EKONOMICKÁ UNIVERZITA V BRATISLAVE

Obchodná fakulta

Evidenčné číslo: 102007/I/2020/360891923480263 72

OCHRANA INFORMAČNÝCH SYSTÉMOV V PODNIKANÍ

Diplomová práca

2020 **Bc. Dóra Muzsay**

EKONOMICKÁ UNIVERZITA V BRATISLAVE

Obchodná fakulta

OCHRANA INFORMAČNÝCH SYSTÉMOV V PODNIKANÍ

Diplomová práca

Študijný program: marketingový a obchodný manažment

Študijný odbor: ekonómia a manažment

Školiace pracovisko: Katedra informatiky obchodných firiem

Vedúci záverečnej práce: Ing. Kuchta Martin, PhD.

Bratislava 2020 Bc. Dóra Muzsay

Čestné vyhlásenie

Čestne vyhlasujem, že diplomovú prácu som písala samostatne a uviedla som každú literatúru, ktorú som použila pri vypracovaní práce.

Dátum: .....

POĎAKOVANIE

Chcela by som sa poďakovať môjmu vedúcemu diplomovej práce, Ing. Martinovi Kuchtovi, PhD. za efektívnu spoluprácu a za užitočné rady, ktoré mi pomohli pri písaní záverečnej práce. Napokon by som chcela poďakovať aj IT manažérom vybranej firmy a správcom systému mestského úradu za všetky hodnotné informácie dôležité pre náš výskum.

ABSTRAKT

MUZSAY, Dóra: *Ochrana informačných systémov v podnikaní* – Ekonomická univerzita v Bratislave. Obchodná fakulta; Katedra informatiky obchodných firiem. – Vedúci záverečnej práce: Ing. Martin Kuchta, PhD. – Bratislava: OF EU, 2020, 65 str.

Cieľom záverečnej práce je analýza bezpečnosti informačných systémov a ochranných opatrení vo vybraných inštitúciách. Záverečná práca zároveň identifikuje hrozby a typy útokov, ktoré hrozia všetkým podnikom bez ohľadu na sektor podnikania. Práca je rozdelená do 5 kapitol. Záverečná práca obsahuje vlastne spracované 3 obrázky a 1 prílohu. Prvá kapitola je teoretickým pilierom práce. To znamená, že sú definované všetky dôležité pojmy týkajúce sa danej problematiky, ako napríklad aktíva podniku, hrozby, najčastejšie útoky v podnikoch alebo bezpečnostná politika. V druhej kapitole sú definované hlavné ciele teoretickej a praktickej časti, charakterizované sú metódy skúmania a jednotlivé kroky, ako prebiehal samotný prieskum. Prieskum bol realizovaný formou hĺbkových pohovorov s kompetentnými osobami vybraných inštitúcií. Porovnávali sme bezpečnostné opatrenia týkajúce sa informačných systémov prijatých v dvoch vybraných organizáciách. Oslovili sme jednu súkromnú spoločnosť a jednu miestnu samosprávu v okrese Dunajská Streda. Výsledok práce indikuje, že organizácie v súčasnej dobe dostatočne využívajú ochranné opatrenia v rámci bezpečnostnej politiky v oblasti informačných systémov a informačných technológií.

Kľúčové slová: informácie, informačný systém, ochrana, bezpečnostná politika

ABSTRACT

MUZSAY, Dóra: *The management of business operations through mobile devices* – University of Economics in Bratislava. The Faculty of Commerce; Department of Business IT. – Thesis Supervisor: Ing. Martin Kuchta, PhD. – Bratislava: FC UE, 2020, 65 p.

The aim of the thesis is to analyze the security of information systems and security measures in selected institutions. The final work also identifies threats and types of attacks that threaten all businesses, regardless of business sector. The thesis is divided into 5 chapters. The final thesis contains actually 3 images and an appendix. The first chapter is the theoretical pillar of the work. This means that all important terms related to the issue are defined, such as company assets, threats, the most common attacks in companies or security policy. The second chapter defines the main goals of the theoretical and practical part, characterizes the methods of research and the individual steps as the research itself. The survey was conducted in the form of regular interviews with competent people from selected institutions. We compared security measures related to information systems adopted in two selected organizations. We contacted one private company and one local government in the district of Dunajská Streda. The result of the work indicates that organizations currently make sufficient use of protective measures in the security policy in the field of information systems and information technology.

Key words: information, information system, protection, security policy

OBSAH

Zoznam obrázkov

Úvod

Dnešnú modernú dobu charakterizuje rýchly vývoj informačných a komunikačných technológií a ich rastúci vplyv na ľudí a na samotnú spoločnosť. Z uvedeného dôvodu musíme držať krok s modernými technológiami, aby sme mohli zvýšiť efektívnosť práce v spoločnosti. To platí aj pre hospodársku sféru, preto je dôležité, aby budúci manažéri a ekonómovia mali dostatočný prehľad a potrebné znalosti aj v tejto oblasti. Musíme si uvedomiť, že v budúcnosti práve oni budú ovplyvňovať zavádzanie a účinné využívanie informačných a komunikačných technológií v každom odvetví spoločnosti.

Záverečná práca je zameraná na ochranu informačných systémov. Vysvetlí základné pojmy súvisiace s témou záverečnej práce a uvádza konkrétne spôsoby na ochranu týchto systémov na praktickej úrovni. Práca je určená pre bežných používateľov, manažérov, resp. odborníkov v praxi, ktorí sa každodenne zaoberajú s informačnými technológiami a ich každodenne využívajú a vyvíjajú; aby získali súhrnný prehľad o tejto problematike. Vyššie uvedené osoby s prečítaním tejto záverečnej práce dostanú celkový obraz o tom, čo všetko má dnes podnik dodržiavať v súvislosti s informačnými systémami vyplývajúc z platnej slovenskej a medzinárodnej právnej legislatívy a aby mali možnosť porovnávať už vo firmách zavedené a využívané bezpečnostné opatrenia. Cieľom záverečnej práce je zároveň osloviť aj študentov, ktorí plánujú v budúcnosti podnikať alebo pracovať v tejto sfére. Pri vysvetľovaní jednotlivých pojmov a procesov bola uprednostnená zjednodušená charakteristika pojmov, aby ich podstata bola zrozumiteľná pre široký okruh čitateľov.

V prvom kroku záverečnej práce sme sa oboznámili so základnými pojmami v oblasti informačných technológií a informačných systémov. Definovali sme hrozby a typy útokov vyskytujúcich sa v podnikoch v oblasti informačných systémov a vysvetlili sme spôsoby vyhnutia sa im alebo manažovanie a zvládnutie krízovej situácie v prípade útokov smerujúcich sa na informačný systém podniku. V druhom kroku práce sme poukázali na dôležitosť ochrany týchto systémov, s cieľom zabezpečiť bezproblémové a efektívne fungovanie súkromných podnikov a inštitucionálnych organizácií v štátnej sfére. Z toho vyplýva, že v dnešnej dobe je veľmi dôležité, aby sme boli schopní postupovať s dobou a úspešne hospodárili so svojimi personálnymi a technickými zdrojmi.

1. Súčasný stav riešenej problematiky doma a v zahraničí

Ľudia často potrebujú rôzne informácie ku každodenným rozhodnutiam. V dnešnej dobe sa stretávame s pojmom informačná spoločnosť, ktorá potrebuje informácie pre svoje rozhodovanie a rozvoj. Tieto pojmy sú mimoriadne dôležité, lebo informácie a informačné zdroje sú základnými predpokladmi pre zakladanie a formovanie podnikových informačných systémov.

S pojmom informácia (pochádza z latinského slova „informare“ = tvoriť, formovať) sme sa prvýkrát stretli v roku 1274, kde mal význam ako súbor aktov, ktoré opisujú trestné činy páchateľa. V súčasnosti vymedzujeme slovo *informácia* v oveľa širšej súvislosti, no podstata pojmu ostala tá istá.

Informáciu môžeme skúmať z viacerých pohľadov. Ak skúmame iba súvislosti a štruktúry medzi jej základnými znakmi, hovoríme o syntaktickom prístupe. Ak skúmame informáciu z hľadiska jej prospešnosti a účelného využitia pre jej príjemcu, tak ide o pragmatický prístup. Informácie sú neoddeliteľnou súčasťou úspešného podnikového riadenia. Tento názor z roku 1993 podporuje aj známy ekonóm Peter Drucker nasledovne:

„ *Informácie sú jediným zmysluplným zdrojom pre podnikanie, ostatné výrobné faktory (práca, pôda, kapitál) sa stávajú druhoradými.„*[1]

Každá informácia má však svoju úžitkovosť. Informácie majú byť spoľahlivé, vhodne načasované, vecné a kvalitné. Takéto informácie majú väčšiu hodnotu ako nejaké vecné a technologické zariadenie podnikov.

Hodnotu informácie, ktorá je vlastne výsledkom spracovania základných údajov, ovplyvňujú aj ďalšie činitele, ako sú:

- výber a zhrnutie vstupných údajov;
- rozsah úpravy vstupných údajov;
- štruktúra úpravy vstupných údajov;

[1] DRUCKER, Peter Ferdinand. *Postkapitalistická společnost*. 1. vydanie. Praha: Management Press, 1993. 40 s. ISBN 80-85603-31-4

- úplnosť výstupných informácií;
- charakter výstupných informácií.

Ak analyzujeme pojem *informácia*, dostávame sa aj k slovu *údaj* alebo *dáta*. Údaje sú základnými zdrojmi pre formovanie vhodných a presných informácií. Ako príklad môžeme uviesť vedenie účtovníctva, pri ktorom nastane premena vstupných údajov na priebežné, neskôr na výsledné informácie. Výsledkom môže byť napríklad informácia o výsledku hospodárenia, o rentabilite alebo účtovná závierka na konci účtovného obdobia.

Informácia v riadení firmy

V dnešnej dobe predstavuje informácia zdroj konkurenčného súťaženia tak na politickej rovine, ako aj v podnikovej sfére. Na jednej strane je zdravé konkurovanie hnacou silou rastu a rozvoja svetovej a zároveň aj domácej ekonomiky. Na druhej strane sú podniky pod konštantným tlakom, lebo sa musia paralelne rozvíjať s najnovšími technológiami a modernými trendami, ak nechcú stratiť svojich zákazníkov.

Kategória prospechu, ktorú firma môže dosiahnuť s využitým informácie, predstavuje samotnú hodnotu informácie. Informácie vo vyššej kvalite podporujú rozhodovacích manažérov a vedú k perspektívnemu podnikovému úspechu.

Môžeme skonštatovať, že informácia je nehmotným statkom firmy vo forme know-how, ktorú môžeme využiť na získanie lepšej pozície na trhu. Popritom môžeme aj s informáciou obchodovať, viacnásobne ju predať v spojení s vnútorným využitím. Zároveň sa však informácie môžu stať obeťou hackerov, preto je odporúčané ich svedomito chrániť.

Informačná spoločnosť a informačný manažment

Za informačnú spoločnosť považujeme takú spoločnosť, kde úroveň života, aspekt sociálnych zmien a rozvoja ekonomiky je vo veľkej miere podmienená vhodnými informáciami a ich využívaním. Informačná spoločnosť okrem toho potrebuje rôzne inovačné zmeny zo strany ľudí v konaní a myslení. V podnikateľskej sfére tu hovoríme o manažéroch a riadiacich pracovníkoch. Rozhodujúcim faktorom týchto zmien v informačných spoločnostiach sú samotné informácie.

„Informačný manažment je transdisciplinárna odbornosť. Je to prepojenie moderného manažmentu, informatiky a systémových prístupov. Môžu sem vystupovať aj

poznatky z oblasti ekonomiky sociológie, psychológie, politológie, marketingu, operačnej analýzy, atď.“[2]

Informačný manažér neustále potrebuje informácie, ktoré charakterizujú minulú, momentálnu a pravdepodobnú situáciu činností v rámci firmy, ako aj samozrejme údaje z vonkajšieho prostredia. V dnešnej zrýchlenej dobe predstavuje kľúčový faktor úspešného vedenia firmy pravidelné využívanie vnútorných a vonkajších informácií. Môžeme skonštatovať, že sú podporným prostriedkom pri rozhodovaní v taktickej, v strategickej a aj v operatívnej úrovni rozhodovania. Tento proces je samozrejme interaktívnym procesom, resp. sa prebieha v obidvoch smeroch. Z vyššie uvedeného vyplýva, že nielen získané informácie ovplyvňujú rozhodovanie manažéra, ale aj vedúci pracovníci svojimi rozhodnutiami majú dosah na stav vo firme a tiež na okolité prostredie.[3]

1.1 Informačné systémy

V dnešnej modernej dobe informačné zabezpečenie firmy má dôležitý význam, nezávisle od veľkosti podniku alebo od oblasti podnikania. Informácie nie sú iba základom úspešného riadenia, inovácií spoločnosti, ale môžu zabezpečiť aj dlhodobú konkurenčnú výhodu na určitom trhu. Preto podniky nemôžu fungovať bez informačných systémov, ktoré nám zabezpečujú získavať, klasifikovať, uchovávať a upraviť informácie.

Na otázku, čo je vlastne informačný systém, by sme mohli takto odpovedať:

“*Informačný systém je vo všeobecnosti definovaný ako súbor ľudí, technických prostriedkov, metód zabezpečujúcich zber, prenos uchovávanie a spracovanie dát za účelom tvorby a prezentácie informácií pre potreby používateľov činných v systémoch riadenia. IS má v tomto ponímaní za úlohu zabezpečiť dostatok relevantných informácií v správnom čase na vykonanie riadiacich funkcií v celom systéme*.”[4]

Pravdou je, že informačné systémy nemusia byť v každom prípade spojené s počítačmi. Jednoduchým príkladom je evidencia inventárnych kariet hmotného majetku v podniku. Navyše sem patrí napríklad aj jednoduchý diár s kontaktmi a naplánovanými stretnutiami obchodných partnerov.

---

[2] GIACKOVÁ, Sylvia. *Informačný manažment*. 2008. [online]. [cit. 2020-02-02]. Dostupné na internete: https://giackova.blog.sme.sk/c/169311/Informacny-manazment.html

[3] KUČERA, Milan a kol. *Podnikové informačné systémy*. Prvé vydanie. Slovenská poľnohospodárska univerzita v Nitre, 2017. 21-24 s. ISBN 978-80-552-17239

[4] KIMLIČKA, Š. 1995. Manažment tvorby informačných systémov: T*eoretické východiská, metódy a postupy vo sfére vedy, výskumu a vzdelávania.* Bratislava: Slovenská technická knižnica, 1995. 45 s., ISBN 80-85165-52.

Rozvoj a rast informačných systémov a ich rastúci význam pre podnik podporuje aj rozvoj informačno-komunikačných technológií (IKT), ktorý umožní získanie neskutočne veľkého objemu dát a informácií. V dnešnej dobe, vďaka týmto technológiám, spracovanie a prenos rôznych informácií sa stali veľmi ľahkými a rýchlymi procesmi, ale z druhého hľadiska môžeme skonštatovať, že u nás sa stráca obrovské množstvo informácií a dát.

Časom sa mení aj vzťah k informačným systémom. Ich automatizácia je dnes dôležitou súčasťou riadenia každého moderného podniku. Automatizácia je vlastne technikou modelovania samočinných postupov a tiež samokontrolovania, ktorá zabezpečí predpoklady pre zmenu procesov k dosiahnutiu týchto operácií. Automatizácia informácií je rýchlo vyvíjajúce sa odvetvie, ktoré nám poskytuje rôzne digitálne riešenia, resp. výsledky bez ľudského činiteľa. Z toho vyplýva, že kým v minulosti na takú prácu bolo potrebné veľa pracovníkov, v dnešnej dobe je vykonaná prostredníctvom automatizovaných strojov, počítačov.

Súčasné informačné systémy sú vo všeobecnosti kombináciou rôznych IKT riešení, informácií, dát a samozrejme ľudí, ktorí ich ovládajú a pritom skúmajú ich výsledky. Keď hovoríme o informačnom systéme, nikdy nehovoríme iba o programovom vybavení, ale je to kombinácia viacerých komponentov, ktoré spoločne ho vytvárajú. Vychádzajúc z týchto poznatkov bola generovaná nová, jednoduchšia definícia informačných systémov, ktorá hovorí, že:

„Informačný systém je kombinácia hardvéru, softvéru, infraštruktúry a vyškoleného personálu organizovaných s cieľom uľahčiť plánovanie, koordináciu a rozhodovanie v organizácii.“[5]

1.1.1 Úlohy a ciele informačných systémov

Faktom je, že každá organizácia má odlišné informačné potreby a je tiež dôležité uviesť, že nie každý informačný systém je vhodný pre akýkoľvek podnik. Tým pádom môžeme skonštatovať, že každý informačný systém je iný, ale majú určité vlastnosti, ako napríklad úlohy a ciele, ktoré majú všetky informačné systémy spoločné.

K najdôležitejším úlohám IS patrí zabezpečiť lepšiu orientáciu v rôznych organizačných problémoch, urýchliť a zvýšiť kvalitu rozhodnutia. Jeho poslaním je teda

[5] *Information system.* 2017. [online]. [cit. 2020-02-02]. Dostupné na internete: http://www.businessdictionary.com/definition/information-system.html

zlepšiť proces rozhodovania a podporovať osobám pretransformovať informácie na rozhodnutie alebo na činnosť.

Cieľom IS je zhromaždenie vhodných informácií, ich uchovanie do budúcnosti a spracovanie za účelom dodania odpovedí na špecifické otázky a v poslednej fáze podať dáta ich užívateľom.

Poznáme teda štyri základné funkcie informačných systémov: zhromažďovanie dát a informácií, uchovávanie dát a informácií, spracovanie údajov a prenos dát a informácií.

Ciele a úlohy informačného systému môžeme charakterizovať z pohľadu jeho komponentov nasledovne:

- expertné – využívané v komplexných systémoch;
- strategické – využívané pri plánovaní;
- taktické – využívané pri rozhodovaní alebo pri kontrole;
- operatívne – využívané pri každodenných úlohách.

Na základe uvedených informácií môžeme vyvodzovať, že prioritným cieľom informačných systémov je podporiť fázy rozhodovania v riadiacom procese. Práve preto je nevyhnutné, aby informačný systém splnil vyššie uvedené funkcie. [6]

1.1.2 Ľudské zdroje – kľúčový prvok informačných systémov

Iba niekoľko manažérov uznáva, že človek je rovnako dôležitým prvkom pre efektívne fungovanie informačných systémov ako samotné zariadenie a programové vybavenie. Informačné systémy vyžadujú veľké zmeny v spoločnosti, a tým aj požiadavky na vzdelanie, resp. kvalifikáciu zamestnancov. Avšak je medzi nimi rozdiel, požiadavky sú spojené s pracovným miestom, so zamestnávateľom a kvalifikáciou vlastných zamestnancov.

V dnešnej dobe je nedostatok kvalifikovaných uchádzačov vo sfére informačnej technológie, práve preto je odporúčané zabezpečiť výchovu vlastných zamestnancov, aby neboli nútení svojich spoľahlivých a skúsených zamestnancov prepustiť. Riadiaci pracovníci tiež by mali mať prehľad o najnovších výpočtových a komunikačných technológiách, aby efektívne rozhodovali o vývoji týchto systémov vo firme. Nakoniec

[6] RÁBOVÁ, Ivana DRLÍK, Martin. *Podnikové informačné systémy, ich architektúra a vývoj*. Prvé vydanie. Univerzita Konštantína Filozofa v Nitre, 2013. 129-132 s. ISBN 978-80-558-0287-9

môžeme tvrdiť, že vyspelý podnik musí stále sledovať a zostať v tempe s vývojom rôznych informačných technológií.[7]

1.1.3 Klasifikácia informačných systémov

Informačné systémy môžeme klasifikovať podľa rozličných vlastností, akými sú napríklad: účel jeho využitia, obsah, stupeň automatizácie, a pod.

1.1.4 Informačné systémy v oblasti riadenia podniku

Informačné systémy v oblasti riadenia sme vyhľadali zo zahraničných zdrojov. Podľa zistených informácií uvedené informačné systémy v oblasti riadenia v značnej miere sa podobajú na slovenské informačné systémy. Analyzované informačné systémy sú nasledovné:

TPS - Transaction Processing System – systém na spracovanie transakcií je typ systému na spracovanie informácií pre obchodné transakcie, ktoré zahŕňajú zber, ukladanie, úpravu a získavanie všetkých dátových transakcií podniku. Charakteristiky systému spracovania transakcií zahŕňajú spoľahlivosť, výkon a konzistentnosť. TPS je tiež známy ako spracovanie údajov v reálnom čase.

Charakteristické znaky systému spracovania transakcií:

- vytvára informácie pre iné systémy;
- je používané zamestnancami spoločnosti;
- orientuje sa na efektívnosť.[8]

OLRT – On-Line-Real-Time – je špeciálny systém zameraný na bezprostredné riadenie rôznych technologických procesov. Charakteristickým znakom je minimálny počet vstupov a výstupov zo strany človeka. Podstatou sú rôzne numerické stroje a zariadenia spojené s počítačom. Počítač stanoví čo sa bude vyrábať na jednotlivých zariadeniach. To znamená, že celý proces zabezpečí počítač bez ľudských zásahov.

MIS - Management Information System - manažérsky informačný systém je použitie informačných technológií, obchodných procesov a ľudí na zaznamenávanie,

[7] KUČERA, Milan a kol. *Podnikové informačné systémy*. Prvé vydanie. Slovenská poľnohospodárska univerzita v Nitre, 2017. 38-40 s. ISBN 978-80-552-17239

[8] *Introduction to Information System.* [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.javatpoint.com/cyber-security-information-system-introduction

ukladanie a spracovanie údajov, na vytváranie zmysluplných informácií. Tieto informácie pomáhajú tvorcom robiť každodenné správne rozhodnutia. Používa sa na taktické rozhodnutie (strednodobé rozhodnutie) na zabezpečenie plynulého chodu organizácie. Pomáha tiež vyhodnotiť výkonnosť organizácie porovnaním predchádzajúcich výstupov so súčasnými výstupmi.

Charakteristické znaky manažérskych informačných systémov:

- vychádza z interných informačných tokov;
- podporuje relatívne štruktúrované rozhodnutia;
- je nepružný a má tiež malú analytickú kapacitu;
- používa sa na nižšej a strednej úrovni riadenia;
- zaoberá sa skôr minulosťou a súčasnosťou, ako budúcnosťou.[9]

DSS - Decision Support System – systém na podporu rozhodovania, je počítačovým aplikačným programom, ktorý používajú vedúci pracovníci a manažéri na analýzu obchodných údajov. Prezentujú ho v takej forme, aby používatelia ľahšie realizovali obchodné rozhodnutia. Tieto systémy sú zvyčajne interaktívne a môžu sa použiť na riešenie problémov, ktoré nie sú vytvorené vo firme. Pomáha pri výmene informácií v rámci spoločnosti.

Znaky systému na podporu rozhodovania sú:

- podpora čiastočne štruktúrovaných alebo nevhodne štruktúrovaných rozhodnutí;
- používajú sa na vyšších úrovniach riadenia;
- má analytickú a / alebo modelovaciu kapacitu;
- zabezpečuje predpovedanie budúcnosti.

EIS - Executive Information System - je to informačný systém na strategickej úrovni, ktorý sa nachádza na vrchole pyramídy. Jeho hlavným cieľom je poskytovať vedúcim predstaviteľom rôzne informácie získané z vnútorných aj vonkajších zdrojov. Ďalším cieľom je analyzovať prostredie, v ktorom organizácia pôsobí a naplánovať vhodné kroky na určenie dlhodobých trendov. Môže sa tiež použiť na monitorovanie výkonnosti organizácie, ako aj na identifikáciu príležitostí a problémov. EIS

[9] *Introduction to Information System.* [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.javatpoint.com/cyber-security-information-system-introduction

je navrhnutý tak, aby ho mohli priamo prevádzkovať riadiaci pracovníci bez potreby sprostredkovateľov.

Úlohy informačných systémov pre vrcholové riadenie:

- zabezpečiť jednoduché používanie;
- podpora neštruktúrovaných rozhodnutí;
- vypracovať predpovede do budúcnosti;
- zvyšovať flexibilitu a efektivitu riešení;
- využívanie interných aj externých zdrojov údajov;
- používanie iba na vyšších úrovniach autority. [10]

Informačné systémy v oblasti riadenia môžeme znázorniť informačnou pyramídou, ohľadom na to, či ide o strategické, taktické alebo operatívne riadenie.

1.1.5 Význam ochrany podnikových IS

V dnešnej dobe predstavujú informačné systémy najdôležitejších činiteľov dlhodobého úspechu alebo práve neúspechu firmy. Z toho vyplýva, že nielen vedúci manažéri, ale aj všetci pracovníci podniku, majú venovať veľkú pozornosť ich ochrane. Povinnosťou vrcholového manažmentu je poznať, aké straty môže zapríčiniť zneužitie alebo zničenie informačného systému organizácie a na základe toho zaviesť vhodné opatrenia na ochranu informačného systému firmy.

Ochrana informačných systémov prestavuje súbor technických, programových a personálnych opatrení s cieľom obmedzenia možných strát, ktoré by nastali vo firme v prípade zneužitia, poškodenia alebo zničenia informačného systému. Ochrana informačného systému sa stáva dôležitou súčasťou komplexu ochranných opatrení v organizácii.

Je nevyhnutné poznamenať, že prijaté ochranné a bezpečnostné opatrenia v oblasti informačného systému firmy v každom prípade zvyšujú obstarávacie a aj prevádzkové náklady, pritom prinášajú určité obmedzenia pre pracovníkov informačného systému a pre používateľov. Samozrejme tieto zvýšené náklady musia byť v súlade s odhadnutými

[10] STAŠÁK, Jozef MAZŮREK, Jaroslav. *Manažérska informatika II.* 1. vydanie. Žilinská univerzita v Žiline/EDIS – vydavateľské centrum ŽU, 2019. 27-30 s. ISBN 978-80-554-1544-4

stratami, pričom odporúčané je spočítať s 10 až 20 % z celkových nákladov firmy na informačný systém, jeho zaistenia a ochrany.[11]

Dôsledkom neustáleho rozvoja informačných technológií a tiež informačných systémov sú rozličné spôsoby na ich zabezpečenia. Takto vznikol nový pojem – **Information Security, - informačná bezpečnosť**, ktorú môžeme definovať takto:

„*Pod pojmom "informačná bezpečnosť" budeme chápať ochranu informácií v priebehu ich vzniku, spracovania, ukladania, prenosov a likvidácie prostredníctvom logických, technických, fyzických a organizačných opatrení, ktoré musí pôsobiť proti strate dôveryhodnosti, integrity a dostupnosti týchto hodnôt*." [12]

1.2 Bezpečnosť informácií v podnikaní

Prudký rozvoj informačných technológií spôsobil nutnosť riešenia nových úloh, ktoré sa týkajú hlavne ochrany a bezpečnosti informačných a komunikačných technológií. V minulosti ľudia riešili utajenia správ, v dnešnej dobe je dôležitá ochrana súkromia, bezpečnosť elektronickej komunikácie a elektronických systémov.

Z oblasti bezpečnosti informačných systémov a informačných technológií by sme mohli vymenovať nasledovné základné pojmy:

- **Aktíva** sú jednotlivými zložkami informačných technológií, ktoré samozrejme majú danú hodnotu pre spoločnosť.
- **Zraniteľnosť** rôznych aktív vyjadruje vlastne citlivosť aktív na vplyv hrozby.
- **Zraniteľné miesto** resp. **hrozbu** definovali správne odborníci Ján Staudek a Petr Hanáček:

„*Pojmom hrozba označujeme možnosť využiť zraniteľné miesto informačného systému k útoku na nej – teda ku spôsobeniu škody na aktívach*."[13]

[11] LENDEL, Viliam – KUBINA, Milan – HITTMÁR, Štefan. *Podnikové informačné systémy.* Žilina: Žilinská univerzita, vyd. Edis, 2013. 189 s. ISBN 978-80-554-0712-8

[12] KUČERA, Milan a kol. *Podnikové informačné systémy*. Prvé vydanie. Slovenská poľnohospodárska univerzita v Nitre, 2017. 149 s. ISBN 978-80-552-17239

[13] STAUDEK, Ján – HANÁČEK, Petr. *Bezpečnost informačních systémů. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technológií.* Úřad pro státní informační systém, 2000. 14 s.

- **Útok** je určitá udalosť, ktorá zapríčiní porušenie pravidiel a definovaných postupov pri prevádzkovaní informačných technológií a systémov. Útok sa môže označovať aj ako bezpečnostný incident.
- **Útočníci** sú osoby, ktorí využívajú zraniteľné miesta a hrozby na útoky. Poznáme dva typy útokov – úmyselné a neúmyselné.
- **Riziko** určí mieru ohrozenia aktív. Z predchádzajúcich informácií vyplýva, že zraniteľné miesta a rôzne hrozby zvyšujú riziko útoku. Hodnota aktív, zraniteľnosť aktív a úroveň hrozby nám umožní určiť úroveň rizika.
- **Protiopatrenia** sú spôsoby na znižovanie úrovne rizika a sú charakterizované nákladmi a efektivitou. Dôležité je, aby náklady vynaložené na zavedenie protiopatrení boli nižšie ako ich efektivita, resp. úžitkovosť chránených aktív.

V súvislosti s informačnými systémami sú určené hlavné bezpečnostné požiadavky, ktoré vychádzajú z predpokladov daného systému, prípadne z aktuálne platných zákonov a noriem.

Bezpečnostné požiadavky:

- **zachovanie dostupnosti –** šanca na vyžiadanie realizovať určitú činnosť;
- **zachovanie dôvernosti –** zabezpečuje sa takým spôsobom, že prístup k aktívam majú iba profesionálne, autorizované osoby;
- **zachovanie integrity –** neumožniť neautorizovaným osobám zmeniť aktíva.

Podľa charakteru rozlišujeme nasledovné druhy hrozieb:

- **fyzické a prírodné** – požiare, nehody, živelné pohromy;
- **ľudské –** úmyselné ľudské hrozby – pochádzajú z externého prostredia – hackeri, špionáž, alebo z interného prostredia – zamestnanci alebo návštevníci spoločnosti;
- **technologické –** poruchy a problémy spôsobené programami – trójske kone, vírusy;
- **technické** – problémy s fyzickými nosičmi údajov, poruchy počítačov a rôznych sietí. [14]

Profesor Loveček tvrdil správne*: „Aktíva v prípade osôb môžu byť ohrozené ich nedbanlivosťou, neznalosťou alebo zábudlivosťou.“*[15]

[14] HUŽVÁR, Miroslav - LACO, Peter. *Informačné technológie v ekonomickej praxi*.1. vydanie. Bratislava: Wolters Kluver, 2014.139-140 s. ISBN 978-80-8168-085-4

Najväčšou hrozbou podniku je únik tajných informácií, zmena alebo zničenie informácií.

Základné časti bezpečnosti informácií

Primárne komponenty bezpečnosti informácií v podniku sú:

1. **information security** - informačná bezpečnosť;
2. **steganographic and cryptographic security** - steganografická a kryptografická bezpečnosť;
3. **cyber security** - kybernetická bezpečnosť.

V nasledujúcej časti práce sa budeme zaoberať charakteristikou jednotlivých oblastí informačnej bezpečnosti.

1. **informačná bezpečnosť** rieši rôzne problémy spojené s bezpečnou prevádzkou počítačov v spoločnosti a tiež ich vhodným pripojením do telekomunikačných a počítačových sietí. Informačná bezpečnosť obsahuje dve zložky:
    a. **sieťová bezpečnosť** sa týka riešenia problémov spojených s komunikáciou pomocou rôznych telekomunikačných sietí a bezpečnostné prepojenie počítačov do týchto sietí, ako terminálov. Základnými komponentmi sieťovej bezpečnosti sú:

- úloha komunikačnej bezpečnosti je zabezpečiť ochranu prenášaných dát na určenej úrovni komunikačných protokolov;
- prístupová bezpečnosť má na starosti úlohy spojené s autentizáciou používateľov, resp. zamestnancov podniku, a tiež riadenie prístupu všetkým používateľom k rôznym systémovým prostriedkom a službám počítačovej a telekomunikačnej siete;
- systémová bezpečnosť rieši najmä otázky, týkajúce sa bezpečnostného oddelenia komunikačných sietí, a tiež sa zaoberá s bezpečnosťou vnútorného prostredia, resp. bezpečnosťou aplikácií a operačného systému v organizácii. Systémová bezpečnosť zahŕňa aj ochranu pred útokmi škodlivým softvérom, ako sú napríklad vírusy.

    b. **počítačová bezpečnosť** zahŕňa riešenie problémov týkajúcich bezpečnej prevádzky a tiež ochrany dát upravených počítačmi. Sem patrí autentizácia, dôvernosť a integrita dát.

[15] LOVEČEK, Tomáš. *Bezpečnosť informačných systémov.* Žilinská univerzita. 2007. 142 s. ISBN 978- 80-8070-767-5

2. **Steganografia** je odbor vedy, ktorý využíva rôzne metódy utajenia komunikácie tak, že v pozadí neutajenej komunikácie prebieha utajený prenos informácie. Je to vlastne špeciálna technika na ukrytie informácií v správe. Podľa použitých techník poznáme:

– technickú steganografiu, ktorá využíva technické metódy na utajenie tajnej informácie (napríklad ukrytie prenosového média);
– a lingvistickú steganografiu, ktorá má za cieľ ukryť tajnú informáciu textom, resp. inou grafickou podobou, ako napríklad notovým zápisom. Utajená komunikácia (secret communication) sa realizuje v pozadí neutajenej komunikácie, samozrejme v elektronickej forme. Prenos tajnej správy prebieha v tzv. podprahových kanáloch, ktoré môže podnik vytvoriť už v existujúcich komunikačných sieťach prostredníctvom metódami modernej steganografie.

Spomínané systémy by mali zabezpečiť hlavne:

– capacity – dostatočnú kapacitu podprahového kanálu;
– security – bezpečnosť utajenej správy;
– undetectability – nedetekovateľnosť utajenej informácie;
– invisibility – percepčná transparentnosť, nevnímateľnosť.

Kryptografická bezpečnosť zabezpečí utajenie správy rôznymi metódami šifrovania, čiže nemá za cieľ utajiť komunikáciu. Znie potom otázka, čo je **šifrovanie**?

Šifrovanie (Encryption) je určitý proces modifikácie danej správy pred odoslaním, aby jej obsah bola utajená. Zo správy, ktorá je zašifrovaná ani po jej zachytení neoprávnenou osobou by sa nemal dosiahnuť náplň vyslanej správy.

Metódu šifrovania označujeme ako tzv. **šifrovací algoritmus**, alebo **šifra**. Okrem algoritmu, šifrovanie vyžaduje ešte dodatočnú, zvyčajne tajnú správu, ktorú poznáme ako **key – kľúč.** Základným predpokladom kryptografie je tvrdenie, že bezpečnosť šifrovania môžeme zabezpečiť iba pomocou utajenia kľúča a nie utajením šifrovacieho algoritmu. Práve preto označujeme tento kľúč ako secret key – **tajný kľúč**.

Podľa historického vývoja kryptografie sa delí na klasickú a modernú kryptografiu.[16]

Klasická kryptografia využíva klasické postupy, ako **substitúcia**, pri ktorej sa vymení každý symbol iným symbolom, ale má rovnaké miesto ako pôvodný symbol.

[16] LEVICKÝ, Dušan. *Úvod do kybernetickej bezpečnosti.* Prvé vydanie. elfa, s.r.o., Park Komenského 7, 040 01 Košice, 2019. 6-7 s. ISBN 978-80-8086-276-3

Výber jednotlivých symbolov na výmenu určí kľúč. Medzi metódy klasickej kryptografie patrí aj **transpozícia**, prostredníctvom ktorej usporiadame všetky symboly nezašifrovanej správy a jednoducho vzniká zašifrovaná správa.

Moderná kryptografia úzko súvisí s rozvojom novej formy komunikácie, to znamená že zachytenie správy počas elektronickej komunikácie v dnešnej dobe je jednoducho realizovateľná. Modernú kryptografiu môžeme rozdeliť podľa použitých kľúčov na:

- secret key cryptography - kryptografiu s tajným kľúčom;
- public key cryptography - kryptografiu s verejným kľúčom.

Kryptografia s tajným kľúčom používa ten istý kľúč na šifrovanie a na dešifrovanie, ktorý je nutné utajiť. Práve preto nazývame kryptografiu s tajným kľúčom ako symetrickú kryptografiu. Komplikácie spojené s kryptografiou s tajným kľúčom vznikajú pri bezpečnej výmene tajných kľúčov, hoci aj pri veľkom počte účastníkov sú tam určené obmedzenia, kde používajú obrovský počet tajných kľúčov.

O kryptografii s verejným kľúčom hovoríme vtedy, ak výmena tajných kľúčov vyrieši algoritmus cez verejne dostupný prenosový kanál. Je to nový pohľad na bezpečnú výmenu tajných kľúčov ale taktiež zabezpečí aj bezpečnú komunikáciu s využitím kryptografie. Kryptografia s verejným kľúčom rozlišuje dva kľúče:

- private key - súkromný kľúč;
- public key - verejný kľúč.

Tieto kľúče sa navzájom podmieňujú, vytvárajú spojenie niekoľko kľúčov, preto označujeme kryptografiu s verejným kľúčom ako asymetrická kryptografia .

3. pojem **kybernetická bezpečnosť** vznikol z dôvodu, že v dnešnej dobe informácie sú spracované väčšinou v elektronickej forme, tým pádom sú spracované rýchlejšie a vo väčších objemoch. Kybernetická bezpečnosť je zložitejší pojem, ktorý zahŕňa nasledujúce časti:

- kybernetický priestor;
- kybernetické ohrozenia a riziká;
- kybernetická kriminalita;
- legislatíva v kybernetickej bezpečnosti;
- kryptografické systémy.

Hlavnou úlohou kybernetiky je prenos informácií a vedenie rôznych dynamických systémov [17]

1.3 Bezpečnostná politika – Security Policy

Bezpečnostné hrozby sa neustále vyvíjajú a požiadavky na dodržiavanie predpisov sú stále zložitejšie. Organizácie sú nútené vytvoriť komplexný bezpečnostný program, ktorý pokryje obe trendy. Bez bezpečnostnej politiky nie je možné koordinovať a presadzovať bezpečnostný program v rámci organizácie, ani nie je možné oznamovať bezpečnostné opatrenia tretím stranám a externým audítorom.[18]

Bezpečnostná politika je primárnym východiskom riadenia bezpečnosti informačných systémov spoločnosti. Vymedzuje základné bezpečnostné ciele, určí bezpečnostné princípy a obmedzenia. Definuje pravidlá a postupy, ktoré určujú metódy ochrany a distribúcie dôležitých informácií a význam informačného systému. Primárnym cieľom bezpečnostnej politiky je obmedziť vplyv vyskytujúcich sa rizík.

Bezpečnostnú politiku vypracuje poverený tím odborníkov, zapojením všetkých organizačných štruktúr v podniku. Veľkosť informačného systému a význam jeho funkcionality má značný vplyv na veľkosť a štruktúru skupiny odborníkov. Bezpečnostnú politiku triedime podľa oblastí:

a) **Bezpečnostná politika štátu** – je najvýznamnejšou časťou celej bezpečnostnej štruktúry. Sem patria zákony, predpisy, nariadenia vlády, smernice a rôzne dokumenty s celoštátnou platnosťou. Tvoria ju Trestný zákon, Zákon o ochrane osobných údajov a Zákon o informačných systémoch verejnej správy.
b) **Podniková (rezortná) bezpečnostná politika –** táto politika vychádza predovšetkým zo štátnych normatívov, ale podniky a rezorty majú zvyčajne svoje typické požiadavky na zaistenie informačných systémov, preto majú detailne určiť svoje požiadavky a princípy upevňovania bezpečnosti.
c) **Systémová bezpečnostná politika –** v hierarchii je na najnižšom a pritom najpodrobnejšie vypracovanom stupni bezpečnostnej štruktúry. Pri väčších informačných systémoch systémová bezpečnostná politika je založená na dvoch

[17] LEVICKÝ, Dušan. *Úvod do kybernetickej bezpečnosti.* Prvé vydanie. elfa, s.r.o., Park Komenského 7, 040 01 Košice, 2019. 11 s. ISBN 978-80-8086-276-3
[18] CASSETTO, Orion. *The 8 Elements of an Information Security Policy*. 2019. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.exabeam.com/information-security/information-security-policy/

krokoch. Najprv sa vypracúva tzv. Globálna systémová bezpečnostná politika, ktorú v druhom kroku podrobnejšie rozpracuje a definuje do tzv. Detailnej systémovej bezpečnostnej politiky.

Zadefinované postupy a pravidlá v bezpečnostnej politike musia byť stále testované a odborníci majú ich aktualizovať podľa zistených zmien a vývoja informačného systému.[19]

1.3.1 Systémová bezpečnostná politika

V tejto časti práce podrobnejšie budeme analyzovať systémovú bezpečnostnú politiku informačných technológií a systémov. Systémovú bezpečnostnú politiku najčastejšie vypracovávajú pre časový interval dvoch až päť rokov. Stanoví pre spoločnosť súbor pravidiel a rôznych princípov s účelom ochrany informačných systémov. Okrem toho stanoví aj konkrétne administratívne, technické, logické a procedurálne opatrenia súvisiace s konkrétnou informačnou technológiou. Čiastočne sa zaoberá s voľbou personálnych a fyzických bezpečnostných opatrení, nakoľko aj tieto môžu ovplyvniť bezpečnosť informačných systémov. Zaoberá sa aj s bezpečnosťou počítačových, resp. elektronických častí informačných systémov.

Systémová bezpečnostná politika skúma, ako chrániť aktíva spoločnosti, určí aj konkrétne ciele, čo sa týka bezpečnosti, identifikuje hrozby, ktoré sú zistené analýzou rizík. Stanovuje bezpečnostné opatrenia, ako autentizáciu, autorizáciu, riadenie prístupu, audit a pod. Všetko rieši v súvislosti implementovaných bezpečnostných opatrení.

Z celkovej bezpečnostnej politiky informačných technológií spoločnosti, systémová bezpečnostná politika preberá určenie triedy minimálnej sily rôznych bezpečnostných mechanizmov a medzitým stanovuje, akým spôsobom má spoločnosť implementovať bezpečnostné funkcie (elektronickými podpismi, šifrovaním, a pod.).

Musíme brať veľký ohľad na výšku investícií, určenú na zabezpečenie informačných systémov a na ostatné nákladové záťaže súvisiace so zabezpečovaním informačných systémov. Autori tejto bezpečnostnej politiky majú poznať riziká, hrozby a zraniteľné miesta vo firme. Realizátori bezpečnostnej politiky ovládajú dostupné bezpečnostné opatrenia, ich cenu a vytvárajú kladný vzťah s rôznymi vonkajšími

[19] KUČERA, Milan a kol. *Podnikové informačné systémy*. Prvé vydanie. Slovenská poľnohospodárska univerzita v Nitre, 2017. 149-150 s. ISBN 978-80-552-17239

dodávateľmi. V prípade, ak spoločnosť alebo jej informačný systém ja príliš rozsiahly, je odporúčané vypracovať samostatne systémovú bezpečnostnú politiku technickej ochrany (hardvér, softvér), systémovú bezpečnostnú politiku fyzickej ochrany, komunikačnú bezpečnostnú politiku. personálnu systémovú bezpečnostnú politiku, atď. [20]

Oblasti systémovej bezpečnostnej politiky:

a. **Fyzická systémová bezpečnostná politika;**
   Táto politika sa týka ochrany fyzických aktív spoločnosti, resp. budôv, počítačov, strojov, médií, prevencie prírodných útokov, prevencie krádeží a pod.
b. **Personálna systémová bezpečnostná politika;**
   Jej úlohou je pokrytie hrozieb predstavovaných zamestnancami, zákazníkmi, dodávateľmi, špiónmi, hackermi a ochrana vlastných zamestnancov spoločnosti.
c. **Technická systémová bezpečnostná politika;**
   Týka sa konkrétnych noriem, zákonov, pravidiel, použitých krokov pre spracovanie citlivých informácií , pre používanie hardvéru a softvéru v organizácii.
d. **Komunikačná systémová bezpečnostná politika;**
   Patrí sem ochrana poštovných zásielok, telefónov, mobilov, prenosu dát cez komunikačných programov, e-mailov a pod.
e. **Prevádzková systémová bezpečnostná politika;**
   Zaoberá sa s programom školení a zvyšovaní vedomostí o možných útokoch, postupmi pri uplatňovaní preventívnych bezpečnostných opatrení. Venuje sa aj havarijným plánom a vypracovaniu metód prevencie a detekcie.

Hlavná štruktúra dokumentu je základom systémovej bezpečnostnej politiky a generickým materiálom na jej implementáciu do ochranného, resp. bezpečnostného programu, ktorý má nasledujúcu koncepciu:

- analýza existujúceho informačného systému rešpektujúca použité informačné technológie;
- stanovenia výsledkov analýzy rizík informačného systému;
- určenia výsledkov analýzy zraniteľných miest informačného systému;

[20] *Systémová bezpečnostná politika IT.* 2014. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.zones.sk/studentske-prace/informatika/9009-systemova-bezpecnostna-politika-it/

- vypracovanie popisu hrozieb pre informačný systém.

Dôležitou súčasťou systémového bezpečnostného programu je osnova školenia pre celý tím informačnej technológie spoločnosti, kam patria vývojári informačných systémov, bezpečnostní manažéri, prevádzkoví zamestnanci, pracovníci, zodpovední za autorizáciu ostatných zamestnancov, koncoví užívatelia, atď. Definujú sa prevádzkové procedúry a tiež podmienky akreditácie systémového bezpečnostného programu. [21]

Metodika procesu vytvárania bezpečnostných politík

Tím odborníkov pri vypracovaní systémovej bezpečnostnej politiky preferoval nasledujúce okruhy:

- princípy udržania fyzickej bezpečnosti;
- nariadenia, zákony a vyhlášky súvisiace s predmetom činnosti spoločnosti;
- bezpečnostné personálne obsadenie spoločnosti;
- zásady etiky manipulácie s rôznymi informáciami;
- zásady a princípy triedenia dôvernosti dát;
- spôsoby zabezpečenia integrity a dôvernosti pri prenose dát v spoločnosti;
- riadiace mechanizmy prístupu správcov a užívateľov informačného systému spoločnosti;
- metódy zainteresovania pracovníkov spoločnosti na bezpečnosti informačného systému;
- identifikácia hrozieb a im zodpovedajúce riziká v cieľovej oblasti;
- spôsoby určenia a ohodnocovania aktív organizácie a metódy analýzy rizík;
- formy rizikových správ – metódy určovania nepredvídateľných udalostí spôsobiacich škody v podnikových aktívach a definovanie vhodných bezpečnostných opatrení;
- metódy hodnotenia bezpečnosti v organizácií, práce a kontrolingu v spoločnosti;
- zásady tvorby havarijných plánov.[22]

[21] *Systémová bezpečnostná politika IT.* 2014. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.zones.sk/studentske-prace/informatika/9009-systemova-bezpecnostna-politika-it/

[22] "VIX" NORIS, Ivan. *Bezpečnosť servera v sieti*, 2002-2007 [online]. [cit. 02-02-2020] Dostupné na internete: http://deja-vix.sk/sysadmin/security.html#top

Životný cyklus bezpečnostnej politiky sa vyznačuje s nasledujúcimi opakovane realizovanými krokmi:

- klasifikovanie vstupných vplyvov;
- analýza možných rizík;
- vypracovávanie bezpečnostnej politiky;
- realizácia bezpečnostnej politiky;
- umiestnenie bezpečnostnej politiky, kontrolná činnosť a formulácia záverov a výstupov.

Samotný proces tvorby systémovej bezpečnostnej politiky nie je jednorázový, lebo sa môžu meniť chránené aktíva spoločnosti, menia sa informačné technológie a menia sa skúsenosti a motivačné faktory útočníkov, atď. [23]

1.4 Najčastejšie útoky v podnikoch

Podrobná analýza a poznanie rôznych útokov je základným predpokladom vytvorenia efektívnych protiopatrení. Môžeme skonštatovať, že väčšina útokov súvisí s internetom, hlavne používaním komunikačných technológií.

- **Sniffing** – odpočúvanie je taký typ útoku, kde cieľom je odcudzenie informácií prostredníctvom počítačovej siete, ako odcudzenie prístupového mena alebo hesla, PIN - osobného identifikačného čísla.
- Metóda **trojské kone** je útok na zisťovanie autentifikačných informácií, t.j. je to program so skrytou funkciou, ktorá umožňuje získanie identifikačných údajov používateľa (PIN - osobné identifikačné číslo, prístupové meno a heslo).
- Ďalším spôsobom zisťovanie hesla je **útok hrubou silou**, kedy útočník pomocou špeciálneho programu zadáva všetky možné kombinácie znakov. Podobná možnosť je **slovníkový útok,** pri ktorom útočník generuje slová zo slovníka.
- O **sociálnom inžinierstve** hovoríme vtedy, ak útočník využíva rôzne informácie o používateľovi – jeho meno, dátum narodenia, prezývku, atď. Sem patrí aj prípad, keď útočník vstúpi do interakcie s používateľom, telefonicky alebo elektronickou poštou, resp. mailom a predstaví sa ako administrátor, ktorý si vyzvedá autentifikačné údaje od používateľa.

[23] *Systémová bezpečnostná politika IT*. 2014. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.zones.sk/studentske-prace/informatika/9009-systemova-bezpecnostna-politika-it/

- **Phishing** sa začína podvodným e-mailom alebo inou komunikáciou, ktorá je určená na prilákanie obete. Správa je navrhnutá tak, aby vyzerala akoby bola od dôveryhodného odosielateľa. Útočníci sú niekedy spokojní so získaním informácií o kreditnej karte obete alebo iných osobných údajov za účelom finančného zisku. Inokedy sa odosielajú e-maily na neoprávnené získavanie údajov, aby sa získali prihlasovacie informácie zamestnancov alebo iné podrobnosti, ktoré sa môžu použiť pri pokročilom útoku na konkrétnu spoločnosť.
- **Pharming** - podobne ako phishing, posiela používateľov na podvodnú webovú stránku, ktorá sa zdá oficiálna . V tomto prípade však obete nemusia kliknúť na škodlivý odkaz, ktorý sa má presunúť na falošnú stránku. Útočníci môžu infikovať jednak počítač používateľa ale aj server DNS - Domain Name System (Systém doménových mien) webových stránok a presmerovať používateľa na falošný web, aj keď je zadaná správna adresa URL - Uniform Resource Locators (Jednotný vyhľadávač prostriedku).

Za hrozbu môžeme považovať aj **spam** – nevyžiadanú elektronickú poštu, ktorá obmedzuje pozornosť používateľa a tiež kapacitu schránky. Sem patria aj poplašné správy – **hoaxy**, ktoré šíria neexistujúce hrozby a riziká. [24]

Okrem najčastejších útokov poznáme aj mnoho ďalších, ktoré vznikli priebežne s rozvojom informačných technológií.

Spear phishing je vlastne e-mail, zameraný na konkrétneho jednotlivca alebo organizáciu, ktorý si vyžaduje neoprávnený prístup k dôležitým informáciám. Tieto útoky nevykonávajú náhodní útočníci, ale s najväčšou pravdepodobnosťou ich robia jednotlivci kvôli obchodným tajomstvám, finančnému zisku alebo vojenskej spravodajskej službe.

Tieto činnosti najčastejšie vykonávajú hackeri. Počítačoví zločinci tiež vykonávajú tieto útoky s cieľom ďalšieho predaja dôverných údajov súkromným spoločnostiam. Tieto útočníci využívajú na sociálne inžinierstvo a individuálne navrhnuté prístupy na efektívne prispôsobenie webových stránok a správ.

Whale phishing, alebo útok na veľryby je druh phishingu, ktorý sa zameriava na vedúce osobnosti v spoločnosti, ako je finančný riaditeľ alebo generálny riaditeľ.

[24] *What Is Phishing?* 2018. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attack

Zameriava sa na odcudzenie dôležitých informácií, lebo osobnosti vyšších pozícií v spoločnosti majú neobmedzený prístup k citlivým informáciám. Väčšina veľrybárskych prípadov manipuluje s obeťou tak, že umožní útočníkovi prevod vysokej hodnoty. Výraz lov veľrýb označuje veľkosť útoku a veľryby sa zameriavajú na osobnosti vyšších pozícií v organizácii .Nakoľko tieto osoby stoja pod väčšou ochranou, pozorovanie lovu veľrýb je v porovnaní so štandardnými útokmi phishingu náročnejšie.

Správcovia zabezpečenia systému môžu znížiť účinnosť takého útoku tým, že navrhujú riadiacim pracovníkom, zúčastniť sa na školeniach o bezpečnostnom povedomí.

Ransomware blokuje prístup k údajom obete a zvyčajne hrozí, že ich vymaže, ak nebude hradiť výkupné . Neexistuje však žiadna záruka, že zaplatenie výkupného obnoví prístup k údajom. Ransomware sa často vykonáva prostredníctvom trójskeho koňa, ktorý dodáva užitočné zaťaženie, a je maskované ako legitímny súbor.

Útok Drive-by je bežný spôsob distribúcie škodlivého softvéru. Kybernetický útočník vyhľadáva nezabezpečenú webovú stránku a na jednej zo stránok umiestňuje škodlivý skript. Tento skript môže nainštalovať škodlivý softvér do vášho počítača, ktorý navštívi túto webovú stránku, alebo sa stane IFRAME (vložený rámec), ktorý presmeruje prehliadač obete na stránku kontrolovanú útočníkom. Tieto útoky sú známe ako jazda autom, pretože nevyžadujú zásah zo strany obete, s výnimkou návštevy kompromitovanej webovej stránky. Keď navštívia napadnutú stránku, automaticky sa infikujú, ak je ich počítač citlivý na škodlivý softvér, najmä ak nepoužili aktualizácie zabezpečenia svojich aplikácií.[25]

Webové útoky

SQL Injection, alebo Injekcia SQL, je druh útoku, ktorý využíva škodlivý kód na manipuláciu so zálohovanými databázami na prístup k informáciám, ktoré nie sú určené na zobrazenie. Zahŕňa to množstvo položiek vrátane súkromných údajov o zákazníkoch, zoznamov používateľov alebo citlivých firemných údajov.

SQL môže mať devastujúce účinky na podnikanie. Úspešný útok SQL môže spôsobiť vymazanie celých tabuliek, neoprávnené prezeranie zoznamov používateľov a v niektorých prípadoch môže útočník získať administratívny prístup k databáze. Pri výpočte

[25] DOBRAN, Bojana. *17 Types of Cyber Attacks To Secure Your Company From in 2020.* 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://phoenixnap.com/blog/cyber-security-attack-types

pravdepodobných nákladov na SQL musí brať do úvahy stratu dôvery zákazníkov v prípade odcudzenia osobných údajov, ako sú adresy, podrobnosti o kreditných kartách a telefónne čísla.

XSS, skriptovanie viacerých stránok je druh porušenia injekcií, pri ktorom útočník odosiela škodlivé skripty do obsahu z dôveryhodných webových stránok. Môže to ovplyvniť webovú stránku a aj používateľov tejto stránky. To znamená, že ak dôjde k útoku XSS na webovú stránku, kód sa automaticky spustí v používateľoch danej stránky pomocou prehliadača. Útoky XSS môžu byť veľmi nebezpečné, ale zmiernenie zraniteľností, je relatívne jednoduché.

Iné typy hrozieb kybernetickej bezpečnosti

Distributed Denial-of-Service (DDoS), alebo Distribuovaný útok má cieľ vypnúť sieť alebo obmedziť službu, a stáva sa neprístupným pre jej používateľov. Útok DDoS odmieta legitímnych používateľov, zamestnancov, majiteľov účtov. Útoky DDoS sa často zameriavajú na webové servery významných organizácií, ako sú obchodné organizácie a vláda, mediálne spoločnosti a bankovníctvo. Aj keď tieto útoky nemajú za následok stratu alebo krádež životne dôležitých informácií alebo iných aktív, ich zmiernenie môže stáť veľa peňazí a času.

Password Attack, v slovenskom preklade, útok heslom, jednoducho znamená pokus o dešifrovanie alebo získanie hesla používateľa s nezákonnými úmyslami. Existuje len niekoľko obranných mechanizmov proti útokom pomocou hesla, ale obyčajne je napravením heslovej politiky, ktorá obsahuje minimálnu dĺžku, časté zmeny a nerozpoznateľné slová.

Útoky na heslá sa často vykonávajú obnovením uložených alebo exportovaných hesiel prostredníctvom počítačového systému. Obnova hesla sa zvyčajne vykonáva nepretržitým skúšaním hesla pomocou počítačového algoritmu. Počítač sa pokúša o niekoľko kombinácií, kým úspešne nezistí heslo.

Brute-Force a Dictionary Network Attacks

Útoky proti slovníkom a hrubou silou sú sieťové útoky, pri ktorých sa útočník pokúša prihlásiť do užívateľského účtu systematickou kontrolou a skúšaním všetkých možných hesiel, kým nenájde správne heslo.

Pojem hrubá sila znamená premáhanie systému opakovaním. Pri hackovaní hesiel si vyžaduje hrubá sila slovníkový softvér, ktorý kombinuje slová s tisíckami rôznych variácií. Útoky slovníkov hrubou silou môžu vykonať 100 až 1000 pokusov za minútu. Po niekoľkých hodinách alebo dňoch môžu útoky hrubou silou nakoniec prelomiť akékoľvek heslo. Útoky hrubou silou opakujú dôležitosť osvedčených postupov týkajúcich sa hesla, najmä v prípade kritických zdrojov, ako sú sieťové prepínače, smerovače a servery.

Insider Threats, vo voľnom preklade vnútorné útoky, sú škodlivé útoky vykonávané v počítačovom systéme alebo sieti jednotlivcom oprávneným na prístup do systému. Osoby, ktoré vykonávajú tieto útoky, majú výhodu pred externými útočníkmi, pretože majú autorizovaný prístup do systému. Môžu používať aj systémové pravidlá a sieťovú architektúru.

Hrozby vnútorných osôb môžu ovplyvniť všetky prvky počítačovej bezpečnosti a môžu sa pohybovať od vstrekovania vírusov trójskych koní po krádež citlivých údajov zo siete alebo systému. Útočníci môžu tiež ovplyvniť dostupnosť systému preťažením kapacity spracovania počítača alebo úložného priestoru počítača spôsobeného zlyhaním systému.

Útoky Man-in-the-Middle - MITM Attacks

Tieto útoky sú typom narušenia kybernetickej bezpečnosti, ktoré umožňujú útočníkovi odpočúvať komunikáciu medzi dvoma stranami. K útoku dochádza medzi dvoma legitímnymi komunikujúcimi stranami, čo útočníkovi umožňuje zachytiť komunikáciu, ku ktorej by inak nemal prístup, odtiaľ pochádza názov „muž-uprostred“. Útočník „počúva“ konverzáciu zastavením prenosu správy s verejným kľúčom a opakovaným vysielaním správy, pričom si požadovaný kľúč vymieňa za vlastný.

Obidve strany komunikujú obvyklým spôsobom bez toho, aby vedeli, že odosielateľ správy je neznámy páchateľ, ktorý sa pokúša správu upraviť a získať prístup skôr, ako sa prenesie do prijímača.

Artificial Intelligence (AI) - Powered Attacks (Útoky poháňané umelou inteligenciou)

Koncept počítačového programu, ktorý sa sám učí, buduje vedomosti, môže byť strašidelný. Už sa však používa v každodenných aplikáciách prostredníctvom algoritmického procesu nazývaného strojové učenie. Softvér strojového učenia je

zameraný na školenie počítača na vykonávanie konkrétnych úloh samostatne. Naučia sa plniť úlohy tým, že ich opakovane robia, zatiaľ čo sa učia o určitých prekážkach, ktoré im môžu brániť.

AI sa dá použiť na prienik do mnohých systémov vrátane autonómnych vozidiel a robotov a ich premeny na potenciálne zbrane. AI robí počítačové útoky, ako je krádež identity, prelomenie hesla a útoky odmietnutia služby. Môže sa tiež použiť na zabíjanie alebo zranenie ľudí, odcudzenie finančných prostriedkov alebo spôsobenie emočných ujmov. Väčšie útoky sa môžu tiež použiť na ovplyvnenie národnej bezpečnosti, zatvorenie nemocníc a prerušenie dodávok energie do celých regiónov.[26]

1.4.1 Malware – škodlivý softvér

V súvislosti s informačnými hrozbami musíme pripomenúť aj škodlivý softvér, v anglickej podobe malware. Zaraďujeme sem trójske kone, počítačové vírusy, internetové červy a podobné.

- **Trójsky kôň** je špeciálny program so skrytou časťou, ktorá je pre používateľa neznáma, resp. nevie o tom. Vo väčšine prípadov je súčasťou jednoduchých voľne šírených programov, ako napríklad hry alebo šetrič obrazovky. Sú stiahnuté dobrovoľne, používateľ sám ich nainštaluje, ale ďalej sa potom nešíria ako vírusy.
- **Počítačový vírus** považujeme za najstaršiu formu škodlivého softvéru. V dnešnej dobe poznáme enormné množstvo vírusov, veľa z nich škodia práve napadnutým počítačom, iné druhy vírusov iba využívajú napadnutý počítač na útok k ostatným počítačom.
- **Internetové červy** sú také formy vírusov, ktoré ani nepotrebujú hostiteľský program na šírenie. Poznáme sieťové červy, ktoré sa šíria prostredníctvom chýb v serveroch, ale sú aj e-mailové červy, ktoré využívajú na šírenie kontaktov samotného používateľa. Škodlivý softvér sa šíri prostredníctvom internetu, hlavne cez e-mailu a webových stránok.

[26] DOBRAN, Bojana. *17 Types of Cyber Attacks To Secure Your Company From in 2020*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://phoenixnap.com/blog/cyber-security-attack-types

1.4.2 Charakteristika a typy vírusov

Počítačový vírus je taký špeciálny program, ktorý okrem svojej ničivej činnosti je ešte schopný spôsobiť aj ďalšie nepríjemnosti v počítačovej sieti. Podobne ako biologické vírusy, aj počítačový vírus môže vytvárať svoje kópie po usadení v pamäti počítača a lokalizovať sa do existujúcich dokumentov a programov tak, aby jeho činnosť zostala skrytá a aby sa mohol ďalej šíriť.

Vírusy môžeme triediť podľa viacerých hľadísk, podľa napadnutých dátových objektov poznáme nasledujúce typy vírusov:

- **Bootovacie vírusy –** vyskytujú sa iba málokedy, ale sú veľmi zákerné vírusy. Napadajú tzv. bootovacie, resp. zavádzacie sektory diskov. V týchto sektoroch sú uložené významné informácie o parametroch diskov a keďže operačný systém počítača získava údaje z tohto sektora po svojom štarte, pri tomto kroku sa aktivuje vírus.
- **Programové vírusy –** umiestňujú svoj kód do ostatných programov a v momente spustenia programu sa aktivujú.
- **Makrovírusy –** počítačové vírusy napadajú vo forme makier rôzne dokumenty, a to hlavne dokumenty najviac používaných počítačových aplikácií, ako napríklad Microsoft Excel alebo Word.

Typické programové vírusy sa šíria iba kopírovaním nainfikovaného softvéru, takže hlavné princípy ochrany pred vírusmi by sme mohli definovať nasledovne: nemajú sa používať programy z neoverených zdrojov a ani nelegálne šírených programov.

Predchádzajúce princípy sú neúčinné pri makrovírusov, lebo makrovírusy sa prenášajú infikovanými dokumentmi a spoločné využívanie a vzájomná výmena dokumentov sú základným službám počítačových sietí. V najviac rizikových aplikáciách, akými sú napríklad Microsoft Excel, Word, je dostupná možnosť vypnúť automatické spúšťanie makier, alebo spustenie ich až po súhlase používateľa. Môžeme skonštatovať, že okrem venovania pozornosti pri spracovaní s externými dokumentmi, je odporúčané na makrovírusy použiť antivírusový softvér.

Najčastejšie možno rozpoznať výskyt vírusu v počítači podľa toho, že sa počítač začne správať inak ako obvykle. Môže sa vyskytnúť, že nemožno spustiť aplikácie, ktoré predtým fungovali bezproblémovo, alebo môže dôjsť aj k spomaleniu počítača.

Ak už predpokladáme, že náš počítač mohol byť napadnutý rôznym vírusom, odporúčané je, aby sme všetky spracované dokumenty uložili a ukončili všetky spustené aplikácie, až potom by sme mali použiť antivírusový program. Najdôležitejšie sú samozrejme preventívne opatrenia. Preventívne opatrenia spočívajú v opatrnom používaní aplikácií a dokumentov, ale v prvom rade v inštalácií vhodného antivírusového programu, v jeho regulárnej aktualizácii a v správnom nastavení.

Antivírusové programy

Antivírusové programy sú také softvérové nástroje, ktoré majú dve hlavné úlohy. Na jednej strane zabezpečia preventívnu ochranu počítača pred napadnutím vírusov, na druhej strane vyhľadajú a odstraňujú vírusy.

Niektoré antivírusové programy používajú „živú“ ochranu na automatické blokovanie spúšťania takýchto vírusov a škodlivého softvéru, a to dokonca aj pri zastavení návštevy webových stránok alebo otvárania e-mailov, ktoré môžu obsahovať vírusy. Iné nástroje, známe ako nástroje nápravy, ponúkajú iba funkciu skenovania a po odstránení škodlivého softvéru musia byť spustené.[27]

Antivírusové programy používajú dva metódy detekcie vírusov:

- **skenovanie** – ide o porovnávanie obsahu počítačových pamätí a diskov s databázou známych vírusov, ktorú vytvoril počítač;
- **heuristická analýza –** pri tejto analýze antivírusový program pozoruje aktivitu ostatných spustených programov a keď vníma pochybné operácie, oznámi používateľovi.

K najlepším svetovým antivírusovým programom zaraďujeme NOD32 spoločnosti Eset, ktorý patrí medzi najlepšie hodnotené programy podľa špecializovaného časopisu Virus Bulletin. [28]

[27] MARTINDALE, Jon. *What is antivirus softvare and how does it work?* 2018. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.digitaltrends.com/computing/what-is-antivirus-software/
[28] HUŽVÁR, Miroslav - LACO, Peter. *Informačné technológie v ekonomickej praxi.*1. vydanie. Bratislava: Wolters Kluver, 2014. 142-144 s. ISBN 978-80-8168-085-4

2. Cieľ práce, metodika práce a metódy skúmania

Cieľ práce

Teoretická časť diplomovej práce predstavuje pojmy súvisiace s ochranou informačných systémov v podnikaní, definuje hrozby a rôzne typy útokov vyskytujúcich sa v podnikoch v oblasti informačných systémov a určuje spôsoby na vyhnutie sa im. Diplomová práca týmto spôsobom zdôrazňuje podstatu ochrany informačných systémov.

Cieľom diplomovej práce je porovnať bezpečnostné opatrenia a ich následnú aplikáciu v oblasti bezpečnosti informačných systémov u podnikateľského subjektu a miestnej samosprávy v okrese Dunajská Streda. Vybrali sme a porovnávali merateľné a sledovateľné bezpečnostné opatrenia prijaté vo vyššie uvedenom podniku a v samospráve, s cieľom poukázať na ich fungovanie v praxi, ktoré sme realizovali formou hĺbkového rozhovoru. Vyššie uvedené bezpečnostné opatrenia sme vyberali z rôznych oblastí bezpečnosti, ako sieťová bezpečnosť, fyzická bezpečnosť, personálna bezpečnosť. Otázky boli formulované tak, aby sa týkali všetkých uvedených oblastí, s cieľom vytvoriť celkový obraz o uplatnených opatreniach v týchto inštitúciách.

Pre dosiahnutie hlavného cieľa boli stanovené nasledovné čiastkové ciele:

- predstavenie informačných systémov a ich druhy;
- definovanie základných útokov v oblasti informačných systémov, ktoré hrozia podniky, štátnu správu a miestne samosprávy;
- určenie protiopatrení pri vypracovaní bezpečnostnej politiky;
- oslovenie dvoch inštitúcií v odlišnej sfére v okrese Dunajská Streda;
- na základe pohovoru s kompetentnými osobami predstaviť používané informačné systémy a prijaté ochranné opatrenia podľa platných prepisov;
- spracovanie získaných údajov od organizácií a analýza výsledkov;
- vyhodnotenie výsledkov a vypracovanie záverečnej správy z prieskumu.

3. Metodika práce a metódy skúmania

Zdrojom diplomovej práce boli rôzne publikácie z odbornej literatúry, týkajúce sa danej témy. Okrem odbornej literatúry domácich a zahraničných odborníkov sme preštudovali aj špeciálne webové stránky s odborným obsahom spojené s informačným systémom a ochranou podnikových aktív. Vymenovali sme základné úkony, ktoré hrozia z rôznych strán všetkým podnikom.

Prvým partnerom získania praktických poznatkov a informácií bola firma z okresu Dunajská Streda, ktorá bola ochotná pomôcť s podmienkou, že ostane anonymná. Konkrétne s nami spolupracoval IT manažér spoločnosti, ktorý má na starosti aj zabezpečenie ochrany informačných systémov v podniku. Vysvetlil nám, aké oblasti spadajú do jeho pracovnej činnosti a zodpovednosti. Podarilo sa nám zrealizovať osobné stretnutie v spoločnosti, kde sme spoločne analyzovali jednotlivé spôsoby ochrany informačného systému a spracovaných dát v spoločnosti.

Druhým partnerom získania poznatkov pri písaní záverečnej práce bol správca informačného systému miestnej samosprávy, ktorý nám ochotne pomohol pri definovaní jednotlivých ochranných opatrení platných v miestnej samospráve.

Ako metódu skúmania sme realizovali osobné pohovory s kompetentnými osobami, podľa vopred určených otázok. Najprv sme definovali merateľné a sledovateľné bezpečnostné opatrenia, prijaté vo vyššie uvedenom podniku a v samospráve tak, aby sme mohli porovnať dve spoločnosti z pohľadu ochrany informačných systémov a dát, využívaných vo svojej oblasti. Zaujímavosťou je, že vybrané organizácie v okrese Dunajská Streda, sú úplne odlišné, lebo jedna firma je súkromný makropodnik vo výrobnej sfére a druhá inštitúcia je miestna samospráva s oveľa menším počtom zamestnancov.
Prieskum sa uskutočnil týmito krokmi:

1. Výber metód získavania údajov – interview, resp. pohovor;
2. Tvorba skúmaných ukazovateľov;
3. Testovanie skúmaných ukazovateľov;
4. Zhromažďovanie primárnych údajov prostredníctvom pohovoru;
5. Spracovanie údajov a ich analýza;
6. Vyhodnotenie výsledkov – interpretovanie;
7. Záverečná správa z prieskumu.

Praktickú časť našej diplomovej práce tvorí porovnávanie bezpečnostných opatrení týkajúcich sa informačných systémov v dvoch inštitúciách v okrese Dunajská Streda.

V prvom rade predstavujeme vybranú súkromnú spoločnosť, ktorá zostáva v maximálnej anonymite.

Ponúkané produkty a predmety činnosti danej spoločnosti sú nasledovné:

- výroba kovových skríň, schránok;
- výroba strojov a zariadení pre všeobecné účely;
- výroba jednoduchých výrobkov z dreva, ich úprava, oprava a údržba;
- kúpa tovaru na účely jeho predaja konečnému spotrebiteľovi (maloobchod) alebo iným prevádzkovateľom živnosti (veľkoobchod);
- sprostredkovateľská činnosť v oblasti obchodu, služieb a výroby;
- uskutočňovanie stavieb a ich zmien;
- prenájom nehnuteľností spojený s poskytovaním iných než základných služieb spojených s prenájmom;
- činnosť podnikateľských, organizačných a ekonomických poradcov;
- prenájom hnuteľných vecí.[29]

Spoločnosť ponúka kompletný rad zákazkových nábytkových riešení z rôznych materiálov vrátane dreva, kovu a skla. Či je už potrebné zariadiť banku, hotel, reštauráciu, obchod alebo akékoľvek iné zariadenie, spoločnosť ho vyrobí podľa konkrétnych požiadaviek.[30]

Druhou vybranou inštitúciou je miestna samospráva v okrese Dunajská Streda, ktorej úlohu by sme mohli charakterizovať nasledovne:

- Zabezpečenie všetkých činností v zmysle zákona SNR č. 369/1990 Zb Zákon o obecnom zriadení.

Pri vypracovaní otázok sme si zvážili podmienky, aby kladené otázky boli merateľné a sledovateľné. Kvôli zabezpečeniu prehľadnosti sme odpovede označili číslami. To znamená, že odpoveď č.1. označuje odpoveď súkromnej spoločnosti a odpoveď č. 2. označuje odpoveď samosprávy.

[29] Výpis z Obchodného registra Okresného súdu Trnava. 2020. [online]. [cit. 2020-02-02]. Dostupné na internete: http://www.orsr.sk/vypis.asp?ID=407548&SID=7&P=1

[30] Wertheim/home. [online]. [cit. 2020-02-02]. Dostupné na internete: /http://www.wertheim.at/home.html

4. Výsledky prieskumu

4.1 Interpretácia získaných informácií

4.1.1 Sieťová bezpečnosť

1. **Aké informačné systémy používate v spoločnosti? Na aké účely používate tieto systémy?**

Odpoveď č. 1. - súkromná spoločnosť:

Pri každodennej práci sú v našej spoločnosti použité rôzne podnikové systémy.. Najrozsiahlejším a najkomplikovanejším systémom v spoločnosti je SAP, ktorý používajú manažéri na vyššej úrovni. Firma získala podnikový systém SAP v roku 2001, to znamená, že spoločnosť používa systém už 19 rokov. Spoločnosť používa nasledujúcich sedem modulov:

- **Finančné účtovníctvo** - SAP Financial Accounting (FI)
- **Kontroling** - SAP Controlling (CO)
- **Skladové hospodárstvo a logistika** - SAP Materials Management (MM)
- **Podpora predaja** - SAP Sales and Distribution (SD)
- **Riadenie ľudského kapitálu** - SAP Human Capital Management (HCM)
- **Manažment kvality** - SAP Quality Management (QM)
- **Plánovanie výroby** - SAP Production Planning (PP)

Odpoveď č. 2. - samospráva:

- **Komplexné riešenie účtovníctva a personálnej agendy, správa vnútroištitucionálnych a klientských dát** - Informačný systém samosprávy CORA GEO (CG ISS) ;
- **Komplexné riešenie pre evidenciu a spracovanie korešpondencie a jej archivácie** – Dokumentačný informačný systém pre samosprávy CORA GEO (CG DISS);
- **Komplexné riešenie spravovania geografických informácií** - Geografický informačný portál samosprávy CORA GEO (CG WebGIS);
- **Komplexné riešenie pre eGOVERNMENT –** CORA GEO (CG eGOV);

- **Komplexné riešenie výstupov pre vedenie samosprávy -** Manažérsky informačný systém CORA GEO (CG MIS).[31]

2. **Aké operačné systémy sú používané vo Vašej firme/ vo Vašej samospráve?**

Odpoveď č. 1. - súkromná spoločnosť:

V súkromnej firme sú používané 2 operačné systémy:

- Linux – používaný na switch operácie – dátové rozvody, na wifi sieť;
- Windows – používaný na dátovom serveri.

Odpoveď č. 2. - samospráva:

V samospráve je používaný operačný systém Windows na všetkých úrovniach (správca systému, používatelia, server).

3. **Chránite Vašu lokálnu sieť pred vírusmi?**

Odpoveď č. 1. - súkromná spoločnosť:

Vybraná spoločnosť používa ANTIVÍRUS – ESET File Security pre Microsoft Windows Server na ochranu lokálnej siete pred vírusmi. Je zakúpený na jeden rok. Na serveroch sa používa ESET Endpoint Security – vo výrobe, kde majú iba vnútornú sieť. (nemajú ani internet)

Odpoveď č. 2. - samospráva:

Samospráva používa na všetkých úrovniach komplexné riešenie softvérového vybavenia ESET.

4. **Obmedzenie prístupu: kontrolujete prístup dovnútra siete? Používate firewall?**

Odpoveď č. 1. - súkromná spoločnosť:

Áno, používame firewall SOPHOS UTM 9.

Odpoveď č. 2.- samospráva:

[31] Odvetvia – Produkty určene pre samosprávu. [online]. [cit. 02-02-2020] Dostupné na internete: https://www.corageo.sk/odvetvia/

Áno, používame firewall KERBER.

5. **Ako pristupujú používatelia z internej siete k Internetu? Používate proxy server?**

Odpoveď č. 1. - súkromná spoločnosť:

Áno, spoločnosť používa proxy server, hlavne na kontrolu používania internetu zamestnancami na internete. Pre podnik nie je výhodné, keď zamestnanci sledujú rôzne webové stránky počas pracovnej doby, preto je proxy server nastavený tak, aby zakázal prístup na spomenuté stránky, zároveň presmeroval zamestnancov na podnikovú sieť. Spoločnosť používa proxy servery aj na súkromné prehliadanie internetu. Niektoré proxy servery zmenia IP adresu a ďalšie identifikačné informácie, ktoré webová požiadavka obsahuje. To znamená, že cieľový server nevie, kto skutočne predložil pôvodnú žiadosť, čo pomáha udržiavať osobné informácie spoločnosti a zvyky pri prehliadaní súkromnejšie.

Odpoveď č. 2. - samospráva:

Áno, samospráva používa proxy server, tento špeciálny typ servera - prostredníka v komunikácii, ktorý sa umiestňuje medzi klienta a servery, s ktorými komunikuje. Proxy server sa tvári voči klientovi ako server a voči serveru ako klient. Výhodou je, že proxy server pozná požiadavku klienta a vie mu doručiť odpoveď, aj keď klient samotný nemôže alebo nevie (kvôli obmedzeniam alebo parametrom siete) priamo komunikovať so vzdialeným serverom.

4.1.2 Fyzická bezpečnosť

6. **Je server pripojený na záložný zdroj, ako dlho vydrží?**

Odpoveď č. 1. - súkromná spoločnosť:

Áno, je v serverovni, záložný zdroj vydrží cca. 4 hodiny.

Odpoveď č. 2. - samospráva:

Áno, nachádza sa v serverovni, a vydrží cca. 15 minút.

7. **Mohli by ste charakterizovať fyzickú ochranu serverovní?**

Odpoveď č. 1. - súkromná spoločnosť:

V obidvoch serverovniach sú stanovené špeciálne bezpečnostné požiadavky, iba v týchto miestnostiach sú špeciálne halónové hasiace prístroje. Halónový hasiaci prístroj je jediný hasiaci prístroj, ktorý v prípade požiaru nezničí elektrické zariadenia. Okrem toho, tieto miestnosti majú stanovenú teplotu medzi 17-20 stupňov Celsia, z čoho vyplýva, že klimatizácia funguje stále. Steny sú z protipožiarnych sadrokartónov a v celej budove sú protipožiarne bezpečnostné dvere.

Odpoveď č. 2. - samospráva:

V serverovni je uložený špeciálne halónový hasiaci prístroj. V tejto miestnosti je teplota nastavená na 18 stupňov Celsia, čiže klimatizácia funguje nepretržite. Steny sú zo špeciálnych protipožiarnych sadrokartónov a v tejto miestnosti sú protipožiarne bezpečnostné dvere.

8. **Aké fyzické média sú použité na prenos a uchovanie údajov, pri akých podmienok je povolené ich užívať?**

Odpoveď č. 1. - súkromná organizácia:

Vo firme je dovolené používať firemné USB s cieľom uchovania a prenosu údajov, ktorý poskytuje a eviduje spoločnosť.

Odpoveď č. 2. - samospráva:

Na prenos a archiváciu dát je možné používať zamestnávateľom vydané a evidované prenosné média USB a HARDDISK (pevný disk), ktoré musia zostať výlučne v budove samosprávy.

4.1.3 Personálna bezpečnosť

9. **Sú zavedené nejaké obmedzenia na počet používateľských procesov?**

Odpoveď č. 1. - súkromná spoločnosť:

Áno, podľa pozície používateľov.

Odpoveď č. 2. - samospráva:
Áno, podľa pozície používateľov v súlade s nakúpenou licenciou softvérového vybavenia.

10. Je používateľ skutočne ten, za koho sa vydáva? (autentifikácia)

Odpoveď č. 1. - súkromná spoločnosť:

Vo vybranej firme je striktne kontrolovateľný administrátormi, ktorí okrem iných určia aj prihlasovacie mená.

Odpoveď č. 2. - samospráva:

V samospráve je kontrolovateľný správcom systému, ktorý určí aj prihlasovacie mená a prvé prihlasovacie heslá.

11. Aké práva má mať používateľ po prihlásení? (autorizácia)

Odpoveď č. 1. - súkromná spoločnosť:

Práva určia tiež administrátori, používateľ má po 42 dňoch vymeniť svoje heslo, ktoré má obsahovať minimálne 8 charakterov a okrem toho sú určené rôzne podmienky, ktoré má heslo spĺňať.

Odpoveď č. 2. - samospráva:

Práva určí správca systému, používateľa systém automaticky vyzve na zmenu hesla každých 90 dní, ktoré musí spĺňať PASSWORD POLICY samosprávny a ktoré nie je verejné.

12. Akí pracovníci majú fyzický prístup k serveru?

Odpoveď č. 1. - súkromná spoločnosť:

Fyzický prístup k serveru majú iba 4 administrátori, ktorí majú aj tzv. systémové kľúče, ktoré otvárajú kancelárie, odkiaľ majú prístup.

Jeden systémový kľúč je uložený na vrátnici, čo je nevyhnutné pre prípad požiaru.

Odpoveď č. 2. - samospráva:

Fyzický prístup k serveru má iba správca systému.

13. **Aké sú podmienky na heslo používateľa? Je nastavená maximálna doba platnosti hesla?**

Odpoveď č. 1. - súkromná spoločnosť:

Heslo musí obsahovať veľké písmená, niekoľko čísel, špeciálne charaktery, dĺžka hesla je min. 8 charakterov, vo firme 13.
Maximálna doba platnosti hesla je 42 dní, po uplynutí určitej doby generujú nové heslo, prostredníctvom on-line platformy - password generator.

Odpoveď č. 2. - samospráva:

Heslo musí byť vytvorené užívateľom v súlade s PASSWORD POLICY samosprávy, ktoré nie je verejné.
Maximálna doba platnosti hesla je 90 dní, po uplynutí vyššie uvedenej doby systém vyzve užívateľa na zmenu hesla.

4.2 Analýza výsledkov

V tejto časti záverečnej práce sme sa zamerali na spôsoby ochrany informačných systémov na praktickej úrovni. Výsledky prieskumu sme vypracovali tak, aby otázky aj odpovede boli jasné a pochopiteľné pre všetkých čitateľov. Častokrát sú použité odborné výrazy, ako napríklad firewall, malware alebo proxy server, ktoré sme sa snažili objasniť.

Okrem odborných výrazov, pri každej otázke sme vytvorili teoretický základ, aby skúmané hľadiská boli pochopiteľné pre čo najširší okruh čitateľov.

V prieskume sme položili trinásť otázok, cieľom ktorých je porovnávanie a vytváranie čo najkomplexnejšieho obrazu o používaných bezpečnostných opatreniach v oblasti informačných systémov vo vybraných organizáciách v okrese Dunajská Streda.

Zistené výsledky pre odborníkov a manažérov slúžia ako východisko na porovnávanie vlastných bezpečnostných opatrení, ktoré sa týkajú informačných systémov. Odpovede slúžia ako odporúčanie pre používateľov, ktorí sa pravidelne zaoberajú s informačnými technológiami na svojom pracovisku a poskytujú súhrnný obraz pre študentov, budúcich podnikateľov.

Aby sme splnili druhoradý cieľ práce a poukázali na dôležitosť ochrany týchto systémov, porovnávali sme získané odpovede s objasnením pojmov týkajúcich sa danej témy a vypracovali sme záver a zhrnutie výsledkov.

1. **Aké informačné systémy používate v spoločnosti? Na aké účely používate tieto systémy?**

Z odpovedí vyplýva, že rozličné odvetvia spoločnosti majú odlišné požiadavky na programové vybavenie, čo je spôsobené rôznorodosťou činností firiem, organizácií a inštitúcií pôsobiacich vo vyššie uvedených odvetviach. Môžeme skonštatovať, že softvérové firmy sú špecifikované na jednotlivé odvetvia spoločnosti.

Najprv by sme chceli stručne charakterizovať používané moduly podnikového systému SAP v súkromnom podniku a poukázať na jeho účely.

Finančné účtovníctvo (FI)

Modul SAP FI, sa zaoberá dohodami o riadení finančných transakcií v podnikoch. Tento modul finančného účtovníctva pomáha zamestnancom spracovať údaje obsiahnuté v

akýchkoľvek finančných a obchodných transakciách v zjednotenom systéme. Modul SAP FI je veľmi flexibilný a funguje dobre v akejkoľvek hospodárskej situácii, či už ide o menšiu alebo väčšiu organizáciu. Modul finančného účtovníctva pomáha človeku získať finančnú pozíciu podniku v reálnom čase na trhu. SAP FI sa spojí s ostatnými modulmi SAP, ako sú SAP SD, SAP MM, mzdy a ďalšie pre lepšie pracovné výsledky.

Kontroling (CO)

Modul SAP CO je ďalším dôležitým modulom SAP ponúkaným podnikom. Riadiaci modul podporuje procesné práce pri plánovaní, vykazovaní a monitorovaní operácií podnikov. Zahŕňa metódy na zobrazenie a usporiadanie nákladov, ktoré sú potrebné pre finančné vykazovanie. Tento modul umožňuje plánovanie, sledovanie, vykonávanie a vykazovanie nákladov. Kontroling zahŕňa správu a konfiguráciu kmeňových dát, ktoré pokrývajú nákladové prvky, nákladové strediská, ziskové strediská, interné objednávky a funkčnú oblasť atď.

Predaj a distribúcia (SD)

Modul SAP SD sa zaoberá správou všetkých transakcií, od dopytov, návrhov, cenových ponúk, cien a ďalších. Modul predaja a distribúcie veľmi pomáha pri kontrole a správe zásob. Modul SAP SD pozostáva z kmeňových dát, konfigurácie systému a transakcií. Niektoré z čiastkových komponentov modulu SAP SD sú kmeňové údaje, podpora predaja, predaj, preprava, fakturácia, správa úverov, informačný systém predaja atď.

Plánovanie výroby (PP)

SAP PP modul je ďalší dôležitý modul, ktorý obsahuje softvér navrhnutý špeciálne pre plánovanie a správu výroby. Tento modul tiež pozostáva z kmeňových dát, konfigurácie systému a transakcií, aby sa uskutočnil postup plánovania výroby. Modul SAP PP spolupracuje s plánovaním kmeňových dát, predaja a operácií, plánovaním distribučných zdrojov, materiálových požiadaviek, plánovaním nákladov na výrobky atď.

Skladové hospodárstvo a logistika (MM)

Modul SAP MM riadi materiály, ktoré sú potrebné, spracované a vyrobené v podnikoch. Týmto systémom sú riadené rôzne typy procesov obstarávania. Niektoré z

populárnych podzložiek v module SAP MM sú kmeňové dáta dodávateľa, plánovanie založené na spotrebe, nákup, správa zásob, overenie faktúry atď.

Manažment kvality (QM)

Modul SAP QM pomáha pri riadení kvality produkcie vo všetkých procesoch v organizácii. Tento modul riadenia kvality pomáha organizácii zrýchliť svoje podnikanie prijatím štruktúrovaného a funkčného spôsobu riadenia kvality v rôznych procesoch. Modul SAP QM spolupracuje pri obstarávaní a predaji, výrobe, plánovaní, kontrole, notifikácii, riadení auditu a tak ďalej.

Riadenie ľudského kapitálu (HCM)

Modul SAP HCM vylepšuje riadenie pracovných procesov a dát v rámci oddelenia ľudských zdrojov podnikov. Týmto modulom sa spracúva právo na najímanie osôb až po vyhodnotení výkonnosti, správa povýšení, kompenzácií, spracovanie miezd a ďalšie súvisiace činnosti HR. Úloha riadenia detailov a tok úloh najdôležitejšieho zdroja, t. j. ľudských zdrojov, sa riadi pomocou tohto modulu SAP ERP HCM.[32]

Ďalej by sme chceli charakterizovať aj systémy CORA GEO použité v samospráve. Prvým systémom je **Informačný systém samosprávy - CG ISS.**

Je to ekonomický podsystém, ktorý umožňuje vykonávať celkovú ekonomickú činnosť v nadväznosti na schválený rozpočet daného úradu. Je vynikajúcim podkladovým materiálom pre správne riadenie obce alebo mesta a rozhodovanie na vyšších úrovniach. Je tiež evidenčným podsystémom, ktorý zastrešuje obsiahlu evidenciu obyvateľstva, podnikateľov a inej súvisiacej agendy na úrade. CG ISS môžeme považovať za administratívny podsystém, spravuje dokumenty v súvislosti s uzneseniami, kanceláriou prvého kontaktu a zabezpečuje evidenciu písomnosti. Jeho obratnosti podporujú prepojenia na mnohé moduly, ktoré mu poskytujú potrebné údaje. CG ISS je aj geografickým podsystémom a efektívne spracováva vložené dáta o dostupných javoch na zemskom povrchu a pod ním.

[32] ESHNA, Verma. 2020 Understanding SAP Modules: SAP FI, SAP CO, SAP SD, SAP HCM and more. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.simplilearn.com/sap-modules-sap-fi-sap-co-sap-sd-sap-hcm-and-more-rar111-article

Dokumentačný informačný systém pre samosprávy je **CORA GEO (CG DISS),** ktorý zabezpečí príjem a odosielanie registratúrnej správy, centrálnu evidenciu, identifikáciu, ako aj prehľadné sledovanie pohybov, ukladanie. Systém CG DISS umožní sledovanie deadline termínov a aktuálneho umiestnenia dokumentu, evidovanie zapožičaných spisov, ako aj tlač vyraďovacích a odovzdávacích zoznamov.

Na riešenie spracovania geografických informácií samospráva používa - **Geografický informačný portál** samosprávy **CORA GEO (CG WebGIS)**, tento portál zabezpečí publikáciu informácií z vnútorného geografického informačného systému mesta alebo obce širokej verejnosti. Mesto alebo obec sa môže samostatne rozhodovať o tom, ktoré údaje a informácie chce publikovať občanom v dostupnom čase s ohľadom na menšiu prácnosť pri obnovovaní informácií v tejto aplikácií.

eGOVERNMENT – CORA GEO (CG eGOV) má za úlohu zabezpečiť efektívnu a bezpečnú komunikáciu s úradom. Má dve sekcie, verejnú a privátnú sekciu. Verejná sekcia je prístupná každému občanovi, sú v nej bežne dostupné údaje o obci či meste a zdrojom slúži vnútorný informačný systém samosprávy. Privátna sekcia je zabezpečená špeciálnym prístupovým menom a heslom, je prístupná iba konkrétnemu občanovi. Táto sekcia umožňuje tak občanom ako aj firmám komunikovať s úradom pomocou žiadostí a rôznych formulárov. Občan alebo firma môže priebežne získať informácie o daňových poplatkoch, vlastníckych alebo zmluvných vzťahoch, priestupkoch, atď.

Komplexné riešenie výstupov pre vedenie samosprávy zabezpečí **Manažérsky informačný systém CORA GEO (CG MIS).** V tomto systéme sa informácie nenapĺňajú, len vyhodnocujú a prezentujú existujúce informácie. Tento systém je určený pre strategické riadenie a plánovanie a kladie veľký dôraz na vizualizáciu.[33]

[33] Odvetvia – Produkty určene pre samosprávu. [online]. [cit. 02-02-2020] Dostupné na internete: https://www.corageo.sk/odvetvia/

2. Aké operačné systémy sú používané vo Vašej firme/ vo Vašej samospráve?

Z odpovedí v pohovore zúčastnených organizácií môžeme skonštatovať, že napriek tomu, že vyššie uvedené spoločnosti a inštitúcie spôsobujú v odlišnom sektore spoločnosti, používajú ten istý operačný systém a väčšie spoločnosti používajú kombináciu operačných systémov.

Operačný systém je taký výrobný program, ktorý má určitú kontrolu nad hardvérom v počítači a umožňuje aj inštaláciu ostatných programov, ktorý vďaka operačnému systému spolupracuje s týmto hardvérom a využíva jeho zdroje. Môžeme povedať, že operačný systém je tým najdôležitejším programom, lebo zabezpečuje využívanie grafickej karty, monitoru, prípadne aj tlačiarne, zároveň ukladanie rôznych súborov na disk a spracovanie spustených programov. V nových počítačoch už sú vopred nainštalované tieto operačné systémy, u nás sú väčšinou použité Windows alebo Linux, v Amerike je populárny systém OS X. [34]

Vo vybraných firmách využívajú dve použité operačné systémy – Windows a Linux, ktoré porovnáme:

Operačný systém Windows najčastejšie používajú úrady, rôzne inštitúcie, školstvo a samozrejme aj domácnosti. Windows môžeme považovať za najrozšírenejšiu platformu. Ľudia využívajú hlavne na hry alebo na kancelársku prácu. Aj Windows má svoje výhody a nevýhody.

Výhody:

- veľa ľudí dokáže ovládať operačný systém Windows, lebo sa stretával s ním pri nákupe nového počítača;
- skoro všetky softvéry sú kompatibilný so systémom Windows;
- existuje k tomu oficiálny kanál na podporu, rôzne diskusné fóra, ale aj platená podpora.

Nevýhody:

- Windows nie je komerčný softvér, užívatelia ho musia nakúpiť a následne musia platiť aj za rôzne programy, ktoré pracujú ne tejto platforme;

[34] Windows, OS X, či Linux? 2016. [online]. [cit. 02-02-2020] Dostupné na internete: https://www.speedex.sk/windows-os-x-ci-linux/

- je „veľký“ operačný systém, zaberá veľmi veľa miesta na pevnom disku;
- je najrozšírenejším operačným systémom, z toho vyplýva, že je napadnutý najviac malwaremi, vírusmi a obsahuje veľa bezpečnostných chýb.

Linux nie je operačný systém, je iba jadro, alebo „kernel“, ktorý umožňuje vývojárom vyrobiť si nejaký operačný systém, ako napríklad Android, Linux Mint.
Výhody:

- Linux je zadarmo, a väčšina programov sa distribuuje so zdrojovým kódom, čiže open source;
- Linux sa používa vo vysoko kritických nasadeniach, ako napríklad v jadrových elektrárňach;
- nie je potrebný žiadny antivírusový program, lebo takmer neobsahuje žiadne vírusy alebo malware;
- k Linuxu nie je potrebné žiadne externé ovládače, po inštalácii je plne funkčný, ovládanie sa veľmi podobá na ovládanie vo Windows.

Nevýhody:

- nové počítače dodávatelia najčastejšie ponúkajú s Windowsom;
- programy nie sú kompatibilné s operačnými systémami, treba ich najskôr portovať a kompilovať pre daný operačný systém;
- pokročilí používatelia sa majú naučiť pracovať s konzolou, t.j. príkazovým riadkom na podrobné vyladenie systému, bežní používatelia nepotrebujú túto vedomosť.[35]

3. Chránite Vašu lokálnu sieť pred vírusmi?

V dnešnej modernej dobe je samozrejmosťou, že nielen menšie ale aj väčšie firmy, a všetky inštitúcie používajú antivírusový program. Z odpovedí vyplýva, že obidve vybrané organizácie majú nainštalovaný ESET antivírusový program.

Najprv by sme chceli opísať, ako majú spoločnosti ochrániť počítače pred vírusmi.

- najdôležitejším krokom je, aby organizácie mali nainštalovaný antivírusový program; je to veľký omyl, že ak máme nainštalované viac antivírusov, znamená

[35] Windows, OS X, či Linux? 2016. [online]. [cit. 02-02-2020] Dostupné na internete: https://www.speedex.sk/windows-os-x-ci-linux/

väčšie bezpečie, naopak, viacnásobná inštalácia rozličných antivírusových programov môže spôsobiť komplikácie;

- všetkým inštitúciám je odporúčané pravidelne aktualizovať vírusovú databázu, buď ručne, alebo môžeme nastaviť aj automatickú aktualizáciu;
- nainštalovaný antivírus musí byť vždy zapnutý, lebo len tak chráni naše počítače;
- odporúčané je občas spustiť skenovanie úložiska počítača, lebo celková kontrola diskov môže odhaliť nebezpečenstvá;
- organizácie s antivírusom by mali používať aj firewall, ktorý chráni počítač pri práci na internete.[36]

Internetová stránka necenzurovane.sk vypracovala recenziu z výsledkov cudzích odborných testov, ktoré posudzujú kvality antivírusov podľa rôznych hľadísk s cieľom určiť, ktorý je najpoužívanejším a najlepším antivírusovým programom v roku 2020. Odborníci porovnávali top antivírusov momentálne nachádzajúcich na trhu: Norton, Kaspersky, ESET, BitDefender, AVG a AVAST.

Z testov antivírusov vyšiel výsledok, že ESET je najlepším antivírusovým programom v roku 2020. Zaujímavý je, že ESET je slovenská spoločnosť založená v roku 1992. Pobočky ESET nájdeme vo viac ako 200 krajinách sveta. Viackrát získala firma ocenenie najlepšej slovenskej firmy. Veľkou výhodou je, že ESET ponúka programy nielen pre domáce využitie ale aj pre použitie v rôznych inštitúciách. Ďalšou výhodou antivírusu ESET je pomerne nízke zaťaženie počítača a zároveň dobre funguje aj na starších počítačoch. V neposlednom rade používateľské prostredie je v slovenskom jazyku. ESET pravidelne vykonáva rýchlu automatickú aktualizáciu vírusovej databázy.[37]

Jedinou nevýhodou antivírusového programu ESET je jeho cena, totiž existujú antivírusové programy, ktoré možno nainštalovať zadarmo alebo lacnejšie ako tento program. Musíme si uvedomiť, že z pohľadu organizácií antivírusový program je základným predpokladom čo sa týka bezpečnostných opatrení informačných technológií. Súkromné podniky a aj ostatné organizácie si majú zvážiť, či zaplatia za spoľahlivú ochranu, alebo riskujú s menej spoľahlivým programom, ktoré nainštalujú zadarmo.

[36] *Najlepšie antivírusy 2020: Porovnanie 13 bezplatných a platených antivírusov*. 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.kodino.com/sk/clanky/najlepsie-antivirusy/

[37] *TOP antivírusy roku 2020*. 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://necenzurovane.sk/antivirusy/#uvod

ESET antivírusový program môžeme považovať za dobrú voľbu pre obidve vybrané inštitúcie.

4. Obmedzenie prístupu: kontrolujete prístup dovnútra siete? Používate firewall?

V záujme zabezpečenia informačného systému obidve oslovené organizácie odpovedali, že majú nainštalovaný firewall vo svojom pracovisku. Z odpovedí vyplýva, že obidve opýtané spoločnosti používajú iný firewall.

Brána firewall je bariéra alebo štít, ktorý zabraňuje neoprávnenému prístupu do a zo súkromnej siete a zvyšuje bezpečnosť zariadení pripojených k sieti, ako je internet alebo sieť lokálnej oblasti. Firewally monitorujú sieťovú komunikáciu a identifikujú a blokujú nechcenú komunikáciu. Od osobných počítačov po veľké spoločnosti sú brány firewall dôležitou súčasťou ochrany zariadení pred hrozbami.

Útočníci často hľadajú zraniteľné zariadenia pripojené k internetu. Firewally sú dôležité pre:

- ochranu počítača pred neželaným prístupom;
- identifikáciu a blokovanie nežiaduceho obsahu;
- predchádzanie červom, vírusom a malwareu;
- vytvorenie bezpečnej siete vo viacčlennom prostredí;
- zabezpečenie súkromných informácií.

Brány firewall môžu blokovať aj konkrétne miesta on-line. Môže to byť užitočné z bezpečnostných dôvodov, ale aj pre blokovanie webových stránok, ktoré môžu mať nevhodný obsah. Filtrovanie obsahu môže byť užitočné pre spoločnosti.

Hoci brána firewall môže zabrániť malwareu, nie je schopná zistiť malware v počítači a zbaviť sa ho. Z tohto dôvodu je odporúčané okrem zavedenia brány firewall nainštalovať antivírusový softvér od spoľahlivého výrobcu. Antivírusový softvér funguje tak, že detekuje škodlivý softvér v súboroch a programoch, ktoré by mohli ohroziť počítač. Všetky zariadenia spoločnosti by mali mať nainštalovaný aktuálny antivírusový program a bránu firewall, aby sa predišlo bežným hrozbám a útokom škodlivého softvéru.[38]

[38] RTI Marketing team. *The importance of a firewall.* 2016. [online]. [cit. 02-02-2020] Dostupné na internete: https://www.1rti.com/the-importance-of-a-firewall/

Aj keď je toto všetko nesmierne dôležité, brána firewall robí viac ako len prevenciu pred počítačovými zločincami v prístupe k údajom. Chráni tiež sieť spoločnosti a počítače spoločnosti pred zneužitím na nezákonné činnosti bez vedomia vlastníka firmy.

Rovnako ako antivírusový softvér, aj samotný firewall musí byť neustále aktualizovaný, aby sa zabezpečilo, že dokáže zistiť najnovšie hrozby. Nedostatok zdrojov, porozumenia, času a školení sú najväčšími faktormi v podnikoch, ktoré nedodržiavajú správne protokoly brány firewall. [39]

5. Ako pristupujú používatelia z internej siete k internetu? Používate proxy server?

Používatelia vo vybraných inštitúciách pristupujú z internej siete k internetu prostredníctvom proxy serveru.

Na otázku, čo je vlastne proxy server, by sme mohli odpovedať nasledovne: je to sprostredkovateľský server, ktorý oddeľuje koncových používateľov od webových stránok, ktoré prehliadajú. Proxy servery poskytujú rôzne úrovne funkčnosti, zabezpečenia a súkromia v závislosti od prípadu použitia, potrieb alebo firemnej politiky. Proxy servery fungujú ako firewall a webový filter, poskytujú zdieľané sieťové pripojenia a údaje vo vyrovnávacej pamäti na urýchlenie bežných požiadaviek. Dobrý proxy server chráni používateľov a internú sieť pred nežiaducimi útokmi. Nakoniec, proxy servery môžu poskytovať vysokú úroveň ochrany osobných údajov.

Každý počítač na internete musí mať jedinečnú adresu IP - Internet Protocol. Túto adresu IP považujeme ako adresu daného počítača. Rovnako ako pošta vie doručiť vašu poštu na vašu ulicu, internet vie, ako poslať správne údaje do správneho počítača pomocou adresy IP. Proxy server je v podstate počítač na internete s vlastnou IP adresou, ktorú pozná daný počítač. Keď používateľ odošle webovú požiadavku, jeho žiadosť pôjde najskôr na proxy server. Proxy server potom vykoná webovú žiadosť v mene používateľa, zhromaždí odpoveď z webového servera a pošle údaje z webovej stránky, aby používateľ mohol vidieť v prehliadači.

Organizácie môžu navyše spojiť svoj proxy server s virtuálnou súkromnou sieťou (VPN), takže vzdialení používatelia majú vždy prístup na internet prostredníctvom

[39] CROOK, Zech. Why every business needs a firewall. 2018. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.bizjournals.com/phoenix/news/2018/11/15/why-every-business-needs-a-firewall.html

firemného proxy. VPN je priame pripojenie k podnikovej sieti, ktoré spoločnosti poskytujú externým alebo vzdialeným používateľom. Pomocou VPN môže spoločnosť kontrolovať a overovať, či ich používatelia majú prístup k zdrojom (e-mailom, interným údajom), ktoré potrebujú, a zároveň poskytujú používateľovi bezpečné pripojenie na ochranu údajov spoločnosti.[40]

6. Je server pripojený na záložný zdroj, ako dlho to vydrží?

Záložné zdroje majú obidve spozorované organizácie, a obidve organizácie ich majú inštalované v serverovni. Môžeme skonštatovať, že technické požiadavky na vybavenie miestnosti severovne v oblasti klimatizácie a požiarnej bezpečnosti, obidve spoločnosti majú skoro totožné.

Záložný zdroj je z anglického slovného **spojenia Uninterruptible Power Supply – UPS**, v slovenskom preklade zdroj nepretržitého napájania. Je efektívne a správne riešenie udržania nášho počítačového, multimediálneho alebo iného pracoviska v činnosti v prípade výpadku elektrickej energie. Sú pomerne malé a nízko hlučné stroje. Výkon a doba neprerušovaného napájania môžu byť odlišné podľa preferencií. V serverovniach, väčších firemných pracovísk poznáme výkonné riešenia na zálohovanie napájania od 1000 do 10 000 VA. Jeho hlavnou úlohou je chrániť zariadenia, informácie a dáta, informačné systémy a samozrejme technológie.[41]

7. Mohli by ste charakterizovať fyzickú ochranu serverovní?

Fyzická ochrana serverovní je veľmi podobná u vybraných organizáciách, z dôvodu, že v súčasnosti platné predpisy stanovia konkrétne bezpečnostné opatrenia. Tieto opatrenia musia dodržiavať všetky spoločnosti bez ohľadu na to, či pôsobia v súkromnej sfére alebo v samospráve. Stanovujú hlavne špeciálne hasiace prístroje, teploty serverovne, protipožiarne steny a protipožiarne bezpečnostné dvere.

[40] PETTERS, Jeff. *What is proxy server and how does it work*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.varonis.com/blog/what-is-a-proxy-server/

[41] Nenahraditeľné záložné zdroje elektrickej energie. 2019. [cit. 02-02-2020] Dostupné na internete: http://www.legrand.sk/electrend/zabezpecenie/nenahraditelne-zalozne-zdroje-elektrickej-energie/

8. **Aké fyzické média sú použité na prenos a uchovanie údajov, pri akých podmienok je povolené ich užívať?**

Striktné podmienky sa vzťahujú aj na fyzické média, zamestnanci môžu ich používať výlučne v budove organizácie. V súkromnej firme používaná média je USB, v samospráve sú USB a HARD DISK, ktoré sú vydané zamestnávateľom a vedia ich vo vlastnej evidencii.

9. **Sú zavedené nejaké obmedzenia na počet používateľských procesov?**

Na základe preštudovaných materiálov môžeme skonštatovať, že používatelia sú nevyhnutnou súčasťou bezpečnostných opatrení v spoločnosti, pretože ich prístup k operačnému systému a rôznym aplikáciám je neoddeliteľný. Pri vstupe používateľa sú nesmierne významné dve hľadiská: autentifikácia – iba skutočný používateľ by mohol vstúpiť do systému; autorizácia – určenie práv používateľa po prihlásení do systému.

Obmedzenia sú zavedené podľa pozície používateľov pri vybraných inštitúciách, u samosprávy obmedzenia sú v súlade s nakúpenou licenciou softvérového vybavenia.

10. **Je používateľ skutočne ten, za koho sa vydáva? (autentifikácia)**

Môžeme skonštatovať, že v obidvoch skúmaných spoločnostiach je zabezpečený najvyšší stupeň autentifikácie každého užívateľa informačnej technológie predmetných spoločností na všetkých jeho úrovniach.

Autentifikácia je vlastne proces overovania totožnosti osoby alebo zariadenia. Bežným príkladom je zadanie používateľského mena a hesla pri prihlásení na webovú stránku. Aj keď kombinácia používateľského mena a hesla je bežným spôsobom overenia totožnosti, existuje mnoho ďalších typov overenia. Napríklad môžeme na odomknutie telefónu použiť štvor-alebo šesťciferný prístupový kód. Na prihlásenie do prenosného alebo pracovného počítača môže byť potrebné jedno heslo. Ďalej uvádzame bežné metódy autentifikácie používané na zabezpečenie siete na porazenie rôznych počítačových podvodníkov.

Biometria sa vzťahuje na používanie známych a zdokumentovaných fyzických atribútov používateľa na overenie jeho totožnosti. Je to ideálne riešenie, pretože žiadny z

dvoch ľudí nemá rovnaké fyzické vlastnosti. Bežné metódy biometrickej autentifikácie zahŕňajú identifikáciu odtlačkov prstov, rozpoznávanie hlasu, skenovanie sietnice a dúhovky a skenovanie a rozpoznávanie tváre. Nevýhodou tejto metódy je, že vyžaduje špecializované skenovacie zariadenie, ktoré nie je pre niektoré priemyselné odvetvia ideálne a sú pomerne drahé.

Token je materiálne zariadenie, ktoré sa používa na prístup k zabezpečeným systémom. Bežné formy zahŕňajú hardvérový kľúč, kartu alebo RFID čip. Token skomplikuje hackerovi prístup k účtu, pretože musí mať dlhé poverenie a samotné hmotné zariadenie, ktoré hacker získa oveľa ťažšie.

Viacfaktorové overenie je návrh autentifikácie, ktorý vyžaduje dva alebo viac nezávislých spôsobov overenia totožnosti. Príkladmi zabezpečenia viacúrovňovej identifikácie a autorizácie oprávnenosti vykonania finančnej transakcie sú bankomaty, lebo na uskutočnenie transakcie potrebujeme kartu (fyzický token) a PIN.

Akákoľvek transakcia, ktorá si vyžaduje vklady z jedného miesta na druhé, napríklad veľký prevod peňazí, by vyvolala telefonický hovor, text alebo oznámenie v aplikácii, ktorá vyžaduje viac autentifikácie na dokončenie transakcie. Z dvoch kanálov je pre hackerov oveľa ťažšie ukradnúť peniaze.[42]

11. Aké práva má mať používateľ po prihlásení? (autorizácia)

Z odpovedí vyplýva, že v obidvoch skúmaných spoločnostiach je zabezpečený najvyšší stupeň autorizácie každého užívateľa informačnej technológie predmetných spoločností na všetkých jeho úrovniach s možnosťou okamžitej a spätnej identifikácie užívateľa v spojitosti s požívanými autentifikačnými nástrojmi.

Autorizácia je bezpečnostný mechanizmus na určovanie úrovní prístupu alebo oprávnení užívateľa/klienta spojených so systémovými prostriedkami vrátane súborov, služieb, počítačových programov, údajov a funkcií aplikácií.

Väčšina webových bezpečnostných systémov je založená na dvojkrokovom procese. Prvým krokom je autentifikácia, ktorá zaručuje identitu užívateľa a druhým

[42] *Common Authentication Methods: Network Security.* 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.alliancetechpartners.com/common-authentication-methods-used-network-security/

krokom je autorizácia, ktorá užívateľovi umožňuje prístup k rôznym zdrojom založeným na identite užívateľa. Moderné operačné systémy závisia od efektívne navrhnutých procesov autorizácie, ktoré uľahčujú zavádzanie a správu aplikácií.

Kontrola prístupu tiež používa autentifikáciu na kontrolu identity spotrebiteľov. Keď sa spotrebiteľ pokúsi získať prístup k prostriedku, proces kontroly prístupu zisťuje, že spotrebiteľ bol oprávnený tento zdroj používať. Autorizačné služby sú implementované bezpečnostným serverom, ktorý môže riadiť prístup k jednotlivým súborom alebo programom.[43]

12. Akí pracovníci majú fyzický prístup k serveru?

Z odpovede vyplýva, že fyzický prístup k serveru majú iba kompetentné osoby, t.j. administrátori a v samospráve správca systému.

13. Aké sú podmienky na heslo používateľa? Je nastavená maximálna doba platnosti hesla?

Presné podmienky hesla nám kompetentné osoby z pochopiteľného dôvodu nevysvetlili. Je zrejmé, že v súkromnom podniku si administrátori vymieňajú heslá častejšie, ako v samospráve. Organizácie majú striktne určené podmienky pri tvorbe hesla, ktoré majú dodržiavať v každom prípade.

Obmena hesla je nevyhnutný proces v každom podniku. Každá organizácia by mala presne určiť, akú heslovú politiku nastaví vo svojej firme. Optimálna doba zmeny hesla je v každej inštitúcii odlišná, nakoľko spracúvajú rôzne dáta a údaje. Dôležité je aj zloženie hesla, malo by obsahovať malé a veľké písmená, znaky, číslice, atď. Dĺžka hesla je rovnako dôležitá a platí známe pravidlo, čím dlhšie, tým bezpečnejšie.[44]

[43] Definition of 'Authorization' [online]. [cit. 02-02-2020]. Dostupné na internete: https://economictimes.indiatimes.com/definition/authorization

[44] TINÁK, Rastislav. *Bezpečné, silné a zapamätateľné heslo – ako ho vytvoriť*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.podnikajte.sk/informacne-technologie/bezpecne-silne-zapamatatelne-heslo-ako-vytvorit

5. Diskusia

Zo získaných odpovedí môžeme skonštatovať, že ochrana informačných systémov a informačných technológií je dôležitá pre obidve vybrané organizácie. Napriek tomu, že ide o úplne odlišné inštitúcie a chránia iné údaje a dáta, zaviedli viaceré ochranné opatrenia v oblasti svojich informačných systémov. V súkromnej firme ide hlavne o ochranu vnútorných firemných informácií, kým v samospráve sú najdôležitejšie dáta klientov, t.j. osobné údaje. Z tohto pohľadu môžeme skonštatovať, že sme vybrali vhodné subjekty na realizovanie prieskumu a vybrané inštitúcie nám k danej téme poskytli potrebné informácie.

Pri analýze odpovedí sme zistili, že opýtané organizácie používajú odlišné informačné systémy, čo vyplýva z predmetu činnosti. Nie je prekvapujúce, že súkromná spoločnosť používa komplexný ERP systém, konkrétne SAP, z ktorého používa sedem modulov: Finančné účtovníctvo, Kontroling, Skladové hospodárstvo a logistiku, Podporu predaja, Riadenie ľudského kapitálu, Manažment kvality a Plánovanie výroby. Správca systému v samospráve nám konkretizoval používaný informačný systém CORA GEO, ktorý používajú na riešenie účtovníctva a personálnej agendy, pre evidenciu a spracovanie korešpondencie a jej archivácie, na spracovania geografických informácií, na riešenie výstupov pre vedenie samosprávy a riešenie pre eGOVERMENT.

Prvým spoločným bodom vybraných organizácií, bol operačný systém Windows, ktorý používajú s uspokojením obidve organizácie. Na switch operácie používa súkromná spoločnosť aj operačný systém Linux.

Obe organizácie, ktoré sa zúčastnili prieskumu, mali zabezpečené záložný zdroj, a zhodli sa na tom, že najideálnejšie miesto má v serverovni.

Čo sa týka fyzickej ochrany serverovne, momentálne platné predpisy dodržiavajú obidve organizácie, majú potrebné špeciálne hasiace prístroje, klimatizáciu a protipožiarnu izbu s protipožiarnymi dverami.

Z piatej otázky sme sa dozvedeli, že organizácie, s ktorými sa rozhovor uskutočnil, majú nainštalovaný firewall, aby zachránili svoje údaje a dáta. To je jeden z najdôležitejších bezpečnostných opatrení čo sa týka informačných systémov. Je pravda, že vybrané inštitúcie majú nainštalovaný odlišný firewall, súkromná firma SOPHOS UT 9 a samospráva KERBER, ale najdôležitejšia je kontrola prístupu do vnútra siete.

Na šiestu otázku sme dostali tiež pozitívnu odpoveď, pretože obmedzenia na počet používateľských procesov sú zavedené na základe pozície používateľov tak v súkromnej sfére, ako aj v samospráve.

Organizácie upredňostňovali vhodnú opatrnosť, čo sa týka prístupu na internet, používaním sprostredkovateľského, resp. proxy servera, ktorý na jednej strane zabezpečí určitú ochranu používateľov, ale chráni aj internú sieť organizácie pred nežiaducimi útokmi.

Ďalším dôležitým pilierom bezpečnostných opatrení informačných systémov a informačných technológií je kvalitný antivírusový program. Pri ôsmej otázke sme zistili, že vybrané inštitúcie majú nakúpený a nainštalovaný antivírusový program ESET. Boli sme zvedaví, prečo uprednostňujú práve tento antivírusový program. Podľa menšej recenzie, ktorú robili odborníci webovej stránky necenzurovane.sk, sa dokázalo, že antivírusový program ESET je z viacerých hľadísk skutočne dobrou voľbou.

Čo sa týka autentifikácie a autorizácie, z odpovedí vyplýva, že v obidvoch organizáciách je zabezpečený najvyšší stupeň autentifikácie a autorizácie užívateľa informačnej technológie na všetkých úrovniach.

Odpovede na jedenástu otázku sme považovali za úplne logické a pochopiteľné, lebo fyzický prístup k serveru majú výlučne kompetentné osoby, resp. administrátori serveru a správca systému v samospráve.

Pri rozhovoroch sme diskutovali tiež o hesle používateľov a zistili sme, že v obidvoch inštitúciách sú stanovené striktné pravidlá, ktoré sa týkajú dĺžky a zloženia hesla a kompetentné osoby majú generovať a zmeniť heslo v stanovenom intervale.

Posledná otázka rozhovoru sa týkala fyzických médií na prenos dát. Dospeli sme k záveru, že organizácie používajú USB a v samospráve aj HARDDISK (pevný disk), ale zamestnanci sú oprávnení ich používať výlučne v budove inštitúcie na základe vedenej evidencie.

Vzhľadom na skutočnosti vyskúmané v tejto diplomovej práci odporúčame analyzovať zavedené bezpečnostné opatrenia v ďalších organizáciách s iným predmetom činnosti, s cieľom získania komplexného obrazu o týchto opatreniach na celom Slovensku, resp. so zámerom možnosti vytvorenia funkčného algoritmu slúžiaceho pre manažéra firiem a organizácii pri výbere najvhodnejšieho informačného systému/technológie a pri tvorbe firemnej bezpečnostnej politiky v oblasti informačného systému/technológie. Ideálne by bolo skúmať danú problematiku v širšom ponímaní, resp. prieskum realizovať viacerými otázkami.

Záver

Záverečná práca je zameraná na ochranu informačných systémov a informačných technológií analyzovaním teoretických poznatkov domácich a zahraničných autorov a bezpečnostných opatrení zavedených v praktickom živote. Za cieľ sme si vytýčili predstavenie pojmov súvisiacich s uvedenou témou a zdôraznenie významu ochrany informačných systémov. Definovali sme typy útokov v oblasti informačných systémov, ktoré hrozia všetkým podnikom a organizáciám, ďalej metódy na vyhnutie sa im. Takýmto spôsobom sme sa snažili splniť cieľ teoretickej časti práce.

Hlavný cieľ našej diplomovej práce sme splnili pomocou vlastného výskumu. Najprv sme vyhľadali dve organizácie, ktoré majú odlišný predmet činnosti a oslovili sme ich, aby sa anonymne zúčastnili v našom prieskume. Stanovili sme sledovateľné a porovnateľné otázky, konkrétne trinásť otázok, na dosiahnutie celkového obrazu výsledku prieskumu. Pri vypracovaní prieskumu sme venovali dostatočnú pozornosť otázkam, ktoré predstavovali rôzne formy bezpečnosti ako fyzická, sieťová a personálna bezpečnosť. V uskutočnenom prieskume sme úspešne porovnávali bezpečnostné opatrenia určené v bezpečnostnej politike u jedného súkromného podniku a jednej miestnej samosprávy v okrese Dunajská Streda. Prieskum sa uskutočnil formou hĺbkových pohovorov vo vybraných inštitúciách. Na základe pohovoru sa nám podarilo predstaviť používané informačné systémy a prijaté ochranné opatrenia vo vybraných inštitúciách. Dozvedeli sme sa, že dotyčné organizácie chránia informačné systémy a technológie odlišným spôsobom, napríklad firewall majú obidve organizácie odlišne nainštalovaný, ale antivírus ESET považovali obidve organizácie za najlepší antivírusový program. Zistili sme, že vybrané organizácie venujú veľkú pozornosť finančným prostriedkom na ochranu informačných systémov. V poslednej fáze napĺňania nášho cieľa bolo vyhodnotenie výsledkov a vypracovanie záverečnej správy z prieskumu.

Na záver by sme mohli skonštatovať, že nielen väčšie, ale aj menšie podniky resp. organizácie, majú prijaté potrebné ochranné opatrenia na vysokej úrovni, čo sa týka informačných systémov a informačných technológií. V dnešnej dobe ochrana týchto systémov je nevyhnutnou súčasťou úspešného fungovania všetkých organizácií, lebo typy útokov sú nespočetné a môže sa stať ich obeťou hocikto.

Zoznam použitej literatúry

Knihy

1. DRUCKER, Peter Ferdinand. *Postkapitalistická společnost*. 1. vydanie. Praha: Management Press, 1993. 197 s. ISBN 80-85603-31-4
2. HUŽVÁR, Miroslav LACO, Peter. *Informačné technológie v ekonomickej praxi.*1. vydanie. Bratislava: Wolters Kluver, 2014. 156 s. ISBN 978-80-8168-085-4
3. KIMLIČKA, Š. Manažment tvorby informačných systémov: T*eoretické východiská, metódy a postupy vo sfére vedy, výskumu a vzdelávania.* Bratislava: Slovenská technická knižnica, 1995. 137 s. ISBN 80-85165-52.
4. KUČERA, Milan a kol. *Podnikové informačné systémy*. Prvé vydanie. Slovenská poľnohospodárska univerzita v Nitre, 2017. 214 s. ISBN 978-80-552-17239
5. LENDEL, Viliam – KUBINA, Milan – HITTMÁR, Štefan. *Podnikové informačné systémy*. Žilina: Žilinská univerzita, vyd. Edis, 2013. 228 s. ISBN 978-80-554-0712-8
6. LEVICKÝ, Dušan. *Úvod do kybernetickej bezpečnosti.* Prvé vydanie. elfa, s.r.o., Park Komenského 7, 040 01 Košice, 2019. 148 s. ISBN 978-80-8086-276-3
7. LOVEČEK, Tomáš. *Bezpečnosť informačných systémov.* Žilinská univerzita. 2007. 142 s. ISBN 978- 80-8070-767-5
8. RÁBOVÁ, Ivana DRLÍK, Martin. *Podnikové informačné systémy, ich architektúra a vývoj*. Prvé vydanie. Univerzita Konštantína Filozofa v Nitre, 2013. 168 s. ISBN 978-80-558-0287-9
9. STAŠÁK, Jozef MAZŮREK, Jaroslav. *Manažérska informatika II.* 1. vydanie. Žilinská univerzita v Žiline/EDIS - vydavateľské centrum ŽU, 2019. 276 s. ISBN 978-80-554-1544-4
10. STAUDEK, Ján – HANÁČEK, Petr. *Bezpečnost informačních systémů. Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technológií.* Úřad pro státní informační systém, 2000. 127 s.

Internetové zdroje

11. GIACKOVÁ, Sylvia. *Informačný manažment*. 2008. [online]. [cit. 2020-02-02]. Dostupné na internete: https://giackova.blog.sme.sk/c/169311/Informacny-manazment.html
12. *Information system.* 2017. [online]. [cit. 2020-02-02]. Dostupné na internete: http://www.businessdictionary.com/definition/information-system.html
13. *Introduction to Information System.* [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.javatpoint.com/cyber-security-information-system-introduction
14. CASSETTO, Orion. *The 8 Elements of an Information Security Policy*. 2019. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.exabeam.com/information-security/information-security-policy/
15. *Systémová bezpečnostná politika IT.* 2014. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.zones.sk/studentske-prace/informatika/9009-systemova-bezpecnostna-politika-it/
16. *What Is Phishing?* 2018. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html#~types-of-phishing-attack
17. DOBRAN, Bojana. *17 Types of Cyber Attacks To Secure Your Company From in 2020*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://phoenixnap.com/blog/cyber-security-attack-types
18. MARTINDALE, Jon. *What is antivirus softvare and how does it work?* 2018. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.digitaltrends.com/computing/what-is-antivirus-software/
19. Výpis z Obchodného registra Okresného súdu Trnava. 2020. [online]. [cit. 2020-02-02]. Dostupné na internete: http://www.orsr.sk/vypis.asp?ID=407548&SID=7&P=1
20. Wertheim/home. [online]. [cit. 2020-02-02]. Dostupné na internete: /http://www.wertheim.at/home.html
21. "VIX" NORIS, Ivan. *Bezpečnosť servera v sieti*, 2002-2007. [online]. [cit. 02-02-2020]. Dostupné na internete: http://dejavix.sk/sysadmin/security.html#top
22. *Odvetvia – Produkty určene pre samosprávu*. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.corageo.sk/odvetvia/

23. ESHNA, Verma. *Understanding SAP Modules: SAP FI, SAP CO, SAP SD, SAP HCM and more.* 2020. [online]. [cit. 2020-02-02]. Dostupné na internete: https://www.simplilearn.com/sap-modules-sap-fi-sap-co-sap-sd-sap-hcm-and-more-rar111-article
24. *Windows, OS X, či Linux?* 2016. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.speedex.sk/windows-os-x-ci-linux/
25. *Nenahraditeľné záložné zdroje elektrickej energie*. 2019. [cit. 02-02-2020]. Dostupné na internete: http://www.legrand.sk/electrend/zabezpecenie/nenahraditelne-zalozne-zdroje-elektrickej-energie/
26. RTI Marketing team. *The importance of a firewall*. 2016. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.1rti.com/the-importance-of-a-firewall/
27. CROOK, Zech. Why every business needs a firewall. 2018. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.bizjournals.com/phoenix/news/2018/11/15/why-every-business-needs-a-firewall.html
28. PETTERS, Jeff. *What is proxy server and how does it work*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.varonis.com/blog/what-is-a-proxy-server/
29. *Najlepšie antivírusy 2020: Porovnanie 13 bezplatných a platených antivírusov*. 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.kodino.com/sk/clanky/najlepsie-antivirusy/
30. *TOP antivírusy roku 2020*. 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://necenzurovane.sk/antivirusy/#uvod
31. *Common Authentication Methods: Network Security.* 2020. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.alliancetechpartners.com/common-authentication-methods-used-network-security/
32. Definition of ‘Authorization‘ [online]. [cit. 02-02-2020]. Dostupné na internete: https://economictimes.indiatimes.com/definition/authorization
33. TINÁK, Rastislav. *Bezpečné, silné a zapamätateľné heslo – ako ho vytvoriť*. 2019. [online]. [cit. 02-02-2020]. Dostupné na internete: https://www.podnikajte.sk/informacne-technologie/bezpecne-silne-zapamatatelne-heslo-ako-vytvorit

Prílohy