VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZVÝŠENÍ BEZPEČNOSTI INFORMAČNÍHO SYSTÉMU OBECNÍHO ÚŘADU

ENHANCE THE SECURITY OF THE INFORMATION SYSTEM IN THE MUNICIPAL ADMINISTRATION

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — MATÚŠ SOLÁR
AUTHOR

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

BRNO 2015

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2014/2015
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Solár Matúš

Manažerská informatika (6209R021)

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

Zvýšení bezpečnosti informačního systému obecního úřadu

v anglickém jazyce:

Enhance the Security of the Information System in the Municipal Administration

Pokyny pro vypracování:

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

Seznam odborné literatury:

ČESKO. Zákon č. 181 ze dne 29. srpna 2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: Sbírka zákonů České republiky. 2014.
ČSN ISO/IEC 27001:2014 Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky. Český normalizační institut, 2014.
DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. Řízení bezpečnosti informací. 2. rozšířené vydání. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.
POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

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

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

L.S.

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

V Brně, dne 28.2.2015

Abstrakt

Táto bakalárska práca sa zaoberá a analyzuje problematiku v prostredí bezpečnosti informačných systémov. Navrhuje možné riešenie, jeho praktickú implementáciu, zvýšenia bezpečnosti v reálnom prostredí štátnej správy, konkrétne obecného úradu. Súčasťou práce je analýza súčasného stavu, ktorá vypovedá o nedostatkoch v danom smere, teoretické východiská a v neposlednom rade návrhy na zvýšenie bezpečnosti, ktoré v prípade praktického zavedenia zaistia požadovaný stav bezpečnosti.

Abstract

This bachelor's thesis deals and analyzes the problems in the area of information system security. It proposes a possible solutions, its practical implementation, improve safety in the real environment of government, namely the municipal office. First part of this work analyzes the current situation, which describes the deficiencies in the given directions. Another part of this work speaks about theoretical background and in the end are explained my practical advices for improving of the security system.

Kľúčové slová

bezpečnosť, bezpečnostná politika, bezpečnosť dát, bezpečnosť informácií, bezpečnostné smernice, zálohovanie dát, riadenie bezpečnosti

Key words

security, security policy, data security, information security, security guidelines, data backup, safety control

Bibliografická citácia

SOLÁR, M. *Zvýšení bezpečnosti informačního systému obecního úřadu.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2015. XY s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D..

Prehlásenie autora o pôvodnosti práce

Prehlasujem, že predložená bakalárska práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporučil autorské práva (v zmysle zákona 121/2000 Zb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 30. mája 2015 .....

podpis študenta

Poďakovanie

Týmto by som sa rád poďakoval vedúcemu mojej bakalárskej práce,
pánovi Ing. Viktorovi Ondrákovi, Ph.D. za cenné pripomienky, poskytnuté rady a v neposlednom rade za ochotu prejavenú pri spracovávaní tejto bakalárskej práce.

Obsah

ÚVOD

Informácie majú v dnešnej dobe vysokú hodnotu pre akúkoľvek organizáciu. Výrobné či nevýrobné podniky, štátne alebo súkromné, malé či veľké podniky, všetky druhy spracovávajú narastajúce množstvo údajov. Motiváciou pre získanie informácií môže byť hneď niekoľko podnetov ako napríklad obohatenie, získanie postavenia na trhu ale aj pomsta či dokazovanie vlastných zručností jednotlivca a mnohé iné.

Informačný systém, ako nástroj na spracovanie dát musí byť spoľahlivý v každej z jeho častí. Iba takým spôsobom môžu byť informácie chránené pred útočníkmi externými ale aj internými. Informácie sú klasifikované ako aktíva a preto je v záujme každej organizácie ich chrániť. Spôsoby a postupy ako chrániť tieto aktíva popisuje informačná bezpečnostná politika. Informačné systémy štátnej správy uchovávajú obrovské množstvá dát, ktoré sa týkajú samotných občanov a z toho dôvodu musí byť kladený dôraz na ich bezpečnosť.

Moja práca je rozdelená do troch hlavných častí.
V prvej časti sa budem zaoberať analýzou súčasného stavu informačného systému obecného úradu v obci Dolný Ohaj. Obec sa nachádza na Slovensku.
V druhej časti budú popísané teoretické východiská v odbore bezpečnosti informačných systémov.
V poslednej, tretej časti, mojej práce budem navrhovať vlastné riešenia pre zvýšenie bezpečnosti informačného systému obecného úradu.

CIELE PRÁCE

Cieľom tejto práce je spracovanie návrhu pre zvýšenie bezpečnosti informačného systému obecného úradu. Ako podklad pre spracovanie návrhu zvýšenia bezpečnosti bude slúžiť analýza súčasného stavu, ktorá odhalí slabé stránky doterajšej bezpečnostnej politiky. Návrh riešenia povedie k zlepšeniu zabezpečenia systémov, vyššej bezpečnosti dát, fyzického prístupu, ochrany prenášaných informácií a tiež k určeniu práv a povinností zamestnancov vo vzťahu k informačným technológiám.

1 ANALÝZA SÚČASNÉHO STAVU

1.1 Základná špecifikácia obecného úradu

Názov: Obecný úrad Dolný Ohaj

Sídlo: Hlavná č. 109/130
941 43 Dolný Ohaj
Slovenská republika

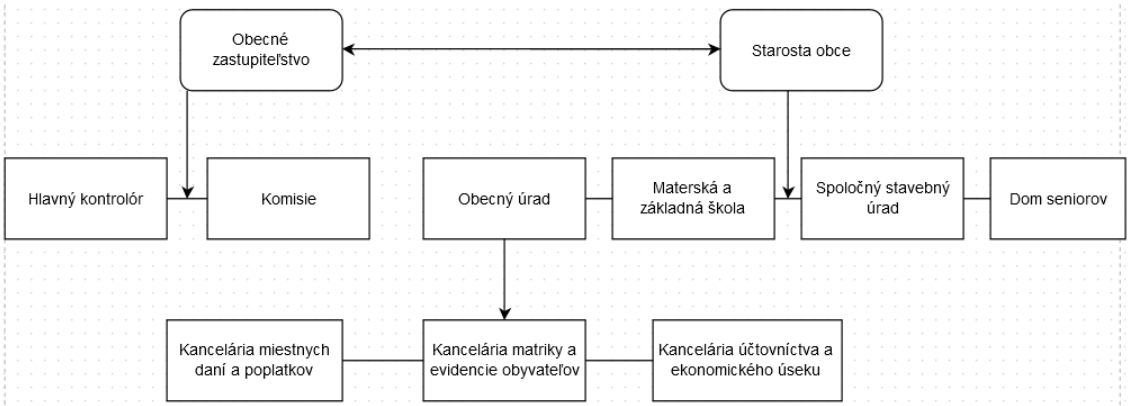
Právna forma

Obec je právnickou osobou, ktorá za podmienok stanovených zákonom a v znení neskorších predpisov samostatne hospodári s vlastným majetkom a finančnými prostriedkami.

Organizačná štruktúra

Úradná moc je vykonávaná v mieste sídla obecného úradu. Na čele organizačnej štruktúry sa nachádza starosta obce spolu s obecným zastupiteľstvom. V administratívnych službách sú traja zamestnanci, každý z nich má vlastnú kanceláriu, tak isto aj starosta obce. Kancelárie sú rozdelené podľa zamerania danej úradníčky a to konkrétne na:

- Kanceláriu miestnych daní a poplatkov,
- kanceláriu matriky a evidencie obyvateľstva,
- kanceláriu účtovníctva a ekonomického úseku,
- kanceláriu starostu obce.



Obrázok č.1.: Organizačná štruktúra obce Dolný Ohaj

Zdroj: (vlastné spracovanie)

Vzťah k vyššej organizačnej jednotke

Obec ako právnická osoba podlieha ďalej správe Vyššieho územného celku (VÚC) a v neposlednom rade spadá pod správu Slovenskej republiky.

Budova obecného úradu

Budova je spoločná s budovou pošty. Pošta sa nachádza v prízemí, obecný úrad je situovaný na prvom poschodí. K jeho priestorom vedú schody. Úrad disponuje štyrmi kanceláriami, jednou rozhlasovou miestnosťou a jednou spoločenskou miestnosťou. Budova susedí s rodinným domov z jednej strany a parkom zo strany druhej.

1.2 Informácie spracovávané jednotlivými kanceláriami

Informácie, s ktorým jednotlivé kancelárie pracujú sú veľmi citlivé a v dnešnej dobe ľahko zneužiteľné.

Matričný úrad obsahuje informácie o jednotlivých občanoch, ako napríklad dátumy narodenia, určenie otcovstva, údaje o príbuzných, rodné čísla, uzatvorené manželstvá a podobne. Evidencia obyvateľstva ako aj matrika je vedená na obecnom úrade aj pre susednú dedinu, čo znamená väčší počet spracovávaných dát.

Kancelária miestnych daní a poplatkov zase spracováva informácie o poplatkoch konkrétnych jednotlivcov, či domácností. Tak isto disponujú osobnými údajmi o občanoch.

Kancelária účtovníctva a ekonómie uchováva informácie o uzatvorených zmluvách obce, mzdách zamestnancov, pokutách vyplatených do obecnej pokladne a podobne.

Všetky tieto dáta sú veľmi citlivé a nakladanie s nimi by malo byť prevádzané podľa určitých písaných pravidiel, čo sa z väčšej časti v súčasnej dobe nedeje. Zákon o kybernetickej bezpečnosti a príslušné normy upravujú tieto postupy a je nanajvýš dôležité chrániť informácie tohto rázu.

1.3 Hardware

1.3.1 Pracovné stanice

OÚ vlastní tri stolné pracovné stanice, ktoré sú umiestnené v kanceláriách zamestnancov a jeden notebook pre potreby starostu. Všetky zmieňované zariadenia sú značky HP.

V kancelárií daní a poplatkov počítač disponuje procesorom od firmy Intel, typ Pentium G2020, operačnou pamäťou RAM DDR3 o veľkosti 4GB, sieťovou kartou a optickou mechanikou.

Pracovné stanice v kanceláriách účtovníctva a matriky sú vybavené procesormi AMD Athlon 64 Dual Core, operačnou pamäťou RAM DDR3 o veľkosti 4GB, sieťovou kartou a tak isto optickou mechanikou. Všetky počítače sú pripojené k LCD monitorom Samsung 21,5''.

Notebook, využívaný starostom obce, je vybavený procesorom AMD Turion II P540 Dual Core, operačnou pamäťou RAM DDR3 4GB, optickou mechanikou a snímačom odtlačkov prstov.

Na všetkých PC je zamestnancom povolené používať flash disky a tak majú pracovné stanice na prednom panely vyvedené USB porty. Notebook starostu obce je starý takmer štyri roky, stolné počítače majú necelých sedem rokov. Doposiaľ nebola ani raz prevedená profylaxia (vyčistenie zariadení od prachu), čo spôsobuje zníženie životnosti hardwaru.

1.3.2 Server

Zariadenie je značky HP rady ProLiant MicroServer, vybavený procesorom Dual-Core Turion II Neo N40L, pamäťou RAM DDR3 4GB, zbernicami 4 x 3,5'' SATA, diskovým poľom RAID (0/1) a 150W zdrojom. Server beží pod operačným systémom Windows Server 2008 R2 foundation.
Na serveri bežia nasledovné služby:

- Súborové (spoločne zdieľané priečinky)
- Zálohovacie (zálohovanie pracovných staníc a samotného serveru)
- Aplikačné (sieťové aplikácie)

Server je umiestnený v kancelárií daní a poplatkov. Nachádza sa na zemi v rohu miestnosti, v malom priestore medzi stenou a skriňou, čo spôsobuje hromadenie prachu v jeho okolí. Neďaleko je navyše umiestnený radiátor a kabeláž pripojená k serveru nie je nijako chránená. Proti výpadku elektrického prúdu je server chránený zariadením UPS Fortron FSP EP650, ktoré je popísané v kapitole 1.3.4.

1.3.3 Sieťové tlačiarne

Pre potreby zamestnancov sa v budove nachádzajú dve tlačiarne. Prvá je značky Canon, typ iR1022A a je k dispozícií všetkým kanceláriám prostredníctvom technológie WiFi. Umiestnená je v kancelárií daní a poplatkov. Druhá tlačiareň, umiestnená v kancelárii starostu, je značky Konica Minolta, typ magicolor 1680MF a je pripojená do siete LAN káblom.

1.3.4 Záložné zdroje – UPS

Každá z kancelárií, okrem kancelárie starostu, je vybavená záložným zdrojom Fortron FSP EP650. Jedná sa o zdroj kompaktnej veľkosti s výkonom 360W/650VA. Disponuje dvoma Schuko zásuvkami pre pripojenie rôznych zariadení. Je možné k nemu pripojiť telefónnu linku konektorom RJ11 a tým je zabezpečená jej ochrana. Technológia záložných zdrojov je Line-in. Zariadenie má ochranu proti preťaženiu, vybitiu a prebíjaniu. USB vstup slúži ako komunikačný port pre rôzne nastavenia. Záložná doba je udávaná na 10 minút pri pripojení jedného PC so zaťažením 120W. Obsahuje taktiež funkciu studeného štartu bez pripojenia do elektrickej siete a dobíjanie aj vo vypnutom stave. Každý z počítačov je pripojený na vlastný záložný zdroj. V kancelárií daní a poplatkov je okrem počítača na zdroj pripojený aj server.

Rekordér kamerového systému obce je napojený na záložný zdroj EATON UPS Nova AVR 625. Zariadenie je technológie Line interactive so vstupným napätím 165V až 280V. Podobne ako zdroje v kanceláriách obsahuje aj tento dve Schuko zásuvky pre pripojenie dvoch počítačov. Výrobca udáva ako dobu zálohovania 20 minút pri pripojení jedného počítaču a 8 minút pri pripojení dvoch. Nie je známe ako dlho vydrží uvedený zdroj napájať rekordér kamerového systému.

1.3.5 Služobné mobilné zariadenia

Každý zo zamestnancov, ako aj starosta obce, majú k dispozícií služobný smartphon, značky LG. Ide o dotykové mobilné zariadenie pracujúce s operačným systémom Android. Tieto mobilné telefóny sú určené pre vybavovanie hovorov spojených s náplňou práce a však podporujú bezdrôtové pripojenie k sieti WiFi, čo umožňuje zamestnancom ľahký prístup na internet. Vďaka nainštalovanému e-mailovému klientovi sa tak isto rýchlo dostanú aj k pracovným e-mailom. Na týchto zariadeniach sú podceňované bezpečnostné zásady, či už sa jedná o politiku hesiel alebo odhlasovanie z aplikácií.

1.3.6 Kamerový systém obce

Obec je monitorovaná kamerovým systémom, ktorý je pomerne nový. Je uložený v Rack-u, zavesenom na stene v miestnosti určenej pre obecné rozhlasové vysielanie. Rack je veľkosti štyri unity, kde využívané sú dve. Jedna unita je obsadená rekordérom kamerového systému, druhá záložným zdrojom UPS. Kamier je v obce aktuálne 5 kusov a systém je analógový v plnom PAL rozlíšení. V pláne je rozšírenie a update na 2hy systém IP vo Full HD rozlíšení. Záznam sa ukladá na nahrávacie zariadenie DVR, s kapacitou 2TB, čo pre 16 kamier v plnom PAL rozlíšení je cca 10 dní záznamu. Keďže kamier je menej, tak kapacita vydrží na dlhšie časové obdobie. Aktuálne legislatíva hovorí o pätnástich dňoch ukladania záznamu. DVR pre kamery beží pod Linuxom upraveným na tieto účely. Záznam z kamier sa automaticky maže po naplnení disku, premazáva najstaršie uložené nahrávky. Ako zobrazovacie médium slúži pre sledovanie záznamov, ale aj aktuálneho diania 32 palcový LCD monitor Samsung. Monitor ako splu s joystickom na ovládanie jednotlivých kamier je umiestnený v kancelárií starostu obce.

1.4 Software

1.4.1 Operačné systémy

Nedávno (august, 2014) prebehol na všetkých pracovných staniciach systémový update. Predtým používaný 32 bitový Windows XP Professional sa stal nevyhovujúci z dôvodu ukončenia podpory zo strany Microsoftu. Aktualizácie, ktoré pomáhali chrániť počítače boli zrušené a tak sa obec rozhodla pre 32 bitový operačný systém Windows 7.

1.4.2 Antivírusová ochrana

Na pracovných staniciach je nainštalovaný antivírusový program ESET NOD32, ktorý je aktualizovaný z internetu pre každú pracovnú stanicu zvlášť. Na jednej pracovnej stanici je nainštalovaný antispyware SpyBot Search & Destroy, ale nie je dostatočne aktualizovaný. Zamestnanci využívajú ako mailového klienta MS Outlook 2010, ktorý má vlastný zabudovaný spamový filter a tak sa do pracovných e-mailových schránok nedostáva priveľa spamu.

1.4.3 Aplikácie

Najviac využívanými programmi sú programi zahrnuté v kancelárskom balíku Microsoft Office 2010. Pre prístup k e-mailom je používaný Microsoft Outlook 2010. Matrika pracuje s programom IVES, ktorý je bežne používaný s štátnej správe. K evidencii obyvateľstva sú využívané programy od Asseco solutions a systém Datalock. Účtovníctvo je vedené tak isto pomocou aplikácie od Asseco solutions.

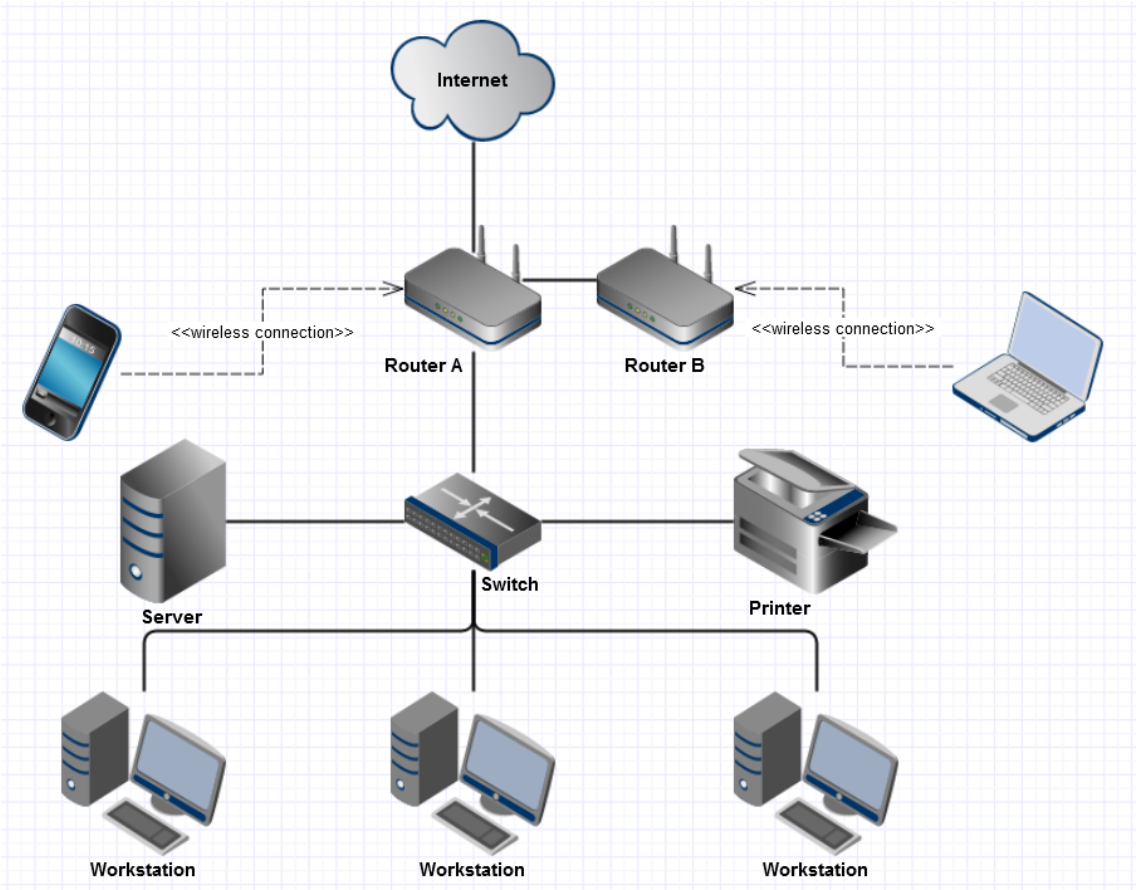
Na prístup k internetovým stránkam je v každej pracovnej stanici nainštalovaný program Mozzila Firefox a Internet explorer 8.

Zamestnanci sa do svojich počítačov prihlasujú ako administrátori, takže majú právo inštalovať akýkoľvek software či už stiahnutý z internetu, alebo inak distribuovaný. Toto nie je nijako kontrolované a ani zakázané.

1.5 Počítačová sieť

1.5.1 Miestna sieť LAN

Miestna sieť je tvorená hviezdicovou topológiu. Táto topológia má svoju výhodu v tom, že ak nastane výpadok jednej zo staníc, či príde k porušeniu kábla, tak ostatné stanice môžu vysielať aj prijímať naďalej. Lokálna sieť je typu Ethernet vo verzii 100BaseT4 s prenosovou rýchlosťou 100Mb/s. Kabeláž je teda tvorená netienenou krútenou dvojlinkou UTP kategórie 5e s PVC plášťom a konektormi RJ-45. Káble sú vedené v plastových vkladacích lištách. Absentujú tu na viacerých miestach dátové zásuvky, káble sú jednoducho vyvedené z lišty a pripojené. Pripojenie k internetu je cez DSL linku.



Obrázok č.2.: Štruktúra počítačovej siete

Zdroj: vlastné spracovanie

1.5.2 Bezdrôtová sieť

Bezdrôtová sieť pokrýva všetky miestnosti v priestoroch obecného úradu. Signál je vysielaný dvoma routrami umiestnenými na jednom mieste a to v kancelárií daní a poplatkov. Jedno zo zariadení je značky D-link, druhé značky TP-link. Táto bezdrôtová sieť, označovaná Wi-Fi je súčasťou počítačovej siete a je využívaná na ľahký prístup k internetu z mobilných zariadení, neumožňuje prístup do siete obecného úradu. Je založená na špecifikácií IEE 802.11g/n a pracuje v pásme 2,4GHz. Frekvencia tohto pásma je bezlicenčná, ale je ovplyvňovaná inými zariadeniami ako napríklad: mikrovlnné rúry, bluetooth a tak ďalej.

Prístup k tejto sieti je otvorený a možný zo všetkých zariadení v dosahu. Zabezpečená je protokolom WPA2, ktorý vyžaduje silnejšie heslá ako majú vo zvyku používať bežný používatelia. Routery obsahujú stavový firewall (SPI firewall), ktorý sleduje všetky naviazané spojenia. Jeho úlohou je prepustiť iba tie pakety, ktoré patria do už povoleného

spojenia. Sieť je určená a využívaná predovšetkým pri poradách, rokovaniach a obecných zastupiteľstvách. Poslanci často pri zastupiteľstvách využívajú súkromné notebooky a vyžadujú prístup na internet. Takéto riešenie bezdrôtovou sieťou má veľkú výhodu v tom, že nie je potreba inštalovať kabeláž.

1.5.3 Virtuálna sieť VPN

V súčasnej dobe nie je implementovaná virtuálna privátna sieť, ktorá by umožňovala zamestnancom prístup do lokálnej siete obecného úradu zo vzdialeného bodu. Pri komunikácií so zamestnancami som zistil, že by takúto možnosť určite uvítali.

1.6 Zálohovanie dát

Dáta sú primárne spracovávané a uložené na pevných diskoch lokálnych staníc. Záloha je zaistená prevedením dát na fileserver, ktorý obsahuje diskovú jednotku v režime RAID1. Všetky zálohy sú prevádzané automaticky pomocou programu Everyday Auto Backup vo verzii 3.5. Tento program je voľne stiahnuteľný. Proces zálohovania je nastavený na Startup, čo znamená, že záloha prebehne pri zapnutí počítača. Toto v praxi znamená, že ak zamestnanec v piatok po pracovnej dobe vypne svoj PC, tak najbližšia záloha bude prevedená v pondelok ráno po príchode do práce a zapnutí počítača. Nie je známe či si zamestnanci zálohujú svoju prácu aj na vlastné zariadenia, ako napríklad USB flash disky alebo iné. Data z notebooku, ktorý má k dispozícií starosta obce, nie sú žiadnym spôsobom zálohované.

Matrika je vedená ako digitálnou formou, tak aj písomnou, čo zabezpečuje dobré zálohovanie. Knihy matriky a vedenia obyvateľstva sú presnou kópiou dát nachádzajúcich sa v digitálnej forme. Knihy sú uzatvorené v kovovej ohňovzdornej skrini, ktorý by mala byť uzamknutá, no častokrát tomu tak nie je.

1.7 Politika hesiel

Každá pracovná stanica vyžaduje pri zapnutí zadanie hesla. Tieto heslá boli naposledy menené pri inštalovaní nových operačných systémov, čo bolo spomenuté vyššie, v kapitole Software. Predtým však heslá neboli menené po dobu niekoľkých rokov. Neexistuje žiadny predpis, ktorý by upravoval politiku hesiel ako takú. Heslo prístupu k bezdrôtovej siete je vystavené na nástenke, čo vlastne spôsobuje, že táto sieť je voľne

prístupná komukoľvek v dosahu.

Osobne som pracoval ako administrátor internetovej stránky pre túto obec asi dva roky. Pri podpísaní dohody o vykonaní práce som dostal prístupové meno a heslo ku systému, ktorý využívajú na editáciu stránok. Po ukončení dohody mi prístup nebol zamietnutý a ešte dlho potom som mal možnosť stránky editovať. Toto je ďalší hrubý priestupok voči politike hesiel a bezpečnosti.

1.8 Fyzický prístup

Budova má jeden vchod, osadený odolnými kovovými dverami, od ktorých má kľúč iba starosta obce. Zámka je bezpečnostná, čo znamená, že kopírovanie alebo množenie kľúču nie je možné bez povolenia starostu a predloženia bezpečnostnej identifikačnej karty. Niekoľko metrov za dverami pred schodiskom sú umiestnené kovové mreže s klasickým zámkom. Vchod budovy je snímaný obecným kamerovým systémom. Priestory úradu sú zabezpečené alarmom značky DSC. Tento alarm pracuje s pohybovými senzormi, ktoré sú umiestnené v každej z kancelárií, na chodbe a taktiež v miestnosti určenej pre obecné rozhlasové vysielanie.

1.9 Povedomie zamestnancov o bezpečnosti ICT

Zamestnanci úradu neboli do súčasnej doby preškolený odborným personálom v smere bezpečnosti informačných a komunikačných technológií. Dostali základné odporúčania od externého správcu sietí ohľadom správania sa pri práci na služobnom počítači, obnove hesiel, ukladania dát a podobne. Tieto rady boli prezentované ústne, v tomto smere neexistuje žiadny písomný dokument. Pri komunikácií so zamestnancami som zistil, že si neuvedomujú dôležitosť bezpečnosti dát s ktorými pracujú. Vedia o tom, že heslá majú byť pravidelne menené a čo majú obsahovať, no toto nie je dodržiavané. Tak isto nie sú dodržiavané pravidlá čo sa týka fyzického prístupu k dokumentom v tlačenej forme a k hardwaru zariadení. Kamerový systém je uložený v uzamykateľnom Rack-u, no kľúče od neho sú neustále v zámke, podobne je to aj s ohňovzdornou skriňou, ktorá slúži pre úschovu matričných kníh.

1.10 Súčasná bezpečnostná politika

V súčasnej dobe neexistuje žiadny písomný dokument, ktorý by upravoval postupy v prípade bezpečnostného incidentu / udalosti. Všetky problémy sú riešené externým správcom siete, no ten sa nie vždy dokáže dostaviť v efektívnom čase. Správcom siete boli zamestnancom ústne podané základné zásady pri spracovávaní informácií. Žiadny zo zamestnancov však nenesie zodpovednosť za žiadnu z častí informačného systému.

1.11 Zhrnutie analýzy súčasného stavu

Starosta obce ako aj obecné zastupiteľstvo majú záujem o zvýšenie bezpečnosti daného informačného systému, preškoliť zamestnancov a venovať pozornosť problematike bezpečnosti ako takej. Tieto opatrenia sú tak isto aj v záujme občanov, nakoľko sa to priamo dotýka aj osoby každého z nich.

Pri analýze súčasného stavu som zistil viacero nedostatkov v súvislosti s bezpečnosťou informačného systému na obecnom úrade. Viaceré z týchto chýb sa dajú odstrániť finančne nenáročným spôsobom a určite to pomôže ku zvýšeniu bezpečnosti.

2 TEORETICKÉ VÝCHODISKÁ

Progres v oblasti vývoja informačných technológií je v súčasnej dobe veľmi vysoký. Neustály pokrok v tejto sfére znamená stále novšie a novšie spôsoby ochrany informácií, ale rovnako aj možnosti útoku. V rozsahu tejto práce nedokážem popísať všetky vedomosti doposiaľ známe o informačnej bezpečnosti, preto sa budem snažiť popísať základnú terminológiu a základné metódy používané pre zvýšenie ochrany informačného systému, z ktorých budem ďalej vychádzať pri návrhu riešení.

2.1 Informačný systém

„Informačný systém je súbor ľudí (zdrojov, spracovávateľov, užívateľov), technických prostriedkov a metód, zabezpečujúcich zber, prenos, uchovávanie a spracovávanie dát za účelom tvorby a prezentácie informácií pre potreby užívateľov (2, s.26).“

Nemusí sa vždy výhradne jednať iba o digitalizovaný systém v podobe, akej sa s ním v dnešnej dobe stretávame najčastejšie prostredníctvom počítačov. Môže ísť aj o písomné dokumenty, zoradené podľa určitých pravidiel, ktoré môžu, ale aj nemusia byť vo vzájomnej interakcii. Podobne môžeme informačným systémom nazvať aj účtovníctvo, či telefónny zoznam (2). V mojej práci sa však budem predovšetkým venovať systémom automatizovaným pomocou počítačov.

Informačný systém má v prvom rade poskytovať užívateľom potrebné informácie v efektívnom čase a čitateľnej či prehľadnej forme. Slúži od zamestnancov v administratívnych službách až po vrcholový management. Každá z týchto osôb má rôzne práva v prístupe k dátam či aplikáciám a to isté sa týka povinností voči systému.

2.1.1 Zloženie informačného systému

Systém je presne tak, ako jeho najslabší článok. Na každú z častí informačného systému treba brať zreteľ a nemôže sa stať, že by bola nejaká z nich zanedbaná. Medzi základné časti patrí:

Hardware - technické vybavenie, slúžiace na spracovanie informácií. Od kvality hardwaru závisí spoľahlivosť a efektivita informačného systému.

Software - určuje akým spôsobom sú spracovávané v organizácií dáta. Aplikačné

programy, operačné systémy, antivírus atď.

Údaje - ďalšia z dôležitých častí informačného systému. Môžu sa deliť podľa viacerých charakteristík, čo bude popísané ďalej.

Peopleware - ľudia, ktorí zabezpečujú a udržiavajú chod informačného systému.

Orgware - organizačné usporiadanie, ktoré zahŕňa všetky predpisy, smernice a dokumenty upravujúce činnosti a chovanie ľudí (5).

2.1.2 Kategórie používateľov

Za účelom zaistenia zodpovednosti boli v európskych kritériách pre hodnotenie bezpečnosti informačných systémov (ITSEC) definované tri kategórie používateľov:

- **Správca -** privilegované akcie v rozsahu svojej plnej pôsobnosti.
- **Operátor -** privilegované akcie v obmedzenom rozsahu preddefinovaným správcom (napr. právo zálohovať systémové dáta).
- **Používateľ -** nemôže vykonávať privilegované operácie (2).

V rámci organizačnej štruktúry informačnej bezpečnosti sú definované role, ktoré popisujú činnosti, zodpovednosti a v neposlednom rade právomoci. Určenie zodpovednosti za konkrétne časti informačného systému je nanajvýš dôležité. Dokument bezpečnostnej politiky mimo iného upravuje delegovanie zodpovedností a prípadné sankcie pri jej porušení.

2.2 Pojem dáta a informácie

Na prvý pohľad slová s rovnakým významom, no existuje medzi nimi rozdiel. Tieto dve slová sa v praxi veľmi často zamieňajú alebo sú považované za synonymá. Každé z týchto slov však nesie odlišnú definíciu, ktorá je popísaná v tejto kapitole.

2.2.1 Dáta

„Dáta – údaje skutočnosti – vhodným spôsobom vyjadrená (zakódovaná) správa, ktorá je zrozumiteľná príjemcovi (človek, počítač) a prispôsobená k ďalšiemu spracovaniu. Bezprostredne odrážajú skúmanú skutočnosť a predstavujú najnižší prvok informačného systému (1, s.37).“

Jedná sa teda o časť informačného systému, ktorá je uchovávaná na vhodných nosičoch a ďalej spracovávaná pre potreby užívateľov. Dáta môžeme nadobudnúť rôznymi spôsobmi, ako napríklad čítaním, meraním, vážením alebo pozorovaním. Môžu byť uložené ako tabuľky, čísla, text alebo v inom formáte. Spracovaním dát dokážeme vytvoriť informáciu, ktorá má hodnotu pre príjemcu.

2.2.2 Informácie

„Význam priradený obrazom (dátam), údajom a z nich utvoreným vyšším celkom (1, s.37).“

Informácie teda vychádzajú zo spracovania dát a nesú so sebou určitú hodnotu pre príjemcu. Znižujú nevedomie príjemcu ohľadom istej udalosti a sú silne subjektívne. Môžu byť vyjadrené rôznymi formami ako napríklad: slovne, grafom, textom a podobne. Informáciou nemôžme označiť hocijakú správu, ale iba tú, z ktorej sa dozvieme niečo nové, alebo nám zvýši naše povedomie o istom jave. S týmto súvisí aj cena informácie a tak ju môžeme označiť za tovar s ktorým sa dá za určitých podmienok obchodovať. Hodnota informácie však závisí na mnohých faktoroch. „***Každá informácia*** *je teda údajom, dátami, ale akékoľvek uložené dáta sa nemusia stať nutne informáciami (2, s.25).“*

2.2.3 Význam dát pre organizáciu

Dáta patria medzi najcennejšie súčasti každej organizácie. „*V súčasnosti sú organizácie závislé od informácií, ktoré spracúvajú. Preto by mala byť informačná bezpečnosť predmetom záujmu každej firmy alebo organizácie štátnej, či verejnej správy (6).“*

2.3 Informačná bezpečnosť

Riadenie informačnej bezpečnosti by malo byť považované za hlavnú súčasť strategického plánu každej spoločnosti. Pokrytím špecifických požiadaviek na bezpečnosť správnym spôsobom, môžu organizácie predchádzať ujmám na finančnom alebo majetkovom zdraví. Jedná sa o predvídanie potencionálnych hrozieb čo najefektívnejšie. Dôkladnou analýzou rizík vieme posúdiť jednotlivé hrozby a prijať vhodné opatrenia. Informačná bezpečnosť sa sústreďuje na elimináciu hrozieb

pôsobiacich na informačné systémy – na ich bezpečnosť, spoľahlivosť a súlad s právnymi predpismi (1).

2.3.1 Atribúty bezpečnosti informácií

*„**Bezpečnosť informácií** (Information security) – zachovanie dôvernosti, integrity a dostupnosti informácií (3, s. 15).“*

Z vyššie uvedeného citátu vidíme, že bezpečnosť informácií sa skladá z troch základných predpokladov. Aby sme mohli hovoriť o bezpečnosti informácií, nesmie byť žiadna z týchto súčastí porušená. V nasledujúcich riadkoch sú v krátkosti vysvetlené všetky tri pojmy:

Dôvernosť informácií – informácie môžu byť sprístupnené iba autorizovanému užívateľovi a nikomu inému.

Integrita – pre zachovanie integrity dát musia byť splnené podmienky správnosti a úplnosti informácie, dáta nemôžu byť zmenené.

Dostupnosť informácií – umožnenie prístupu k informáciám v požadovanom čase pri zachovaní dôvernosti (2).

2.4 Informačné aktíva

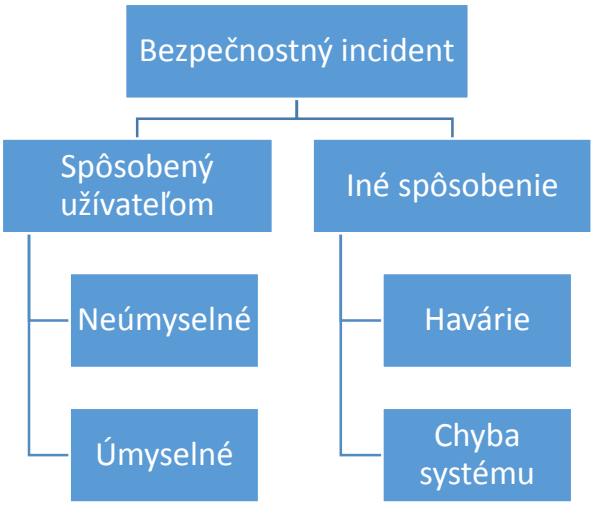
Informačným aktívom môžeme označiť takú súčasť informačného systému, ktorá je v interakcii s informačným systémom. Poškodenie, či strata takéhoto aktíva by mohla spoločnosti priniesť finančné či ekonomické problémy. Nakoľko informačný systém je celok zložitý a rozsiahly, narušenie niektorých z jeho častí môže narušiť bezpečnosť. V prípade, že narušenie niektorého z aktív sa premietne v znížení bezpečnosti systému, hovoríme o aktíve informačnej bezpečnosti. Tieto aktíva môžu mať formu hmotnú, ako napríklad počítačové vybavenie a ďalšie technické zariadenia ale aj nehmotnú a to napríklad databázy, súbory, programové vybavenie a tak ďalej (5).

Z analýzy aktív vychádza plán riadenia bezpečnosti každého konkrétneho informačného systému. Počas spracovania tejto činnosti sa ukážu slabé miesta, teoreticky napadnuteľné, a musia byť vykonané postupy pre ich odstránenie.

2.5 Bezpečnostná udalosť, incident

Základným rozdielom medzi bezpečnostnou udalosťou a incidentom je, že **udalosť je činnosť a incident je stav aktíva**. Bezpečnostnému incidentu predchádza realizácia bezpečnostnej hrozby na zraniteľnosť aktíva, čiže udalosť. Incident potom nastáva pri skutočnom poškodení alebo zmenení stavu na danom aktíve.

Delenie bezpečnostných incidentov, respektíve spôsoby ich vzniku sú zobrazené na obrázku č.3.:



Obrázok č.3.: Bezpečnostné incidenty

Zdroj: (2, vlastné spracovanie)

V prípade nedostatočných bezpečnostných opatrení dochádza k bezpečnostným incidentom. Tomuto sa dá predísť **prevenciou pred incidentmi.** Ide o znižovanie pravdepodobnosti vzniku a dopadu incidentu na organizáciu. Zaužívaným prístupom, ktorý zlepšuje bezpečnostnú úroveň a znižuje riziko výskytu incidentu je vykonávanie pravidelných analýz rizík. *„Analýza rizík by mala byť vykonávaná periodicky, čím sa zabezpečí adekvátnosť a aktuálnosť všetkých požiadaviek na špecifické bezpečnostné opatrenia (6).“* Analýza odhalí riziká, ktoré môžu reálne hroziť informačnému systému. Každé riziko musí byť klasifikované podľa stupňa jeho závažnosti a môže byť opatreniami znížené, prenesené alebo akceptované. Incident ako taký nemusí spôsobiť organizácii veľké škody, no môže prísť k situácii keď jeho výsledkom budú vyčísliteľné

finančné škody, poškodenie mena organizácie či narušenie jej činnosti. Riadením bezpečnostných incidentov sa zoberá manažment incidentov informačnej bezpečnosti.

2.6 Hrozby a riziká

Slabé miesta v informačnom systéme vytvárajú priestor pre bezpečnostné **hrozby a riziká**. To spôsobuje **zraniteľnosť** systému.

*„**Zraniteľnosť** (Vulnerability) – je slabé miesto aktíva (3, s.16).“* V každom z informačných systémov sa nájdu miesta, ktoré sú zabezpečené menej. Vynaloženie finančných prostriedkov na zabezpečenie istého aktíva by malo byť primerané jeho hodnote pre informačný systém.

2.6.1 Delenie hrozieb

Hrozbou môžeme označiť využitie zraniteľného miesta aktíva. Táto udalosť môže spôsobiť škodu na aktívach. Hrozby môžeme deliť na:

- **Objektívne hrozby:** prírodné, fyzikálne, technické.

Medzi prírodné hrozby radíme predovšetkým živelné pohromy, v dôsledku ktorých môže nastať napríklad výpadok elektrického prúdu, požiar a iné.
Fyzikálnou hrozbou môže byť označené elektromagnetické vyžarovanie.
Technické hrozby zahŕňajú udalosti typu: krádež, zničenie vybavenia, zmazanie súborov, softwarové chyby atď.

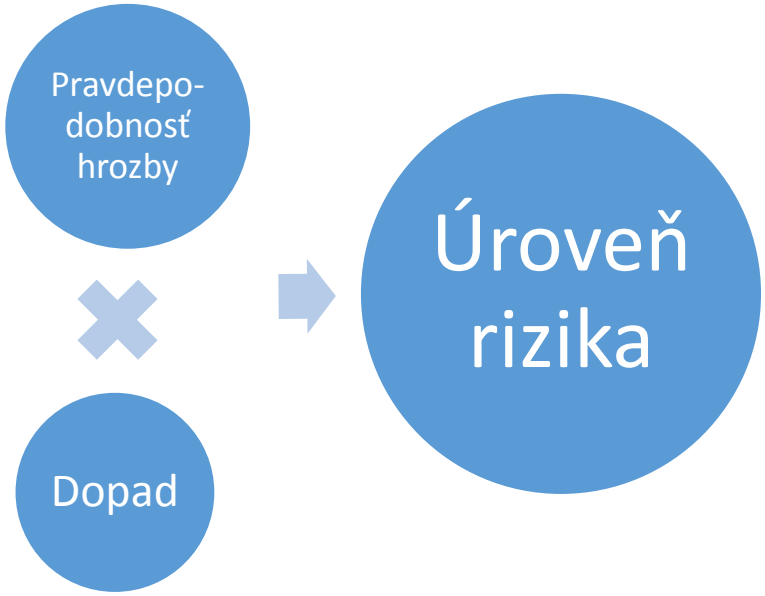
- **Subjektívne hrozby:** neúmyselné, úmyselné (2).

Ide o hrozby spôsobené ľuďmi. Ľudia ako súčasť informačného systému sú často nazývaný jeho najväčšou hrozbou.
Neúmyselnou hrozbou môže byť identifikovaná napríklad činnosť pracovníka s nedostatočnými znalosťami a skúsenosťami v oblasti IT.
Úmyselná hrozba sa ďalej delí na hrozbu externú a internú. Externou hrozbou je myslený útočník, ktorý nie je v priamom vzťahu s organizáciou či jej informačným systémom. Môže ísť o konkurenciu, hackerov ale aj teroristov. Interná hrozba predstavuje pre organizáciu najväčšie nebezpečenstvo. *„Odhaduje sa, že 80% útokov na IT je vedených*

zvnútra, útočníkom, ktorý môže byť prepustený, nahnevaný, chamtivý zamestnanec; veľmi efektívne z hľadiska vedenia útoku je súčinnosť oboch typov útočníkov (2, s.41).“

2.6.2 Riziko

Úroveň rizika predstavuje kombinácia hrozby a zraniteľnosti. Rozumieme ním pravdepodobnosť využitia zraniteľného miesta informačného systému. Môže byť popísané násobkom pravdepodobnosti hrozby a dopadu uskutočnenej hrozby.



Obrázok č.4.: Úroveň rizika popísaná interakciou hrozby a zraniteľnosti

Zdroj: (5, vlastné spracovanie)

2.7 Útočník

Útočníkom je pôvodca útoku. Motiváciou pre útočníka môže byť finančné obohatenie, pomsta bývalého zamestnanca, získanie informácií o konkurentovi, dokazovanie vlastných zručností či mnohé iné podnety. Ide teda o pomerne širokú škálu ľudí, ktorí by sa potenciálne mohli stať útočníkmi.

Základné delenie útočníkov môže byť popísané v troch kategóriách, kde prvú z nich zastupujú útočníci **amatéri.** Táto skupina útočníkov napadá informačný systém cez náhodne objavené zraniteľné miesta. Ďalšou kategóriou sú **hackeri.** Cieľom ich činnosti je vo väčšine prípadov dokazovanie si vlastných schopností úmyselným narušením ochrany systému. Poslednou, treťou, kategóriou sú **profesionálny zločinci**, ktorí môžu byť označení ako najnebezpečnejší z uvedených troch typov útočníkov. Ich útoky sú podporované výbornými technickými prostriedkami. Jedná sa o teroristické a špionážne organizácie, ktoré môžu dokonca ohroziť bezpečnosť štátu (2).

Cieľom útoku môže byť znehodnotenie či pozmenenie dát, krádež citlivých informácií o organizácii, podsunutie falošnej informácie, znefunkčnenie informačného systému organizácie trvalé či dočasné a mnoho ďalších. Narušením niektorého z predpokladov bezpečnosti (integrity, dostupnosti, dôvernosti) sa stáva útok úspešným.

V súčasnej dobe predstavujú veľkú hrozbu a otvárajú nové možnosti pre útočníka mobilné technológie. Smartphony majú inštalované rôzne aplikácie podporujúce napríklad platby cez internetbanking, e-mailových klientov a ďalšie. Pamäť mobilných telefónov dokáže pojať vďaka svojej veľkosti obrovské množstvo údajov. Bezpečnosť týchto zariadení by nemala byť zanedbávaná najmä vzhľadom na to, že množstvo aplikácií umožňuje prístup dovnútra organizácie. Na internetovom portály http.://itnews.sk boli zverejnené informácie týkajúce sa tejto témy:

- 84% prienikov je uskutočňovaných na aplikačnej vrstve, čo umožňuje útočníkovi dostať sa k dátam cez mobilné zariadenie
- 9 z 10 mobilných aplikácií bolo v prieskume označených ako náchylné na útok
- Nárast malwaru bol na zariadeniach s OS Android na úrovni 614%

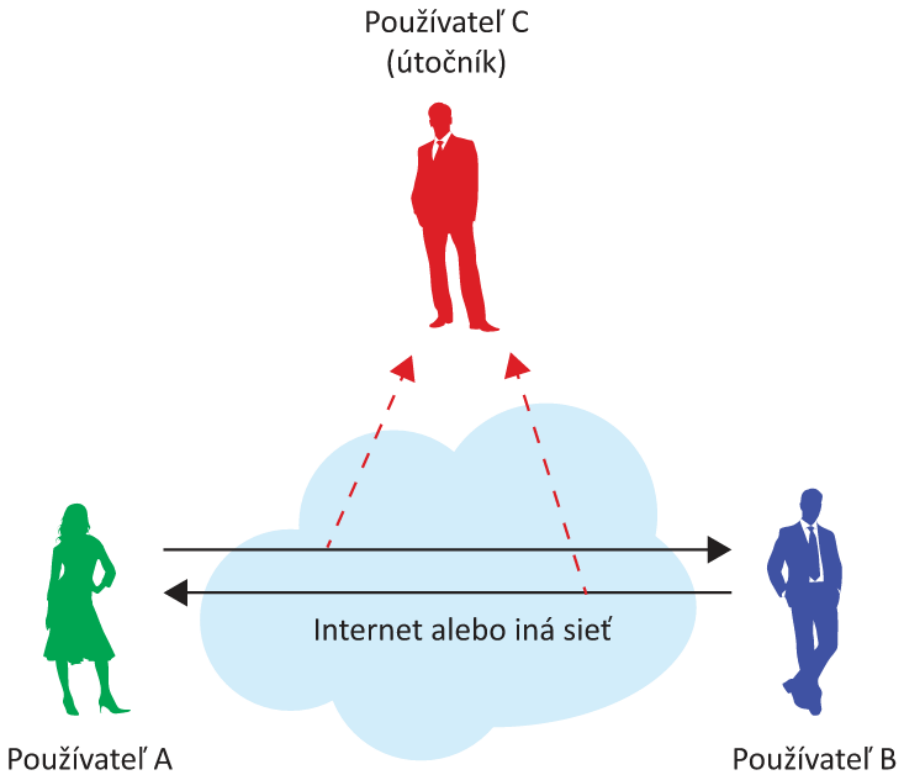
2.8 Útok

Útok je cieľavedomá činnosť, ktorá môže spôsobiť narušenie informačnej bezpečnosti. Môžeme ich rozdeliť do dvoch základných kategórií:

- Pasívne útoky
- Aktívne útoky

2.8.1 Pasívny útok

Pasívny útok ohrozuje dôvernosť dát. Je prevažne založený na odpočúvaní a monitorovaní komunikačného kanála. Útočník pri pasívnom útoku neovplyvňuje systémové prostriedky. Hlavným cieľom takého útoku je získanie prenášanej informácie.



Obrázok č.5.: Model pasívneho útoku

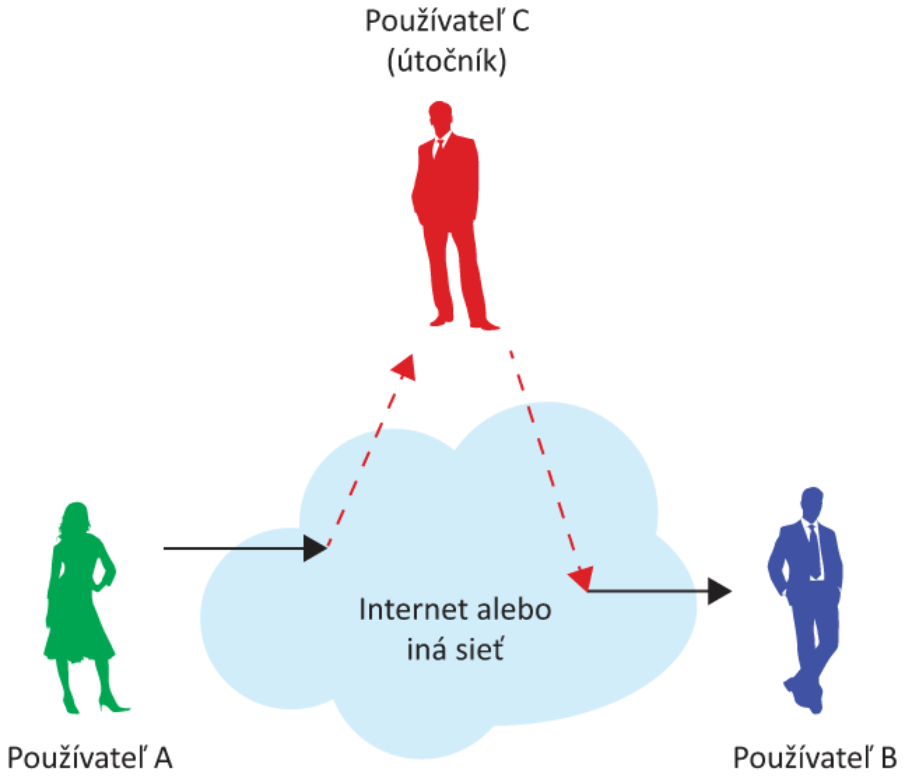
Zdroj: (4, s.13)

2.8.2 Aktívny útok

Aktívny útok je zameraný na modifikáciu systémových prostriedkov a ovplyvňovanie ich činnosti. Útočník pri aktívnom type útoku ohrozuje ako integritu, tak aj dôvernosť a dostupnosť dát. Cieľom je vymazať, pridať alebo nejakým iným spôsobom pozmeniť prenos informácie kanálom.

Môže ísť o:

- Predstieranie identity – útočník sa vydáva za autorizovaného užívateľa s cieľom získania prístupu do systému.
- Opakovanie – dátový prenos je úmyselne opakovaný. Útočník zachytí dáta, ktoré následne opäť prepošle pod predstieranou identitou.
- Modifikácia správ – odchytenie správy z komunikácie, následne jej pozmenenie a opätovné vloženie do komunikačného kanála (4).



Obrázok č.6.: Aktívny útok s pozmenením správy

Zdroj (4, s.14)

2.9 Škody

Realizovaním hrozby dochádza k bezpečnostnému incidentu a tým môžu vznikať škody. Každá škoda znamená pre organizáciu problém finančného alebo technického rázu. Strata jedného zo základných predpokladov bezpečnosti (dôvernosť, integrita, dostupnosť) môže spôsobiť také škody, že organizácia nebude schopná vykonávať niektorú so svojich základných činností.

Druhy škôd vznikajúce realizovaním hrozby:

- **Priame straty**, ktoré môžu mať charakter nielen materiálny ale aj abstraktný. Ide o zverejnenie obchodného zámeru, škody spôsobené nelegálnymi finančnými transakciami či náklady na obnovenie výroby.
- **Nepriame straty** sa týkajú mena podniku, ktoré môže utrpieť vplyvom nedodržania dohodnutých podmienok a tým dôjde k finančnej strate.
- **Nekvalitné alebo zlé rozhodovanie**, ktoré je dôsledkom zlých informácií.
- **Zvýšené náklady** vynaložené na získanie potrebných informácií, ktoré nemôžeme získať v dôsledku poškodeného IS (2).

2.10 Prostriedky zabezpečenia

Použitie kvalitného technického vybavenia zvyšuje spoľahlivosť a kvalitu informačných systémov. Pod týmto pojmom teda môžeme rozumieť predovšetkým zaistenie utajenia, dostupnosti a integrity informácií (2).

2.10.1 Bezpečnostné opatrenia

Bezpečnostným opatrením môžeme rozumieť akýkoľvek prostriedok, ktorý zníži úroveň rizika jednej alebo niekoľko hrozieb. Opatrenia môžu byť smerované na tieto aspekty (5):

- **Zníženie alebo odstránenie pravdepodobnosti výskytu hrozby** – školenie užívateľov môže znížiť množstvo chýb, ktoré vedú k strate dát.
- **Zníženie alebo odstránenie zraniteľnosti aktíva** – implementácia vhodného firewallu
- **Zníženie alebo vylúčenie dopadu na organizáciu** – dátové zálohy môžu znížiť dopad straty dát na prijateľnú mieru (5).

2.10.2 Rozdelenie bezpečnostných opatrení

Bezpečnostnými opatreniami sú:

- *Organizačné opatrenia* – riadenie projektov, rozhodovanie
- *Technické opatrenia* - HW zariadenia, software
- *Fyzické* - kontrola fyzického prístupu, zámky, bezpečnostné dvere
- *Administratívne* – smernice, postupy, organizačná štruktúra (5)

V závislosti na tom, ktorý z faktorov informačnej bezpečnosti (dostupnosť, dôvernosť, integrita) môže hrozba ovplyvniť budeme opatrenia deliť na:

- **prevencia** (celková eliminácia bezpečnostnej hrozby) – serverový cluster zabráni nedostupnosti služby v prípade výpadku jedného z členov clusteru
- **minimalizácia** (zníženie úrovne rizika hrozby) – školenie užívateľov zníži množstvo užívateľských chýb
- **detekcia** (včasné zistenie incidentu) – odhalenie neoprávneného prístupu pomocou bezpečnostných logov.
- **obnova** (uvedenie aktív do pôvodného stavu pred incidentom) – zálohovanie (5)
-

2.11 Riadenie identít

2.11.1 Autentizácia

Autentizáciou rozumieme jednoznačné rozpoznanie užívateľa.

Kontrola prístupu osôb

Riadenie a kontrolovanie prístupu osôb do priestorov, kde sa nachádzajú časti systému, je veľmi dôležité pre optimálnu bezpečnosť každého informačného systému. Jedným z riešení je kontrola pomocou hardwarových zariadení. Najznámejšími prostriedkami sú:

- **Identifikačné karty** – tieto tokeny jednoznačne identifikujú danú entitu. V závislosti na technickom prevedení a princípoch na ktorých pracujú to môžu byť karty s čiarovým kódom, magnetické, optické, čipové karty, karty s čiarovým kódom a tak ďalej. Hardwarový zámok je ďalšou z možností, ale v súčasnej dobe je jeho bezpečnosť považovaná za prekonanú (2).

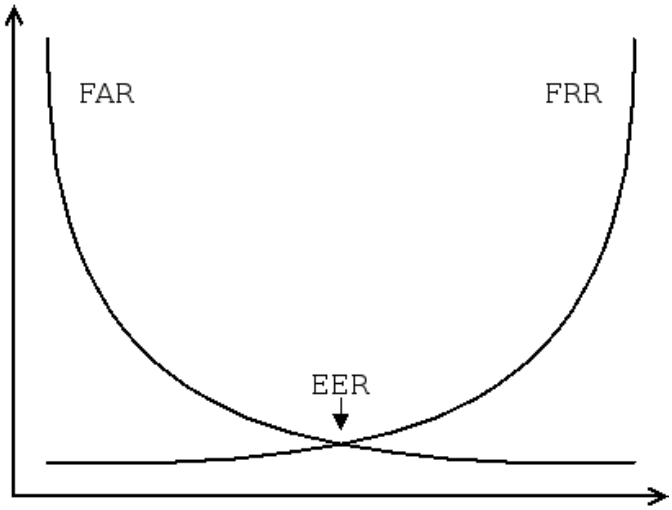
- **Biometrické systémy**

Zvýšenie bezpečnosti fyzického prístupu osôb rieši model trojfaktorovej autentizácie, ktorý je založený na bodoch:

- Čo viem? (PIN, heslo...)
- Čo mám? (token, ID karta...)
- Čo som? (biometrická vlastnosť)

  Biometrické systémy sa zaoberajú práve treťou časťou tejto multifaktorovej autentizácie. V prvom rade musí byť odobraná prvá vzorka, ktorá bude uložená v databáze a následne bude slúžiť na porovnanie so vzorkou odobranou neskôr. V súčasnosti sa najviac používajú: hlas, rušné písmo, odtlačky prstov, tvár, sietnica a rohovka oka (2).

  Nastavenie chybovosti pri biometrických systémoch závisí od systému ktorý je ním zabezpečovaný. Nízky počet chybných prijatí je dôležitý pri vysoko bezpečnostných aplikáciách a naopak nízka pravdepodobnosť odmietnutia oprávneného užívateľa je dôležitá pri komerčných aplikáciách.



Obrázok č. 7.: EER pri biometrických systémoch

Zdroj: vlastné spracovanie

- **FAR** (False Acceptance Rate) – chybné prijatie
- **FRR** (False Rejection Rate) – chybné odmietnutie
- **ERR** (Equal Error Rate) – chybovosť

2.11.2 Autorizácia

Autorizácia znamená overenie oprávnenia osôb, či objektov na prácu s dátami. Teda poskytnutie užívateľovi iba tie služby, pre ktoré je daný užívateľ oprávnený. Užívateľom môže byť človek, ale aj iný informačný systém (5).

2.11.3 Audit

Audit je ďalšou z častí riadenia identít. V širšom slova zmysle ide o podrobné a kritické skúmanie stavu niečoho. Môže ísť napríklad o kontrolu bezpečnosti a integrity konkrétneho systému počítača, revíziu zhody so softwarovými požiadavkami, postupmi a podobne.

2.12 Sieťová ochrana

2.12.1 Sieťová hardwarové ochrana

Fyzické zabezpečenie komunikačných zariadení je možné predovšetkým v sieťach typu LAN, pretože je takmer nemožné zabezpečiť rozsiahle siete proti odpočúvaniu či prerušeniu. Lokálne siete sa zabezpečujú najmä týmito spôsobmi (2):

- Ochrana komunikačných portov – znemožnenie použitia prázdnych zásuviek
- Riadenie pripojenia do siete – vhodné umiestnenie prípojok do siete
- Zabezpečenie káblových spojov – zamedzenie neoprávnenej osobe napojiť sa na tieto spoje (trubky s inertným plynom)

2.12.2 Firewall

Firewall je zariadenie, ktoré sa používa na zabezpečenie vnútornej siete organizácie. Ochrana je realizovaná oddelením internej siete od vonkajšieho okolia. Všetky dáta vstupujúce alebo vystupujúce zo siete cez firewall sú analyzované s cieľom, či tieto dáta spĺňajú špecifické bezpečnostné pravidlá. Firewall potom rozhodne medzi dvoma činnosťami: buď komunikáciu blokuje, alebo ju povolí. Komunikácia vychádzajúca z internej siete von je vo väčšine prípadov povolená, no naopak komunikácia ktorá je iniciovaná z internetu do internej siete je zvyčajne zakázaná.

2.12.3 Antivírus

Antivírusový software je počítačový program, ktorého cieľom je identifikovať a eliminovať škodlivé programy. Trojské kone, Spyware alebo víry môžu spôsobiť v organizácií škody. Antivírus musí byť však pravidelne aktualizovaný, aby bol schopný fungovať efektívne.

2.12.4 Proxy server

Proxy server funguje ako medzník medzi klientom a cieľovým serverom. Vystupuje ako klient a prekladá požiadavky na cieľový server. Môže ísť o špecializovaný hardware, či program bežiaci na počítači. Analyzuje obsah komunikácie, ukladá požiadavky do vyrovnávacej pamäte cache a zefektívňuje komunikáciu.

2.12.5 VPN

VPN – virtuálna privátna sieť. Ide o prepojenie medzi dvoma bodmi realizované cez sieť ako je napríklad internet. Klient VPN na základe protokolu TCP/IP virtuálne volá port na servery VPN. Pri typickom nasadení siete iniciuje klient virtuálne pripojenie medzi dvomi bodmi k serveru vzdialeného prístupu. Server prijme volanie, overí volajúceho a prenesie dáta medzi klientom VPN a privátnou sieťou (8).

2.12.6 Honeypot

Jedná sa o informačný systém, ktorého úlohou je priťahovať potencionálnych útočníkov. Využívané sú prevažne na včasnú detekciu malwaru. Malwary často menia svoju stratégiu útokov a preto je nutné ich nalákať a analyzovať ich chovanie.

2.13 Zálohovanie dát

Ako už bolo spomenuté, dáta majú pre každú organizáciu vysokú hodnotu. Ich stratou, poškodením či zmenením môže dochádzať ku škodám. Správnym zálohovaním sa môžeme týmto problémom vyhnúť.

2.13.1 Čo zálohovať

Je nutné určenie priority dát pri zálohovaní. Zálohovacie médiá majú obmedzenú kapacitu a ich cena je vysoká. Je rozumné zálohovať iba dáta jednotlivých aplikácií, nie aplikácie samotné. Tie sú totiž ľahko obnoviteľné pomocou inštalačného softwaru.

2.13.2 Zálohovacie médiá

Záloha dát na lokálny pevný disk – najrýchlejší spôsob a zároveň najmenej bezpečný.

Záloha dát na externý disk a sieťový disk – chráni dáta pred haváriou celého počítača.

Záloha dát a optické médiá – možnosť vytvorenia viacerých kópií a uloženia na viaceré miesta. Nevýhodou je prácnosť zálohovania a životnosť týchto médií.

Záloha dát na sieťové úložiská – bežný spôsob zálohovania. Ukladá sa na server alebo sieťové disky.

Záloha dát na FTP server - výhodou je uloženie záloh, ktoré môžu byť umiestnené stovky kilometrov od zdrojových dát.

Záloha dát na pásku – rozšírená hlavne vo veľkých organizáciách prostredníctvom páskových mechaník alebo zálohovacích knihovní.

Záloha do virtuálneho prostredia – záloha funkčného prostredia (3).

2.13.3 Frekvencia zálohovania

Frekvencia zálohovania závisí od toho, akou rýchlosťou narastá objem dát, alebo ako často sú dáta menené. V organizáciách, kde sa denne pracuje a dochádza k nárastu a zmenám sa odporúča zálohovať denne, v niektorých prípadoch dokonca viackrát za deň.

2.13.4 Spôsoby zálohovania

Normálna metóda zálohovania skopíruje všetky súbory na záložné médium.

Prírastková metóda dovoľuje zálohovanie iba zmenených súborov od poslednej zálohy.

Rozdielová metóda zálohuje zmenené súbory. Rozdiel od posledných metód je v tom, že pre obnovu potrebujeme poslednú normálnu zálohu, poslednú prírastkovú zálohu a všetky rozdielové od poslednej normálnej alebo prírastkovej.

Denná metóda zálohuje dáta vytvorené alebo zmenené počas dňa (3).

2.14 Normy a zákony

2.14.1 ČSN ISO/IEC 27001:2014

ČSN ISO/IEC 27001:2014 je druhé vydanie, ktoré ruší a nahradzuje vydanie predchádzajúce: ČSN/IEC 27001:2006. Norma má 28 stránok a bola preložená z anglického originálu. Táto medzinárodná norma špecifikuje požiadavky na ustanovenie, implementovanie, udržiavanie a neustále zlepšovanie systému riadenia bezpečnosti informácií v rámci kontextu rizík činnosti organizácie. Zahŕňa také požiadavky na posúdenie a ošetrenie rizík bezpečnosti informácií, prispôsobené potrebám organizácie. Požiadavky tejto normy sú všeobecne použiteľné a aplikovateľné vo všetkých organizáciách bez ohľadu na ich typ, veľkosť a povahu činností. Celý názov normy je: ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosťi informací – Požadavky.

2.14.2 Zákon o kybernetickej bezpečnosti

Tento zákon nadobudne platnosť v Českej republike dňom 1.1.2015. Bol schválený obidvomi komorami Parlamentu a podpísaný prezidentom Českej republiky dňa 29.augusta 2014. Vyšiel v Zbierke zákonov ako zákon č. 181/2014 Sb.

Tento zákon upravuje práva a povinnosti fyzických a právnických osôb a pôsobnosť a právomoc orgánov verejnej moc a ich vzájomnú spoluprácu v oblasti kybernetickej bezpečnosti (10).

Na Slovensku je kybernetická bezpečnosť zastrešená prostredníctvom CSIRT.SK (Computer Security Incident Response Team), čo je špecializovaná jednotka pre riešenie počítačových incidentov. Zabezpečuje služby, ktoré sú spojené so zvládaním bezpečnostných incidentov, odstraňovaním ich následkov a následnou obnovou činnosti informačných systémov a súvisiacich informačných a komunikačných technológií v rámci infraštruktúry SR (9).

Istú legislatívu v tomto smere popisuje Zákon o informačnej bezpečnosti. Zákon o kybernetickej bezpečnosti teda v súčasnej dobe na území SR neexistuje. Do budúcnosti

je však predpoklad, že SR ako členský štát Európskej únie bude musieť tento zákon prijať. Z toho dôvodu budem pri spracovaní vlastných návrhov brať do úvahy český Zákon o kybernetickej bezpečnosti a jeho prevádzacie smernice.

3 VLASTNÝ NÁVRH RIEŠENÍ

V tejto časti práce sa budem venovať návrhu vlastných riešení pre zvýšenie bezpečnosti informačného systému Obecného úradu. Návrhy budú prispôsobené finančným a personálnym podmienkam obce, ktoré som konzultoval so starostom a poslancami obecného zastupiteľstva. Infraštruktúra nie je natoľko rozsiahla aby si vyžadovala obsiahlu bezpečnostnú stratégiu, pôjde teda predovšetkým o konkrétne a realizovateľné návrhy pre zvýšenie bezpečnosti.

Obec nedisponuje takými finančnými prostriedkami aby mohli dlhodobo zamestnávať odborníkov v oblasti IT a tak bude realizáciu návrhov vykonávať externý špecialista, s ktorým už Obecný úrad spolupracuje dlhšiu dobu.

3.1 Bezpečnostná analýza

Úvodná kapitola – Analýza súčasného stavu odhalila viacero nedostatkov, ktoré ohrozujú bezpečnosť skúmaného informačného systému a dát, ktoré obsahuje.

3.1.1 Bezpečnostný cieľ

Základným bezpečnostným cieľom je samozrejme ochrana informácií, ktoré sú obsiahnuté v informačnom systéme. Tento cieľ môže byť dosiahnutý pri dodržaní pravidiel, ktoré boli popísané v kapitole 2.3.1 a síce: dôvernosť, integrita a dostupnosť informácií. Pre splnenie podmienky dôvernosti môžu byť dáta sprístupnené iba autorizovanému užívateľovi a nikomu inému. Integrita znamená správnosť a úplnosť informácií a dostupnosť značí umožnenie prístupu k informáciám v požadovanom čase pri zachovaní dôvernosti.

Splnenie týchto troch podmienok je teda stanovené ako základné bezpečnostné ciele. .

3.1.2 Nedostatky vyplývajúce z analýzy

Oblasti informačnej bezpečnosti, ktoré potrebujú zvýšenú pozornosť a zmenu sú zväčša:

- Prevedenie počítačovej siete (umiestnenie server, kabeláž atď.)
- Zálohovanie dát

- Profylaxia HW a SW
- Politika hesiel
- Prístup k bezdrôtovej sieti
- Povedomie zamestnancov o bezpečnosti (školenia)
- Kontrola inštalovaného softwaru na pracovných staniciach
- Fyzický prístup k serveru, kamerovému systému, matričnej skrini...

3.1.3 Identifikácia a ocenenie aktív

Pre ohodnotenie aktív v tabuľke je použitá škála 1 až 5, pričom najdôležitejšie aktíva sú označené hodnotou „5“.

Typ aktíva	Identifikované aktívum	Hodnota aktíva
Informácie	Databáza serveru	5
	Databáza matriky	5
Hardware	Pracovné stanice	3
	Server	4
	Sieťové tlačiarne	2
	Záložné zdroje	3
	Služobné mobilné zariadenia	1
	Kamerový systém	3
	Switch, routre	4
Software	Operačné systémy	3
	Databázový systém	4
	Antivírová ochrana	3
	Pracovné aplikácie	3
	Software kamerového systému	3
Služby	Pripojenie serveru	5
	Pripojenie k internetu	2
Počítačová sieť	LAN	4
	Wi-Fi	1

Tabuľka č.1.: Identifikácia a ocenenie aktív

Zdroj: Vlastné spracovanie

3.1.4 Identifikované hrozby a súvisiace zraniteľnosti

Vstupom pre identifikáciu hrozieb je identifikácia a ocenenie aktív. Pre aktíva definované v predchádzajúcej kapitole sú v tabuľke nižšie uvedené jednotlivé hrozby a zraniteľnosti. V tabuľke sú potom ďalej uvedené pravdepodobnosti jednotlivých hrozieb spolu s príkladmi zraniteľností. Pre ohodnotenie pravdepodobnosti hrozby som použil opäť škálu 1 až 5, kde najpravdepodobnejšia hrozba je označená hodnotou „5“.

Identifikovaná hrozba	Pravdepodobnosť hrozby	Príklad zraniteľnosti
Poškodenie Hardwaru	4	Zariadenie vystavené prachu, teplu, vlhkosti
Zlyhanie Softwaru	2	Chyby vo vývoji
Spreneverenie aktív	3	Nedostatočné fyzické zabezpečenie
Škodlivý software	5	Nedostatok aktualizácií softwaru potrebné pre ochranu pred nežiadúcim škodlivým kódom
Neúmyselná modifikácia dát	4	Slabé znalosti užívateľov v oblasti bezpečnosti
Neautorizovaný prístup do IS	3	Ukladanie a zapisovanie hesiel, nedostatočná aktualizácia a slabé heslá
Mechanické poškodenie siete	5	Zlé prevedenie lokálnej siete, aktívne aj pasívne prvky vystavené nebezpečenstvu
Strata dát	4	Nesprávne nastavené zálohovanie

Tabuľka č.2.: Identifikácia hrozieb a súvisiacich zraniteľností

Zdroj: Vlastné spracovanie

3.1.5 Matica zraniteľností

V tabuľke sú doplnené identifikované aktíva spolu s ich hodnotou. Ďalej tabuľka obsahuje identifikované hrozby a ich pravdepodobnosti. Vyplnené bunky tabuľky obsahujú posúdenie zraniteľností jednotlivých aktív jednotlivými hrozbami.

	Popis hrozby	Poškodenie HW	Zlyhanie SW	Sprenevernie aktív	Škodlivý SW	Modifikácia dát	Neautoriz.. prístup	Strata dát
	Pravdepodob. hrozby (T)	4	2	3	5	4	3	4
Popis aktíva	**Hodnota aktíva (A)**							
DB serveru	5					4		3
DB matriky	5					4		3
Pracovné stanice	3	3		2			3	
Server	4	4		3			3	
Sieť. tlačiarne	2	2						
UPS	3	1						
Mobilné zar.	1	1					4	
Kamerový sys.	3	2						4
Switch, routre	4	3						
Operačné sys.	3		2		4		3	
DB systémy	4		3		3		3	
Antivíroví SW	3							
Prac. aplikácie	3		2		2			
SW kam. sys.	3		3					
Prip. serveru	5	3	2					
Prip. internetu	2	2						
Kabeláž LAN	4	4						
Wi-Fi	1						2	

Tabuľka č.3.: Matica zraniteľností

Zdroj: Vlastné spracovanie

3.1.6 Matica rizík

Ďalším krokom bezpečnostnej analýzy je výpočet miery rizika. K výpočtu som použil vozrec **R = T * A * V**, kde:

- R je miera rizika
- T je pravdepodobnosť vzniku hrozby
- A je hodnota aktíva
- V je zraniteľnosť daného aktíva

	Popis hrozby	Poškodenie HW	Zlyhanie SW	Sprneverenie aktív	Škodlivý SW	Modifikácia dát	Neautoriz.. prístup	Strata dát
	Pravdepodob. hrozby (T)	4	2	3	5	4	3	4
Popis aktíva	**Hodnota aktíva (A)**							
DB serveru	5					80		60
DB matriky	5					80		60
Pracovné stanice	3	36		18			27	
Server	4	64		36			36	
Sieť. tlačiarne	2	16						
UPS	3	12						
Mobilné zar.	1	4					12	
Kamerový sys.	3	24						48
Switch, routre	4	48						
Operačné sys.	3		12		60		27	
DB systémy	4		24		60		36	
Antivíroví SW	3		30					
Prac. aplikácie	3		12		35			
SW kam. sys.	3		18					
Prip. serveru	5	60	20					
Prip. internetu	2	16						
Kabeláž LAN	4	64						
Wi-Fi	1						6	

Tabuľka č. 4.: Matica rizík

Zdroj: Vlastné spracovanie

Hranice pre vyhodnotenie závažnosti rizika navrhujem stanoviť takto:

- Nízke riziko (prijateľné) = 0 až 24 – označené žltou farbou
- Stredné riziko = 25 až 79 – označené oranžovou farbou
- Vysoké riziko = 80 a vyššie – označené červenou farbou

Bezpečnostná analýza teda odhalila 2 vysoké riziká, 17 stredných rizík a 13 nízkych (prijateľných) rizík.

3.2 Opatrenia k zvýšeniu bezpečnosti

Bezpečnostná analýza odhalila hrozby, riziká a ich pravdepodobnosti. Opatrenia popísané v tejto časti práce vychádzajú práve z bezpečnostnej analýzy.

3.2.1 Pracovné stanice

Ako vyplýva z analýzy súčasného stavu, pracovné stanice v kanceláriách sú zastarané a práca s nimi vyžaduje trpezlivosť a čas. Navrhujem výmenu týchto troch zariadení za novšie a výkonnejšie. Optimálnym riešením by boli zariadenia od firmy Lenovo a to konkrétne:
Lenovo IdeaCentre H30-05, ktoré disponujú týmito špecifikáciami:

Procesor:	AMD Quad Core A6-6310
RAM:	4GB
Grafika:	AMD Radeon R4
HDD:	1TB 7200 otáčok
OS:	Windows 8.1 64-bit
Ďalšie:	USB 3.0, DVD, čítačka kariet USB klávesnica a myš

3.2.2 Profylaxia HW

Odporúčam profylaxiu HW (t.j. vyčistenie zariadení od prachu a tak ďalej) minimálne raz za obdobie jedného roka a to špecializovaným externým pracovníkom, ktorý prevedie všetko, čo je potrebné na udržanie pracovných staníc v čo najlepšom stave v rátane výmeny chladiacej pasty, podložiek a podobne.

3.2.3 Záložné zdroje UPS

V kancelárií starostu obce absentuje záložný zdroj pre prípad výpadku elektrickej energie. Navrhujem zakúpenie zariadenia Fortron PPF3600120.

Výkon: 360 W / 650 VA

Napätie: 220/230/240 V

Prenosová doba: 2 – 6 ms

Výstup: 2 x Schuko zásuvka, ochrana telefónnej linky RJ11

Záložný čas: jedno PC so zaťažením 120 W: 10 minút

Odporúčam vytvoriť: **Plán obnovy HW vybavenia**. Obsahom plánu by malo byť :

- Finančné vyčíslenie potrebných prostriedkov
- Termín zahájenia a ukončenia projektu
- Formálne určenie zodpovednosti za obnovu
- Parametre a špecifikácia HW zariadení
- Kontrola

3.2.4 Prevedenie počítačovej siete

Súčasné umiestnenie serveru je absolútne nevhodné. Server je umiestnený v jednej z kancelárií na zemi, kde je neustále v prachu. Bezprostredne v jeho blízkosti je umiestnený radiátor. Kabeláž ktorá k nemu vedie nie je žiadnym spôsobom chránená.

Navrhujem umiestniť server do miestnosti určenej pre rozhlasové vysielanie, nakoľko Obecný úrad nemá priestory na vytvorenie miestnosti určenej pre server a ostatné dôležité aktívne prvky siete. Server by mal byť chránený pred prachom, teplom a v neposlednom rade pred nepoverenými osobami. Preto je nutnosťou zakúpenie nového Racku, ktorý musí spĺňať tieto podmienky.

V tejto miestnosti sa nachádza tak isto Rack, v ktorom je uložený kamerový systém obce. Rack je veľkosti štyri unity, z ktorých sú dve voľné. Tento priestor vidím ako najvhodnejšie reálne riešenie umiestnenia switchu. Tento switch je aktuálne nevhodne umiestnený v kancelárií a má k nemu prístup prakticky ktokoľvek.

Z dôvodu v akom stave sa momentálne server nachádza by bolo vhodné aby prešiel profylaxiou a bol vyčistený od prachu a nečistôt.

V každej z kancelárií absentujú dátové zásuvky a tým je kabeláž ohrozená mechanickým poškodením. **Navrhujem zabudovanie univerzálnej kabeláže** podľa platných noriem, s dostatočným počtom dátových zásuviek.

3.2.5 Fyzická bezpečnosť

Obecný úrad je budova otvorená verejnosti a tak je potrebné zamedziť prístup neautorizovaným osobám do priestorov rozhlasovej miestnosti v ktorej budú umiestnené dôležité aktívne prvky siete (server, switch ale aj DVR rekordér kamerového systému a podobne).

Navrhujem vymeniť stávajúce dvere za bezpečnostné s bezpečnostným zámkom. Prístup do tejto miestnosti bude riadený starostom obce, ktorý bude mať ako jediný kľúče od tejto miestnosti.

Nutnosťou je vypracovanie:

Smernice o fyzickom prístupe zamestnancov do priestorov OÚ. Popisom tejto smernice bude:

- Vykonanie náležitostí pri príchode a odchode z práce
- Špecifikovanie povolenia prístupov pre jednotlivých zamestnancov do jednotlivých priestorov
- Postup pri strate kľúčov a podobne.

Smernice o fyzickom prístupe zamestnancov do serverovej miestnosti. Popisom tejto smernice bude:

- Správanie sa v danej miestnosti
- Prístup do serverovej miestnosti kontrolovaný starostom obce
- Protipožiarne opatrenia
- Klimatické podmienky
- Požiadavky na dvere a umiestnenie vybavenia

3.2.6 Antivírusová ochrana

Kvalitná antivírusová ochrana je nutná k ochrane každého zariadenia, nielen pracovných staníc, ale tak isto aj serveru a mobilných zariadení. Komplexným riešením je Antivírusový systém od firmy ESET. Ako optimálne riešenie vidím konkrétne produkt ESET Secure Office +, ktorý zahŕňa tieto oblasti zabezpečenia:

Pracovné stanice – systém poskytuje antivírovú a antispywarovú ochrany počítačov. Technológia ThreatSense obsahuje skenovanie založené na technológií cloud, kontrolu výmenných zariadení a vzdialenú správu koncových staníc.

Pomocou nástroja vzdialená správa je možné spravovať všetky stanice a mobilné zariadenia s nainštalovaným riešením ESET z jedného miesta.

Mobilné zariadenia – zabezpečí mobilné zariadenie nielen pred hrozbami na internete, ale taktiež pred nechcenými výdajmi za podvodné hovory. Zabudovaný modul Anti-Theft umožní zariadenie po krádeži sledovať, lokalizovať a prípadne aj vzdialene premazať.

Súborové servery - preverená antivírusová a antispywarová ochrana s optimalizáciou na serverové operačné systémy. ESET File Security spoľahlivo ochráni všetky serverové súbory a dôležité dokumenty.

Firewall a antispam - antivírus, personálny firewall, kontrola obsahu webu, antispam a ďalšie funkcie, ktoré zabezpečia sieť.

3.2.7 Prístupové práva k pracovným staniciam

Ako vyplýva z Analýzy súčasného stavu, zamestnanci Obecného úradu majú v súčasnej dobe neobmedzené práva na svojich pracovných staniciach a to z dôvodu, že sa prihlasujú ako administrátori. Navrhujem teda optimalizovať ich práva na takú mieru, aká je potrebná pre výkon ich pracovnej náplne. Externý poverený správca siete spracuje nutné práva zamestnancov a vytvorí užívateľské kontá. Na konte administrátora bude zmenené heslo a zamestnanci nebudú mať k tomuto účtu prístup.

Vhodným riešením je systém vyvinutý pre počítače s OS Microsoft – Active Directory. Active directory zahŕňa v sebe celú radu služieb. Jeho primárnou rolou je však poskytovanie centrálnych služieb pre autentizáciu a autorizáciu, teda správa účtov.

Zamestnanci po prihlásení k ich kontu „User“ môžu vykonávať väčšinu úloh, ako napríklad spustenie aplikácií, používanie lokálnych a sieťových tlačiarní a vypnutie a zamknutie pracovnej stanice, zálohovanie dát a podobne. Zamedzené im budú činnosti ako napríklad inštalácia nových aplikácií.

Postupy a špecifikácie prístupu k pracovným staniciam bude popisovať:

Smernica o riadení prístupu, ktorej popisom bude:

- Kto udeľuje práva užívateľom a na základe akých podmienok
- Akým spôsobom budú kontrolované úspešné a neúspešné prihlásenia
- Špecifikácia autorizácie jednotlivých zamestnancov

3.2.8 VPN a Firewall

Vytvorenie Virtuálnej privátnej siete je nutné z dôvodu vzdialeného prístupu k dokumentom a aplikáciám v lokálnej sieti. Ďalším z dôvodov je chránenie obsahu prenosných notebookov pripojeným na internet mimo lokálnej siete napríklad cez WiFi. Pripojením cez VPN dosiahneme šifrované pripojenie na internet. Nakoľko VPN šifruje internetovú prevádzku a zabraňuje ostatným, ktorí by sa mohli potencionálne snažiť odchytiť heslá alebo iné údaje je toto jednoduchou bezpečnostnou praktikou.

Navrhujem vytvorenie Virtuálnej privátnej siete na základe protokolu SSL (Secure Sockets Layer), ktorý poskytuje vysokú úroveň zabezpečenia. Ďalším možným riešením je VPN na založená na protokole OpenVPN. Ide o open-source VPN systém, ktorý je založený na SSL kóde. Tento protokol však na rozdiel od predchádzajúceho vyžaduje inštaláciu klienta, pretože Windows ani mobilné zariadenia ho natívne nepodporujú. Oba protokoly sú bezplatné a netrpia problémami s pripojením.

Firewall je z hľadiska bezpečnosti nutným prvkom každej lokálnej siete. Pre zabezpečenie VPN, jej prístupu k nej a ochrany lokálnej siete z vonku odporúčam zariadenie Vigor 2960.
Vigor 2960 je bezpečnostný Dual-WAN firewall. Kombinuje vysoko rýchlostný prístup

k internetu a obsiahlu bezpečnosť vďaka pokročilému firewallu a funkciám VPN navrhnutých pre aplikácie menších podnikových pobočiek.

Špecifikácia zariadenia Vigor 2960:

- Spĺňa požiadavky vysokorýchlostného internetu
- Nepretržitosť prevádzky vďaka funkciám Dual Wan Load-balancing a záloha
- 200 VPN tunelov pre bezpečný vzdialený prístup
- Podpora sietí IPv6 vrátane migrácie
- Chránený službami 3DES (Triple Data Encryption Standard) alebo AES (Advanced Encryption Standard)

Pre prístup k VPN navrhujem vytvoriť:

Smernicu na pripojenie a prácu cez VPN, ktorej obsahom bude:

- Spôsob pripojenia
- Prístup k jednotlivým častiam siete cez VPN
- Povolené operácie
- Kontrola prístupu

3.2.9 Zálohovanie dát

Zálohovanie dát prevedením na fileserver, ktorý obsahuje diskovú jednotku v režime RAID1 je v poriadku. Problém je v spôsobe zálohovania a síce prostredníctvom programu Everyday Auto Backup, ktorý je nastavený na Startup. Tento aktuálne využívaný program je voľne šíriteľný, čo znamená že bol zadarmo. Jeho možnosti nastavení sú obmedzené a nepostačujú pre potreby Obecného úradu.

Jedným z lepších a vhodnejších softwarov by mohol byť Cobain Backup 11 Gravity, ktorý je tak isto voľne šíriteľný, no jeho nastavenia a spoľahlivosť sú kategoricky lepšie. Tento software umožňuje zálohovať kamkoľvek po sieti a prípadne cez internet prostredníctvom FTP serverov. Program ponúka nastaviť zálohovanie v rôznych časových intervaloch s detailným plánovaním. Ďalšou z výhod je podpora kompresie zálohovaných súborov zabalením do archívov formátu ZIP alebo 7Z. Záložné kópie je možné šifrovať a chrániť heslom. Cobain Backup využíva šifrovanie AES.

Navrhujem vytvorenie internej smernice:

Smernica o zálohovaní dát, ktorej popisom bude:

- Doba zálohovania
- Frekvencia zálohovania
- Zálohovacie médiá
- Šifrovanie dát a zaobchádzanie so šifrovanými dátami
- Likvidácia nepotrebných dát
- Kontrola

3.2.10 Politika hesiel

Z analýzy súčasného stavu vyplýva, že neexistuje platný dokument, ani interné pravidlá, ktoré by upresňovali politiku hesiel v prostredí Obecného úradu. Navrhujem preto vypracovať internú **smernicu**, ktorá bude bližšie špecifikovať používanie hesiel, ich aktualizáciu, podmienky dostatočne bezpečného hesla a podobne. So smernicou musia byť zamestnanci riadne zoznámený. Svojim podpisom zamestnanec potvrdí, že problematike politiky hesiel porozumel a akceptuje smernicu.

Hlavné zásady bezpečného hesla

- Dĺžka hesla minimálne 8 znakov
- Nutne používané znaky v hesle – čísla (0 – 9), veľké a malé písmená
- Heslo nesmie byť zhodné s predchádzajúcim
- Heslo nesmie obsahovať užívateľské meno (login)
- Heslo musí byť udržiavané v tajnosti, nikde zaznamenávané

3.2.11 Povedomie zamestnancov o bezpečnosti ICT

Pre bezpečnosť informačného systému je nesmierne dôležité, aby si zamestnanci uvedomovali dôležitosť informácií obsiahnutých v IS a samy sa snažili svojim správaním udržiavať samotný informačný systém v bezpečí. Preto vidím ako nutnosť rozvíjať ich povedomie o informačných technológiách a ich ochrane. Doposiaľ zamestnanci nepodstúpili žiadne **školenie**, ktoré by bolo zamerané na bezpečnosť a ochranu

informácií. Navrhujem preto preškoliť každého z administratívnych pracovníkov v tejto oblasti.

Hlavné body, vyplývajúce z pohovorov s jednotlivými zamestnancami a odhalení ich nedostatkov, ktoré by malo **školenie** nutne obsahovať:

- Informácie ako dôležité aktívum
- Podstata zabezpečenia informácií
- Zásady zaobchádzania s dátami, prevažne ich zálohovanie
- Zásady bezpečnej práce na internete
- Tvorba, používanie, zmena hesiel
- Dôležité základné prvky siete a manipulácia s nimi

3.3 Časový plán

V časovom pláne sú zhrnuté dôležité míľniky zvýšenia bezpečnosti OÚ. Pri stanovovaní časového horizontu bola braná do úvahy finančná, technologická a implementačná náročnosť daných opatrení. Niektoré opatrenia, ako napríklad zvyšovanie povedomia zamestnancov o bezpečnosti IS/ICT nie sú ukončené konkrétnym dátumom, ale mali by prebiehať kontinuálne do budúcnosti a priamou úmerou zlepšovať vedomosti zamestnancov v danej problematike.

Konkrétne bezpečnostné opatrenie	**Časový horizont do:**
Výmena pracovných staníc + inštalácia potrebného SW	1.10.2015
Profylaxia serveru a ostatného HW	15.6.2015
Nákup záložného zdroju UPS	1.7.2015
Vybudovanie univerzálnej kabeláže	1.1.2016
Zvýšenie fyzickej bezpečnosti	1.8.2015
Optimalizácia prístupových práv užívateľov	15.7.2015
Implementácia VPN a Firewall	1.11.2015
Optimalizácia zálohovania	15.6.2015
Zakúpenie licencií k antivírusovému SW a jeho inštalácia	1.7.2015
Zvyšovanie povedomia zamestnancov o bezpečnosti IS/ICT	kontinuálne

Tabuľka č. 5.: Časový plán jednotlivých opatrení

Zdroj: Vlastné spracovanie

3.4 Ekonomické Zhodnotenie

V tejto časti zhodnotím náklady vynaložené na zvýšenie bezpečnosti IS a ich ekonomické prínosy.

Obecný úrad samotný netvorí žiadny zisk, preto je náročné ekonomicky zhodnotiť prínosy bezpečnostnej stratégie. Existujú však rôzne ekonomické a finančné ukazovatele, prostredníctvom ktorých je možné takúto kontrolu previesť.

Bezpečnostná politika a jej správne prevádzanie v praxi môže akémukoľvek subjektu, či už sa jedná o súkromné firmy, alebo verejnú správu ušetriť nemalé peniaze. V nasledujúcej tabuľke sú zhrnuté náklady, ktoré by v prípade zavedenia mojich návrhov do praxe vznikli.

Účel	**Náklad v €**
Nové pracovné stanice	**759** (3 x 253)
Profylaxia HW	**65** (5 x 13)
Záložný zdroj – UPS	**60**
Vybudovanie univerzálnej kabeláže	**1500**
Licencie na antivírus	**200** (5 x 40)
Firewall	**400**
Externá firma – inštalácia	**1000**

Tabuľka č.6.: Rozpočet
Zdroj: Vlastné spracovanie

Zakúpením nových pracovných staníc a pravidelnou profylaxiou hardwaru a softwaru sa zvýši pracovný výkon zamestnancov, čo pozitívne ovplyvní fungovanie Obecného úradu. Prerobenie počítačovej siete, ochrana jej dôležitých aktívnych ale aj pasívnych prvkov zabráni možnému poškodeniu a následnému výpadku informačného systému. Kvalitný a dobre aktualizovaný antivírus ušetrí peniaze za opravu softwaru. Náklady vynaložené na zvýšenie bezpečnosti informačného systému posilnia ekonomickú stabilitu do budúcnosti.

4 ZÁVER

V mojej práci som sa zaoberal zvýšením bezpečnosti informačného systému v prostredí reálneho a konkrétneho Obecného úradu. Podarilo sa mi zanalyzovať nedostatky, bezpečnostné hrozby a riziká, z ktorých som vychádzal pri vypracovaní konkrétnych opatrení zvyšujúcich bezpečnosť informačného systému. Každé z technických opatrení je podporené organizačným opatrením.

Pri vypracovávaní tejto práce som zistil, že bezpečnosť informačných a komunikačných technológií je v oblasti štátnej správy stále dosť zanedbávaná. Informačné systémy týchto a podobných subjektov obsahujú veľké množstvo dôležitých a zneužiteľných dát, ktoré by mali byť v záujme ich ochrany riadne zabezpečené.

Ciele mojej práce boli splnené a po aplikovaní mojich návrhov do praxe, budú dáta ale aj celý informačný systém Obecného úradu lepšie chránené proti rôznym druhom útokov, nehôd a podobne.

5 ZOZNAM POUŽITÝCH ZDROJOV

Knihy:

(1) DOUCEK, Petr, Luděk NOVÁK, Lea NEDOMOVÁ a Vlasta SVATÁ. *Řízení bezpečnosti informací.* 2. rozšířené vydání. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

(2) POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

(3) ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(4) SORIANO, Miguel. *Informačná a sieťová bezpečnosť.* České vysoké učení technické v Praze. ISBN 978-80-01-05299-0.

(5) ONDRÁK, Viktor. *Management informační bezpečnosti.*

Elektronické zdroje:

(6) DEKÝŠ, Peter. *Správa informačnej bezpečnosti v malej a stredne veľkej spoločnosti.* [online]. ESET: © 2014 [cit. 22.11.2014]. Dostupné z: http://www.eset.com/sk/firmy/services/clanky/sprava-informacnej-bezpecnosti/. Pozn.: článok uverejnení v časopise eFocus, marec 2010.

(7) KALUŽA, František. *Outsourcing z pohľadu riadenia informačnej bezpečnosti.* [online]. Copyright © 2003-2014 by authors. [cit. 23.11.2014]. Dostupné z: http://www.securityrevue.com/article/2011/06/outsourcing-z-pohladu-riadenia-informacnej-bezpecnosti/

(8) *Co je to VPN*. [online] Copyright © 2014 Microsoft. [cit. 1.12.2014]. Dostupné z: http://technet.microsoft.com/cs-cz/library/cc731954%28v=ws.10%29.aspx

(9) TOMKA, Dušan. *Zákon o kybernetickej bezpečnosti.* [online]. Copyright © epravo.sk, s.r.o. 2014. [cit. 5.12.2014]. Dostupné z: http://www.epravo.sk/top/clanky/zakon-o-kybernetickej-bezpecnosti-758.html.

České technické normy a zákony:

(10) Zákon č. 181 ze dne 29. srpna 2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů. In: *Sbírka zákonů České republiky*. 2014

(11) ČSN ISO/IEC 27001:2014 *Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky*. Český normalizační institut, 2014

6 ZOZNAM POUŽITÝCH OBRÁZKOV