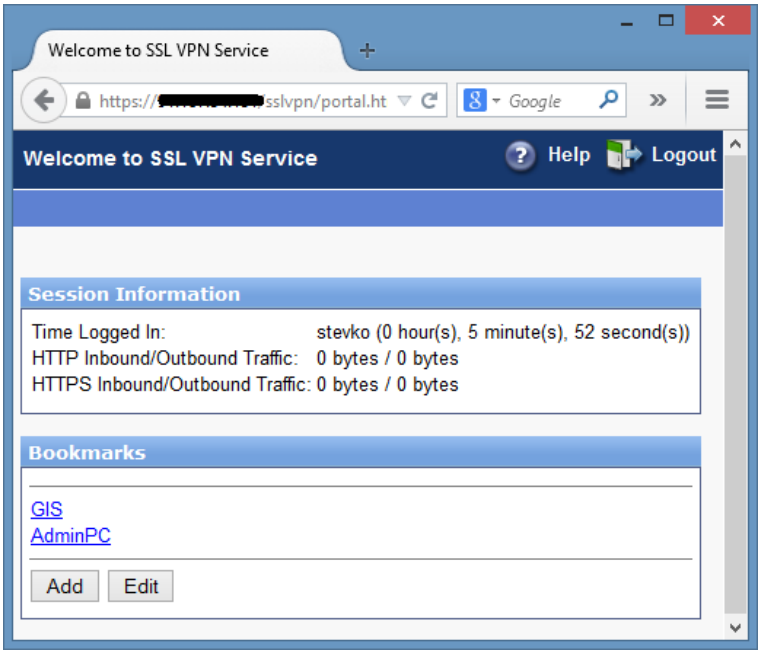
Obr. 20: Vytvoření pravidla pro přístup do interní sítě přes SSL VPN

Po vytvoření pravidla nám již zbývá jen konfigurace samotného portálu. Tuto konfiguraci provedeme v oblasti VPN – SSL – Portal. Nastavíme zde povolené aplikace pro přístup do interní sítě, můžeme vytvořit uživatelům záložky s oblíbenými destinacemi atd. (Obr. 21).



Obr. 21: Konfigurace SSL VPN portálu

Nyní se uživatel může přihlásit a začít pracovat (Obr. 22). Výhodou tohoto řešení je jednak otevřený pouze jediný port (HTTPS 443) pro vnější komunikaci, a také možnost využívat k práci buď webového prohlížeče pro přístup k interním webovým serverům nebo integrovaných java pluginů, které zprostředkovávají přístup k telnetu, vzdálené ploše atd.

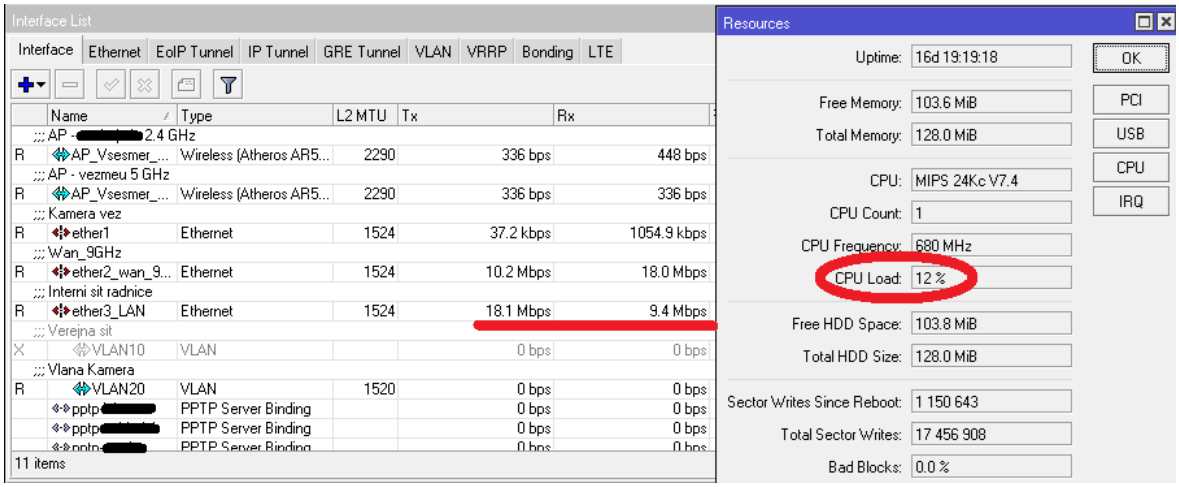


Obr. 22: SSL VPN portál

10 ZHODNOCENÍ A MOŽNÝ ROZVOJ

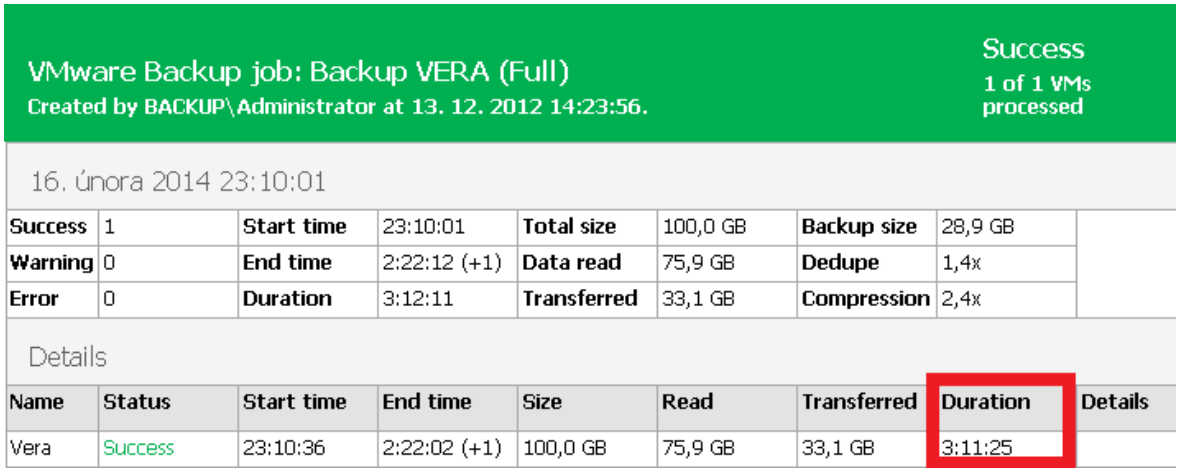
Proběhlá úprava bezpečnosti informačního systému městského úřadu byla velice kladně přijata jak ze strany zaměstnanců, tak vedení úřadu. Změny totiž nijak výrazně nenarušily provoz úřadu ani zvyklosti běžných uživatelů. Významně se ovšem navýšila bezpečnost celého informačního systému. Některá opatření již byla i neplánovaně prověřena v praxi.

Dopady úprav lze mimo jiné vidět jak na snížení zátěže hlavního internetového routeru (Obr. 23), tak na výrazném zvýšení propustnosti vnitřní sítě úřadu.



Obr. 23: Snížení zátěže internetové routeru

Díky tomu se například značně urychlilo zálohování serverů (Obr. 24, 25) a přístup k datům jednotlivých serverů.



Obr. 24: Doba zálohování hlavního IS před úpravami

VMware Backup job: Backup VERA (Full)
Created by BACKUP\Administrator at 13. 12. 2012 14:23:56.

Success
1 of 1 VMs processed

20. února 2014 23:10:09

Success	1	**Start time**	23:10:09	**Total size**	100,0 GB	**Backup size**	29,4 GB
Warning	0	**End time**	23:34:12	**Data read**	100,0 GB	**Dedupe**	1,4x
Error	0	**Duration**	0:24:03	**Transferred**	33,6 GB	**Compression**	2,4x

Details

Name	**Status**	**Start time**	**End time**	**Size**	**Read**	**Transferred**	**Duration**	**Details**
Vera	Success	23:10:47	23:34:04	100,0 GB	100,0 GB	33,6 GB	0:23:17	

Obr. 25: Doba zálohování hlavního IS po úpravách

Jelikož bylo ověřeno, že navržená a implementovaná opatření měla nějaký smysl, bylo rozhodnuto o pokračování navyšování bezpečnosti celého IS.

Během tohoto roku má proběhnout připojení všech stanic a serverů do doménového prostředí, aby měli uživatelé všude stejné přihlašovací údaje a nebyl takový problém s jejich pravidelnou změnou. Plánované je také nasazení ověřování dle standardu IEEE 802.1X. Nadále bylo rozhodnuto o investici do optické kabeláže na propojení s příspěvkovými organizacemi. Tímto budou odstraněny na zranitelnost náchylné a málo výkonné bezdrátové spoje. Také to umožní umístění zálohovacího serveru zcela mimo budovu úřadu.

Město v současnosti žádá o dotaci z evropských fondů v oblasti IT. Její získání by umožnilo v krátké době ještě významnější navýšení bezpečnosti, jako je pořízení druhého diskového pole, zajištění vysoké dostupnosti IPS, replikace záloh do dvou lokalit, automatické ověřování funkčnosti záloh atd.

ZÁVĚR

Cílem této práce bylo zajištění bezpečnosti informačního systému městského úřadu. Městský úřad svůj informační systém provozuje již řadu let, ale nikdy neměl komplexní přehled o jeho rozsahu a stavu, anebo byly tyto informace značně zkreslené.

Proto byly úřadem zadány požadavky ke zjištění aktuálního stavu systému, nalezení případných bezpečnostních hrozeb a v rámci rozumných opatření tyto hrozby eliminovat.

V teoretické části práce byly popsány nejčastěji vyskytující se hrozby pro informační systémy a ochranné prostředky na zajištění jejich bezpečnosti.

V praktické části práce byl probrán aktuální stav systému a následně byly pomocí bezpečnostní analýzy nalezeny jeho zranitelné oblasti. K odstranění těchto problematických oblastí byly navrženy patřičné kroky, které byly potom implementovány do praxe. Dá se říci, že všechny požadavky úřadu se podařilo splnit.

Je si potřeba ovšem uvědomit, že problematiku bezpečnosti nelze dlouhodobě brát na lehkou váhu. Bezpečnost je totiž trvalý proces, proto je potřeba průběžně analyzovat stav systému a případně dle objevených hrozeb na tyto situace reagovat.

SEZNAM POUŽITÉ LITERATURY

[1] JAŠEK, Roman. *Ochrana znalostí a dat v podnikových informačních systémech*. Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2002, 115 s. ISBN 8073180952.

[2] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: bezpečnost*. Vyd. 1. Praha: Computer Press, 2001, xvi, 565 s. ISBN 807226513x.

[3] MALANÍK, David. *Význam fyzického zabezpečení IT systémů.* Security Revue září 2010. ISSN 1336-9717.

[4] NORTHCUTT, Stephen et al. *Bezpečnost sítí: velká kniha*. Vyd. 1. Brno: CP Books, 2005, 589 s. ISBN 80-251-0697-7.

[5] THOMAS, Thomas M. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.

[6] Zákon o informačních systémech veřejné správy. In: *365/2000 Sb.* 2000.

[7] Metodické pokyny: Co je a co není ISVS. *Ministerstvo vnitra České republiky* [online]. 2009 [cit. 2014-05-14]. Dostupné z: http://www.mvcr.cz/clanek/co-je-a-co-neni-isvs.aspx

[8] Bezpečnost síťové infrastruktury Panduit NISS - s námi je to snadné. In: [online]. [cit.2014-05-17]. Dostupné z: http://www.kassex.cz/files/default/content/NISS/PNISS-CZ-V1.30-INFO.pdf

[9] Význam bezpečnostní politiky. *SystemOnLine* [online]. 2001 [cit. 2014-05-18]. Dostupné z: http://www.systemonline.cz/clanky/vyznam-bezpecnostni-politiky.htm

[10] Analýza stavu bezpečnosti. *AEC* [online]. 2001 [cit. 2014-05-18]. Dostupné z: http://www.aec.cz/cz/sluzby/analyza-stavu-bezpecnosti

[11] Fortinet Product Matrix. In: *Fortinet* [online]. 2014 [cit. 2014-05-22]. Dostupné z: http://www.fortinet.com/sites/default/files/productdatasheets/Fortinet_Product_Matrix.pdf

[12] Multimediaexpo.cz. *Autentizace* [online]. 2013 [cit. 2014-05-24]. Dostupné z: http://www.multimediaexpo.cz/mmecz/index.php/Autentizace

[13] Configure Automatic Updates in a Non–Active Directory Environment. *Microsoft: TechNet* [online]. [cit. 2014-05-25]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc708449%28v=ws.10%29.aspx

[14] Kdo je to hacker?. *NICM* [online]. 2014 [cit. 2014-05-10]. Dostupné z: http://www.nicm.cz/kdo-je-to-hacker

[15] SVATUŠKA, Josef. VPN na platformě FortiGate. In: [online]. 2010 [cit. 2014-05-20]. Dostupné z: wh.cs.vsb.cz/sps/images/4/4a/Svatuska-VPN-na-platforme-FortiGate.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ASIC	Application-specific integrated circuit
BBU	Battery backup unit
DHCP	Dynamic Host Configuration Protocol
DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
GIS	Geografický informační systém
HTTPS	Hypertext Transfer Protocol Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet protokol
IPS	Intrusion Prevetion System
IIS	Internet Information Services
IS	Informační systém
ISVS	Informační systém veřejné správy
IT	Informační technologie
LTO	Linear Tape-Open
MAC	Media Access Control
MěÚ	Městský úřad
NAT	Network Address Translation
PAT	Port Address Translation
PoE	Power over Ethernet
SSL	Secure Sockets Layer
UPS	Uninterruptible power supply

VLAN	Virtual Local Area Network
VoIP	Voice over IP
VPN	Virtual Private Network
WSUS	Windows Server Update Services

SEZNAM OBRÁZKŮ