Implementace požadavků kybernetické bezpečnosti do specifického prostředí lokální sítě veřejné správy.

Implementation of the Requirements of Cybersecurity into the Specific Environment of the Local Network of Public Administration.

Bc. Jan Pšeja

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jan PŠEJA**
Osobní číslo:	**A10882**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Forma studia:	**kombinovaná**
Téma práce:	**Implementace požadavků kybernetické bezpečnosti do specifického prostředí lokální sítě veřejné správy**
Téma anglicky:	**The Implementation of Cybersecurity Requirements into the Specific Environment of a Public Administration Local Network**

Zásady pro vypracování:

1. **Proveďte rešerši informačních zdrojů tématu kybernetická bezpečnost v prostředí veřejné správy.**
2. **Analyzujte cílové prostředí, ve kterém bude projekt realizován.**
3. **Navrhněte způsoby změn, které povedou ke stavu požadovanému zákonem č. 181/2014 Sb..**
4. **Realizujte navržené změny v prostředí městského úřadu v Kroměříži.**
5. **Vyhodnoťte provedená opatření a proveďte diskusi nad výstupem projektu.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **SELECKÝ, Matúš. Penetrační testy a exploitace. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
2. **TRULOVE, James. Sítě LAN: hardware, instalace a zapojení. 1. vyd. Praha: Grada, 2009, 384 s. ISBN 978-80-247-2098-2.**
3. **KABELOVÁ, Alena a Libor DOSTÁLEK. Velký průvodce protokoly TCP/IP a systémem DNS. 5., aktualiz. vyd. Brno: Computer Press, 2008, 488 s. ISBN 978-80-251-2236-5.**
4. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.**
5. **KRETCHMAR, James M. Administrace a diagnostika sítí: pomocí OpenSource utilit a nástrojů. 1. vyd. Brno: Computer Press, 2004, 216 s. ISBN 80-251-0345-5.**
6. **Zákon č. 181/2014 Sb., o kybernetické bezpečnosti. In: 75/2014. 2014. Dostupné z: http://www.zakonyprolidi.cz/cs/2014-181.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **6. února 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. Mgr. Roman Jašek, Ph.D.
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 připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- 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/bakalářské 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

Práce řeší formou projektu implementaci bezpečnostních pravidel dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnost do lokální sítě městského úřadu obce Kroměříž. Bezpečnostní procesy by měly být nastaveny v souladu s legislativou a bezpečnostními standardy, jako je například řada ISO/IEC 27k. Stanovování cílů v této oblasti se přitom musí odvíjet od cílů celé organizace, a proto je nutné v případě subjektů veřejné správy a zdravotnictví uvažovat jejich specifické aspekty.

Klíčová slova:

kybernetická bezpečnost, ISO 27001, informační systém, komunikační systém, bezpečnostní politika, analýza rizik

ABSTRACT

This thesis comes in the form of the project implementation of safety rules in accordance with the requirements of Act no. 181/2014 of cyber security to the local network of the city office of the municipality Kroměříž. Security processes should be set in accordance with legislation and safety standards, such as the series ISO / IEC 27k. Setting objectives in this area, the application shall depend on the goals of the organization, and therefore it is necessary for entities of public administration and health care to consider their specific aspects.

Keywords:

Cyber security, ISO 27001, information system, communication system, public administration, security policy, risk analysis

Chtěl bych poděkovat vedoucímu práce panu doc. Mgr. Romanu Jaškovi, Ph.D. a to nejenom za cenné rady a příkladný přístup, ale především za jeho čas, věnovaný této práci.

Dále bych chtěl poděkovat své ženě Janě za veškerou podporu během mého studia.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Přijetím zákona 184/2014 Sb. o kybernetické bezpečnosti a navazujících vyhlášek došlo k posunu problematiky informační bezpečnosti na všech úrovních státní i veřejné správy. Agendové informační systémy jsou dnes páteří výkonu veřejné správy a díky těmto systémům je způsob zpracování, uchování informací organizací mnohem snazší a jejich využití mnohem efektivnější. S rostoucí závislostí na informačních technologií roste i riziko jejich zneužití nebo napadení.

Vzhledem k objemu uložených dat a rozsahu zpracování osobních údajů a přístupu k nim roste i riziko bezpečnostního incidentu a potřeba tyto aktiva vhodně chránit.

Cílem diplomové práce je navrhnout úpravu bezpečnostní politiky v souvislosti se zákonem 184/2014 v prostředí města Kroměříže. Práce je rozdělena na teoretickou a praktickou část.

V teoretické části je souhrn aktuální legislativy a norem související s kybernetickou bezpečností. Následně je hodnocena situace v rámci obcí s rozšířenou působností v území Zlínského kraje. Další kapitola je věnována možnostem zabezpečení lokálních sítí a monitoringu datových toků. Závěrem je popsáno cílové prostředí městského úřadu obce Kroměříž.

Praktická část je věnována SWOT analýze, návrhu vhodných řešení a to jak administrativních tak i technologických. Současně jsou popsány další možnosti řešení v souvislosti s probíhajícím projektem financovaných z EU fondů. Následně jsou vybraná opatření implementována v praxi a to zejména v oblasti personální – práce s pracovníky tak i v rovině technologické kdy bude popsána výměna firewallu a nasazení NetFlow monitoringu.

I. TEORETICKÁ ČÁST

1 LEGISLATIVA

Obecní úřady obcí s rozšířenou působností vznikly od 1. ledna 2003 podle Zákona č. 314/2002 Sb. o stanovení obcí s pověřeným obecním úřadem a stanovení obcí s rozšířenou působností a jsou mezičlánkem přenesené působnosti samosprávy mezi krajskými úřady a obecními úřady.

Obcí s rozšířenou působností je taktéž město Kroměříž, které takto vykonává řadu působností nejen pro svůj správní obvod, ale zpravidla i pro další obce v okolí.

Jde zejména následující agendy přenesené státní působnosti:

- evidence obyvatel,
- vydávání cestovních a osobních dokladů, řidičských průkazů, technických průkazů,
- živnostenské oprávnění,
- výplata sociálních dávek,
- sociálně-právní ochrana dětí
- péče o staré a zdravotně postižené,
- vodoprávní řízení, odpadové hospodářství a ochrana životního prostředí,
- státní správa na úseku lesů, myslivosti a rybářství
- doprava a silniční hospodářství [1]

Jde o agendy vykonávané na základě zákonů, tedy jasně a konkrétně definované činnosti vykonávané podobně na úrovni všech obcí s rozšířenou působností.

Dále obce vykonávají řadu samosprávných činností, jde zejména o správu městského majetku a služby, rozvoj a investiční činnosti v území obce a jiné.

K zajištění výkonu všech agend využívají obce zpravidla více informačních systémů, některé jsou celostátně unifikované (například činnost živnostenských úřadů), jiné se mohou značně lišit (evidence městského majetku) [2].

Ze základní legislativy České republiky v oblasti informatiky je pro provozování ISVS nejvýznamnější **zákon č. 365/2000 Sb.**[3], o informačních systémech veřejné správy ve znění pozdějších předpisů. Zákon byl novelizován následujícími právními úpravami:

- č. 517/2002 Sb.,
- č. 413/2005 Sb.,
- č. 444/2005 Sb.,

- č. 70/2006 Sb.,
- č. 81/2006 Sb.,
- č. 110/2007 Sb.,
- č. 130/2008 Sb.
- a dále navazující vyhlášky
  - **Vyhláška č. 528/2006 Sb.**, o informačním systému o ISVS Vyhláška stanovuje povinnost správcům ISVS podávat informace o provozu ISVS do informačního systému o ISVS. Dále vyhláška obsahuje informace o dostupnosti a obsahu zpřístupněných informačních systémů.
  - **Vyhláška č. 529/2006 Sb.**[4], o dlouhodobém řízení ISVS
    V této vyhlášce jsou stanoveny požadavky na strukturu, obsah informační koncepce a provozní dokumentaci ISVS.

Pro provozování ISVS jsou důležité i následující předpisy:

- **Zákon č. 101/2000 Sb.**, o ochraně osobních údajů, ve znění pozdějších předpisů,
- **Zákon č. 106/1999 Sb.**, o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- **Zákon č. 148/1998 Sb.**, o ochraně utajovaných skutečností, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek,
- **Zákon č. 227/2000 Sb.**, o elektronickém podpisu, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek.
- **Zákon č. 499/2004 Sb.**, o archivnictví a spisové službě a o změně některých zákonů
- **Zákon č. 300/2008 Sb.** o elektronických úkonech a autorizované konverzi dokumentů
- **Zákon č. 301/2008 Sb.**, kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.
- **Vyhláška č. 442/2006 Sb.**, kterou se stanoví struktura informací zveřejňovaných o povinném subjektu způsobem umožňujícím dálkový přístup

- **Vyhláška č. 64/2008 Sb.**, o formě uveřejňování informací souvisejících s výkonem veřejné správy prostřednictvím webových stránek pro osoby se zdravotním postižením (vyhláška o přístupnosti)

A dále

- **Nařízení vlády č. 495/2004 Sb.,** kterým se provádí zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu)
- **Vyhláška č. 496/2004 Sb.**, o elektronických podatelnách
- **Vyhláška č. 193/2009 Sb.**, o stanovení podrobností provádění autorizované konverzi dokumentů
- **Vyhláška č. 194/2009 Sb.**, o stanovení podrobností užívání informačního systému datových schránek
- Metodický pokyn řízení kvality informačních systémů veřejné správy

1.1 Zákon č. 365/2000 Sb. o informačních systémech veřejné správy

Zákon o informačních systémech veřejné správy stanoví práva a povinnosti správců informačních systémů veřejné správy a dalších subjektů, jež souvisejí s vytvářením, užíváním, provozem a rozvojem informačních systémů veřejné správy. Dále upravuje působnost Ministerstva vnitra jako ústředního správního úřadu pro tvorbu a rozvoj informačních systémů veřejné správy. Jednou z povinností správců informačních systémů veřejné správy je zavést a trvale uplatňovat jejich dlouhodobé řízení[4]. Orgány veřejné správy vytvářejí a vydávají informační koncepci, uplatňují ji v praxi a vyhodnocují její dodržování. V informační koncepci pak orgány veřejné správy stanoví své dlouhodobé cíle v oblasti řízení kvality a bezpečnosti spravovaných informační systémů a vymezí obecné principy jejich pořizování, vytváření a provozování. Ke všem provozovaným informační systémům je nutno vytvořit a vydat provozní dokumentaci. Obsah a strukturu dokumentů, jejich rozsah a postupy orgánů veřejné správy je stanoven vyhláškou 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy). K této vyhlášce byl Ministerstvem vnitra České republiky publikován komentář jako pomůcka pro zpracování požadované dokumentace. Komentář obsahuje příklady zpracovaných informačních koncepcí pro typické orgány veřejné správy: ústřední orgán státní správy,

obec s rozšířenou působností, obec s pověřeným obecním úřadem a obec, která vykonává přenesenou působnost pouze v základním rozsahu. Zákon vytváří podmínky, aby kvalitní informační systémy mohly být dobrým nástrojem pro výkon veřejné správy.

1.2 Zákon č. 181/2014 Sb. o kybernetické bezpečnosti

V návaznosti na výše uvedený zákon byl od roku 2013 připravován zákon o kybernetické bezpečnosti. Návrh zákona projednala v červnu 2013 vláda Petra Nečase, aby byl následně 2. ledna 2014 předložen vládou Jiřího Rusnoka poslanecké sněmovně k projednání. K prvnímu čtení návrhu zákona o kybernetické bezpečnosti došlo 14. února 2014, po projednání ve výborech poslanecké sněmovny parlamentu České republiky došlo dne 18. června 2014 k hlasování a zákon byl 161 hlasy přijat. Následně byl projednán a schválen Senátem i podepsán prezidentem republiky. Zákon vstoupil v platnost k 1. lednu 2015.

Zákon definuje v návaznosti na další předpisy Evropské unie a další normy (zejména skupina ISO 27000) požadavky na kybernetickou bezpečnost a současně definuje požadavky pro její splnění jak pro státní, tak i pro privátní sféru. V rámci zákona jsou taktéž nově ustanoveny dvě organizace – vládní CERT, který má v kompetenci informační systémy na úrovni vlády, ministerstev a obecně státní správy a národní CERT, který se doplňkově zabývá informačními systémy subjektů privátní sféry.

O výsledné podobě právní úpravy rozhoduje nejen znění zákona ale i podoba jeho prováděcích předpisů (vyhlášek a opatření obecné povahy). Mnohem významnější bude jejich naplňování v praxi i celkové klima, které se kolem kybernetické bezpečnosti vytvoří.

V ideálním stavu bude celá komunita (státní i privátní sektor) bojující za kybernetickou bezpečnost jednotná a „potáhne za jeden provaz“. Naopak nejhorším možným výsledkem by byl vznik názorové nekonzistentnosti celé komunity a její rozpad na několik vzájemně soupeřících, mezi sebou nekomunikujících skupin. Nebo („typické“) sklouznutí do stavu, kdy celý boj za kybernetickou bezpečnost zdegeneruje do dalšího papírování a byrokratické zátěže bez reálných dopadů na to, co se děje v celém on-line prostoru [5].

Cílem zákona je zejména snažit se ochránit tu část infrastruktury, která je pro fungování státu významná a jejíž narušení by vedlo k poškození nebo ohrožení zájmů České republiky. Zákon nemá za cíl řešit všechna rizika v kyberprostoru, např. informační kriminalitu (CyberCrime), porušování autorských práv, různé podvodné aktivity, krádeže elektronických dat, šíření závadného elektronického obsahu atd.

1.2.1 Členění infrastruktury

Zákon definuje dvě skupiny organizací a jejich informačních systémů:

Kritická informační infrastruktura (KII) - prvek nebo systém prvků výrobních a nevýrobních systémů a služeb, jejichž nefunkčnost by měla závažný dopad na bezpečnost státu, ekonomiku, veřejnou správu a zabezpečení základních životních potřeb obyvatelstva.

Významný informační systém (VIS) - informační systém spravovaný orgánem veřejné správy, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon činnosti veřejné správy.

Společně se zákonem byla zveřejněna vyhláška definující soubor činností a opatření, kterým musí v souladu s tímto zákonem každá dotčená organizace vyhovět. Součástí vyhlášky je i definice organizací s významným informačním systémem.

Obě definované skupiny organizací nemají společné prvky, tedy významné informační systémy (VIS) z definice nejsou součástí kritické informační infrastruktury (KII). S čímž souvisí i očekávání, že při narušení bezpečnosti významných informačních systémů mohou být důsledky sice „významné“, ale nikoli ještě „kritické“ (jako u systémů z kritické informační infrastruktury). Tomu pak odpovídají i určité rozdíly v ukládaných povinnostech: ty jsou u prvků kritické informační infrastruktury přeci jen vyšší (přísnější), než u „pouze“ významných informačních systémů.

Každá dotčená organizace musí aplikovat soubor preventivních bezpečnostních opatření a plnit další reaktivní činnosti dle zákona. Bezpečnostní opatření se dělí na organizační a technická.

Organizačními opatřeními se rozumí soubor procesů k zajištění vyšší bezpečnosti. Znění zákona se významně shoduje s normou ISO 27000. Technickými opatřeními se rozumí soubor technických nástrojů k zajištění vyšší bezpečnosti. Typicky se jedná o správnou implementaci a správu Firewallů, IPS sond, NetFlow sond, MDM systémů, kryptografických prostředků, ochrany proti škodlivému software, SIEM nástrojů a dalších bezpečnostních prostředků.

1.2.2 Požadavky plynoucí ze zákona

V rámci zákona se pracuje s pojmy „událost“ a „incident“, které jsou definovány takto:

- Kybernetická (bezpečnostní) událost - událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.
- Kybernetický (bezpečnostní) incident/událost - představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací.

Zákon o kybernetické bezpečnosti stanovuje povinnost detekce a zejména hlášení kybernetických bezpečnostních incidentů.

V základní rovině jsou požadavky na kritickou informační infrastrukturu i významné informační systémy identické. V některých konkrétních bodech jsou u kritické informační infrastruktury zvýšené požadavky na bezpečnost oproti významným informačním systémům.

Systémy z kritické informační infrastruktury (na rozdíl od významných informačních systémů) budou muset mít vlastního manažera kybernetické bezpečnosti, architekta kybernetické bezpečnosti, auditora kybernetické bezpečnosti, garanta svých aktiv, a dokonce celý „výbor pro řízení kybernetické bezpečnosti“. Jde ale pouze o „role“ (které někdo plní), nemusí se nutně jednat o „celé“ zaměstnance, kteří by nedělali nic jiného.

Mezi významné informační systémy by měla patřit například čtveřice základních registrů (ROB, ROS, RUIAN a RPP), včetně jejich „obalu“ (ISZR), a také převodníku ORG. Dále třeba všechny agendové informační systémy, které slouží jako editační (skrze které editoři zapisují referenční údaje do základních registrů). Dalším systémem budou třeba datové schránky (ISDS), Portál veřejné správy (PVS), stejně jako centrální registr vozidel (CRV), centrální registr řidičů, registr pojištěnců všeobecného zdravotního pojištění, Rejstřík trestů, či třeba systémy z oblasti sociálního zabezpečení a mnohé další.

Významné informační systémy jsou definovány tak, že jejich správcem musí být některý orgán veřejné moci. To by mělo vylučovat jakékoli (informační či komunikační) systémy z privátního sektoru.

Nicméně privátní systémy se mohou stát (a některé nejspíše i stanou) součástí kritické informační infrastruktury, kde omezení jen na veřejný sektor není, a ani by nemělo smysl. Kritická informační infrastruktura by měla být určitou podmnožinu „obecné“ kritické infrastruktury vybranou s ohledem na potřebu kybernetické bezpečnosti. A do této „obecné“ kritické infrastruktury již dnes patří řada systémů a prvků z privátního sektoru,

jde například o technologické prvky pevných i mobilních sítí elektronických komunikací (jejich ústředny, datová centra i třeba BTS pokrývající „strategické lokality“). Nebo třeba některé velké banky, velké pojišťovny atd.

Pravdou je, že předkladatel návrhu zákona (Národní bezpečnostní úřad) se nikdy netajil svou snahou minimalizovat „zásahy“ zákona do privátního sektoru. Důvodem je zřejmě obava NBÚ, aby nebyl nařčen z nějakého špehování, monitorování či obdobných aktivit, vnímaných širší veřejností čím dál tím negativněji. Lze se ovšem obávat, že bez určitých zásahů a omezení to nebude možné - dnešní „kyberprostor“ je totiž v rozhodující míře v rukou privátního sektoru. A tak se i on stává terčem nejrůznějšího ohrožení, útoků atd.

1.2.3 Navazující vyhlášky

Zákon o kybernetické bezpečnosti doplňuje koncem roku 2014 vydané nařízení vlády a vyhlášky definující kritickou infrastrukturu i významné informační systémy.

Nařízení vlády č. 315/2014, kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

Vyhláška č. 316/2014 o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)

Vyhláška č. 317/2014 o významných informačních systémech a jejich určujících kritériích

1.3 ISO 27001 - Systém řízení informační bezpečnosti

Systém řízení informační bezpečnosti (Information security management systém - ISMS) je sada pravidel zabývajících se řízením informační bezpečnostní politiky nebo rizik souvisejících s IT a je definována v rámci ISO normy 27001

Základním principem ISMS je návrh organizace na zavedení a udržování uceleného souboru politik, postupů a systémů k řízení rizik svých informačních aktiv. Tímto lze dosáhnout přijatelné úrovně informační bezpečnosti. Stejně, jako u všech procesů řízení, musí ISMS zůstat účinný a efektivní v dlouhodobém horizontu, přizpůsobovat se změnám ve vnitřní organizaci a vnějšímu prostředím. Proto je u toho procesu řízení využit přístup "Plan-Do-Check-Act" (PDCA), tedy „Plánuj-Dělej-Kontroluj-Jednej“:

- fáze „plánu“ souvisí s navrhováním ISMS, posouzením bezpečnostních informačních rizik a výběrem vhodných kontrol

- výkonná fáze „do“ zahrnuje implementaci a provozování kontroly
- cílem kontrolní „check“ fáze je přezkoumat a posoudit výkon (efektivitu a účinnost) ISMS
- ve fázi změny „act“ jsou provedeny změny v případě potřeby tak, aby ISMS fungovala opět na špičkový výkon

Podle bezpečnostních expertů a statistik je nutno zajistit řešení následujících témat:

- administrátoři bezpečnosti informačních technologií musí věnovat přibližně jednu třetinu času řešení technických aspektů, zbývající dvě třetiny budou vynaloženy na vytváření politik a postupů provádění bezpečnostních hodnocení a analýze rizik, řešení krizového plánování a podpoře povědomí o bezpečnosti;
- bezpečnost závisí více na lidech než na technologiích;
- zaměstnanci jsou daleko větší hrozbou pro bezpečnost informací, než cizinci zvenčí;
- bezpečnost je jako řetěz - jen tak silný jako jeho nejslabší článek;
- stupeň zabezpečení závisí na třech faktorech: míře přijatelného rizika, funkčnosti systému a na nákladech vynaložených na bezpečnost;
- bezpečnost není stav, ale běžící proces.

Tyto skutečnosti nutně vedou k závěru, že informační bezpečnost je především otázkou řízení a nikoli čistě technologický problém.

Zřízení, údržba a průběžná aktualizace ISMS poskytují silný signál, že společnost používá systematický přístup k identifikaci, vyhodnocování a řízení informačních bezpečnostních rizik.

Kritické faktory ISMS:

- Důvěrnost: Ochrana informací před nepovolanými osobami.
- Integrita: Ochrana informací před modifikací neoprávněnými uživateli.
- Dostupnost: Poskytování informací všem oprávněným uživatelům.

Skutečnost že společnost bude schopna úspěšně řešit důvěrnosti informací, integritu a dostupnost má za důsledek:

- kontinuitu fungování
- minimalizace škod a ztrát
- respekt k obrazu organizace

- dodržováním právních předpisů [6]

Veřejné nebo státní organizace, velké firmy, banky a finanční instituce, telekomunikační operátoři, nemocnice a zdravotní instituce mají mnoho velmi vážných důvodů pro řešení informační bezpečnosti. Právní a regulační požadavky, které jsou zaměřeny na ochranu citlivých nebo osobních údajů, jakožto i obecné požadavky bezpečnosti postupně donutí výše zmíněné organizace věnovat maximální pozornost a prioritu informační bezpečnosti a snížení souvisejících rizik [7].

Za těchto okolností je vývoj a implementace samostatného a nezávislého procesu řízení informační bezpečnosti - a to ISMS - jedinou využitelnou alternativou.

Rozvoj ISMS na základě normy ISO 27000 zahrnuje následujících šest kroků:

- Definice bezpečnostní politiky,
- Definice ISMS rozsahu,
- Posouzení rizik (jako součást řízení rizik),
- Řízení rizik,
- Výběr vhodných kontrol,
- Prohlášení o aplikovatelnosti

Kritické faktory pro úspěch informační bezpečnosti:

- mají kontinuální, neotřesitelnou, viditelnou podporu a zapojení vrcholového managementu organizace
- musí být řízena centrálně na základě společné strategie a politiky v celé organizaci
- musí být nedílnou součástí celkového řízení organizace a odrážet přístup organizace k řízení rizik, definici a kontrole cílů, kontrol a stupně potřebné jistoty
- bezpečnostní cíle a činnosti vycházejí z firemních cílů a požadavků a způsobu řízení činnosti
- je potřeba provádět pouze nezbytné úkoly a vyhnout se nadměrné kontrole a plýtvání cennými zdroji
- musí být plně v souladu s organizační filozofií a myšlením tím, že systém, který místo toho, aby bránil lidem v použití informačních technologií, jim umožní mít tyto pod kontrolou
- musí být součástí průběžného školení a zvyšování povědomí zaměstnanců a současně se vyhnout používání kázeňských opatření a "policejních" nebo "vojenských" postupů

- jde o nikdy nekončící proces

1.4 Zákon 181/2014 a informační systémy veřejné správy

Dopady zákona 181/2014 Sb.[8], o kybernetické bezpečnosti na provoz informačních systémů veřejné správy.

Systém	Povinná osoba dle § 3 písm.	Ano nebo ne ?
Poskytovatel služeb elektronických komunikací	**a)**	**Zřídka**
Subjekt zajišťující síť elektronických komunikací	**a)**	**Zřídka**
Subjekt zajišťující významnou síť	**b)**	**Spíše vůbec**
Správce informačního systému kritické informační infrastruktury	**c)**	**V praxi ne**
Správce komunikačního systému kritické informační infrastruktury	**d)**	**V praxi ne**
Správce významného informačního systému	**e)**	**Ne**

Tabulka 1 – Dopad zákona 181/2014 na obce [9]

Z výše uvedeného plyne, že Zákon o kybernetické bezpečnosti se měst a obcí aktuálně týká spíše okrajově a ve specifických případech. Informačních systémů obcí se ovšem týká zákon č. 365/2000 Sb., o informačních systémech veřejné správy a z něj plynoucí povinnost zabezpečit používané informační systémy dostatečným způsobem. Seznam organizací dotčených Zákonem o kybernetické bezpečnosti je dán vyhláškou a je možné očekávat, že v budoucnu bude rozšířen i o města a obce. Povinnost zajišťovat bezpečnost

informací mají obce již dlouho u spravovaných a provozovaných informačních systémů veřejné správy. Systematicky řídit bezpečnost informací je tak bez ohledu na legislativu rozumné a nezbytné.

Požadavky definované v zákoně o kybernetické bezpečnosti na zabezpečení informační systémů lze aplikovat na datové sítě a provozované informační systémy obcí s rozšířenou působností. Dojde tak ke kvalitativnímu zlepšení bezpečnosti bez nutnosti splnit striktně všechny požadavky určené pro významné informační systémy.

Z provedených rešerší plyne, že případy případných kybernetických útoků na datové sítě úřadů nejsou v současnosti ve veřejných zdrojích dokumentovány. Domnívám se, že k nim dochází, ale jejich následky nebývají významné, případně nejsou publikovány a pro širokou veřejnost tak nejsou mediálně zajímavé.

Okrajově dokumentovány jsou útoky na weby řady českých bank [10], které proběhly před několika lety prakticky bez povšimnutí. Tato téma tedy nejsou mediálně zajímavá a dosah případného dokonaného kybernetického útoku na síť veřejné správy (v tomto případě městského úřadu) je minimálně sporný. Prostředky datové sítě úřadu budou pro případné útočníky spíše prostředkem pro další útok „někam dále“ – zneužití pro rozesílání spamu nebo součást DDoS sítě. Data městského úřadu mají cenu spíše v místním kontextu (okresu případně kraje) a lze je asi získat snadněji prostřednictvím sociálního inženýrství (nebo korupce) než kybernetickým útokem.

Problematika kybernetické bezpečnosti není jen věcí technologickou ale především problémem personálním. Základní změnou tak musí být zapojení všech pracovníků úřadu tedy tajemníka, vedoucích odborů i řadových pracovníků úřadu a dále i volených zástupců, zejména starosty a členů rady města tak i zastupitelů (zejména opozičních).

Kybernetická bezpečnost není „konečným stavem“, kterého je možné dosáhnout, jde o dlouhodobý proces – cestu, který je potřeba trvale řešit. Cílem je zmenšení možného terče a minimalizace následků případného kybernetického útoku. Smyslem tedy je při akceptovatelné výši investic dosáhnout takového stavu, kdy pro případné útočníky nebudeme zajímaví nebo případný útok dokážeme rychle detekovat a minimalizovat jeho následky.

Administrativní změnou tak tedy musí být vytvoření takového stavu, kdy bude možné dlouhodobě plánovat investice a s tím související změny v informačních systémech úřadu. Což souvisí zejména s trvalou podporou politiků – zastupitelů a to jak koaličních tak

zejména opozičních. Ač je kybernetická bezpečnost mediálně nepříliš zajímavé a těžce popsatelné téma tak moderní transparentní úřad je také informačně – technologickou záležitostí. Trvalá podpora politiků umožní strategické dlouhodobé plánování, významným prvkem všech projektů realizovaných z EU fondů je totiž pětiletá udržitelnost, tedy doba po kdy výstup projektu musí být používán „tak jak je“. Po skončení udržitelnosti dojde často i ke konci morální životnosti zejména hardware ale často i software a následně je nutné řešit obnovu takových technologií a to již zcela z finančních prostředků města.

Jak je popsáno v úvodní části, zda se, že město Kroměříž je jednou z mála obcí s rozšířenou pravomocí ve Zlínském kraji, které nemají jasně a průběžně definovaný rozpočet na informační technologie.

1.5 Řešení kybernetické bezpečnosti v obcích Zlínského kraje.

V rámci této práce jsem oslovil v rámci Zlínského kraje všechny obce s obecními úřady s rozšířenou působností s cílem získat „příklad dobré praxe“ v oblasti bezpečnosti.

Ve Zlínském kraji existuje celkem 13 obcí s rozšířenou působností, které se mezi sebou liší především počtem obyvatel a s tím souvisejícím počtem úředníků a velikostí úřadu. Rozsah vykonávaných agend je totožný a je dán především zákonem – jde tedy o přenesenou působnost.

S velikostí úřadu souvisí taktéž rozsah informačních technologií, jejich personální zabezpečení a usazení v rámci úřadu.

Všechny obce jsem oslovil s dotazem na zkušenost s monitoringem datových toků uvnitř sítě (tedy sledování NetFlow) a zajištění autorizace zařízení v rámci sítě (autorizace podle 802.1x). A to jak již existující řešení nebo případně blízké plány (například v souvislosti s projekty financovanými Evropskou unií).

Obec	Obyvatel	NetFlow	Firewall	Komentář
Bystřice pod Hostýnem	8393	ANO	Linux	Plánují sledování NetFlow, vlastní FlowMon sondu, ale dosud aktivně nenasadili.

Holešov	11 726	NE	Linux	Správu IT outsourcují
Kroměříž	28 921	NE	Kerio / Mikrotik	Obměna technologií plánována v rámci projektu z IOP výzvy 22.
Luhačovice	5 112	NE	Linux	
Otrokovice	18 230	NE	Linux	Plánovali v rámci EU projektu, zrušen pro nedostatek financí. Nyní neplánují.
Rožnov pod Radhoštěm	16 672	ANO	Linux	Provozují PRTG monitoring, plánují pořízení FlowMon sondy v rámci EU projektu.
Uherské Hradiště	25 266	ANO	FortiGate	V rámci EU projektu plánují pořízení NetFlow sond a kolektoru s analýzou provozu.
Uherský Brod	16 720	ANO	Linux / FortiGate	Provozují monitoring na bázi SNMP, o nasazení NetFlow diskutují, o 802.1x neuvažují z důvodů komplikovanosti a souvisejících problémů.
Valašské Klobouky	5 039			Bez odpovědi
Valašské	22 733	NE	Linux	Aktuálně neprovozují,

Meziříčí				krátkodobě neplánují, dlouhodobě nevylučují.
Vizovice	4 698			Bez odpovědi
Vsetín	26 668			Bez odpovědi.
Zlín	75 278	ANO	Linux	Externě outsourcuje provoz a monitoring sítě, sleduje bezpečnostní incidenty, testuje kolektor na bázi opensource, plánuje pořízení komerčního a řešení pro snížení dopadů DDoS útoků. Autorizaci 802.1x neplánují. Bezpečnost sítě prověřují penetračními testy.

Tabulka 2 – Přehled odpovědí obcí Zlínského kraje

Ze třinácti dotázaných obcí s rozšířenou působností ve Zlínském kraji odpovědělo celkem deset včetně města Kroměříže, tři obce nereagovaly. Dotaz byl přímo adresován konkrétní osobě – informatikovi úřadu.

Pouze dvě obce využívají služeb outsourcingů a to Holešov, který správu svých informačních technologií svěřil zcela externímu subjektu a vlastní informatiky – zaměstnance nemá a město Zlín, které outsourcuje správu své metropolitní sítě, ale informatiky pro chod informačních systému úřadu má. Zlín je na rozdíl od ostatních dotázaných obcí navíc statutárním městem a je z pohledu personálního i ekonomického s ostatními obcemi nesrovnatelný. Z dotazu byl taktéž cíleně vynechán krajský úřad, z hlediska významu, velikosti, personálního zajištění i ekonomických možností je totiž s kteroukoliv jinou obcí nesrovnatelný.

Z odpovědí plyne, že kybernetickou bezpečnost vnímají všichni informatici jako významnou. Opatření pro posílení kybernetické bezpečnosti (například zavedení monitoringu datových toků - NetFlow) jsou ovšem poměrně nákladná – vyžadují spolupracující aktivní prvky a další komponenty, což vyžaduje výměnu jinak plně funkčních prvků. O potřebě investovat tímto směrem je ovšem nutné přesvědčit vedení příslušných obcí což bývá problematické.

Obecně lze říct, že úřady jsou technicky vybaveny docela dobře. V současné době je potřebný nad síťovým provozem nepřetržitý 24 hodinový dohled, ale skoro nikdo to nedělá, především z personálního důvodu. Není totiž možné přijmout další potřebné specialisty – typu bezpečnostní manažer, bezpečnostní IT technik a vybavit ho i příslušnými pravomocemi.

Nasazení souhrnu účinných bezpečnostních opatření představuje pouze „zmenšení terče“ pro útočníky, riziko existuje vždy [11].

Dosud publikované bezpečnostní problémy se zatím v České republice dotkly „jen“ některých telefonních operátorů nebo bank. A úspěšně se na ně zapomnělo. Možná to zatím není ani zajímavé téma pro novináře.

I z těchto důvodů není téma kybernetické bezpečnosti u vedení obcí a měst nijak populární a necítí potřebu do této oblasti významně investovat. Pokud již k investici dojde, jde o projekty řešené s podporou evropský fondů – aktuálně například probíhají projekty z Integrovaného operačního programu, výzvy 22. Z oslovených měst řeší projekt čtyři – Zlín, Uherské Hradiště, Uherský Brod a Kroměříž. Otrokovice o projekt taktéž usilovaly, ale po volbách na podzim 2014 došlo ke změně investičních priorit a od projektu ustoupily.

2 MOŽNOSTI ZABEZPEČENÍ DATOVÉ SÍTĚ

Zabezpečení sítě se skládá z politik, pravidel a definic přijatých správci sítě k povolení oprávnění nebo zabránění neoprávněných přístupů. Zabezpečení sítě řeší komunikaci mimo síť, přístup ke sdíleným zdrojům i zajištění koncových stanic. Uživatelé mají přiřazeny identifikátory a hesla, která jim umožňují přístup k informacím a aplikacím podle jejich oprávnění.

Další částí zabezpečení je dohled nad sítí, tedy monitorování přenášených dat mezi jednotlivými uzly uvnitř sítě i vzájemně mezi sítěmi, například přes Internet. Monitorování a dohled nad sítí umožňuje sledovat a analyzovat jednotlivé datové toky, vhodně optimalizovat rozložení sítě, nebo naopak hledat případná slabá místa. Ať už jde o slabá místa technická, například nedostačující kapacita datových spojů nebo lidská, například nepovolenou komunikaci / transport dat (například odesílání nebo stahování abnormálního množství dat z Internetu). Monitoring se často provádí tajně, na základě pověření organizace, jednotlivce (to ve vnitřních sítích) nebo na základě požadavku státních orgánů (policie, soud). Každá z takových aktivit může pochopitelně narážet na limity zákona o ochraně osobních údajů. Je tedy kupříkladu možné sledovat objem datových toků mezi jednotlivými komunikujícími zařízeními / uzly, ale již je problematické analyzovat obsah této komunikace nebo jej kdekoliv ukládat.

Počítačové a síťové programy pro monitoring a dozor jsou dnes rozšířené a téměř veškerý internetový provoz je nebo může být potenciálně sledován, a to i nezákonně.

Bezpečnou komunikaci lze zajistit pomocí „end-to-end“ šifrování (E2EE), tedy nepřetržité ochrany dat přenášených mezi dvěma komunikujícími stranami. Vysílací strana zajišťuje šifrování dat tak, aby je mohl dešifrovat pouze cílový příjemce. End-to-end šifrování zabraňuje zprostředkovatelům, jako jsou poskytovatelé internetových nebo aplikačních služeb, aby mohli sledovat nebo manipulovat s obsahem komunikace. Příkladem takového šifrování je PGP pro e-mail, ZRTP pro telefonii a TETRA pro rádio.

Nastavení pravidel pro komunikaci přes firewall se běžně označuje termínem „bezpečnostní politika firewallu“. Bezpečnostní politika zahrnuje nejen samotná pravidla komunikace mezi sítěmi, ale u většiny dnešních produktů také různá globální nastavení, překlady adres (NAT), instrukce pro vytváření šifrovaných spojení mezi šifrovacími branami (VPN), vyhledávání možných útoků a protokolových anomálií (IDS), autentizaci a někdy i autorizaci uživatelů a správu šířky přenosového pásma (bandwidth management).

2.1 Firewally

Firewall je síťové zařízení pro řízení zabezpečení a přístupových pravidel sítě. Firewall je obvykle nakonfigurován tak, aby odmítnul žádosti o přístup z neověřených či nepovolených zdrojů a zároveň umožňuje akce ze zdrojů uznávaných a povolených. Zásadní význam firewallu roste v oblasti bezpečnosti sítí souběžně s neustálým nárůstem kybernetických útoků[12].

Firewall může být software nebo hardware založený na bezpečnostním systému, který kontroluje příchozí a odchozí síťový provoz na základě analýzy datových paketů a určení, zda by měly nebo neměly být povoleny prostřednictvím aplikované sady pravidel. Firewall vytváří bariéru mezi důvěryhodnou tedy bezpečnou interní sítí a jinými sítěmi (např. Internetem) u kterých se nepředpokládá, že by byly bezpečné a důvěryhodné. Základní softwarový firewall je dnes již běžnou součástí nejrozšířenějších operačních systémů. Je taktéž součástí většiny bezdrátových přístupových bodů.

Firewally se během svého vývoje rozdělily zhruba do následujících kategorií:

- Paketové filtry - jde o filtry první generace (první v roce 1988). Paketové filtry provádějí kontrolu nad jednotlivými datovými pakety, které jsou přenášeny mezi koncovými zařízeními. Paketové filtry nesledují, zda je konkrétní paket součástí existujícího toku provozu (to znamená, že nejsou uloženy žádné informace o stavu spojení). Místo toho filtruje každý paket pouze na základě informací obsažených v paketu samém (nejčastěji pomocí kombinace zdrojové a cílové adresy paketu, jeho protokolu a pro TCP a UDP číslem portu). Filtrování pracuje na prvních třech vrstvách referenčního modelu OSI. Výhodou je vysoká rychlost zpracování.
  Typickými představiteli jsou ipchains v linuxovém jádře verze 2.2.
- Stavové paketové filtry – jsou filtry druhé generace (1990), oproti paketovým využívají informace až do 4 (transportní) vrstvy modelu OSI. Proti první generaci se navíc určuje, zda paket je začátek nového připojení je součástí již existujícího připojení nebo není částí žádného spojení.
  Typickým představitelem jsou iptables v linuxovém jádře od verze 2.4.
- Aplikační brány – filtr třetí generace (1994), filtrace probíhá na aplikační vrstvě a firewall tak může „vidět“ do vybraných aplikací nebo protokolů (např. HTTP, FTP, DNS a dalších).

Zásadní výhodou je vysoké zabezpečení známých protokolů, nevýhodou je náročnost na použitý hardware. Aplikační firewally jsou schopny zpracovat mnohem méně spojení a mají mnohem vyšší zpoždění.

2.2 Proxy

Proxy server je specializovaný software zajišťující komunikaci z jedné sítě do druhé a to obvykle provoz HTTP a HTTPS. Provoz může být ukládán (obvykle na lokální disk) a současně i logován (kdo, kam a kdy). Při přístupu na stejné URL jsou pak data (jsou-li ještě platná) čtena z lokálního disku místo ze zdrojového počítače. A může působit jako firewall tím, že reaguje na pravidla pro spojení případně pravidla pro cílové webové adresy.

2.3 Monitoring provozu

Při on-line monitorování provozu můžeme analyzovat provoz v rámci aktivního prvků nebo na firewallu. Výstup monitoringu můžeme využít pro analýzu vytížení sítě nebo pro detekci anomálií a možných chyb nastavení jiných potíží. Předpokladem je ovšem schopnost sledovat probíhající provoz, k tomu může sloužit řada řešení.

2.3.1 Span port

Switch Port Analyzer (SPAN) port je typicky využíván pro přesměrování provozu za účelem monitorování. Jedná se o port v aktivním prvku, nastaveném tak aby kopíroval odchozí/příchozí data z jednoho nebo více portů na určený (span) port. Výhodou je jednoduchost instalace pouhým nastavení aktivního prvků. Nevýhodou je možnost provozovat pouze jeden takový port v rámci aktivního prvku a při přesměrování více portů může objem provozu rychle překročit datovou propustnost span portu.

2.3.2 Hub

Hub (nebo také rozbočovač) se pro sdílení provozu na síti vkládá většinou v síťové topologii mezi 2 switche, router a switch, server a switch apod. Jelikož dnešním standardem v lokálních sítích je plně duplexní gigabit není řešení s hubem vhodné. Z konstrukce hubu vyplývá omezení na poloduplexní provoz, což významně degraduje propustnost lokální sítě.

2.3.3 NetFlow / sFlow

NetFlow je v současnosti nejrozšířenější průmyslový standard vyvinutý společností Cisco pro měření a monitorování počítačových sítí na základě IP toků[13]. Tok je v terminologii NetFlow definován jako sekvence paketů se shodnou pěticí údajů: cílová/zdrojová IP adresa, cílový/zdrojový port a číslo protokolu. Pro každý tok je zaznamenávána doba jeho vzniku, délka jeho trvání, počet přenesených paketů a bajtů a další údaje. NetFlow statistiky vytvořené nad IP provozem poskytují informace o tom, kdo komunikoval s kým, kdy, jak dlouho, jak často, nad kterým protokolem a kolik bylo přeneseno dat.

Obrázek 1 – Princip NetFlow statistik

Řešení založené na NetFlow se skládá ze tří částí: monitoringu průtoku dat, kolektoru naměřený dat a jejich analýzy. Aktivní prvky, které podporují NetFlow mohou shromažďovat statistické údaje provozu na všech rozhraních, kde je monitoring povolen a průběžně exportovat statistické záznamy do alespoň jednoho kolektoru. Kolektor je obvykle jeden centrální server sloužící pro shromažďování všech záznamů. Analýza dat následně zjišťuje obvyklé charakteristiky datových toků a hledá komunikační anomálie.

NetFlow shromažduje informace z prvních tří OSI vrstev[13], tok dat pak definuje jako sedmici hodnot: rozhraní, zdrojová a cílová IP adresa, protokol, zdrojový a cílový port (pro TCP a UDP, 0 pro ostatní) a typ služby.

Aktivní prvek udržuje tabulku aktivních toků a odešle záznam o průtoku, až zjistí, že tok je ukončen. Alternativně mohou být statistiky odesílány v pevném a pravidelném intervalu, i když tok stále pokračuje.

3 CÍLOVÉ PROSTŘEDÍ

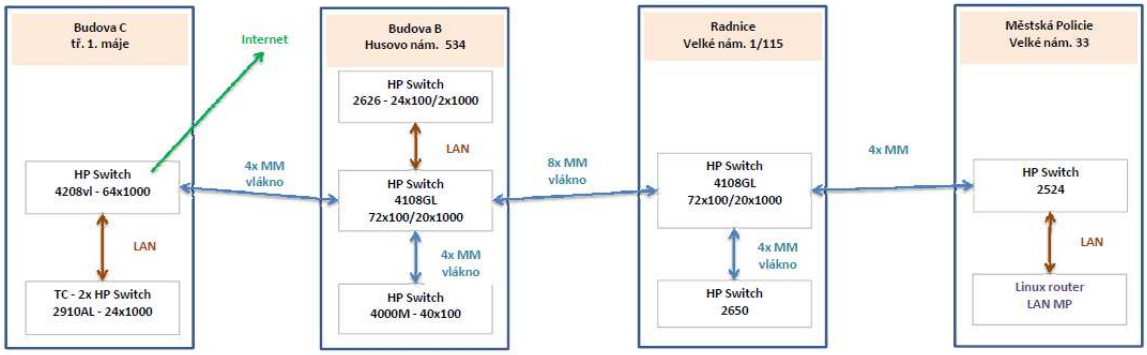
Projekt bude realizován v prostředí lokální datové sítě městského úřadu v Kroměříži. Tento sídlí ve třech lokalitách – na Velkém náměstí v budově číslo popisné 115 – sídlo radnice, v budově číslo popisné 33 – sídlo Městské policie a dále v komplexu tří sousedících a propojených budov na ulici Tř. 1. Máje 3191 (budova „C“), Tř. 1. Máje 533 (budova „D“) a Husovo náměstí 534 (budova „B“).

Město Kroměříž je obcí s rozšířenou působností, zajišťující služby přenesené působnosti (tedy dané zákony České republiky) pro samotné město Kroměříž a dalších 45 obcí a měst ve spravovaném území.

Město řídí 27 volených zastupitelů, z jejichž středu vzniká devíti členná rada města včele se starostou města. Nejvyšším představitelem úřadu je tajemnice města. Organizačně je aktuálně městský úřad členěn do devíti odborů, desátý – Kancelář úřadu, pod kterou aktuálně patří i oddělení informatiky je podřízený přímo tajemnici města.

3.1 Lokální datová síť

Lokální síť úřadu byla po dílčích etapách vybudovaná mezi roky 2000 (základ sítě v budově radnice) až po rok 2008 (připojení budovy „C“). Významným milníkem byla reforma státní správy v roce 2002, kdy od 1. 1. 2003 došlo k převodu řady činností z končících okresních úřadů právě na nově definované ORP . Tímto krokem došlo k dvojnásobnému nárůstu počtu úředníků a s tím souvisejícímu nárůstu objemu i složitosti IT technologií.



Obrázek 2 – Schéma lokální sítě města Kroměříž

Infrastruktura úřadu je v současnosti postavena na aktivních prvcích společnosti Hewlett-Packard různého stáří a odlišných technických možností. Všechny prvky podporují management z příkazové řádky, management prostřednictvím web přístupu (nutností je instalovaná podpora JVM) nebo SNMP sledování. Propojení mezi budovami je realizováno optickými vlákny v provedení multimode . Tato technologie byla v době realizace v roce 2004 vybrána vzhledem k cenové dostupnosti, vnější optické trasy jsou vedeny v HDPE trubkách, vnitřní pak v lištách.

Označení	**Počet portů**			**Podpora NetFlow**
	100 Mbit	1Gbit	SFP/Optika	
HP ProCurve Switch 4108GL	72	20	3	Ne
HP ProCurve Switch 4108GL	72	20	3	Ne
HP ProCurve Switch 4000M	40		1	Ne
HP ProCurve 2910al-24G Switch		24		Ano
HP ProCurve 2910al-24G Switch		24		Ano
HP ProCurve Switch 4208vl		68	1	Ne
HP ProCurve 2626	24	2		Ne
HP ProCurve Switch 2650	48	1	1	Ne
HP ProCurve Switch 2524	24		1	Ne

Tabulka 3 – Přehled aktivních prvků v síti

Všechny výše uvedené aktivní prvky jsou umístěny v samostatných rozvaděčích spolu s další pasivní infrastrukturou (zakončení strukturované kabeláže, optiky, telefonních linek a další). Rozvaděče jsou většinou umístěny v kancelářích informatiků, jiných pracovníků úřadu nebo v dalších uzavřených prostorách. Výjimkou je rozvaděč v prvním patře budovy městské policie, který je volně na chodbě.

3.2 Technologické centrum

Klíčové aplikační servery jsou od roku 2012, kdy došlo v rámci projektu financovaného z EU fondů [14] k vybavení nové serverové místnosti – tzv. technologického centra, provozovány jako virtualizované. V rámci projektu došlo k pořízení dvou rozvaděčů, osazených celkem třemi servery (dva pro virtualizaci, jeden pro management s podporou

virtualizace), dvěma diskovými poli pro data, páskovou knihovnou pro zálohování a záložními zdroji. Síťové služby zajišťují dva aktivní prvky HP 2910al.

Pro virtualizaci je využívána technologie společnosti VMWare ESXi ve verzi 5.5. Po spuštění nových serverů pro virtualizaci proběhla postupná migrace existujících aplikační serverů z fyzických počítačů do virtuálního prostředí. Tímto krokem došlo k značné koncentraci aplikačních serverů na jednom místě. Jedním z klíčových serverů je souborový server, zde slouží úřadu historicky systém Novell Netware ve verzi 5.1 provozovaný na dvou serverech. Pro autorizaci uživatelů slouží služba NDS ve verzi 8 plně svázaná s prostředím Novell. Úřad má v současnosti již zakoupeny licence pro MS Windows server ve verzi 2008 R2 doplněný sadou přístupových licencí pro klienty.

Jako klienti slouží pro pracovníky úřadu standardní stolní počítače vybavené operačním systémem Microsoft Windows řady XP, 7 nebo 8 vše ve verzi Professional. Dále kancelářský balík Microsoft Office, sadu běžného aplikační software (internet browser, úprava fotografií, prohlížeč PDF a další). K zabezpečení mají počítače instalovaný antivirový software a využívají lokální firewall, který je součástí operačního systému. Všechny počítače jsou připojeny do lokální sítě prostřednictvím strukturované kabeláže. Uživatelé využívají řadu síťových zdrojů a jsou k nim autorizování prostřednictvím Novell NDS (většina) případně Windows AD (menšina). Základním sdíleným zdrojem jsou souborový server, databázový systém Oracle a MS SQL server a taktéž poštovní server.

3.3 Informační systém

Informační systém úřadu je tvořen několika částmi – ekonomickým systémem Ginis od společnosti Gordic, elektronickou spisovou službou a informačním systémem Cityware od společnosti Geovap, aplikací pro správní řízení a stavební úřad od společnosti VITA. Napříč úřadem je užíván právní systém ASPI. Dále jsou využívány další desítky dílčích specializovaných aplikací pro výkon konkrétních činností.

3.4 Připojení k internetu

Připojení sítě městského úřadu k síti internet je v současnosti zajištěno mikrovlnným pojítkem v pásmu 17Ghz s plně duplexní rychlostí 100Mbit. Služby hraničního routeru zajišťuje MIKROTIK Cloud Router Switch CRS125. Tento zajišťuje především routing v omezené míře i lokální firewall. Za routerem je vytvořena logická DMZ síť se subnetem platných adres a taktéž oddělená WAN síť. Tato WAN síť vznikla v průběhu let 2005 až

2007, kdy došlo s podporou projektů financovaných z EU fondů k vybudování rozsáhlé mikrovlnné sítě v pásmu 2,4 a 5GHz propojující řadu příspěvkových organizací města s úřadem samotným. WAN síť byla od počátku budována jako oddělená od interní LAN sítě úřadu.

Samotná LAN úřadu je do internetu připojena prostřednictvím softwarového routeru na bázi virtuálního počítače s komerčním licencovaným řešením Kerio Control. Router je zapojen jako jeden z klientů do DMZ. Do DMZ jsou taktéž zapojeny vybrané aplikační servery jako například servery zajišťující přístup do Informačního systému základních registrů nebo webové servery s aplikacemi pro veřejnost (například materiály zastupitelstva, rezervační systém pro prodej vstupenek Domu Kultury a další).

Kerio Control je provozován ve verzi 8. Úřad vlastní licenci pro 260 uživatelů ovšem bez integrovaného antiviru. Router je v současnosti provozován jako virtuální stroj zajišťující pro vnitřní síť firewall a proxy server pro uživatele autorizované podle IP adres a dále služby jako DHCP i DNS a částečně i limitování uživatelů podle objemu přenesených dat.

Služby poštovního serveru poskytuje řešení Kerio Connect ve verzi 8.4.2 s licencí pro 265 uživatelů včetně antiviru Sophos a podpory pro zařízení s technologií Microsoft ActiveSync. Poštovní server běží na vizualizovaném počítači s operačním systémem Microsoft Windows 2008 R2. Server je umístěn uvnitř LAN úřadu a s Internetem je propojen prostřednictvím několika přesměrovaných portů na Firewallu (služby SMTP, POP3 i POP3s, IMAP i IMAPs, HTTP i HTTPS).

3.5 Personální zabezpečení provozu IS

Oddělení informatiky vzniklo v rámci organizační struktury úřadu k 1. 1. 2003 v rámci reformy veřejné správy, vzniku obcí s rozšířenou působností a přesunu řady agend i pracovníků ze zanikajícího Okresního úřadu v Kroměříži na Městský úřad Kroměříž. Oddělení bylo začleněno v rámci odboru vnitřních věci. V letech 2011 až 2013 byla informatika v rámci změny organizační struktury začleněna jako samostatný Odbor informačních technologií s oddělením informatiky a útvarem podatelny. Následně od 1. 1. 2014 s další optimalizací došlo ke zrušení odboru a přesunu oddělení informatiky společně s útvarem podatelny pod Kancelář úřadu podřízené přímo tajemníkovi úřadu.

Během této doby nikdy neměla informatika vlastní samostatný rozpočet umožňující střednědobé a dlouhodobé plánování rozvoje informačních technologií. Z tohoto důvodu

byl rozvoj řešen ad-hoc na základě konkrétních událostí a větší investice probíhaly v rámci projektů financovaných z EU fondů. Došlo tak v letech 2005 a 2006 k vybudování menší bezdrátové sítě a propojení řady organizací zřízených městem s městským úřadem a v letech 2012 až 2014 k vybudování technologického centra. Projekty budované s podporou EU fondů s sebou nesou povinnost pětileté udržitelnosti a tudíž provozních nákladů. Současně vzniká potřeba řešit komplexní obměnu technologií po skončení technické podpory výrobce. Po skončení technické podpory bude nutné řešit nákup (obměnu) technologií.

Personálně všechny tvoří v současnosti oddělení jeden vedoucí, čtyři pracovníci zařazeni na pozici informatika a jedna referentka, součástí oddělení je dále úsek podatelny zajišťující zpracování veškerých přijímaných a odesílaných písemností (listinných i elektronických včetně datových schránek) a dále servis stran úřední desky (povinně zveřejňované informace).

Informatici mají rozdělený úřad dle odborů a taktéž dle provozovaných agendových informačních systémů, referentka zajišťuje podporu pro elektronickou spisovou službu napříč úřadem a dále péči o webové prezentace úřadu. Jeden z informatiků společně s vedoucím oddělení zajišťují dohled nad aktivními prvky v síti i monitorují provozní parametry firewallu Kerio Control.

II. PRAKTICKÁ ČÁST

4 NÁVRH ZMĚN

Před samotným návrhem možných změn jsem provedl spolu s kolegy informatiky – zaměstnanci úřadu SWOT analýzu jakožto prostředek pro zhodnocení a nalezení silných i slabých stránek v lokální síti města Kroměříž s přihlédnutím k požadavkům zákona 365/2000 [3] o informačních systémech veřejné správy i zákona 184/2014 [8] o kybernetické bezpečnosti.

Následně navrhnu několik dílčích realizovatelných změn především administrativního charakteru. Jejich realizace je možná „silami“ již zaměstnaných pracovníků úřadu bez významnějšího dopadu na rozpočtové zdroje.

Závěrem této kapitoly budu specifikovat technické požadavky pro probíhající projekt „**Konsolidace IT a nové služby TC ORP Kroměříž**“ jehož součástí je i rozsáhlejší řešení kybernetické bezpečnosti datové sítě úřadu.

4.1 SWOT analýza

Pro další hodnocení stavu kybernetické bezpečnosti datové sítě Města Kroměříž jsem zvolil SWOT analýzu.

	POMOCNÉ (k dosažení cíle)	**ŠKODLIVÉ** (k dosažení cíle)
VNITŘNÍ (atributy organizace)	**STRENGHTS** (silné stránky) • Plná kontrola nad vnitřním prostředím • Důvěra vedení úřadu i města. • Dobré odborné zázemí (pracovníci IT)	**WEAKNESSES** (slabé stránky) • Nedostatečné financování (neexistence rozpočtu, plánů) • Neaktuální informační koncepce • Nízká podpora politické reprezentace • Lidský faktor (řadoví pracovníci) • Zastaralý síťový software (Novell NDS) • Úroveň současného zabezpečení (aktivní prvky, firewall, antivir)
VNĚJŠÍ (atributy prostředí)	**OPPORTUNITIES** (příležitosti) • Externí finanční zdroje, zejména projekty z EU fondů • Spolupráce s jinými městy / úřady	**THREATS** (hrozby) • Vnitřní útok – omezení nebo zahlcení provozu uvnitř sítě • Vnější útok – omezení přístupu do internetu / dostupnost a kompromitace služeb

Tabulka 4 – SWOT analýza IS úřadu

4.1.1 Silné stránky

Silnou stránkou úřadu je značná kontrola nad vnitřním provozním prostředím, používáme totiž aplikace a systémy poskytované centrálně (aplikace pro přenesenou působnost danou zákonem a garantované ministerstvy) a dále aplikace pro zajištění chodu úřadu a města (aplikace určené pro samosprávu). Prostředí úřadu je z pohledu aplikací poměrně homogenní a všechny aplikace fungují na mnoha dalších úřadech v rámci republiky.

Značnou výhodou je i důvěra vedení města informačních technologiím, byť zde jde dlouhodobě hlavně o jejich využívání a propagaci. Jak je uvedeno dále, ač vedení města má v různých volebních obdobích informační technologie ve velké oblibě je tato oblast podfinancovaná.

Velkou výhodou je i dobrá odborná úroveň pracujících informatiků.

4.1.2 Slabé stránky

Zásadní slabou stránkou je zcela nedostačující a nesystémové řešení financování IT technologií. Dlouhodobou neexistencí jasně definovaného pravidelného objemu finančních prostředků investovaných do informačních technologií vede ke dlouhodobé tvorbě „vnitřního technologického dluhu“ a nemožnosti systémově plánovat alespoň ve střednědobém horizontu. Tato skutečnost taktéž vede k mnoha ad-hoc řešením vycházejícím z omezených zdrojů neinvestičního charakteru.

Významnou slabou stránkou je dlouhodobě nízká politická podpora informačním technologiím. Což lze dokumentovat zejména chybějícím rozpočtem, tímto jsme naprostá výjimka mezi obcemi s rozšířenou působností v rámci Zlínského kraje.

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy ukládá obcím jisté povinnosti ve vztahu k provozování a plánování informačních systémů, taktéž vyhláška č. 529/2006 Sb. [4] o dlouhodobém řízení informačních systémů veřejné správy upravuje jak mají obce postupovat při řízení svých informačních aktivit. V rámci zpracování SWOT analýzy jsem zjistil, že poslední taková informační koncepce byla z důvodu atestace zpracována na počátku roku 2008, její platnost byla pětiletá a skončila počátkem roku 2013.

Z hlediska bezpečnosti nelze opomenout rizika plynoucí z „nezodpovědnosti“ řadových pracovníků. Tato rizika souvisí zejména s používáním běžných aplikací jako je e-mail nebo web prohlížeč a návazně viry a spamem. Naopak riziko zavlečení virů nebo škodlivého kódu prostřednictvím diskety nebo USB Flash je dnes prakticky minimální, oproti dobám před rokem 2000 tento způsob šíření škodlivého kódu prakticky vymizel.

Značným rizikem je taktéž využívání zastaralého systému Novell NDS jako klíčového autorizačního nástroje v rámci sítě. Aktuálně provozovaná verze 5.1 pochází z roku 2000, vývoj Novell Netware skončil před pěti léty. Pro autorizaci všech uživatelů a propojení na další aplikace je velmi žádoucí přejít na řešení Microsoft Windows server s Active Directory.

Současné řešení zabezpečení připojení vnitřní sítě úřadu do internetu je založeno na softwarovém nástroji Kerio Control. S rostoucími požadavky na nastavení oprávnění, řízení provozu a služby typu QoS a současně navyšováním rychlosti připojení k síti

Internet je toto řešení z pohledu kybernetické bezpečnosti nedostačující a je vhodné jej nahradit samostatným plně konfigurovatelným specializovaným hardwarovým firewallem.

4.1.3 Vnější příležitosti

Klíčovou aktuální příležitostí pro město Kroměříž jsou externí finanční zdroje, zejména projekty s možností financování z EU fondů. Vzhledem k nízké míře financování informačních technologií z rozpočtu města je financování prostřednictvím projektů v současnosti jediným způsobem pořízení větších investičních celků, tedy zařízení s pořizovací cenou nad 40.000 Kč – což jsou jak klíčové servery, aktivní prvky tak i dražší softwarové licence.

Aktuální příležitostí byla vyhlášená výzva 22 [15] ze dne 14 února 2014 v rámci Integrovaného operačního programu. Tématem výzvy byla „Konsolidace IT a nové služby TC obcí“.

V rámci výzvy byly podporované tyto aktivity:

1) Konsolidace HW a SW úřadu včetně virtualizace aplikací, desktopů, serverů, infrastruktury
2) Rozvoj služeb TC ORP a návaznost na TCK
3) **Zvýšení bezpečnosti a bezpečnostní infrastruktura TC ORP**
4) Elektronizace procesů, digitalizace dat a propojení lokálních AIS s registry veřejné správy

Významnou příležitostí je i spolupráce s dalšími městy podobné velikosti jako je město Kroměříž. Taková města totiž mají podobně velké úřady a vzhledem k nutnosti zajišťovat totožné služby řeší i podobné problémy. V rámci Zlínského kraje hraje též významnou rolu spolupráce s oddělením informatiky krajského úřadu, které pořádá semináře k aktuálním tématům případně nepravidelné schůzky s možností sdílení informací z praxe. Zatím co před rokem 2002 působily v území kraje čtyři okresní úřady, dnes v souvislosti s reformou státní správy působí v kraji třináct měst zajišťující služby obce s rozšířenou působností – tedy rozsáhlým výkonem přenesené státní správy.

Příležitostí jsou případné změny v legislativě státní správy, které vytvářející potřebu nebo tlak pro změny v dotčených oblastech. Takovou změnou byl například systém CzechPoint a Datové schránky, kdy došlo k zásadní změně výkonu řady činností a navazujícím

změnám ve fungování informačních technologií. Stejnou změnou bylo zavedení a spuštění Informačního systému základních registrů, který vedl ke změně řady postupů směrem k občanům a návazně i úpravě informačních systému.

Aktuální změnou je zákon o kybernetické bezpečnosti [8], který byl schválen v roce 2014 a vstoupil v platnost k 1 lednu 2015.

4.1.4 Vnější hrozby

Zásadní hrozbou je napadení interních systémů (lokální počítače, servery) nevyžádaným nebo nežádoucím software (viry, mallware a další). Takto nakažené počítače mohou být zneužity jak k získání interních informací (sledování práce na lokálním počítači s cílem například získat autorizovaný přístup – jména a hesla) tak i k šíření nežádoucího software na další vnitřní systémy tak i dále do internetu. Nakažené počítače se taktéž mohou stát součástí širšího bootnetu s možností zneužití například DDoS útoku nebo rozesílání spamu. Důsledkem rozsáhlého útoku může být celkový kolaps vnitřní sítě (zahlcení) v mírnější verzi může být infrastruktura dlouhodobě a nepozorovaně zneužívána (spam) [11].

Další možnou hrozbou je vnější útok na veřejné služby poskytované úřadem, tedy zejména webové servery nebo na páteřní router. Tento útok může být veden pomocí DDoS – tedy velkým množstvím dotazů na poskytované služby (například web server). Útokem na páteřní router může dojit k zahlcení připojení úřadu a omezení dostupnosti služeb využívaných úřadem (například přístup k Informačnímu systému základních registrů, službám CzechPointu nebo systému Datových schránek). Důsledkem bude omezení některých služeb pro občany, celková schopnost úřadu poskytovat služby ovšem nebude dotčena. Dalším cílem útoku může být zahlcení web serveru s oficiálními stránkami města nebo turistickým portálem, tedy zamezit poskytování služeb případně jeho kompromitace s cílem měnit poskytované informace. Výsledkem bude dle rozsahu útoku poškození veřejného mínění o úřadu nebo městě, nedojde ovšem k omezení vnitřního provozu úřadu a poskytovaných služeb.

4.2 Administrativní změny

Nejkomplikovanější možnou změnou jsou změny administrativní případně procesní, tedy změny realizované vlastními pracovníky / týmem pracovníků bez významnějšího podílu rozpočtu města.

Tyto změny často vyžadují popsání současných postupů a návrh jejich případných změn vedoucích ke zlepšení. Je velmi důležité, aby navržené změny byly přijaty většinou zaměstnanců a získaly tak jejich podporu, bez ní může jít pouze o další velmi popisné a zcela nefunkční postupy.

Dobře navržené a provedené administrativní změny mohou být velmi levné a v konečném důsledku mohou přinést organizaci i úspory.

4.2.1 Komise pro informatiku a web

Komise rady města jsou zřízeny jako iniciativní a kontrolní orgány. Komise mohou poskytnout radě města odborné zázemí, které potřebuje mít pro své rozhodování, z podnětů a připomínek komisí by měla rada města čerpat při své práci. V případě fungování se mohou stát velmi významným prvkem v řízení obce, a to mimo jiné proto, že v nich mohou usednout místní odborníci, nečlenové zastupitelstva, kteří mají zájem a zkušenosti k tomu, aby byli obci i mimo její orgány prospěšní.

Komise nemají žádnou samostatnou rozhodovací pravomoc, nemohou ukládat úkoly obecnímu zastupitelstvu, obecní radě ani starostovi. Komise mohou působit jako iniciativní orgán, tedy navrhovat řešení problémů, přicházet s podněty, čím je třeba se zabývat a proč, plní určité úkoly svěřené jim obecní radou, a to i na vlastní žádost a z iniciativy komise.

Na základě jednání se starostou města, členy rady a tajemnicí úřadu navrhuji ustanovení „Komise pro informatiku a web“ v jejíž gesci by byl především koncepční rozvoj samosprávných informačních systémů. Systémy sloužící pro přenesenou působnost danou zákony nelze příliš ovlivnit nebo měnit, jsou často poskytovány centrálně případně se jedná o de-facto standard pro danou oblast (například stavební úřady).

Cílem komise bude mimo jiné řešení dlouhodobého financování informatiky, zapojení města a jeho organizací do případných projektových příležitostí daných výzvami EU s cílem snížit investiční zátěž města.

Komise rady obvykle fungují po celé volební období, tedy v tomto případě až do podzimu 2018.

4.2.2 Informační koncepce

Jak bylo zjištěno v rámci SWOT analýzy má město téměř dva roky neplatnou informační koncepci a původní pochází z roku 2008 a nebyla průběžně aktualizována. Od roku 2008

došlo v oblasti legislativy i vývoje informačních technologií celosvětově i v rámci provozu města Kroměříž k řadě změn.

Jednou z významných změn je například elektronizace spisové služby a provoz datových schránek, což je významný informační systém zasahující výkon všech agend napříč úřadem.

Z tohoto důvodu bude další změnou v rámci tohoto projektu vytvoření nové informační koncepce v souladu s požadavky zákona č. 81/2006 Sb. (novela zákona č. 365/2000 Sb.), o informačních systémech veřejné správy.

Informační koncepce bude vycházet z aktuálního stavu počátku roku 2015 a bude následně součástí podkladů pro novou atestaci informačního systému města Kroměříž s platností pět let.

4.2.3 Vzdělávací opatření

Jak plyne z předešlého, jsou jednoznačně nejslabším článkem kybernetické bezpečnosti samotní uživatelé.

Z tohoto důvodu bude nově navržen proces vzdělávání a dlouhodobé práce se všemi uživateli tak aby postupně došlo ke zlepšení vědomostí o kybernetické bezpečnosti. Například uživatel seznámený s postupy sociálního inženýrství se bude mnohem lépe orientovat v situacích, které mohou představovat útok a to nejen v pracovním procesu ale i v soukromém životě.

Výsledkem takových školení a dlouhodobé práce s uživateli může být posílení jejich loajality, což je pro zaměstnavatele – město Kroměříž značnou výhodou. Takoví pracovníci jsou následně zárukou pro zajištění informační bezpečnosti úřadu.

Dobře a pochopitelně vytvořené vzdělávání v oblasti bezpečnosti pomáhá zaměstnancům snáze rozpoznat možná rizika a předejít tak vzniku větších škod. Rozhodující není kvalita zpracovaných dokumentů ale systém, který mají všichni zaměstnanci organizace ve svých hlavách.

4.2.4 Politika hesel

Jak je uvedeno v analýze stavu, probíhá na městském úřadě v Kroměříži aktuálně přechod ze síťového operačního systému Novell Netware na Microsoft Windows Server. Po dokončení bude k dispozici autorizační platforma Active Directory. Souběžně existuje

několik autorizačních databází uživatelů s hesly. Dalším krokem bude snížení počtu míst s uloženými účty uživatelů a sjednocení uživatelských autorizací na platformě Active Directory.

V nastavení informačních systémů úřadu v současnosti nejsou definovány požadavky na složitost hesla ani na jeho minimální délku. Uživatel se přihlašuje k počítači, ke sdíleným síťovým zdrojům, ke své poště a do jednotlivých aplikací. Některé systémy jsou propojené (hesla k počítači a k síti), jiná jsou trvale uložena v rámci nastavení (poštovní klient). U většiny aplikací je možná uživatelská změna hesla.

Tento systém je nutné postupně měnit, kvalitu hesel zvyšovat a postupně upravovat i minimální požadavky na jejich složitost. Součástí vzdělávání úředníků se tak musí stát i poučení o tvorbě vhodných hesel. Současně bude vhodné poučit uživatele o bezpečnosti práce s elektronickým podpisem.

4.3 Technologické změny

Technologické změny již představují možnou investici do infrastruktury a tedy výdaje z rozpočtu města. Rozpočet města bývá schvalován zastupitelstvem města již koncem kalendářního roku a investiční výdaje (tedy v částce nad 4é.000 Kč) neplánované jsou komplikovaněji prosaditelné.

Souběžně v období prosinec 2014 až současnost probíhá projekt „Konsolidace IT a nové služby TC ORP Kroměříž“. V případě jeho úspěšné realizace dojde k řadě investic právě do infrastruktury úřadu se zaměřením především na zlepšení bezpečnosti.

Z tohoto důvodu se mnou navržené změny omezí na ekonomicky přijatelné a snadněji realizovatelné položky. V oblasti software budu preferovat především open source řešení.

4.3.1 Výměna firewallu

Dosud využívala lokální síť města pro přístup do internetu řešení společnosti Kerio – produkt Kerio Control ve verzi 8. Úřad vlastní licenci pro 260 uživatelů ovšem bez integrovaného antiviru. Kerio Control je využíváno jako firewall, proxy server a DHCP server a je provozováno jako virtuální stroj v prostředí VMWare. Při instalaci byla využita připravená distribuce VMware Virtual Apliance. Významným omezením je nízká propustnost datových toků, vliv na rychlost neměla žádná změna hardwarových parametrů (navýšení operační paměti nebo počtu procesorů případně výměna síťových karet). Dle

průběžného monitoringu nevykazoval virtuální stroj žádné abnormální požadavky na zdroje VMWare prostředí a jiné virtuální stroje sdílející totožný hardware pracují bez potíží.

Při jakémkoliv nastavení tak je měřená propustnost v pracovní době maximálně 4MBit/s na jeden počítač a celá datová síť úřadu byla schopna využít maximálně 15MBit/s dostupné kapacity (do konce roku 2014 50MBit/s od ledna 2015 až 100MBit/s plně duplexní). Další vadou byla nemožnost odebírat jakékoliv průběžné informace o probíhajících spojeních, objemu přenesených dat a podobně.

Výhodou řešení je snadné ovládání prostřednictvím webového administračního prostředí.

Kerio Control tedy je provozován jako stavový firewall s funkcí proxy s možností webové administrace. Cena technické podpory a práva aktualizace na nové verze stále úřad 78.000 Kč s DPH ročně.

Cílem změny je navrhnout a implementovat jiný firewall zajišťující stejnou funkcionalitu s vyšší propustností a možností monitoringu vybraných parametrů nejlépe s přímou podporou NetFlow záznamů.

4.3.2 Monitoring NetFlow záznamů

V souvislosti s výměnou firewallu s cílem získat takový, který podporuje technologii NetFlow bude potřeba uvnitř sítě vytvořit nový server určený pro ukládání, zpracování a prezentaci NetFlow záznamů a případně i pro jejich dílčí analýzu případně monitoring abnormálních hodnot. Přes firewall prochází veškerý provoz z / do internetu což představuje nejzajímavější data pro možný monitoring.

Pro ukládání dat bude využita kapacita virtualizačních serverů VMWare a v rámci existující serverové farmy technologického centra bude vytvořen další virtuální stroj pro provoz NetFlow kolektoru.

V rámci změny budou porovnány možná open-source řešení a jedno z nich nasazeno pro ukládání, zpracování i zobrazení datových toků přes firewall lokální sítě.

4.4 Konsolidace IT a nové služby TC ORP Kroměříž

Dne 14. 2. 2014 došlo z Integrovaného operačního programu, oblasti intervence 2.1 – Zavádění ICT v územní veřejné správě k vyhlášení výzvy 22 s tématem „Konsolidace IT a nové služby TC obcí“[15]. Jak je uvedeno výše je jednou z aktivit „Zvýšení bezpečnosti a

bezpečnostní infrastruktura TC ORP“. Zpráva o této příležitosti byla předložena na 75 jednání rady města konané dne 13. 3. 2014 a bylo schváleno zpracování Studie proveditelnosti pro vyhlášenou výzvu. Studie byla vypracována pracovníky města ve spolupráci s externím dodavatelem Ing. Barborou Stránskou.

Následně na 84 jednání rady dne 11. 6. 2014 bylo schváleno podání projektu a současně požadavek na financování projektu z rozpočtu roku 2015. Financování projektu následně schválilo zastupitelstvo města na svém 35 zasedání dne 27. 6. 2014.

Město Kroměříž podalo dne 30. 6. 2014 projekt „Konsolidace IT a nové služby TC ORP Kroměříž“, kterému bylo přiděleno evidenční číslo **CZ.1.06/2.1.00/22.09604**.

V jednotlivých podporovaných aktivitách řešíme:

1. V aktivitě „Konsolidace HW a SW úřadu včetně virtualizace aplikací, desktopů, serverů, infrastruktury“:

- virtualizaci telefonní ústředny - jen softwarové řešení, nákup hardware není možný, přístroje a další bude nutno nakoupit samostatně - cílem je služba pro občany - hlasový průvodce a možnost audio záznamu (nahrávání hovoru) pro řešení případných problémů s klienty / úředníky například na úseku péče o dítě nebo stavebním odboru
- konsolidaci aktivních prvků – cílem je výměna páteřních síťových prvků v rámci úřadu za nové s podporou technologie NetFlow (současné budou přesunuty co by podružné nebo jako záloha) - cílem je plná kontrola nad provozem v síti (souvislost se zákon o kybernetické bezpečnosti)
- konsolidace SAN infrastruktury - zde jde o doplnění diskových polí = úložná kapacita dostupná v síti pro ukládání například audio z telefonní ústředny nebo monitorovaná data o provozu v síti
- konsolidaci SQL serveru - souvislost s aktivitami v bodě 4 - softwarová licence na databázi pro ukládání geodat, využití i pro další agendy v rámci úřadu

3) v aktivitě „Zvýšení bezpečnosti a bezpečnostní infrastruktura TC ORP“:

- bezpečnost - nákup nového výkonnějšího firewallu včetně antiviru, monitoring datových prvků (sběr dat a analýzu z prvků z první aktivity) - souvislost se zákonem o kybernetické bezpečnosti

- energetickou nezávislost - motorgenerátor pouze pro technologické centrum a zde umístěné prvky pro zajištění provozu serverů a související infrastruktury

4) v aktivitě „Elektronizace procesů, digitalizace dat a propojení lokálních AIS s registry veřejné správy“
- GIS portál - nákup software pro Grafický informační systém s přístupem pro úředníky tak i pro občany s cílem mít všechny datové vrstvy na jednom místě a přístupné pro všechny - návaznost na SQL server z aktivity 1

V rámci projektu bude pořizován především investiční hardware (železo) a v menší části taktéž software (aplikace), většinu navržených investic by úřad dříve či později musel řešit ať v souvislosti s legislativními požadavky nebo přirozenou obměnou. V projektu nebylo možno řešit jakékoliv „měkké aktivity“ - tedy studie, analýzy a podobně. Součástí projektu není navyšování pracovníků úřadu, nedojde ovšem ani k úspoře pracovních míst.

Náklady na celý projekt jsou vyčísleny na 4.800.000 Kč s DPH. Provozní náklady na projekt mohou, dle předběžné kalkulace dosáhnou částky až 1.500.000 Kč s DPH za pět let (udržitelnost projektu). Projekt může být zahájen po podpisu smlouvy s Centrem pro regionální rozvoj a musí být ukončen k 30. 11. 2015.

Tento projekt v sobě nese i možná (především legislativní) rizika:

- Pokud nebudou u každé části zakázky alespoň dvě nabídky, bude nutné tuto část soutěžit znovu (projekt je nutno realizovat jako celek). U každé z aktivit jsou dostatečné finanční prostředky jak na nákup, tak i na technickou podporu.
- Kterýkoliv z účastníků se může proti průběhu veřejné zakázky odvolat, toto vyvolá zdržení pro vypořádání námitek.
- Může dojít ke zpochybnění veřejné zakázky případně i podání k Úřadu pro hospodářskou soutěž (bude nutné čekat na jeho rozhodnutí). Toto riziko je z časových důvodů zcela fatální.
- Vyšší moc

V případě, že dojde ke vzniku těchto rizik, může být realizace projektu z EU fondů ukončena a následně bude jednáno o dalším postupu (například řešení z vlastních zdrojů v menším rozsahu apod.).

4.5 Bezpečnostní testy

V současnosti není personálně možné obsadit nové role vyžadované jako součást kybernetické bezpečnosti – oblast požadavků na významný informační systém. Důvodem jsou chybějící pracovníci (například na personálním oddělení nebo krizovém řízení) vybaveni patřičnými znalostmi. Z ekonomických důvodů je taktéž nepravděpodobné zaměstnání nových pracovníků.

Bezpečnostní testy proto budou probíhat formou externího auditu, který si úřad objedná u specializované firmy.

Testy budou zaměřeny na zranitelnost komunikační infrastruktury úřadu, zejména na stav aktivních prvků sítě, jejich zabezpečení a vytížení. Dále na serverové operační systémy, zejména jejich aktuálnost, instalované služby a nastavení oprávnění řízení přístupů [16]. Analýzu chování sítě i serverů zaměřenou na kontrolu „zvláštních“ procesů a síťových spojení. Volitelně budou testovány i koncové stanice zejména na stav aktualizací operačního systému, internetových prohlížečů a známých bezpečnostních zranitelností.

Testování bude probíhat vždy jednou ročně s cílem získat informaci o aktuální kondici bezpečnosti sítě. Výsledkem auditu bude technická zpráva s manažerským shrnutím, všemi odhalenými zranitelnostmi a vhodnými doporučeními.

První testování proběhne v létě 2015 před případnou realizací projektu z EU fondů..

5 REALIZACE NAVRŽENÝCH ZMĚN

V této části projektu dojde k postupné realizaci navržených změn a to nejdříve administrativních a následně i technologických.

5.1 Administrativní změny

Jak jsem uvedl již dříve, představují administrativní změny především logistickou a personální zátěž, po ekonomické stránce mohou být v případě realizace vlastními silami ekonomicky dostupné.

5.1.1 Komise pro informatiku a web

Rada města projednala návrh na zřízení „Komise pro informatiku a web“ na svém 10 jednání dne 30. 3. 2015 a usnesením číslo 245 schválila její zřízení. Členy komise se stanou odborníci nominovaní jednotlivými politickými stranami. Ke jmenování členů komise vzhledem k probíhajícím jednáním „vládních“ i „opozičních“ zastupitelů dosud nedošlo. Obtížené je zejména získat vhodné odborníky ochotné se angažovat v této komisi, kteří jsou současně i přijatelní pro zastupitele.

MĚSTO KROMĚŘÍŽ

Městský úřad Kroměříž
Velké náměstí 115
767 01 Kroměříž

tel. +420 573 321 111
fax +420 573 331 481
www.mesto-kromeriz.cz

Kroměříž 2. dubna 2015

Výpis z usnesení z 10. schůze Rady města Kroměříže konané 30. března 2015

Rada města Kroměříže po projednání

z ř i z u j e

komisi Rady města Kroměříže pro informatiku a web, podle předložené důvodové zprávy.

Mgr. Jana Kutá
tajemnice Městského úřadu Kroměříž

MĚSTSKÝ ÚŘAD
KROMĚŘÍŽ

Obrázek 3 – Ustanovení komise pro informatiku a web

Působnost komise pro informatiku a web bude zejména v těchto oblastech:

- koncepce IT systému města, organizací a zařízení, které město založilo, zřídilo nebo vlastní, s cílem zefektivnění a zrychlení rozhodovacích procesů s využitím IT,
- návrh investic do IT systému města a organizací a zařízení, které město založilo, zřídilo nebo vlastní,
- spolupráce na koncepci komunikace radnice s veřejností, transparence rozhodovacích procesů a participace veřejnosti v procesech radnice,
- spolupráce na organizačních a technických opatřeních zabezpečující otevřenost radnice, transparentnost úředních a rozhodovacích procesů a celkovou vstřícnost k občanům,
- návrh struktury oficiálních webových stránek města Kroměříž,
- návrh realizaci nových komunikačních forem a aktualizaci stávajících,
- stanovisek k podnětům a návrhům občanů, organizací působících v Kroměříži, RMK, příslušných odborů úřadu a svých členů, které spadají do působnosti komise.

Ustanovení další komise rady města představuje pro rozpočet města pouze minimální výdaje a to v oblasti mezd. Zastupitelé nominovaní do komisí mají nárok na odměnu, ovšem pouze na jednu a to bez vazby na počet komisí. Externisté z řad odborníků nominovaní politickými stranami vykonávají svou činnost pro komise zcela zdarma.

5.1.2 Informační koncepce

Jak jsem zjistil v rámci SWOT analýzy chybí v současnosti informačním systémům na městě Kroměříž Informační koncepce, která by byla v souladu se zákonem č. 365/2000 Sb. o informačních systémech veřejné správy v aktuálním znění a jeho vyhláškou č. 529/2006 Sb.[4], o dlouhodobém řízení ISVS.

V této vyhlášce jsou stanoveny požadavky na strukturu, obsah informační koncepce a provozní dokumentaci ISVS [17].

Z tohoto důvodu jsem společně s kolegy informatiky zpracoval informační koncepci dle osnovy danou vyhláškou.

Informační koncepce mapuje všechny informační systémy využívané pro výkon agend zejména přenesené působnosti (tedy dané zákonem). Jde o tyto agendy:

- eSSL – Spisová služba
- Vita SW - Přestupkové řízení
- Vita SW – Stavební úřad
- Vita SW – Vodoprávní úřad
- ESPI 9 – Evidence správních řízení
- EVI 9 – Evidence odpadů, zařízení
- Evidence myslivosti
- Geovap – poplatky
- ROB – Registr obyvatel
- Kvasar - Ovzduší SQL

A dále o provozní agendy:

- GINIS – INT – Interface
- GINIS – UCR – Účetní a rozpočtové výstupy
- Flux – Personalistika a mzdy

Na úřadě jsou dále provozovány přibližně dvě desítky dalších informačních systému, nemají ovšem vazbu na ISVS – tedy jejich provoz souvisí s vnitřní potřebou úřadu (například ekonomika) nebo jde o zcela samosprávné činnosti (evidence majetku města), nečerpají tedy data z Informačního systému základních registrů nebo jejich provoz není definován zákonem. V informační koncepci nebudou uvedeny a jejich seznam byl vytvořen a bude veden zcela odděleně.

Informační koncepce by měla v souladu s doporučením Ministerstva vnitra České republiky obsahovat tyto části:

- Základní informace o organizaci
- Přehled zdrojů a legislativy
- Soupis provozovaných ISVS a provozních agend s vazbou na ISVS
- Záměry a zásady při pořízení nových IS
- Způsob řízení kvality provozovaných IS

- Řízení bezpečnosti IS, dlouhodobé cíle v této oblasti, základní požadavky na bezpečnost, definice rolí a odpovědnosti
- Ustanovení bezpečnostní komise a bezpečnostního správce
- Způsob financování IS úřadu
- A odpovědnost za dodržování IK

V průběhu měsíce února 2015 jsem zpracoval výše popsanou koncepci. Koncepce byla 10 března 2015 schválena tajemníkem úřadu s platností od 1 dubna 2015.

Zpracovaná informační koncepce je přílohou tohoto projektu.

5.1.3 Zvyšování znalostí v oblasti bezpečnosti

Dosud byla problematika kybernetické bezpečnosti vnímána jako čistě technologická záležitost řešená informatiky bez jakékoliv nutné spoluúčasti zaměstnanců.

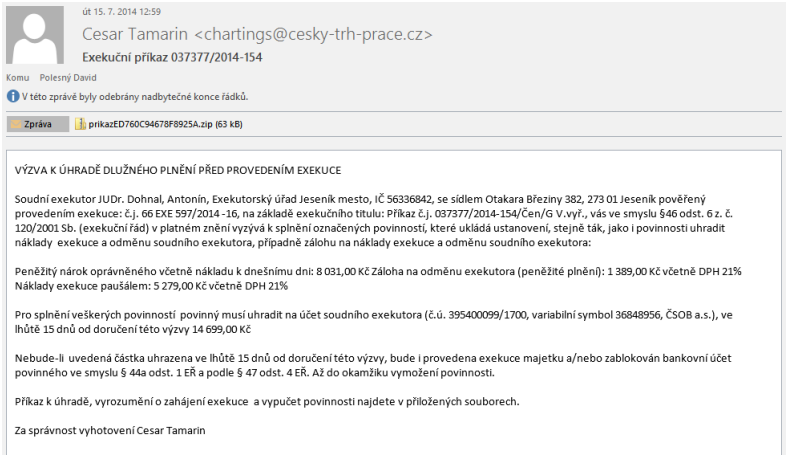
V současnosti využívají všichni pracovníci výpočetní techniku ke své práci. Většina uživatelů má běžný stolní počítač, řada z nich využívá notebook, mnozí taktéž mají přidělený služební chytrý telefon. U všech nově přijímaných je automatickou součástí kvalifikačních podmínek znalost práce s počítačem.

Touto znalostí je ovšem myšleno běžné ovládání počítače – tedy čistě uživatelská znalost práce s operačním systémem, ovládání kancelářských programů, práce s internetem a e-mailem. Následně jsou školeni v používání specializovaných aplikací – agendových informačních systémů.

Všichni nově přijímaní zaměstnanci procházejí vstupním školením o bezpečnosti práce, nově je rozšířeno o samostatné školení v oblasti kybernetické bezpečnosti s informačními technologiemi. Školení pracovníků zajišťují pracovníci oddělení informatiky a jeho součástí jsou tyto oblasti:

- seznámení s běžným aplikačním software užívaným na úřadě (operační systémy, kancelářské balíky, poštovní klient, intranet, specializované agendové informační systémy) s důrazem zejména na skutečnost, že tyto programy komunikují česky. Poučený uživatel má upozorní informatiky na výskyt atypického chování nebo komunikace počítače s uživatelem.

- seznámení s problematikou bezpečného chování na internetu – neotvírání nevyžádaných e-mailů (spamu), zejména jejich příloh nebo navštěvování k práci nepotřebných nebo nedůležitých webových stránek. Webové stránky nebo přílohy e-mailů jsou v posledních letech zdrojem většiny potíží koncových stanic v síti úřadu a byly i příčinou několika lokálních „infekcí“ škodlivého kódu v rámci sítě úřadu.


út 15. 7. 2014 12:59

Cesar Tamarin <chartings@cesky-trh-prace.cz>

Exekuční příkaz 037377/2014-154

Komu Polesný David

V této zprávě byly odebrány nadbytečné konce řádků.

Zpráva prikazED760C94678F8925A.zip (63 kB)

VÝZVA K ÚHRADĚ DLUŽNÉHO PLNĚNÍ PŘED PROVEDENÍM EXEKUCE

Soudní exekutor JUDr. Dohnal, Antonín, Exekutorský úřad Jeseník mesto, IČ 56336842, se sídlem Otakara Březiny 382, 273 01 Jeseník pověřený provedením exekuce: č.j. 66 EXE 597/2014 -16, na základě exekučního titulu: Příkaz č.j. 037377/2014-154/Čen/G V.vyř., vás ve smyslu §46 odst. 6 z. č. 120/2001 Sb. (exekuční řád) v platném znění vyzývá k splnění označených povinností, které ukládá ustanovení, stejně tak, jako i povinnosti uhradit náklady exekuce a odměnu soudního exekutora, případně zálohu na náklady exekuce a odměnu soudního exekutora:

Peněžitý nárok oprávněného včetně nákladu k dnešnímu dni: 8 031,00 Kč Záloha na odměnu exekutora (peněžité plnění): 1 389,00 Kč včetně DPH 21%
Náklady exekuce paušálem: 5 279,00 Kč včetně DPH 21%

Pro splnění veškerých povinností povinný musí uhradit na účet soudního exekutora (č.ú. 395400099/1700, variabilní symbol 36848956, ČSOB a.s.), ve lhůtě 15 dnů od doručení této výzvy 14 699,00 Kč

Nebude-li uvedená částka uhrazena ve lhůtě 15 dnů od doručení této výzvy, bude i provedena exekuce majetku a/nebo zablokován bankovní účet povinného ve smyslu § 44a odst. 1 EŘ a podle § 47 odst. 4 EŘ. Až do okamžiku vymožení povinnosti.

Příkaz k úhradě, vyrozumění o zahájení exekuce a vypučet povinnosti najdete v přiložených souborech.

Za správnost vyhotovení Cesar Tamarin

Obrázek 4 – Příklad virového e-mailu [18]

Součástí je taktéž poučení o způsobech zálohování, jeho rozsahu a typů dat, která jsou automaticky zálohována. Závěrem jsou poučeni o obvyklých krocích, které je vhodné učinit při podezření na kompromitaci jejich počítače – kontaktovat věcně příslušného informatika, nesnažit se samostatně o řešení. Je vhodnější vyvolat několik planých poplachů než případné problémy nebo abnormální chování počítače ignorovat případně jej neodborně řešit. Školení zaměřené na kybernetickou bezpečnost se taktéž stane součástí každoročního bezpečnostního školení všech zaměstnanců úřadu.

Dalším krokem je seznámení uživatele s problematikou tvorby kvalitních hesel [19]. Doporučujeme používat hesla komplikovanější, ale dobře zapamatovatelná. Vhodné heslo je například složeno z více nesouvisejících slov nejlépe v kombinaci s číslicemi nebo alespoň malých a velkých písmen s optimální délkou nad 10 znaků. Příkladem vhodného hesla je například „*Modr7Medv2d*“. Součástí je taktéž ukázka změny hesle v informačních systémech využívaných městským úřadem.

Další administrativní změnou je zavedení evidence uživatelů a jejich přístupů k jednotlivým částem informačního systému. Zde je nutná úzká spolupráce personalistů,

informatiků a příslušných vedoucích odborů. Personalisté vedou evidenci zaměstnanců – mají informace o nově vzniklých, změněných i ukončených pracovních poměrech. Vedoucí odborů rozhodují o zařazení pracovníků i o jimi vykonávaných agendách a rozsahu potřebných oprávnění. Informatici vytváří nové účty, přidělují hesla i nastavují oprávnění, zajišťují běžný chod informačních systémů.

Vytvořená evidence je vedena u informatiků a obsahuje seznam pracovníků a přidělených přístupů do jednotlivých agend. Součástí jsou jak interní agendové systémy, tak i přístupy do externích obvykle webových systému jako CzechPoint, evidence dopravy, živnostenský rejstřík a další.

Nově jsou ve spolupráci s tajemníkem úřadu a personalisty definovány procesní postupy zejména při ukončení pracovního poměru zaměstnancem, dlouhodobé pracovní neschopnosti nebo mateřské dovolené. Všechny tyto změny probíhají na základě informace personalistů, změny probíhají ve lhůtě do 5 pracovních dnů. Účty jsou v prvním kroku blokovány, následně odstraněny. Před definitivním smazáním musí proběhnout předání „digitálních dat“ – například informací v elektronické spisové službě, v agendových informačních systémech a dalších. Nově taktéž dochází při dlouhodobé pracovní neschopnosti a mateřské dovolené k dočasnému zablokování uživatelského účtu.

Poslední administrativní změnou řešenou v rámci tohoto projektu je vytvoření evidenčních karet k jednotlivým počítačům. Za zdroj dat je brána současná evidence hardware a software vedená na oddělení informatiky. Evidenční karta je nově předávána spolu s počítačem a obsahuje jak soupis předané techniky včetně jejich parametrů (konfigurace) tak i soupis instalovaného software (operační a kancelářský software, antivirus, internetové prohlížeče, vybrané informační systémy a další). Součástí karty je poučení o zákaz uživatelské instalace software, ukládání soukromých dat a zákazů zásahů do hardware. Cílem je jasně definovat odpovědnost jednotlivých pracovníku za jím svěřené prostředky. Karta je podepisována dotčeným pracovníkem a předávajícím informatikem.

Všechny výše popsané změny vstoupili po dohodě s tajemníkem úřadu v platnost od 1 dubna 2015.

5.2 Technologické změny

Jak jsem uvedl již v analytické částí při návrhu změn budu v tomto projektu provádět pouze změny ekonomicky přijatelné především z rozpočtových důvodů a probíhajícího projektu financovaného z EU fondů.

Prvním krokem bude výměna firewallu dalším pak nasazení monitoringu NetFlow toků.

5.2.1 Výměna firewallu

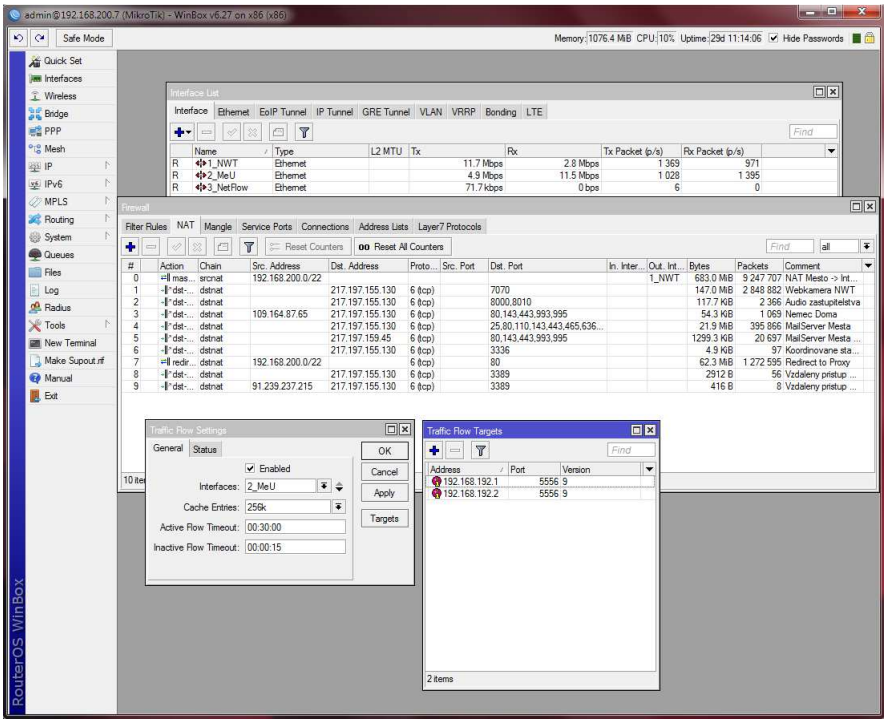
Dosud využívala lokální síť města pro přístup do internetu řešení společnosti Kerio – produkt Kerio Control ve verzi 8. Kerio Control byl provozován jako stavový firewall s funkcí proxy s možností webové administrace, pokročilé vlastnosti jako antivir nebo filtrace webových adres nebyla provozována z licenčních důvodů. Cena technické podpory a práva aktualizace na nové verze stále úřad 78.000 Kč s DPH ročně.

Firewall stejných parametrů jsem hledal jako náhradu, hlavním kritériem byla minimálně srovnatelná funkčnost a ekonomicky dostupné řešení nejlépe s podobným komfortem pro obsluhu (webová administrace). Cílová hardwarová platforma musí být x86 z důvodů provozu ve virtualizačním prostředí.

Výchozími požadavky bylo řešení firewallu (stavového paketového filteru a NAT) a proxy serveru, volitelně podpora pro VPN sítě. Z ekonomického důvodu jsem zcela pominul možnost integrace antiviru případně řešení s podporou detekce průniku (IDS). Tyto funkcionality budou řešeny až v rámci nákupu z probíhajícího projektu financovaného z EU fondů (jak bylo uvedeno dříve).

Vhodným řešením by mohl být softwarový router postavený na volně dostupné Linuxové distribuci. Linuxové jádro s případnými modifikacemi je základem většiny moderních softwarových routek a je ostatně i základem pro používané řešení Kerio Control. Pro Linuxové systémy využívané na městském úřadě používáme distribuci CentOS. Jde o volně dostupnou distribuci založenou na zdrojových kódech Redhat Enterprise Linuxu. Velkou výhodou tohoto řešení určeného pro firemní sektor je stabilita a dlouhá doba podpory bezpečnostních aktualizací (až 10 let). U CentOS verze 6 jsou aktualizace garantovány až do konce listopadu 2020, u aktuální verze 7 pak až do konce června 2024. Na linuxovém routeru je možné dosáhnout všech výše požadovaných funkcionalit. Vzhledem k absenci linuxového specialisty mezi informatiky na městském úřadě by byla nutná instalace externistou s nízkou mírou možné kontroly nad kvalitou dodaného díla.

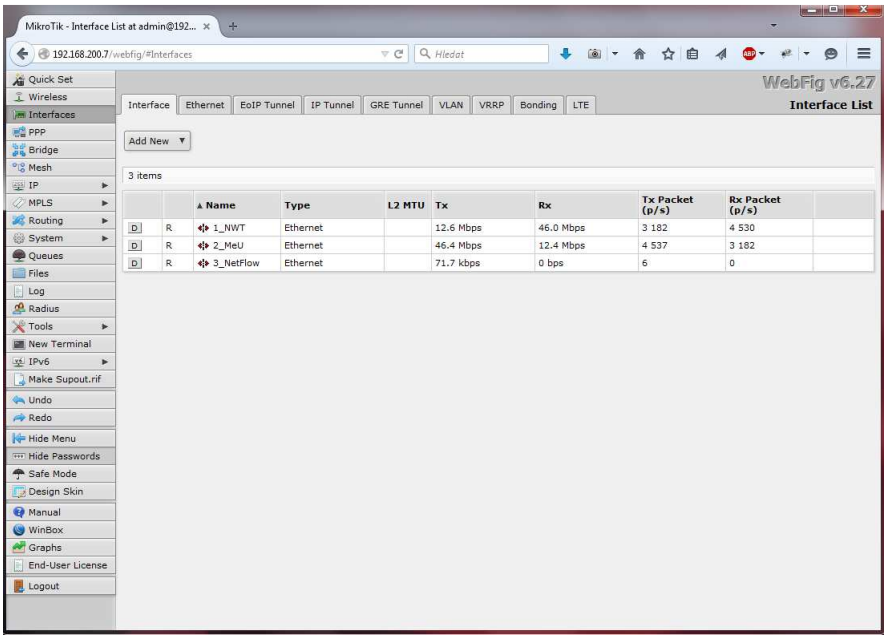
Další alternativou pak je volba hotového řešení, takovým řešením je například produkt společnosti MikroTik z Litvy (sídlo v Rize, založena roku 1995). Společnost produkuje především bezdrátové přístupové i klientské body a routery, vše za velmi příznivých cenových podmínek. Softwarovým základem všech zařízení je RouterOS založený na linuxovém jádru 2.6.x. RouterOS je taktéž dostupný jako samostatný produkt pro instalaci na platformě x86. Software obsahuje všechny vyžadované funkcionality, jeho webové rozhraní je velmi blízké řešení Kerio Control, výhodou je i samostatná administrační konzole. Zásadním argumentem pak je přímá podpora pro technologii NetFlow.



Obrázek 5 – Administrační konzola RouterOS

RouterOS podporuje řadu funkcí – routing, firewall, proxy server, DHCP server, služby virtuální privátní sítě různých typů (ipsec, pptp, openvpn a další), služby pro zajištění potřebné šířky pásma (QoS), pokročilé logování i tvorbu NetFlow statistik.

Vzhledem k využívání WiFi routerů společnosti Mikrotik co by přístupových i koncových bodů v rámci WAN sítě úřadu jsem jako vhodnější vybral právě RouterOS. Řešení pro platformu x86 s licencí úrovně čtyři lze pořídit do 1000 Kč.



Obrázek 6 – Webová administrace pro RouterOS

Pro nový router jsem vytvořil virtuální počítač stejných parametrů, jako byl počítač pro Kerio Control. Má tedy k dispozici dvě síťové karty, celkem 4 GB RAM, dvě procesorová jádra a 2GB diskového prostoru pro proxy cache. Samotná instalace pak zabírá 256MB diskového prostoru. Počátkem měsíce dubna proběhla migrace všech nastavení na RouterOS, tedy došlo k přesunu funkcí firewallu a proxy serveru. DHCP server zůstal dočasně na Kerio Control, který byl přesunut na záložní adresu pro zachování originální konfigurace a možnost rychlého návratu při případných potížích.

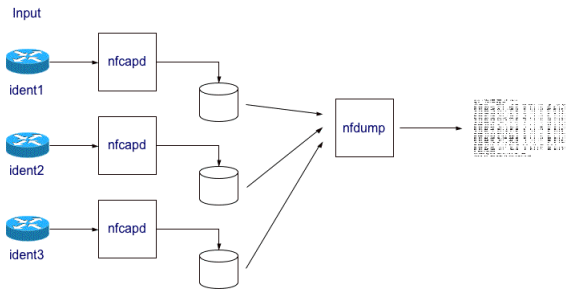
Migrace byla naplánována na noc ze čtvrtka na pátek – pro detekci možný problémů v pátečním nižším provozu. Po migraci se vyskytly pouze drobné problémy dané příliš restriktivním nastavením proxy serveru. Po jejich úpravě vše fungovalo dle očekávání a nový router založený na RouterOS byl ponechán v provozu. Po nasazení došlo ke značnému nárůstu prostupnosti připojení, kdy při testech dosahuje jednotlivý počítač rychlosti až 60MBit/s a blížíme se tedy očekávaným technickým možnostem 100Mbitové vnitřní sítě úřadu (ač páteřní optické spoje jsou 1Gbit, většina koncových počítačů je připojena na rychlosti 100Mbit).

5.2.2 Nasazení NetFlow

Pro zpracování NetFlow záznamu jsem zvolil volně dostupný nástroj nfdump-tools [20] šířený pod BSD licencí a dostupný ve formě zdrojových kódů.

První verze byla uvolněna již v roce 2004, aktuální verze 1.6.13 pochází z prosince 2014. NFDump-tools je určen pro příkazový řádek a podporuje NetFlow záznamy ve verzi 5, 7 i 9. Nástroje obsažené v nfdump-tools:

- nfcapd - NetFlow capture daemon - čte NetFlow záznamy ze sítě a ukládá je do souborů. Pro ukládání každého NetFlow toku (typicky jedno zařízení) ke potřebná jeden spuštěný nfcapd proces.
- nfdump - NetFlow dump - čte NetFlow záznamy ze souborů uložených nfcapd. Má podobnou syntaxi jako tcpdump. Umožňuje vytvářet řadu statistik NetFlow toků podle IP adresy, porty atd.
- nfprofile - NetFlow profiler - čte NetFlow záznamy ze souborů uložených nfcapd a zpracovává je podle předem připravených filtrů.
- nfreplay - NetFlow replay - čte NetFlow záznamy ze souborů uložených nfcapd a odesílá je na jiný počítač.



Obrázek 7 – Příklad nasazení nfdump-tools [20]

Všechny záznamy jsou průběžně ukládány na disk (obvykle co 5 minut) do souborů v adresářové struktuře rok/měsíc/den. Analýza může probíhat souběžně a jde vždy o zcela oddělený proces.

Na sadu nástrojů nfdump-tools navazuje volně šiřitelné webové rozhraní NFsen [21], taktéž k dispozici ve formě zdrojových kódů.

NfSen umožňuje:

- Zobrazení informací o NetFlow tocích s využitím RRD (Round Robin Database)
- Procházení uložených NetFlow záznamů a jejich zpracování
- Nastavit upozornění (alert), založeného na různých podmínkách
- Využití dalších externích pluginů

Nasazení nástroje nfdump-tools společně s nfsen proběhlo v následujících krocích:

1) doplnění firewall routeru o třetí síťovou kartu, určenou pro předávání netflow streamů.
2) Vytvoření dalšího virtuálního počítače v konfiguraci 2x jádro, 4GB RAM, 40GB HDD, 2x LAN (jedna pro přístup ze sítě úřadu a druhou pro spojení s firewallem) s instalací Linuxové distribuce CentOS.
3) Nainstalovaný Linux jsem doplnil balíčky potřebnými pro provoz web serveru, práci s daty ve formátu RRD, podporou jazyka PHP a kompilátorem jazyka C pro překlad zdrojových kódů.
4) Dále jsem do Linuxu instaloval balík nástrojů NFDump pro zajištění funkce NetFlow kolektoru a NFSen jakožto webovou nástavbu nad získanými daty, vše v aktuálních verzích [22]
5) Posledním krokem byla aktivace služby Traffic-Flow [23] na RouterOS a nastavení cílové adresy kolektoru což lze provést v příkazovém režimu takto:

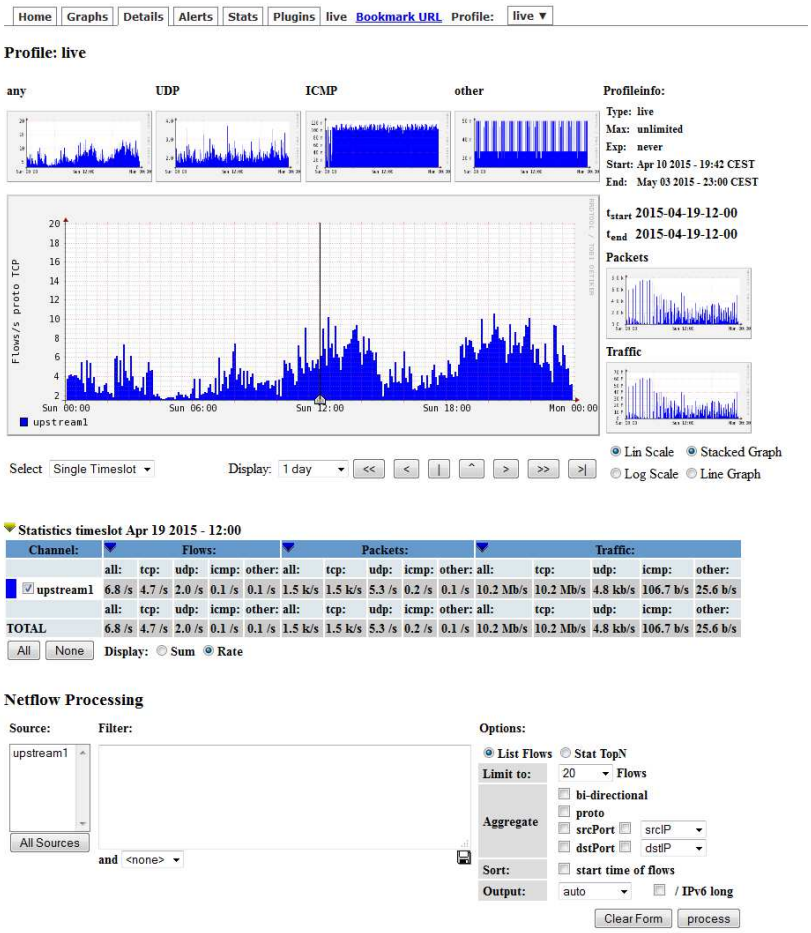
   /ip traffic-flow

   set enabled=yes interfaces=ROZHRANÍ

   /ip traffic-flow target

   add address=IP_ADRESA:PORT version=9

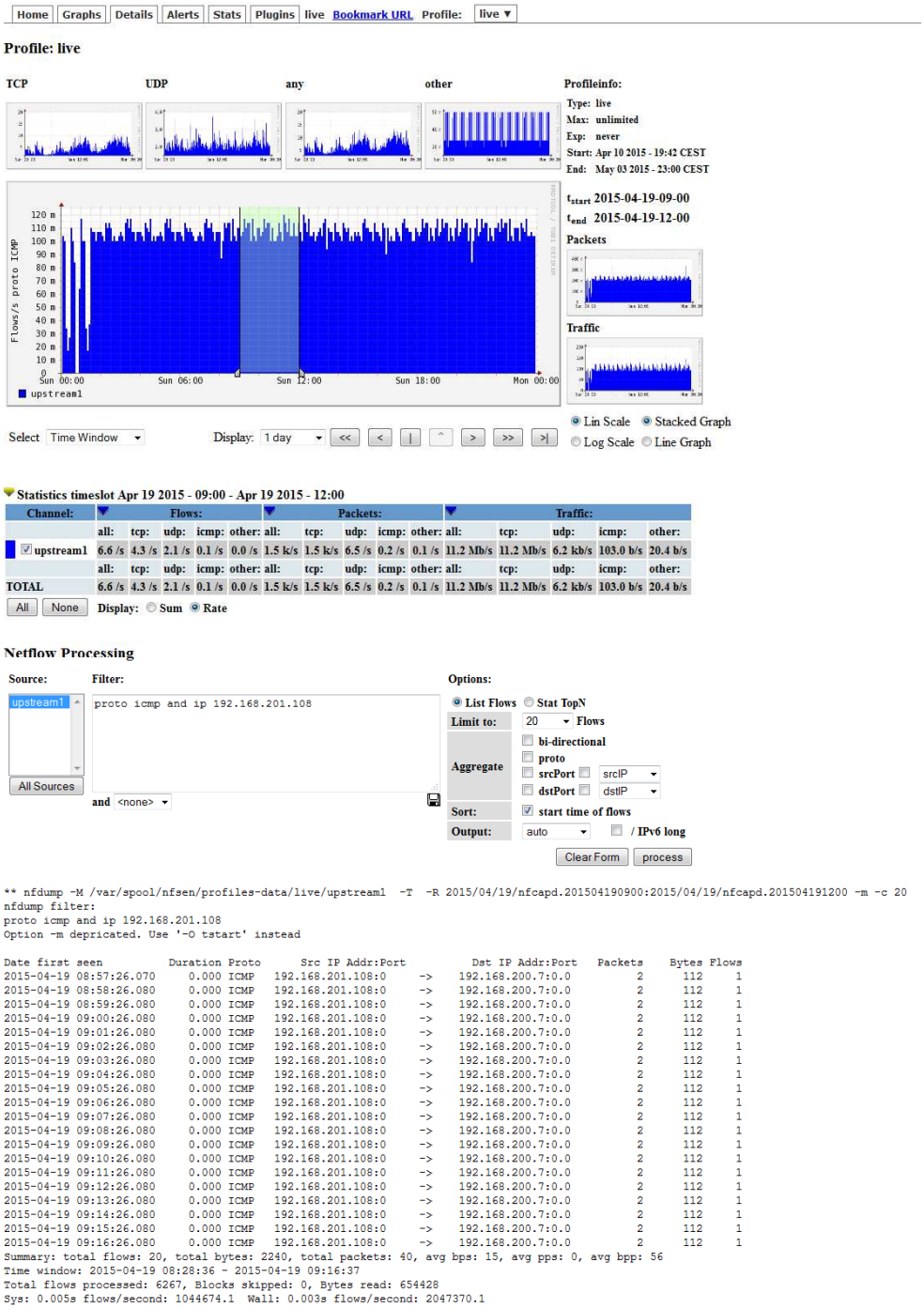
Kde ROZHRANI je síťová karta zařízení nad kterou jsou vytvářeny NetFlow záznamy a IP_ADRESA:PORT je adresa počítače na který budou odesílány záznamy.



Obrázek 8 – záznam netflow komunikace

Webové rozhraní umožňuje zobrazovat získaná data a to jak v konkrétním okamžiku (timeslot), tak i za delší období (time windows) a to rozčleněná podle protokolů TCP, UDP, ICMP a další. Rozhraní dále umožňuje sestavení jednoduchých dotazů pro další bližší analýzu uložených dat.

V zobrazených datech je například patrná značná aktivita protokolu ICMP, tuto aktivitu jsem dále analyzoval:




```
** nfdump -M /var/spool/nfsen/profiles-data/live/upstream1  -T  -R 2015/04/19/nfcapd.201504190900:2015/04/19/nfcapd.201504191200 -m -c 20
nfdump filter:
proto icmp and ip 192.168.201.108
Option -m depricated. Use '-O tstart' instead

Date first seen          Duration Proto      Src IP Addr:Port          Dst IP Addr:Port   Packets    Bytes Flows
2015-04-19 08:57:26.070     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 08:58:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 08:59:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:00:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:01:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:02:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:03:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:04:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:05:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:06:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:07:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:08:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:09:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:10:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:11:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:12:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:13:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:14:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:15:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
2015-04-19 09:16:26.080     0.000 ICMP   192.168.201.108:0     ->    192.168.200.7:0.0          2      112     1
Summary: total flows: 20, total bytes: 2240, total packets: 40, avg bps: 15, avg pps: 0, avg bpp: 56
Time window: 2015-04-19 08:28:36 - 2015-04-19 09:16:37
Total flows processed: 6267, Blocks skipped: 0, Bytes read: 654428
Sys: 0.005s flows/second: 1044674.1  Wall: 0.003s flows/second: 2047370.1
```

Obrázek 9 – analýza netflow záznamů – hledání zdroje ICMP

Ve zvoleném rozsahu časů po filtraci komunikuje opakovaně (co jedna minuta) na ICMP několik vnitřních IP adres vysíláním ICMP paketu „Echo_Request“ s odpovědí „Echo_Reply“. IP adresy mají přidělená zařízení pro obsluhu rezervačního systému pro

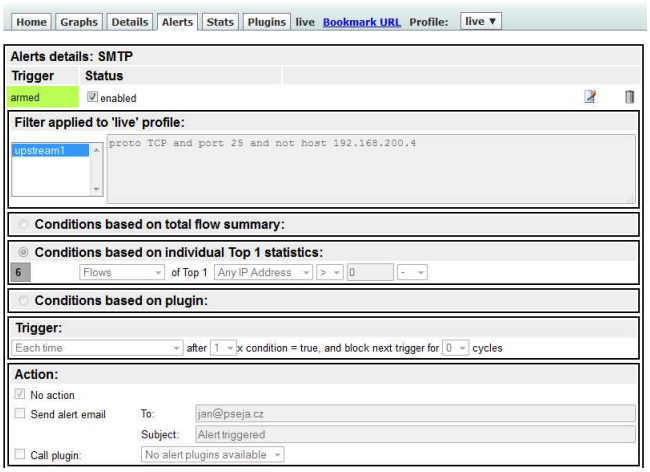
klienty čekající na odbavení (například technické průkazy). Aktivita běží pouze v pracovní době – v noci jsou totiž tato zařízení vypnutá. Zařízení vysílá pakety po jedné minutě po celou dobu aktivního provozu, dotazem na dodavatele a výrobce – společnost Kadlec Elektronika s.r.o. jsem zjistil, že jde o běžnou povolenou komunikaci, kdy si zařízení ověřuje dostupnost lokální sítě pomocí pingu na lokální bránu.

Uložená data lze taktéž analyzovat přímo z příkazového řádku:

nfdump -M /var/spool/nfsen/profiles-data/live/upstream1 -T -R 2015/04/19/nfcapd.201504190600:2015/04/19/nfcapd.201504191800 -a -B -m "proto TCP and (port 25 or port 110) and not host 192.168.200.4"

V tomto příkladu jsou analyzována data za jeden pracovní den v intervalu obvyklé pracovní doby (06:00 až 18:00) s cílem najít komunikaci na portech 25 (SMTP) nebo 110 (POP3) nesouvisející s vnitřní adresou 192.168.200.4 (mail server úřadu). Hledám tedy klienty, kteří se snaží odesílat nebo přijímat poštu z internetu. Poštovní klienti úřadu komunikují pouze s poštovním serverem úřadu a přímý přístup k poště mimo úřad by neměl být nastavený (uživatelé mohou používat webové rozhraní veřejných e-mailových služeb).

Tento dotaz nalezl tři komunikující počítače, objem komunikace byl ovšem nízký a šlo tedy o nastavení klienta. Konfigurace na dotčených počítačích byla změněna a uživatelé byli v tomto směru poučeni o zákazu modifikace nastavení.



Obrázek 10 – nastavení upozornění v prostředí NFsen

Podobně lze vytvořit upozornění (alert) přímo v prostředí NFsen, po splnění podmínky může být odeslán e-mail – upozornění na nežádoucí aktivitu. Případně může být toto upozornění pouze počítáno pro následnou podrobnější analýzu.

Nasazení nástroje nfdump i nfsen je velmi snadné a lze jej zvládnout i se základní zkušeností s prostředím Linuxu. Nasazením sledování NetFlow toků jsem získal velmi dobrý nástroj pro analýzu chování síťové komunikace z / do internetu. Pro seznámení s problematikou a pro hlídání menší datové sítě jsou tyto nástroje zcela postačující. Pro síť s téměř 200 klienty bude zajímavější nasadit i kvalitnější analytický modul, který je součástí projektu z EU fondů.

5.2.3 Stav projektu Konsolidace IT služeb

Ačkoliv v prosinci prezentovaný harmonogram předpokládal schválení projektu v realizaci do konce února 2015 došlo k tomuto kroku až k 3 dubnu 2015.

Obrázek 11 – Stav projektu Konsolidace IT

Následně byla ke schválení odeslána zadávací dokumentace, po jejím schválení řídícím orgánem projektu – Centrem pro regionální rozvoj Olomouc byla soutěž v souladu se zákonem č. 137/2006 Sb. o veřejných zakázkách vyhlášena radou města. K tomu došlo na 11 jednání rady dne 27 dubna 2015 a soutěž byla zahájena. Termín pro podání nabídek je 25 květen 2015. Lze předpokládat, že po všech navazujících legislativních krocích bude samotná realizace (pokud bude soutěž úspěšná) zahájena v srpnu 2015 s termínem ukončení do 30 října 2015.

ZÁVĚR

Cílem diplomové práce bylo navrhnout a implementovat formou projektu bezpečnostní pravidla dle požadavků zákona č. 181/2014 Sb., o kybernetické bezpečnosti do lokální sítě městského úřadu.

V teoretické části své práce jsem shrnul legislativní rámec, využil znalosti situace v obdobných obcích s rozšířenou působností ve Zlínském kraji a provedl dílčí dotazníkový průzkum a následně shrnul celkovou situaci v informačních a komunikačních technologiích na městském úřadu v Kroměříži.

V praktické části jsem se nejdříve zaměřil na SWOT analýzu s cílem najít možná slabá místa a to jak uvnitř úřadu i tak popsat vnější rizika. Následně jsem navrhnul řadu změn a to především administrativního rázu. Dle výstupů teoretické části spočívá největší riziko v lidském faktoru, proto je třeba věnovat největší pozornost průběžnému školení pracovníků úřadu.

Zásadním výstupem administrativní části změn pak je vytvoření zcela nové informační koncepce úřadu, která již je v souladu s požadavky zákona č. 365/2000 Sb., o informačních systémech státní správy. V informační koncepci jsem shrnul klíčové informační systémy zajišťující výkon přenesené působnosti. Při tvorbě informační koncepce jsem taktéž narazil na řadu příležitostí pro zlepšení fungování lokální sítě především v administrativní rovině.

Dále jsem v technické rovině realizoval výměnu centrálního firewallu úřadu a získal tím nejen lepší služby při srovnatelné bezpečnosti ale především zdroj dat – NetFlow záznamů pro další analýzu. Závěrem praktické části jsem nasadil softwarové řešení pro ukládání a analýzu NetFlow záznamů. Zjistil jsem, že nasazení takového řešení v podmínkách lokální sítě městského úřadu je nejen poměrně levné ale především velmi snadné.

Nasazením NetFlow kolektoru jsem splnil podmínku plynoucí se zákona č. 184/2014 Sb. o kybernetické bezpečnosti uloženou pro významné informační systémy, mezi které můžeme řadit i lokální sít obce s rozšířenou působností. Tedy schopnost detekovat zdroje možných útoků z / proti lokální síti obce. Tedy schopnost data průběžně ukládat a následně i analyzovat.

ZÁVĚR V ANGLIČTINĚ

The aim of the thesis was to design and implement the project in the form of safety rules in accordance with the requirements of act of cyber security to the local network of the municipality.

In the theoretical part of my thesis I summarized the legislative framework, used knowledge of the situation in similar municipalities with extended powers in the Zlin region and conducted a partial survey questionnaire and then summed up the overall situation in the information and communication technologies in the municipal office in Kroměříž.

In the practical part, I initially focused on the SWOT analysis to find possible weak points both inside the office and to describe external risks. Then I suggested a number of changes, mainly administrative in nature. According to the outcomes of the theoretical part, the biggest risk in the human factor, so we need to pay most attention to ongoing staff training office.

A crucial outcome of the administrative changes then create a completely new concept of office information that is already in compliance with the requirements of the act of information systems of local government. The concept of the information I summarized the key information systems securing the exercise of delegated powers. In creating the concept of information, I also came across a lot of opportunities for improving the functioning of local networks especially at the administrative level.

Then I realized exchange technical level firewall central office and received by not only better service at a comparable safety but also the data source - NetFlow records for further analysis. Finally, the practical part, I put software solution for storing and analyzing NetFlow records. I found that the deployment of such solutions in terms of the local network of the municipal authority is not only relatively cheap but also very easy.

By deploying NetFlow collector, I met the condition of flowing the act of cyber security imposed for major information systems, among which we can also arrange local network municipalities with extended powers. Thus, the ability to detect sources of potential attacks from / to the local network community. Thus, the ability to store data continuously and subsequently analyzed.

SEZNAM POUŽITÉ LITERATURY

1. **HALÁSKOVÁ, Martina.** Veřejná správa. [Online] 2007. http://projekty.osu.cz/pvsos/doc/verejna_sprava.pdf..

2. Co je a co není informační systém veřejné správy. [Online] http://www.verejna-sprava.cz/Pages/Legislativa.aspx?blogId=5.

3. Zákon č. 365/200 Sb. o informačních systémech veřejné správy. [Online] 2000. http://www.zakonyprolidi.cz/cs/2000-365.

4. Vyhláška č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy. [Online] MVČR, 2006. http://www.zakonyprolidi.cz/cs/2006-529.

5. **PETERKA, Jiří.** S jakým přijetím se ve sněmovně setkal zákon o kybernetické bezpečnosti? [Online] www.lupa.cz, 17. 2 2014. http://www.lupa.cz/clanky/navrh-zakona-o-kyberneticke-bezpecnosti-prosel-prvnim-ctenim/.

6. **JAŠEK, Roman.** *Informační a datová bezpečnost.* Zlín : Zlín: Univerzita Tomáše Bati, Fakulta managementu a ekonomiky, 2006. ISBN 80-7318-456-7.

7. **NOVÁK, Luděk.** Systém řízení informační bezpečnosti. [Online] http://www.cybersecurity.cz/data/srib.pdf.

8. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti. [Online] 2014. http://www.zakonyprolidi.cz/cs/2014-181.

9. **KOTZIAN, Robert.** Dopad Zákona o kybernetické bezpečnosti na města a obce. [Online] 04 2015. https://www.isss.cz/archiv/2015/download/prezentace/cimib_kotzian.pdf.

10. **DOČEKAL, Daniel.** Weby českých bank ochromil DDoS útok, NBÚ žádá od postižených data. [Online] 3. 6 2013. http://www.lupa.cz/clanky/web-ceske-sporitelny-neni-dostupny-vcetne-online-sluzeb-servis24/.

11. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ.** *Teorie bezpečnosti počítačových sítí.* Kralice na Hané : Kralice na Hané, 2008. SBN 978-80-86686-35-6.

12. **TRULOVE, James.** *Sítě LAN: hardware, instalace a zapojení.* Praha : Grada, 2009. ISBN 978-80-247-2098-2.

13. **KABELOVÁ, Alena a Libor DOSTÁLEK.** *Velký průvodce protokoly TCP/IP a systémem DNS.* Brno : Computer Press, 2008. ISBN 978-80-251-2236-5.

14. Výzva IOP č. 06 Technologická centra obcí s rozšířenou působností. [Online] 2009. http://www.strukturalni-fondy.cz/cs/Jak-na-projekt/Vyzvy-a-akce-%281%29/06-IOP/Vyzva-IOP-c-06-Technologicka-centra-obci-s-rozsir.

15. Vyhlášení výzvy č. 22 IOP - Konsolidace IT a nové služby TC obcí. [Online] 14. 02 2014. http://www.strukturalni-fondy.cz/cs/Jak-na-projekt/Vyzvy-a-akce-%281%29/06-IOP/Vyhlaseni-vyzvy-c-22-IOP-Konsolidace-IT-a-nove-slu.

16. **SELECKÝ, Matúš.** *Penetrační testy a exploitace.* Brno : Computer Press, 2012. ISBN 978-80-251-3752-9.

17. Příklady informačních koncepcí. [Online] www.mvcr.cz. http://www.mvcr.cz/clanek/priklady-informacnich-koncepci.aspx.

18. Do nitra zákeřného spamu: co skrývá exekuční příkaz? [Online] www.zive.cz, 18. 7 2014. http://www.zive.cz/clanky/do-nitra-zakerneho-spamu-co-skryva-exekucni-prikaz/sc-3-a-174621.

19. Jak je na tom Vaše heslo? [Online] www.muni.cz, 27. 5 2014. https://security.ics.muni.cz/18-Jak-je-na-tom-vase-heslo.

20. NFDump tools. [Online] sourceforge.net, 2014. http://nfdump.sourceforge.net/.

21. NFsen. [Online] sourceforge.net, 2014. http://sourceforge.net/projects/nfsen/.

22. Installing Nfsen 1.6.12 on Centos. [Online] 05 2014. http://meefirst.blogspot.cz/2014/05/installing-nfsen-1612-on-centos_27.html.

23. Miktotik:IP/Traffic Flow. [Online] Mikrotik, 2013. http://wiki.mikrotik.com/wiki/Manual:IP/Traffic_Flow.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory
AIS	Agendový informační systém
BTS	Base Transceiver Station – základnová stanice mobilní sítě
CERT	Computer Emergency Response Team
CRV	Centrální registr vozidel
DDoS	Distributed Denial of service - Odmítnutí služby
DHCP	Dynamic Host Configuration Protocol
DMZ	demilitarized zone - zabezpečená místní síť
DNS	Domain Name Server – překlad jmen na adresy
ESXi	virtualizační řešení společnosti VMWare
FTP	File Transfer Protokol – přenos souborů
HDPE	Vysokohustotní polyethylen
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HW	Hardware
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection Systém – systém detekce anomálií
IK	Informační koncepce
IMAP	Interactive Mail Access Protocol
IMAPs	Interactive Mail Access Protocol Secure
IOP	Integrovaný operační program
IPS	Intrusion prevention systém – systém prevence průniku
IS	Informační systém
ISDS	Informační systém datových schránek
ISMS	Information Security Management Systém – systém řízení bezpečnosti

ISVS	Informační systém veřejné správy
ISZR	Informační systém základních registrů
JVM	Java virtual machine – pro běh aplikaci v jazyce Java
KII	Kritická informační infrastruktura
MDM	Mobile device management – systém pro zabezpečení mobilních zařízení
NAT	Network Adress Translation
NDS	Novell directory service – adresářová služba Novellu
ORG	převodník – systém základních registrů
ORP	Obec s rozšířenou působností
OSI	Open Systems Interconnection
PDF	Portable document format – formát přenositelných dokumentů Adobe
PGP	Pretty Good Privacy – zabezpečení e-mailu šifrováním
POP3	Post Office Protocol 3
POP3s	Post Office Protocol 3 Secure
PPTP	Point-to-Point Tunneling Protocol - Protokol dvoubodového tunelového spojení
PRTG	Paessler Router Traffic Grapher – nástroj pro monitoring sítí
PVS	Portál veřejné správy
QoS	Quality of services – kvalita služby
ROB	Registr obyvatel
ROS	Registr osob
RPP	Registr práv a povinností
RUIAN	Registr územní identifikace
SAN	Storage area network – síť sloužící pro ukládání dat
SIEM	Security Information and Event Management
SMTP	Simple Mail Transfer Protocol

SMTPs	Simple Mail Transfer Protocol Secure
SNMP	Simple Network Management Protocol
SW	Software
SWOT	Strengths, Weaknesses, Opportunities, Threats – analytická metoda
TC ORP	Technologické centrum obce s rozšířenou působnosti
TCK	Technologické centrum kraje
URL	Uniform Resource Locators
VIS	Významný informační systém
VPN	Virtual priváte network – virtuální privátní sít
WAN	Wide Area Network – rozsáhlá datová síť
ZRTP	kryptografický protokol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: INFORMAČNÍ KONCEPCE MĚÚ KROMĚŘÍŽ

Městský úřad Kroměříž

Informační koncepce

Projekt:	Atestace IS Městského úřadu Kroměříž dle Zákona č. 365/2000 Sb. o informačních systémech veřejné správy, ve znění pozdějších předpisů
Předmět:	Informační koncepce
Zpracoval: Bc. Jan Pšeja a kolektiv oddělení informatiky	Datum: 10. 3. 2015

Obsah

1 Úvod

Informační koncepce je dokument, v němž Městský úřad Kroměříž stanovuje své dlouhodobé cíle v oblasti dlouhodobého řízení IS. Jsou v něm definovány cíle v oblasti bezpečnosti a kvality spravovaných ISVS. Rovněž jsou stanovena základní pravidla pro pořizování a provozování ISVS.

1.1 Základní údaje o organizaci

V následující tabulce jsou uvedeny základní identifikační údaje Městského úřadu Kroměříž.

Název organizace:	Město Kroměříž
IČ:	00287351
Adresa:	Velké nám. 115/1, Kroměříž 767 01
Telefon:	573 321 111
Fax:	573 331 481
E-Mail:	posta@mesto-kromeriz.cz
WWW:	www.mesto-kromeriz.cz
Kontaktní osoba:	Bc. Jan Pšeja – vedoucí oddělení informatiky

1.2 Základní údaje o Informační koncepci

Název dokumentu:	Informační koncepce Městského úřadu Kroměříž
Datum schválení	10.3.2015
Způsob schválení:	Schváleno dne 10.3.2015 tajemníkem úřadu.
Doba platnosti:	5 let
Aktuální verze:	1.0

1.3 Údaje o předchozích verzích

V této kapitole jsou uvedeny všechny změny provedené v dokumentu tak jak byly po jeho schválení postupem času prováděny.

Změny dokumentu jsou prováděny především po provedení zásadních změn v Informačním systému Městského úřadu Kroměříž (dále jen IS MěÚ) nebo po provedení pravidelného vyhodnocení dodržování Informační koncepce. Změny provedené oproti každé předchozí verzi jsou vždy uvedeny v příslušné tabulce.

1.3.1 Aktuální verze

Označení verze	1.0
Datum vytvoření	24.2.2015
Datum schválení	10.3.2015
Způsob schválení:	Schváleno dne 10.3.2015 tajemníkem úřadu.
Platnost od kdy	1.4.2015
Umístění dokumentu	Intranet úřadu – sekce IS města – položka Atestace
Počet stran	31
Přílohy	0
Provedené změny	Jedná se o první verzi dokumentu

2 Zdroje a východiska

2.1 Přehled zdrojů použitých pro tvorbu Informační koncepce

Zdroji z města Kroměříž použitými pro tvorbu Informační koncepce jsou jak dokumenty strategické, tak dokumenty zaznamenávající stav IS k danému datu a další záměry:

- Strategický plán rozvoje Kroměříže
- Programové prohlášení Rady města Kroměříž

Inspirativním a významným faktorem při budování a rozvíjení informačního systému by měly být pravidelné schůzky informatiků krajského úřadu a městských úřadů Královéhradeckého kraje, jejichž hlavním cílem je vzájemná spolupráce, řešení důležitých otázek v oblasti informatiky a předávání informací.

Vzhledem k členství ČR v EU, je nutné brát v úvahu i strategické dokumenty EU týkající se informačních technologií.

Informační koncepce musí zohledňovat informační strategie, globální strategie či jiné podobné strategické dokumenty jak vyšších organizačních celků, tak úřadu samotného.

Za stěžejní dokumenty a projekty v celostátním měřítku pak lze považovat tyto:

- Státní informační a komunikační politika,
- Koncepce budování informačních systémů veřejné správy,
- Akční plán realizace státní informační politiky,
- Program informatizace územních orgánů veřejné správy,

2.2 Legislativní rámec

Ze základní legislativy ČR v oblasti informatiky je pro provozování ISVS nejvýznamnější zákon č. 365/2000 Sb., o informačních systémech veřejné správy ve znění pozdějších předpisů. Zákon byl novelizován následujícími právními úpravami:

- č. 517/2002 Sb.,
- č. 413/2005 Sb.,
- č. 444/2005 Sb.,
- č. 70/2006 Sb.,

- č. 81/2006 Sb.,
- č. 110/2007 Sb.,
- č. 130/2008 Sb.

Pro provozování ISVS jsou důležité i následující předpisy:

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění zákona č. 517/2002 Sb. a vyhlášky č. 529/2006 Sb. o dlouhodobém řízení informačních systémů veřejné správy,
- Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů,
- Zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů,
- Zákon č. 148/1998 Sb., o ochraně utajovaných skutečností, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek,
- Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů a v duchu prováděcích vyhlášek.
- Zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů
- Zákon č. 301/2008 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronických úkonech a autorizované konverzi dokumentů.

3 Přehled provozovaných ISVS a provozních agend s vazbou na ISVS

Pro účely Informační koncepce byl sestaven seznam všech informačních systémů a agend používaných v rámci úřadu. Kompletní seznam je přílohou této Informační koncepce.

Pro účel Informační koncepce pak byly ze seznamu vybrány agendy a informační systémy, které splňují definici ISVS a dle platné legislativy tedy podléhají procesu dlouhodobého řízení ISVS.

V dokumentu jsou popsány ISVS a provozní systémy splňující následující podmínky:

- úřad je správcem ISVS (úřad agendu sám pořídil),
- provozní agenda má vazbu na jiný ISVS

V dokumentu tedy nejsou popsány provozní systémy, které nemají žádnou vazbu na jakýkoliv ISVS.

Každý provozovaný ISVS je pak popsán za pomoci následujících atributů:

- úplný název agendy,
- zkratka názvu agendy,
- související právní předpisy,
- útvar zajišťující provoz ISVS,
- charakteristika ISVS,
- zpracovávaná data,
- technické a programové prostředí,
- současný stav ISVS,
- předpokládané změny

Každá provozní agenda s vazbou na ISVS je popsána následujícími atributy:

- úplný název agendy,
- zkratka názvu agendy,
- související právní předpisy,
- útvar zajišťující provoz agendy,

- charakteristika agendy,
- současný stav agendy,
- popis vazby na ISVS

3.1 Informační systémy veřejné správy

3.1.1 ESPI 9 – Evidence správních řízení

Úplný název ISVS:	ESPI 9 – Evidence správních řízení
Zkratka názvu:	ESPI
Právní předpisy:	Zákon č. 500/2004 Sb., správní řád
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence správních řízení v oblasti životního prostředí.
Zpracovávaná data:	Data o správních řízeních a jejich účastnících.
Technické a programové prostředí:	Windows 7
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.2 EVI 9 – Evidence odpadů, zařízení

Úplný název ISVS:	EVI 9 – Evidence odpadů, zařízení
Zkratka názvu:	EVI
Právní předpisy:	Zákon č. 185/2001 Sb., o odpadech, vyhláška č. 381/2001 Sb., vyhláška č. 383/2001 Sb.
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence odpadů při každém vzniku, zneškodnění nebo předání odpadu, generování hlášení a statistických výkazů.
Zpracovávaná data:	Data o odpadech.
Technické a programové prostředí:	Windows 7
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.3 Evidence myslivosti

Úplný název ISVS:	Evidence myslivosti
Zkratka názvu:	EMY
Právní předpisy:	Zákon č. 449/2001 Sb., o myslivosti
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence honebních společenstev, loveckých psů, ulovené zvěře atd, myslivecké plánování a statistiky, protokoly honiteb, …
Zpracovávaná data:	Údaje o honitbách a o vykonávané myslivecké činnosti
Technické a programové prostředí:	Windows 7
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.4 Geovap - Poplatky

Úplný název ISVS:	Geovap – poplatky
Zkratka názvu:	PPL
Právní předpisy:	Zákon č. 565/1990 Sb. o místních poplatcích
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence plátců, automatizovaná správa místních daní a poplatků, sledování plateb, evidence splátek a půjček, evidence neplatičů, exporty dat do účetního systému.
Zpracovávaná data:	Data o odpadech.
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.5 VITA SW - Přestupkové řízení

Úplný název ISVS:	VITA SW - Přestupkové řízení
Zkratka názvu:	PRS

Právní předpisy:	Zákon č. 200/1990 Sb., o přestupcích, zákon č. 500/2004 Sb., správní řád
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence přestupků a jiných správních deliktů, vedení přestupkového, příkazního, blokového řízení.
Zpracovávaná data:	Údaje o přestupcích, řízeních a pachatelích
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.6 Geovap – ROB – Registr obyvatel

Úplný název ISVS:	ROB – Registr obyvatel
Zkratka názvu:	ROB
Právní předpisy:	Zákon č. 133/2000 Sb., o evidenci obyvatel a rodných číslech.
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence obyvatel, vedení agendy ohlašovny.
Zpracovávaná data:	Údaje o osobách, jejich partnerech, rodičích, dětech a trvalém pobytu.
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.7 Geovap - eSSL – Spisová služba

Úplný název ISVS:	eSSL – Spisová služba
Zkratka názvu:	eSSL
Právní předpisy:	Zákon č. 499/2004 Sb., o archivnictví a spisové službě
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Komplexní vedení spisové služby, automatizovaná evidence a oběh písemností v celém jejich životním cyklu.
Zpracovávaná data:	Údaje o písemnostech
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.

Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.8 Kvasar - Ovzduší SQL

Úplný název ISVS:	Kvasar - Ovzduší SQL
Zkratka názvu:	OVZ
Právní předpisy:	Zákon č. 86/2002 Sb., o ochraně ovzduší
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence zdrojů znečišťování ovzduší, evidence poplatníků a poplatků za znečišťování ovzduší
Zpracovávaná data:	Údaje o zdrojích znečištění, poplatnících a poplatcích
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.9 VITA SW - Stavební úřad

Úplný název ISVS:	Vita SW – Stavební úřad
Zkratka názvu:	STU
Právní předpisy:	Zákon č. 183/2006 Sb., o územním plánování a stavebním řádu
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Evidence správních řízení a podpora činnosti obecního stavebního úřadu.
Zpracovávaná data:	Údaje o územních a stavebních řízeních a jejich účastnících.
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.1.10 Vodoprávní úřad

Úplný název ISVS:	Vita SW – Vodoprávní úřad
Zkratka názvu:	VDU
Právní předpisy:	Zákon č. 254/2001 Sb., o vodách
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž

Charakteristika:	Evidence správních řízení a podpora činnosti vodoprávního úřadu.
Zpracovávaná data:	Údaje o správních řízeních a jejich účastnících.
Technické a programové prostředí:	Windows 7 + Oracle SQL v11
Současný stav:	ISVS je v rutinním provozu.
Předpokládané změny:	Pro tento ISVS nejsou plánovány ani připravovány žádné změny.

3.2 Provozní agendy s vazbou na ISVS

3.2.1 GINIS – INT – Interface

Úplný název ISVS:	GINIS – INT – Interface
Zkratka názvu:	INT
Právní předpisy:	Zákon č. 563/1991 Sb., o účetnictví
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Účetní agenda, výkaznictví
Současný stav:	V rutinním provozu.
Vazba na ISVS:	Výstupní rozhraní pro předávání finančních výkazů krajskému úřadu.

3.2.2 GINIS – UCR – Účetní a rozpočtové výstupy

Úplný název ISVS:	GINIS – UCR – Účetní a rozpočtové výstupy
Zkratka názvu:	UCR
Právní předpisy:	Zákon č. 563/1991 Sb., o účetnictví
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž
Charakteristika:	Účetní agenda, výkaznictví
Současný stav:	V rutinním provozu.
Vazba na ISVS:	Předávání finančních výkazů krajskému úřadu.

3.2.3 Flux - Personalistika a mzdy

Úplný název ISVS:	Flux – Personalistika a mzdy
Zkratka názvu:	PAM
Právní předpisy:	Zákon č. 262/2006 Sb., zákoník práce, nařízení vlády č. 564/2006 Sb.
Provoz zajišťuje:	Oddělení informatiky MěÚ Kroměříž

Charakteristika:	Personální a mzdová agenda
Současný stav:	V rutinním provozu.
Vazba na ISVS:	Aplikace poskytuje data do Informačního systému o platech dle předepsané datové struktury.

4 Záměry na pořízení nových ISVS

Městský úřad Kroměříž v současnosti neplánuje pořízení nebo vybudování nového ISVS.

4.1 Zásady při pořizování nových ISVS

Vlastnímu pořízení nového ISVS předchází v podmínkách Městského úřadu Kroměříž nejprve formulace záměru na pořízení nového ISVS.

Záměr na pořízení ISVS je materiál v písemné nebo elektronické formě, který obsahuje základní fakta o novém ISVS včetně důvodu k jeho pořízení.

Záměr na pořízení ISVS obsahuje následující údaje:

- název ISVS,
- související právní předpisy
- důvod pořízení,
- zpracovávaná data a poskytované služby,
- útvar zajišťující provoz ISVS,
- náklady na pořízení a provozní náklady,
- požadavky na lidské zdroje,
- termín realizace a termín spuštění rutinního provozu.

Záměr na pořízení ISVS je vypracován vnitřním útvarem úřadu (odbor, oddělení) obvykle na základě požadavku vedoucího odboru, tajemníka úřadu, člena zastupitelstva města, popř. zřízené komise či výboru.

O akceptaci či odmítnutí záměru rozhoduje pracovní skupina složená z:

- vedoucího oddělení informatiky,
- vedoucího příslušného odboru,
- tajemníka úřadu.

Složení pracovní skupiny se může operativně měnit v závislosti na typu navrhovaného ISVS. Pokud pracovní skupina doporučí záměr realizovat, je nadále pořízení nového ISVS řešeno jako samostatný projekt.

Celý systém řízení projektu má definovanou strukturu a je závazný pro všechny subjekty, které se na projektu podílejí během celého životního cyklu projektu.

Při realizaci projektu jsou určeny následující základní role:

Vedoucí projektu

- odpovídá za průběh projektu a řídí projektový tým,
- je zodpovědný za výběr dodavatelů a případných externích spolupracovníků
- mimo jiné je i zodpovědný za dosahování cílů projektu.

Projektový tým

- je zodpovědný za realizaci zadání projektu během celého životního cyklu projektu,
- zajišťuje kompletně řešení projektu spolu s případnými externími dodavateli a spolupracovníky,
- podléhá vedoucímu projektu.

Garant projektu

- je nejvyšším orgánem řízení projektu a vrcholným rozhodovacím orgánem,
- rozhoduje zejména o strategicky významných okolnostech,
- pravidelně sleduje a kontroluje průběh dosahování cílů projektu,
- je koordinátorem projektu a jeho vazeb na okolí,
- určuje konkrétní termíny v průběhu projektu,
- je zodpovědný za celkovou koncepci a architekturu řešení konkrétního projektu.

V podmínkách Městského úřadu Kroměříž se obvykle jedná o vedoucího odboru, popř. tajemníka úřadu.

5 Řízení kvality ISVS

Informační systém Městského úřadu Kroměříž je systém dosti rozsáhlý – přistupuje k němu cca. 200 uživatelů a celkem je provozováno na pět desítek různých agend. Správa informačního systému takového rozsahu klade nároky nejen na hardware a sítě, ale celkem logicky i na systém jeho dlouhodobého řízení.

5.1 Stanovení dlouhodobých cílů kvality ISVS

Z výše uvedených důvodů probíhá budování IS MěÚ jako informačního systému, který bude:

- bez výhrad splňovat platnou legislativu ČR,
- umožňovat rychlejší dosahování cílů úřadu ve všech oblastech,
- budován s důrazem na transparentnost – veškeré postupy jsou dokumentovány,
- uživatelům důvěryhodným zdrojem aktuálních a ověřených informací s vysokou mírou použitelnosti a vysokou užitnou hodnotou – kvalita služeb,
- bezpečný a spolehlivý.

5.2 Role a odpovědnosti v oblasti řízení kvality

Při budování IS MěÚ je důsledně uplatňován projektový způsob řízení. Totéž platí i v oblasti zajištění kvality. Každá změna, popřípadě pořízení nové části informačního systému (agenda, informační systém, technické řešení, ...) v IS MěÚ je vždy řešena jako samostatný projekt.

Jednotlivé role při budováni IS MěÚ (a zároveň v systému zajištění kvality) jsou delegovány na jednotlivé organizační složky úřadu v závislosti na povaze konkrétního projektu.

Celý systém řízení projektu má definovanou strukturu a je závazný pro všechny subjekty, které se na projektu podílejí během celého životního cyklu projektu.

Ve vztahu k řízení systému jakosti jsou to zejména následující:

Vedoucí projektu

- odpovídá za průběh projektu a řídí projektový tým,
- je zodpovědný za výběr dodavatelů a případných externích spolupracovníků
- mimo jiné je i zodpovědný za dosahování cílů v oblasti zajištění kvality.

Projektový tým

- je zodpovědný za realizaci zadání v oblasti zajištění kvality během celého životního cyklu projektu,
- zajišťuje kompletně řešení projektu spolu s případnými externími dodavateli a spolupracovníky,
- podléhá vedoucímu projektu.

Garant projektu

- je nejvyšším orgánem řízení projektu a vrcholným rozhodovacím orgánem,
- rozhoduje zejména o strategicky významných okolnostech,
- pravidelně sleduje a kontroluje průběh dosahování cílů v oblasti zajištění kvality,
- je koordinátorem projektu a jeho vazeb na okolí,
- určuje konkrétní termíny v průběhu projektu,
- je zodpovědný za celkovou koncepci a architekturu řešení konkrétního projektu.

V podmínkách Městského úřadu Kroměříž se obvykle jedná o vedoucího odboru, popř. tajemníka úřadu.

5.3 Způsob plnění požadavků na kvalitu ISVS

Nedílnou součástí zadání každého projektu (pořízení nebo změna stávajícího ISVS) je stanovení požadavků na kvalitu.

Provádí se vždy konkretizací všech základních cílů řízení kvality a jejich povaha je vždy závislá na povaze konkrétního projektu.

Typickými požadavky na kvalitu jsou například:

- včasná aktualizace údajů,
- identifikace autorů dat,

- stanovení metodiky testování ISVS,
- organizační směrnice provozu ISVS,
- rozsah dokumentace implementace a provozu ISVS,
- a další.

Za stanovení dílčích požadavků je zodpovědný garant projektu, popřípadě vedoucí projektu.

Implementaci požadavků na kvalitu pak provádí projektový tým v závislosti na termínech řešení a s ohledem na postupu řešení jednotlivých úloh.

5.4 Vyhodnocování řízení kvality

Vyhodnocování řízení kvality provádí garant projektu spolu s vedoucím projektu. Vyhodnocování kvality je součástí obvyklých kontrolních činností při řízení každého projektu. Součástí tohoto procesu je dokumentace systému řízení kvality, která je součástí projektové dokumentace.

Jedná se obvykle o následující dokumenty:

- zápisy ze schůzí organizačních složek projektu,
- průběžné zprávy o stavu projektu,
- zprávy o výsledcích testování.

5.5 Řízení kvality při rutinním provozu ISVS

Při běžném provozu ISVS pracovník odpovědný za řízení kvality provádí pravidelné kontroly dosahování cílů řízení kvality a plnění konkrétních požadavků na kvalitu. Proces vyhodnocování pak provádí pracovník odpovědný za řízení kvality ve spolupráci se správci (administrátory) jednotlivých ISVS.

Pracovník odpovědný za řízení kvality udržuje seznam požadavků na kvalitu, které byly stanoveny při pořízení každého ISVS. Ze seznamu jsou vyřazeny požadavky na kvalitu, které nejsou při běžném provozu relevantní (měly význam pouze ve fázích pořízení či implementace daného ISVS). Zbylé požadavky pak podléhají pravidelnému vyhodnocování.

Vyhodnocování probíhá minimálně 1x ročně a o jeho výsledcích se provádí zápis, který je součástí provozní dokumentace IS MěÚ.

6 Řízení bezpečnosti ISVS

Strategickým dokumentem v oblasti řízení bezpečnosti je Bezpečnostní politika informačního systému Městského úřadu Kroměříž. Je souhrnem bezpečnostních předpisů a zásad definujících způsob zabezpečení provozu provozovaných ISVS.

Pomocí bezpečnostní politiky jsou stanovena základní pravidla zajišťující bezpečný provoz, integritu uložených dat a řízení přístupů k datům pro oprávněné uživatele na základě jejich funkčního zařazení v organizační struktuře organizace.

Bezpečnostní politika určuje normy, pravidla a předpisy, které definují způsob správy, ochrany a distribuce citlivých informací a jiných konkrétních informačních zdrojů v rámci úřadu. Specifikuje bezpečnostní opatření a způsob jejich implementace, určuje způsob použití, který zaručuje přiměřenou bezpečnost odpovídající požadavkům bezpečnostní politiky úřadu.

Bezpečnostní politika IS MěÚ rovněž obecně definuje bezpečné používání informačních zdrojů.

6.1 Stanovení dlouhodobých cílů v oblasti bezpečnosti

Základními bezpečnostními cíli je zajištění následujících stavů a činností:

1) ochrana dat a prostředků ISVS,
2) trvalé a kvalitní zajištění dostupnosti, důvěrnosti, integrity a autentizace dat,
3) zajištění bezpečné komunikace s okolím.

6.2 Základní požadavky na bezpečnost

Požadavky na bezpečnost ISVS jsou konkretizací bezpečnostních cílů:

TRVALÉ A KVALITNÍ ZAJIŠTĚNÍ DOSTUPNOSTI, DŮVĚRNOSTI, INTEGRITY A AUTENTIZACE DAT

- zajištění soukromí uživatelů – ochrana uživatele před zjištěním nebo zneužitím jeho identity jinými uživateli nebo cizími osobami,

- identifikace a autentifikace uživatelů – zajištění přístupu k datům (prohlížení, aktualizace) IS MěÚ pouze pro oprávněné uživatele a to na základě jejich funkčního zařazení,
- řízení provozu a monitoring počítačové sítě,
- existence systému pravidelného zálohování a archivace dat,
- existence plánu obnovy provozu IS (nebo jeho kritických částí) po havárii,

OCHRANA DAT A PROSTŘEDKŮ IS

- zajištění personální bezpečnosti,
- zajištění fyzické bezpečnosti prostředků IS MěÚ,
- existence systému komplexní ochrany před škodlivými programy (viry, nepřátelské kódy),
- vybudování bezpečnostních mechanismů vůči napadení zevnitř (bezpečnostní pravidla, jak se mají uživatelé chovat),
- ochrana IS MěÚ před napadením z externích sítí – bezpečnostní opatření zamezující možnosti průniku do vnitřní sítě (ochrana serverů, aktivních prvků a uživatelských stanic),
- ustanovení správce agendy (ISVS nebo provozní agendy).

ZAJIŠTĚNÍ BEZPEČNÉ KOMUNIKACE S OKOLÍM

- bezpečná komunikace mezi úřadem a jinými subjekty (především s orgány veřejné správy),
- používání bezpečných komunikačních cest,
- používání prostředků pro šifrování přenášených dat.

6.3 Role a odpovědnosti v oblasti řízení bezpečnosti

Bezpečnost IS MěÚ spadá do oblasti provozní problematiky úřadu, proto schvalování a vyhlašování realizace bezpečnostní politiky včetně základního personálního obsazení a stanovení rolí a odpovědností v oblasti bezpečnosti provádí tajemník úřadu.

Pro bezpečnost IS jsou přijata následující organizační opatření:

- definování bezpečnostní komise, její pravomoci a odpovědnosti,
- definování bezpečnostního správce, jeho pravomoci a odpovědnosti,

- definování odpovědnosti a povinností uživatelů IS MěÚ.

6.3.1 Bezpečnostní komise

Bezpečnostní komise má tyto členy:

- vedoucí oddělení informatiky – předseda komise,
- zástupce odboru kanceláře tajemníka úřadu, oddělení krizového řízení,
- zástupce odboru správy Měú.

Bezpečnostní komise:

- je poradním orgánem tajemníka úřadu,
- formuluje zásady bezpečnostní politiky,
- zodpovídá za řízení přístupu k informačním systémům a informačním aktivům,
- koordinuje implementaci opatření v oblasti bezpečnosti IS MěÚ,
- zodpovídá za průběžné monitorování a ověřování funkčnosti zavedených bezpečnostních opatření,
- navrhuje a podporuje iniciativy týkající se bezpečnosti IS MěÚ,
- prosazuje, aby podpora bezpečnostní politiky ze strany vedení byla viditelná v celém úřadě,
- definuje bezpečnostní cíle a sleduje jejich zavádění,
- navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS MěÚ,
- navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS v rámci celého úřadu,
- navrhuje metody a postupy v oblasti bezpečnosti,
- kontroluje, aby bezpečnost byla součástí procesu plánování v oblasti informatiky,
- prosazuje zvyšování bezpečnostního uvědomění uživatelů IS MěÚ,
- definuje potřebné požadavky na lidské znalosti a na finanční náklady,
- řeší disciplinární problémy vůči bezpečnosti,
- hodnotí účinnost bezpečnostní politiky.

6.3.2 Bezpečnostní správce

Bezpečnostní správce:

- zodpovídá za dodržování bezpečnosti IS MěÚ,
- spolupracuje s bezpečnostní komisí a správcem IS MěÚ,
- řídí zavádění bezpečnostních opatření podle definovaných bezpečnostních cílů,
- průběžně monitoruje bezpečnostní incidenty a účinnost bezpečnostní politiky a ověřuje funkčnost zavedených bezpečnostních opatření,
- podílí se na zvyšování bezpečnostního uvědomění uživatelů IS MěÚ,
- zodpovídá za to, aby bezpečnostní politika byla součástí plánování v oblasti informatiky,
- navrhuje hlavní kroky vedoucí ke zvýšení bezpečnosti dat a prostředků v IS,
- navrhuje specifické role a odpovědnosti v oblasti bezpečnosti IS MěÚ v rámci celého úřadu,
- navrhuje metody a postupy v oblasti bezpečnosti IS MěÚ,
- zajišťuje, aby dodavatelé služeb IT dodržovali bezpečnostní politiku úřadu a ostatní relevantní vnitřní předpisy.

6.4 Způsob plnění požadavků na bezpečnost

Za plnění konkrétních bezpečnostních požadavků odpovídá pro každý ISVS pracovník oddělení informatiky - správce (administrátor) konkrétního ISVS.

Jeho povinností je dbát na to, aby při běžném provozu informačního systému byly dodržovány postupy stanovené pro splnění bezpečnostních požadavků.

Tyto postupy mohou být různého charakteru, nejčastěji však jde o:

- zákonné normy,
- interní směrnice úřadu (provozní řád, bezpečnostní politika, ...),
- doporučení dodavatele ISVS.

6.5 Plnění bezpečnostních požadavků při implementaci nového ISVS

Řízení bezpečnosti při implementaci nového ISVS je opět nedílnou součástí konkrétního projektu. Za splnění jednotlivých bezpečnostních požadavků, které jsou součástí projektové

dokumentace, odpovídá vedoucí projektu. Plnění pak provádí projektový tým, respektive jeho jednotliví členové odpovědní za realizaci dílčích projektových úloh.

Důležitou součástí řízení bezpečnosti při implementaci nového ISVS je projektová dokumentace, týkající se oblasti bezpečnosti.

Jedná se zejména o:

- smlouvy (se zaměstnanci a externími subjekty),
- předávací a akceptační protokoly,
- interní směrnice úřadu,
- zápisy ze schůzí organizačních složek projektu,

6.6 Vyhodnocování řízení bezpečnosti ISVS

Vyhodnocování řízení bezpečnosti ISVS se děje formou prověrek a testů. Proces řídí bezpečnostní správce, který při jejich provádění spolupracuje se správcem (administrátorem) konkrétního ISVS.

Bezpečnostní prověrka je konána pro každý ISVS nejméně 1x ročně obvykle na pokyn bezpečnostního správce. Dále může být vykonána mimořádně (mimo obvyklý termín) na pokyn bezpečnostní komise nebo bezpečnostního správce.

Bezpečnostní prověrka může mít formu:

- kontroly dodržování organizačních postupů (interních směrnic, ...),
- kontroly logovacích souborů,
- kontroly provozních deníků,
- kontroly přístupových práv k ISVS,
- pokusu o uložení nekorektních dat,
- simulace pokusu o neoprávněný přístup k ISVS.

O průběhu a výsledcích bezpečnostní prověrky se provádí zápis, který je součástí provozní dokumentace oddělení informatiky úřadu.

7 Vyhodnocování dodržování IK

Sledování (a pravidelné vyhodnocování) dodržování zásad stanovených v Informační koncepci je proces, který napomáhá k plnění dlouhodobých cílů Městského úřadu Kroměříž. Vyhodnocování je pak důležitou činností při vlastním provozu IS MěÚ.

Vyhodnocování dodržování Informační koncepce probíhá vždy 1x ročně. O výsledku vyhodnocení se zhotovuje zápis, který je součástí dokumentace IS MěÚ.

7.1 Popis procesu vyhodnocování dodržování IK

Vyhodnocování dodržování Informační koncepce provádí pracovní skupina ve složení:

- zástupce kanceláře úřadu,
- vedoucí oddělení informatiky.

Pracovní skupina může být v případě potřeby rozšířena o odborné pracovníky jak z řad zaměstnanců úřadu, tak o externí spolupracovníky.

Pracovní skupina provádí vyhodnocování v následujících oblastech a jejím cílem je zjistit zda:

- aktuální verze IK obsahuje aktuální a pravdivý popis všech používaných ISVS a provozních systémů s vazbou na ISVS (včetně plánovaných změn),
- aktuální verze IK obsahuje všechny záměry na pořízení nových ISVS,
- požadavky na bezpečnost a kvalitu jsou jednotlivými agendami respektovány a plněny,
- plnění požadavků na bezpečnost a kvalitu příznivě ovlivňuje plnění
- dlouhodobých cílů v těchto oblastech,
- při pořizování nových ISVS (a při provádění změn) jsou uplatňovány zásady uvedené v IK,
- postupy a zásady stanovené v IK nejsou v rozporu s jinými vnitroorganizačními směrnicemi se vztahem k IS MěÚ (Provozní řád IS, Bezpečnostní politika, ...),
- postupy a zásady stanovené v IK jsou skutečně v praxi dodržovány,
- nedostatky zjištěné při posledním vyhodnocování dodržování IK byly odstraněny,
- jsou dodržovány zásady financování IS MěÚ uvedené v IK,
- jsou dodržovány zásady provádění aktualizace IK,

- jsou s aktuálním zněním IK seznámeni všichni pracovníci úřadu, pro které je tento dokument relevantní.

Vyhodnocení probíhá pro každou výše uvedenou oblast zvlášť a ve stejném duchu je i pořízen zápis o vyhodnocování. Při zjištěných nedostatcích je zároveň stanoven způsob jejich odstranění včetně uvedení termínu a osob odpovědných za jejich odstranění.

Konečná verze zápisu je schválena a podepsána všemi osobami, které se na vyhodnocování podílely. Schválená verze je pak dohodnutým způsobem zpřístupněna příslušným pracovníkům úřadu.

8 Postupy při provádění změn IK

Udržování Informační koncepce v aktuálním stavu je základní předpoklad splnění zákonných povinností při realizaci dlouhodobého řízení IS MěÚ.

8.1 Role a odpovědnosti

Při procesu provádění změn IK plní zásadní role následující útvary a pracovníci:

Pracovník odpovědný za aktualizaci Informační koncepce,

který je odpovědný za finální podobu dokumentu IK a za udržování stanoveného způsobu provádění změn včetně archivace jednotlivých verzí dokumentace IK.

Pracovník odpovědný za dodržování Informační koncepce,

který navrhuje změny IK na základě výsledků vyhodnocování dodržování IK.

Oddělení informatiky úřadu,

které má přehled o všech používaných ISVS a provozních systémů s vazbou na ISVS.

Pracovní skupina pro vyhodnocování dodržování IK,

která (mimo jiné) provádí kontrolu aktuálnosti IK a navrhuje postupy k odstranění zjištěných nedostatků.

8.2 Popis procesu provádění změn IK

Řízení změn v IS MěÚ je vždy dokumentováno. Stejné povinnosti proto podléhá i provádění změn Informační koncepce. Ke změně Informační koncepce může dojít z rozličných důvodů, ať organizačních, legislativních nebo technických.

Nejčastěji dochází ke změnám Informační koncepce z následujících důvodů:

Změna v organizační struktuře úřadu.

Při organizačních změnách dochází k přesunu kompetencí, popř. vykonávaných činností mezi jednotlivými organizačními jednotkami (odbory, oddělení). Mohou vznikat nové organizační jednotky, další mohou zanikat. Pakliže se provedená organizační změna týká osob či útvarů, kterým jsou přiřazeny určité odpovědnosti v rámci Informační koncepce, je nutné přistoupit k aktualizaci IK.

Za provedení těchto změn je odpovědné oddělení informatiky a pracovník odpovědný za aktualizaci Informační koncepce.

Pořízení nového ISVS (provozního systému s vazbou na ISVS)

Při pořizování nového ISVS se postupuje podle postupů popsaných v příslušných kapitolách tohoto dokumentu. Každému pořízení ISVS předchází vypracování (a schválení) záměru na pořízení a zpracování projektové dokumentace.

Změna v ISVS

Změnou zde rozumíme ty změny, které mají za „následek“ změnu funkčnosti, změnu rozsahu zpracovávaných dat nebo poskytovaných služeb. Veškeré změny jsou dokumentovány a stávají se součástí provozní dokumentace ISVS.

Za úplnost provozní dokumentace zodpovídá administrátor příslušného ISVS. Za změnu se naopak nepovažují provozní zásahy, jako oprava chyb software a podobné činnosti.

Provádění změn v ISVS se děje v režimu tzv. změnového řízení.

Nejprve musí být vypracován návrh na změnu ISVS, který obsahuje důvod vzniku požadavku, soupis požadavků na změnu, analýzu současného a cílového stavu ISVS. Dále je navržen způsob realizace provedení změny včetně časového harmonogramu a odhadu nákladů. Návrh na změnu může být předložen organizační jednotkou, která zajišťuje provoz ISVS, popřípadě oddělením informatiky.

Ve fázi realizace změny ISVS je pak stanovován závazný harmonogram činností, schvalovány použité nástroje a určeny postupy pro testování provedených změn.

Ukončení provozu ISVS

Z různých důvodů může být rozhodnuto o ukončení provozu ISVS. Obvykle se tak děje při přesunu vykonávaných činností mezi složkami veřejné správy nebo při nahrazení jednoho ISVS druhým. Návrh na ukončení provozu ISVS může být předložen organizační jednotkou, která zajišťuje provoz ISVS, popřípadě oddělením informatiky.

V každém případě ukončení provozu je stanoven časový harmonogram ukončení provozu. Důležitým krokem je i stanovení způsobu jak bude nakládáno s daty ISVS a jak bude naloženo s programovým vybavením a s provozní dokumentací.

Následně jsou definovány lhůty pro skartaci a likvidaci dokumentace, dat a datových nosičů.

Za dodržení všech stanovených postupů odpovídá oddělení informatiky úřadu.

9 Financování IS úřadu

Základním zdrojem pro financování IS MěÚ je schválený rozpočet. Veškerý provoz a rozvoj informačního systému musí být v souladu s danými rozpočtovými pravidly. Schvalování rozpočtu provádí Zastupitelstvo města Kroměříž.

Výše celkového ICT rozpočtu je dána souhrnem provozních a investičních nákladů během kalendářního roku. Za přípravu rozpočtu IS MěÚ je odpovědné oddělení informatiky úřadu, který příslušné finanční částky zařadí do návrhu rozpočtu na příští rok.

Financování IS MěÚ může být v některých případech financováno i z různých dalších zdrojů, jako jsou např. různé dotační tituly. Získané finanční částky jsou pak zařazovány do rozpočtu města pomocí rozpočtových změn.

10 Útvar odpovědný za dodržování IK

Za realizaci informační koncepce, tzn. na naplňování dlouhodobých cílů v oblasti informatiky, provoz ISVS a provozních systémů s vazbami na ISVS, dodržování postupů stanovených v Informační koncepci a odstraňování nedostatků při vyhodnocování dodržování Informační koncepce je odpovědné oddělení informatiky úřadu.

Dodržování Informační koncepce s sebou nese povinnost plnit různé zákonné povinnosti, tak jak stanovuje aktuální právní rád České republiky. Za splnění těchto zákonných povinností je rovněž odpovědné oddělení informatiky úřadu.