EKONOMICKÁ UNIVERZITA V BRATISLAVE

FAKULTA PODNIKOVÉHO MANAŽMENTU

Evidenčné číslo: 104006/D/2023/36157578834625028

Manažment informačnej bezpečnosti podniku v európskom priestore

Diplomová práca

2023 **Bc. Martin Vatolík**

EKONOMICKÁ UNIVERZITA V BRATISLAVE

FAKULTA PODNIKOVÉHO MANAŽMENTU

Manažment informačnej bezpečnosti podniku v európskom priestore

Diplomová práca

Študijný program: Všeobecný manažment

Študijný odbor: Ekonómia a manažment

Školiace pracovisko: Katedra informačného manažmentu

Vedúci záverečnej práce: doc. Ing. Vladimír Bolek, PhD.

Bratislava 2023 **Bc. Martin Vatolík**

Poďakovanie

Chcem sa úprimne poďakovať, môjmu školiteľovi doc. Ing. Vladimírovi Bolekovi, PhD., za podporu a pomoc pri písaní bakalárskej aj diplomovej práce. Jeho odborné rady, návrhy a odporúčania mi pomohli zvýšiť produktivitu práce a zdokonaliť moje zručnosti. Vážim si jeho pomoc a trpezlivosť počas môjho celého vysokoškolského štúdia.

Bratislava 2023

ABSTRAKT

VATOLÍK, Martin: *Manažment informačnej bezpečnosti podniku v európskom priestore.* – Ekonomická univerzita v Bratislave. Fakulta podnikového manažmentu; katedra informačného manažmentu. – doc. Ing. Vladimír Bolek, PhD. – Bratislava: FPM, 2023, počet strán 85.

Diplomová práca je vypracovaná na tému informačnej bezpečnosti v podnikoch a jej implementáciou podľa bezpečnostných štandardov. Cieľom tejto práce je posúdiť zavedené normy informačnej bezpečnosti v podniku a realizovateľnosť implementácie novej smernice o informačnej bezpečnosti NIS2 (The Network and Information Security) v rámci malej spoločnosti. Súčasťou práce je komparatívna analýza právnych predpisov v oblasti informačnej bezpečnosti v európskom regióne a súhrn odporúčaní pre podniky, ktoré by mali zohľadniť výsledky tejto analýzy. Výsledky dokumentu sumarizujú najdôležitejšie východiská pre spoločnosti pri riadení informačnej bezpečnosti a navrhujú opatrenia na zabezpečenie efektívneho riadenia.

Úvodná časť diplomovej práce je venovaná stručnému zhrnutiu problematiky informačnej bezpečnosti v podnikoch a zdôrazňuje význam implementácie bezpečnostných štandardov. V prvej kapitole je zhrnutý súčasný stav tejto témy v rôznych krajinách a sú identifikované hlavné problémy a hrozby informačnej bezpečnosti.

Kapitola dva definuje cieľ práce navrhnúť odporúčané pravidlá pre správu a ochranu informačných aktív v podniku.

Ďalšia kapitola, kapitola 3, sa zameriava na metodiku práce a výskumné metódy použité na dosiahnutie cieľov práce.

Kapitola štvrtá prezentuje výsledky diplomovej práce. Jej súčasťou je komparatívna analýza právnych úprav informačnej bezpečnosti v európskom regióne a návrh súhrnu odporúčaní pre podniky.

Záverečná kapitola sa zaoberá implementáciou navrhovaných opatrení a ich účinnosťou pri ochrane informačných aktív v podniku.

Kľúčové slová: informačná bezpečnosť, bezpečnostné štandardy, správa informačných aktív, legislatívna úprava, odporúčania pre podnik, norma NIS2

ABSTRACT

VATOLÍK, Martin: Information security management of the enterprise in the European area. - University of Economics in Bratislava. Faculty of business management; department of information management. – Assoc. Ing., Vladimír Bolek, PhD. – Bratislava: FPM, 2023, number of pages 85.

Thesis deals with the issue of information security in the enterprise and its implementation in accordance with security standards. The aim of the thesis is to define recommended rules that will help an enterprise to effectively manage and protect all its valuable information assets. Within the thesis, a comparative analysis of the legislative regulation of information security in the European area is carried out in order to propose a summary of recommendations for the enterprise, which will take into account the results of this analysis. The output of the thesis will be a summary of the most important starting points for enterprises in managing information security and proposing measures to ensure its effective management.

The introduction of the diploma thesis is devoted to a brief summary of information security issues in the enterprise and emphasizes the importance of implementing security standards.

Chapter one will summarize the current status of the issue addressed in different countries and identify the main challenges and threats in the field of information security.

Chapter two defines the objective of the thesis, which is to propose recommended rules for the management and protection of information assets in the enterprise.

The following chapter three focuses on the methodology of the thesis and the research methods that were used to achieve the objective of the thesis.

Chapter fourth will present the results of the thesis, which will include a comparative analysis of the legislative regulation of information security in the European area and a proposal of a summary of recommendations for the enterprise.

The last chapter will discuss the implementation of the proposed measures and their effectiveness in protecting information assets in the enterprise.

Keywords: information security, security standards, information asset management, legislative regulation, recommendations for business, NIS2 standard.

Obsah

Úvod

Pojmy ako informatika, informácia, kybernetika, dáta a informačná bezpečnosť, vďaka súčasnej dobe a trendom ani netreba vysvetľovať. Tieto trendy jasne dokazujú zavádzanie informácií a ich transformáciu do digitálnej podoby v podobe informačných systémov. Dátové systémy používa takmer každý človek na svete a niektorí si to možno ani neuvedomujú. Cez tieto systémy prechádza nespočetné množstvo údajov rôzneho druhu. Od bežných používateľských údajov až po tie najcitlivejšie údaje. Veľká časť týchto údajov je pre podnik životne dôležitá a nemôže bez nich fungovať, preto je veľmi dôležité, či a ako sú tieto údaje chránené. Touto témou sa zaoberá aj kapitola Riadenie bezpečnosti informácií v podniku a budeme sa jej venovať ďalších kapitolách.

Pretože informačná bezpečnosť sa stala veľmi dôležitou a horúcou témou v dnešnom svete IT a podnikov tak táto práca sa zaoberá témou informačnej bezpečnosti v podnikovom prostredí so zameraním na riadenie informačnej bezpečnosti a riziká spojené s narušením informačnej bezpečnosti. V úvodnej časti práce budeme analyzovať súčasnú situáciu v doma a v zahraničí, pričom sa zameriame na trendy v oblasti informačnej bezpečnosti a stav vývoja v jednotlivých krajinách. Potom sa zameriame na samotnú tému informačnej bezpečnosti, definujeme súvisiace pojmy a rozoberieme ich význam v podnikateľskom prostredí. Kapitola Riziká informačnej bezpečnosti definuje hlavné hrozby a riziká, ktorým dnes organizácie čelia. Ďalej sa postupujeme na riadenie informačnej bezpečnosti podniku, opíšeme postupy a metódy ochrany citlivých údajov a zabezpečenie ich dostupnosti pre oprávnených používateľov.

V druhej kapitole diplomovej práce je bližšie vymedzený cieľ práce a jej obsah. Cieľom tejto práce je posúdiť zavedené normy informačnej bezpečnosti v podniku a realizovateľnosť implementácie novej smernice o informačnej bezpečnosti NIS2 (The Network and Information Security) v rámci malej spoločnosti.

V tretej kapitole sa zameriavame na metodiku práce a metódy skúmania. V tejto kapitole sa zameriavame na postup a metódy, ktoré boli použité pri skúmaní informačnej bezpečnosti v podniku. Táto kapitola bližšie popisuje výskumný prístup, použité metódy a techniky, ktoré boli použité pri zhromažďovaní a spracovaní dát.

Štvrtá kapitola obsahuje výsledky práce, ktoré sú založené na komparatívnej analýze legislatívnej úpravy informačnej bezpečnosti v európskom priestore.

V poslednej kapitole sa nachádza diskusia, ktorá zhŕňa všetky dosiahnuté výsledky a odporúčania pre podnik. Diskusia sa zameriava na diskutovanie dosiahnutých výsledkov a ich prínosov pre podnik. Táto kapitola zahŕňa tiež diskusiu o obmedzeniach výskumu a možnostiach ďalšieho vývoja v oblasti informačnej bezpečnosti v podniku. Výsledky a odporúčania práce by mali byť použité ako základ pre budúce zlepšenie informačnej bezpečnosti v podniku.

1 Súčasný stav riešenej problematiky doma a v zahraničí

Technický pokrok zo sebou priniesol vysokú mieru informatizácie spoločnosti, ktorá sa stala na informačných technológiách závislá. Komunikačné kanály musia byť dostatočne kyberneticky zaistené informačnými systémami, inak hrozí riziko ich zneužitia. Preto je potrebné poznať rôzne možnosti informačnej bezpečnosti a prostredie v ktorom sa bude ochrana aplikovať. Informačná bezpečnosť je dôležitejšia každým novým rokom a preto nároky na ňu sa zvyšujú. Je však rozdiel v akom prostredí sa kybernetická bezpečnosť aplikuje, či na území Slovenskej republiky alebo na úrovni eurozóny, kde sa môžu pravidlá a koncepcie uplatňovania informatickej bezpečnosti líšiť.

1.1 Informačná bezpečnosť

Informačná bezpečnosť, je to stav určitého systému, ktorý umožňuje plnenie rôznych funkcií na splnenie požadovaných potrieb. Z tohto vyplýva že existuje pôvod nebezpečenstva a objekt, ktorý pre tento dôvod potrebuje ochranu. Tieto zdroje ohrozenia môžu byť najrôznejšieho charakteru od fyzického (materiálneho) až po nehmotné, čiže aj virtuálneho pôvodu.

Čo je teda informačná bezpečnosť sa dá vyjadriť rôznymi citáciami ako: „zachovanie dôvernosti, integrity a dostupnosti informácií“ [1].

„Informačná bezpečnosť je zodpovednosť za ochranu informácií počas ich vzniku, spracovania, ukladania, prenosu a likvidácie prostredníctvom technických, fyzických a organizačných opatrení, ktoré musia pôsobiť proti strate dôveryhodnosti, integrity a dostupnosti týchto hodnôt.“[2]

Skupina zahraničných autorov Whitman a Mattord vysvetľuje, že „informačná bezpečnosť (anglická skratka Infosec) je ochrana informácií a ich kritických charakteristík (dôvernosť, integrita a dostupnosť), vrátane systémov a hardvérov, ktoré používajú, uchovávajú a prenášajú tieto informácie, prostredníctvom uplatňovania politiky, školení a programov na zvyšovanie povedomia a technológie.“[3]

[1]CALDER, Alan. A Business Guide To Information Security: How to Protect your company is IT Assets Reduce Risks and Understand the Law. Kogan Page Published, 2005. s.136. ISBN 0-7949-4395-2.
[2]SIVÁK, Rudolf. *Slovník znalostnej ekonomiky.* Bratislava: Sprint 2. 2011. s.119. ISBN 978-80-89393
[3]WHITMAN, Michael E., HERBERT J. Mattord. *Management of information security*. Cengage Learning, [Elektronický zdroj] 2013. [Cit. 2023-05-01] Dostupné na: https://books.google.sk/books?hl=en&lr=&id=naB0AgAAQBAJ&oi=fnd&pg=PP1&dq=Information+security+&ots=yB5EUqZ27S&sig=mQl_rG3x5MnuY4R13NpRNt7E-aQ&redir_esc=y#v=onepage&q=Information%20security&f=false

Autorka Kostrecova píše o bezpečnosti ako „stav ochrany, pri ktorom možno predpokladať, že nedôjde k ohrozeniu aktív firmy alebo organizácie. Aktívum je objekt, subjekt, štruktúra, vzťah alebo proces, ktorého narušením môže hodnotený systém utrpieť stratu.“[4]

Môžeme konštatovať na základe citácií, že informačná bezpečnosť zhrňuje súbor zásad a kontrol, ktoré spoločnosti implementujú do svojich systémov na zabezpečenie cenných virtuálnych informácií a aktív, voči informačným hrozbám. Tieto opatrenia chránia pred neautorizovaným prístupom.

Informačná bezpečnosť nie je novodobým pojmom a objavuje sa už dávno pred príchodom technológií ako počítač, telefón atď.. Tento pojem môžeme rozdeliť do dvoch skupín období. Prvé obdobie sa viaže na roky pred digitálnym vekom a to konkrétne až do februára 1883. Auguste Kerckhoffs bol lingvista a profesor nemčiny. V tento deň publikoval článok v Journal of Military Science, ktorý nevedomky poskytol základ, na ktorom by bola založená celá moderná kryptografia. Kerckhoffs je teraz považovaný za otca počítačovej bezpečnosti a Kerckhoffsov princíp bol jadrom tvorby algoritmov. Je pôvodcom hesiel a PIN kódov, ktoré sú dodnes také dôležité pre opatrenia v oblasti bezpečnosti informácií. Druhé obdobie môžeme nazvať ako digitálny vek, čiže začiatok 70. roky 20. storočia. V týchto rokoch sa skutočný zrod informačnej bezpečnosti začal projektom s názvom The Advanced Research Projects Agency Network (ARPANET). ARPANET bola sieť vyvinutá pred internetom. Pozostával z dvoch sietí: 1. ARPANET pre výskumníkov a 2. MILNET pre vojenské účely. MILNET vyžadoval silné bezpečnostné opatrenia, ako je šifrovanie a obmedzené riadenie prístupu. V tom čase sa na ochranu citlivých údajov používali základné počítačové bezpečnostné opatrenia, ako sú heslá. V 70-tych rokoch bol internet stále žiarením v očiach jeho tvorcov. Napriek tomu, že neexistovala globálna sieť, veľké organizácie a vlády začali prepájať počítače pomocou telefónnych liniek. Starý dobrý modem až príliš zjednodušoval infiltráciu počítačov, a tak sa zrodila prvá skupina hackerov. Pomocou telefónnych liniek sa nabúrali do systémov a ukradli cenné dáta a osobné informácie. S rastúcim počtom hackerov nedokázali obmedzené systémy informačnej bezpečnosti držať krok s neustále sa prispôsobujúcimi hackerskými prístupmi používanými na prienik do počítačových systémov. Avšak, až keď sa malá skupina tínedžerov z Milwaukee úspešne nabúrala do viac ako 60 vojenských a firemných počítačov, kde ukradli

[4] KOSTRECOVÁ, Eva. *Informačná bezpečnosť*. 1. vyd. Bratislava: Slovenská technická univerzita v Nakladateľstvo STU, 2013. s. 7, ISBN 978-80-227-3927-6

viac ako 70 miliónov dolárov z amerických bánk sa informačnej bezpečnosti začala klásť omnoho väčšia dôležitosť. So zavedením celosvetového webu v roku 1989, začali nezabezpečené informácie predstavovať nový zdroj príjmov, ktorý umožnil narušiteľom vytvárať veľmi zložité systémy na kradnutie údajov od ľudí a vlád. Hoci bezpečnostné kontroly, ako sú brány firewall a antivírusové programy, pomohli zabrániť informačným krádežiam, v tom čase bol internet nezabezpečeným ihriskom pre kyberzločincov. Hoci ochrana údajov existuje už od 70. rokov 20. storočia , po roku 2010 poskytovalo zabezpečovanie údajov prístup k bezpečnosti, aby sa zabránilo neoprávnenému prístupu. Informačná bezpečnosť zašifruje údaje tak, aby boli pre hackerov nečitateľné. Šifrovanie môže prebiehať na viacerých úrovniach, čím chráni nielen siete, ale aj jednotlivé digitálne súbory v úložisku aj počas prenosu údajov. Organizácie implementujú zásady informačnej bezpečnosti, aby zabezpečili, že zamestnanci budú dodržiavať najlepšie postupy na zabránenie narušeniam údajov ich systémov správy údajov a archívov .[5,6]

Pochopenie histórie informačnej bezpečnosti poskytuje prehľad o tom, ako sa vyvíjala digitálna bezpečnosť, z kedysi jednoduchých opatrení až k viacstupňovo zabezpečeným systémom, pri ktorých najvyššia priorita je najvyššia ochrana. Kybernetická bezpečnosť v súčasnej dobe znamená, že experti v tomto obore musia zamerať všetko svoje úsilie na maximalizáciu výhod vznikajúcich technológií. Spoločnosti sa musia orientovať na nové trendy v informačnej bezpečnosti, ktorej význam sa v najbližších rokoch bude zvyšovať a nie klesať.

1.1.1 Význam informačnej bezpečnosti

Informačná bezpečnosť a jej implementácia do podnikového prostredia má najvyššiu dôležitosť pri ochrane podnikových informačných aktív. Tieto aktíva môžeme chápať ako rôzne citlivé údaje ako dôverné informácie spoločnosti, osobných údajov zákazníkov a zamestnancov, ktoré sú ukladané v kybernetickom priestore. Pri narušení údajov môže dôjsť minimálne k strate dôvery, reputácie a v horšom prípade aj k finančným stratám, prostredníctvom stratených tržieb, pokút a nápravných opatrení.

[5] Meservy, K. - A brief history of information security. The Circuit: The Official Newsletter of the IEEE Computer Society of the IEEE Circuits and Systems Society. [online] New York: IEEE, June 2013, Vol. 25, No. 2, pp. 23-27 [cit. 28. 2023-04-28]. ISSN 1059-7043. Dostupné na: https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present

[6]DE LEEUW, K. - BALEN, R. The History of Information Security: A Comprehensive Handbook. [online] In: Handbook of Information and Communication Security. Amsterdam: Elsevier, 2010, p. 1-28 [cit. 2023-05-01]. ISBN 978-0-444-51608-4. Dostupné na: https://www.elsevier.com/books/the-history-of-information-security/de-leeuw/978-0-444-51608-4

Systém opatrení informačnej bezpečnosti chráni organizácie pred možnými hrozbami súvisiacimi s technológiami a inými, bežnejšími hrozbami, ako sú napríklad nedostatočne informovaní zamestnanci alebo neefektívne postupy. Medzi najdôležitejšie dôvody, prečo je potrebne mať dobre zvládnutú informačnú bezpečnosť v podniku sú:

- **Ochrana funkčnosti organizácie:** so správnym bezpečnostným systémom môžu byť firemné dáta v bezpečí a jej prevádzka môže plynulo pokračovať niekoľko dní alebo týždňov. Naopak, ak by došlo k odcudzeniu citlivých informácií o klientoch alebo zamestnancoch, viedlo by to k súdnym sporom a poškodeniu dobrého mena.
- **Ochrana údajov organizácie:** zaistenie bezpečnosti informačnej infraštruktúry, aby boli údaje vždy chránené. To znamená zálohovať dôležité súbory, mať nasadené brány firewall a zabezpečiť, aby boli nainštalované všetky aktualizácie softvéru.
- **Zníženie rizika narušenia údajov**: porušenie údajov môže spôsobiť veľa rôznych vecí. Môže ísť o ľudskú chybu alebo zlomyseľné pokusy o narušenie tretích strán, ako sú počítačoví zločinci, ktorí chcú získať prístup k informáciám pre svoj zisk alebo politickú agendu. Implementáciou solídnych zásad týkajúcich sa správy hesiel a školiacich programov pre zamestnancov sa dajú znížiť šance, že dôjde k porušeniu.
- **Ochrana pred škodlivým softvérom:** malvér môže byť čokoľvek od vírusov cez spyware až po trójske kone. Tieto typy softvéru môžu infikovať počítač, mobilné zariadenia a ďalšie systémy, ktoré sa pripájajú na internet. Môžu ukradnúť osobné informácie alebo dokonca odstrániť súbory z počítača. Preto je bezpečnosť informácií nevyhnutná, pretože chráni pred hackermi, ktorí chcú získať prístup k súkromným informáciám.

Účelom informačnej bezpečnosti je vytvoriť, implementovať a riadiť informačný systém piatimi základnými postupmi: [7]

[7] DQs Global, Blogová sekcia. Ciele ochrany informačnej bezpečnosti a ich význam [online]. In: DQs Global: Blog. Bratislava: DQs Global, 2019 [citované 2023-04-28]. Dostupné na: https://www.dqsglobal.com/sk-sk/blog/ciele-ochrany-informacnej-bezpecnosti-a-ich-vyznam

1. Strategické zosúlaďovanie informačnej bezpečnosti s obchodnou stratégiou na podporu cieľov organizácie;
2. Efektívne riadenie rizík tým, že sa vykonajú vhodné opatrenia na riadenie a zmiernenie rizík a zníženie potenciálnych dôsledkov na informačné zdroje na prijateľnú úroveň;
3. Vytvorenie hodnoty optimalizáciou investícií do informačnej bezpečnosti na podporu cieľov organizácie;
4. Účinný a efektívny manažment zdrojov s využitím znalostí a infraštruktúry informačnej bezpečnosti;
5. Meranie výkonnosti na základe merania, monitorovania a poskytovania výstupov metrík riadenia informačnej bezpečnosti na dosiahnutie cieľov organizácie.[8]

Ciele informačnej bezpečnosti môžeme zhrnúť do troch základných skupín a to "dôvernosť", "integrita" a "dostupnosť".[9]

Dôvernosť: Aby mohla byť zaručená, musí sa jasne definovať, kto a akým spôsobom je oprávnený pristupovať k týmto citlivým údajom. Súvisí to napríklad s príslušnými oprávneniami na prístup a používaním kryptografických techník.

Integrita znamená ochranu pred neoprávnenými zmenami a vymazaním informácií, plus spoľahlivosť a úplnosť informácií. Preto je dôležité, aby podniky prijali opatrenia na rýchle odhalenie zmien údajov alebo na zabránenie neoprávnenej manipulácii s údajmi od základu.

Dostupnosť znamená, že informácie, systémy a budovy musia byť vždy k dispozícii oprávneným osobám. Keďže napríklad zlyhanie systému je spojené s veľkými rizikami, mala by sa pre tento komplex tém vykonať analýza rizík. Zaznamenajte tu pravdepodobnosť zlyhania, čas výpadku a potenciál poškodenia najpotrebnejších systémov.

Zabezpečovanie informácií v podniku je teda nevyhnutným procesom, ktorému by mal každý podnik venovať čo najvyššiu prioritu. Tento proces vychádza z určitých zložiek na ktorých je postavený systém riadenia informačnej bezpečnosti podniku.

[8]BOOTH, Wayne C. - COLOMB, Gregory G. - WILLIAMS, Joseph M. The Craft of Research: Fourth Edition [online]. Chicago : The University of Chicago Press, 2016, 4. vydanie, 320 s. [cit. 2023-05-01]. ISBN 978-0226239873. Dostupné na: http://common.books24x7.com.proxy.cityu.edu/toc.aspx?bookid=30815
[9]ONLINEMANIPAL, Information Security in Digital Transformation [online]. In: Manipal ProLearn. Manipal, 2021 [cit. 2023-04-28]. Dostupné na: https://www.onlinemanipal.com/blogs/information-security-in-digtial-transformation.

1.1.2 Kritéria informačnej bezpečnosti

Postupom vývoja informačnej bezpečnosti, ktorý prebieha už mnoho rokov, tak aj informovanosť užšej a širšej verejnosti a spotrebiteľov sa zvyšuje. Hlavným problémom, už nie je neinformovanosť, ale bližšia špecifikácia informačnej bezpečnosti, teda podľa akých kritérií a požiadaviek, ktoré ovplyvňujú informačnú bezpečnosť by mal užívateľ postupovať.

„Kritériá informačnej bezpečnosti predstavujú súbor požiadaviek, ktoré musí systém spĺňať, aby bol považovaný za bezpečný. Tieto požiadavky sú zvyčajne vyjadrené ako zásady, štandardy a postupy, ktorými sa riadi návrh a implementácia systému.“[10]

Podobne opisuje kritéria aj autor M. Kabay, ktorý hovorí, že „kritériá informačnej bezpečnosti predstavujú súbor pravidiel, smerníc a noriem používaných na meranie účinnosti bezpečnostných opatrení organizácie. Používa sa na určenie úrovne rizika spojeného s používaním a uchovávaním údajov a na zabezpečenie primeraných a účinných bezpečnostných opatrení.“ [11]

Kritériá zahŕňajú fyzické, technické a administratívne kontroly, ktoré sa používajú na ochranu informačných aktív organizácie. Kritériá fyzickej bezpečnosti zahŕňajú opatrenia, ako je fyzická kontrola prístupu, dohľad, hasiace a detekčné systémy a kontroly napájania a prostredia. Technické bezpečnostné kritériá zahŕňajú používanie technológií, ako je šifrovanie a autentifikácia na ochranu údajov a systémov organizácie pred neoprávneným prístupom a manipuláciou. Administratívne bezpečnostné kritériá zahŕňajú vývoj a implementáciu politík a postupov na ochranu informačných aktív organizácie pred neoprávneným prístupom alebo manipuláciou. [12]

Tieto kritéria priamo pôsobia na spokojnosť a dôveru, ktorú vníma spotrebiteľ a sú nevyhnutné pre hodnotenie bezpečnosti existujúcich systémov alebo vytváranie nových systémov s bezpečnými architektúrami. Zahŕňajú technické, organizačné a procedurálne opatrenia, ktoré musia byť splnené, aby sa zabezpečila bezpečnosť systému alebo siete. Tieto kritériá možno použiť na vyhodnotenie bezpečnostných požiadaviek a bezpečnostného

[10]RANUM, Marcus J. - KUMAR, Ravi - SCHNEIER, Bruce. Critical Infrastructure Security. [online] In: Elsevier Science & Technology Books: Computer Science. San Diego: Elsevier, 2003, 1st edition, 284 pages [cit. 2023-05-01]. Dostupné na: https://www.elsevier.com/books/critical-infrastructure-security/ranum/978-0-12-514031-2

[11]COMPTON, J - SLOAN, L. What Are Information Security Criteria? In: Computerworld: [online]. IDG Communications, Inc., 2012 [cit. 2023-04-28]. Dostupné na: https://www.computerworld.com/article/2500941/what-are-information-security-criteria.html.

[12]NIST Special Publication 800-14 Revision 2. (2013). Addressing the Cybersecurity
Risk to Critical Infrastructure: NIST Framework. [online]. National Institute of Standards and Technology. [cit. 2023-04-28]. Dostupné na: https://csrc.nist.gov/publications/detail/sp/800-14/rev-2/final.

návrhu systému. V tejto kapitole si identifikujeme kritéria, ktoré zlepšujú systém informačnej bezpečnosti. Kritéria hodnotenia informačnej bezpečnosti vychádzajú z: [13,14,]

TCSEC (Trusted Computer Systems Evaluation Criteria) orange book - kritériá špecifikujú bezpečnosť počítačového systému ako jeho schopnosť zachovania dôvernosti údajov.

ITSEC (Information Technology Security Evaluation Criteria) chápe bezpečnosť systému ako zachovanie atribútov dôvernosti, integrity a dosiahnuteľnosti údajov. Bezpečnosť objektu (môže ním byť ucelený systém, ako aj jeho jednotlivé komponenty – produkty) sa hodnotí podľa bezpečnostných funkcií, ktoré poskytuje, a podľa stupňa istoty v účinnosť týchto mechanizmov. V druhom prípade sa ešte rozlišuje medzi istotou v účinnosť bezpečnostných mechanizmov („sú postačujúce pre daný bezpečnostný cieľ?“) a istotou v správnosť ich návrhu a implementácie.

ITSEC nemá hierarchiu tried, ako je to v prípade TCSEC. Hierarchicky sú usporiadané len požiadavky na kvalitu návrhu a implementácie.

CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) sú kombináciou ITSEC a TCSEC. Vývojom týchto kritérií začali vznikať Common Criteria. Kritériá zobrazujú 2 typy požiadaviek: a/ požiadavky na funkcionalitu, t.j. kritériá orientované na 4 politiky: dôvernosť, integrita, dostupnosť, sledovateľnosť; požiadavky na zaistenie.

CC (Common Criteria) - v CC sa pojem bezpečnosť chápe nielen ako dôvernosť + integrita + dosiahnuteľnosť, ale zohľadňujú sa aj iné aspekty, ktoré sa nedajú jednoznačne zaradiť do jednej z týchto kategórií (napríklad ochrana súkromia používateľov hodnoteného produktu).

V Common Criteria sa používa nové štruktúrované kritérií – zoskupovanie bezpečnostných požiadaviek na triedy, ktoré sa delia na rodiny, ktoré sa skladajú z komponentov: a/trieda (class) – spoločný bezpečnostný zámer, ale rozdielne pokrytie bezpečnostných cieľov; b/ rodina (family) – spoločné ciele, rozdielny dôraz resp.

[13]DOD85 - Department of Defense Trusted Computer System Evaluation Criteria. [online]. In: Proceedings of the 21st National Information Systems Security Conference. Washington D.C.: National Institute of Standards and Technology, 1998, s. 13-15 [cit. 2023-04-28]. Dostupné na: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.

[14]KOLLÁR, Miroslav – RUSKO, Vojtech. "BEZPEČNOSTNÉ MANAŽÉRSTVO A SYSTÉM INFORMAČNEJ BEZPEČNOSTI." [online]. s. 148–149, ISBN 978-80-89281-85-5 [cit. 2023-04-28]. dostupné na: https://www.sszp.eu/wp-content/uploads/2012_konf_MaZP_B11__Rusko-Kollar.pdf

rigoróznosť; c/ komponenty (components) – v CC najmenšie zoskupenie bezpečnostných požiadaviek.

Môžeme povedať, že kritériá informačnej bezpečnosti sú základnou súčasťou bezpečnostnej pozície každej organizácie. Sú určené na ochranu informačných aktív organizácie pred neoprávneným prístupom a manipuláciou. Kritériá zahŕňajú fyzické, technické a administratívne kontroly, ktoré sa musia pravidelne revidovať a aktualizovať, aby sa zabezpečilo, že zavedené opatrenia sú účinné a aktuálne. Organizácie musia tiež zabezpečiť, aby všetci zamestnanci poznali bezpečnostné kritériá a boli vyškolení v ich používaní. Okrem toho by organizácie mali vykonávať pravidelné bezpečnostné audity a testy na zabezpečenie účinnosti kritérií. Zavedením účinných kritérií informačnej bezpečnosti môžu organizácie chrániť svoje informačné technológie a systémy pred neoprávneným prístupom a manipuláciou. Avšak aj pri najsilnejších informačných opatreniach budú stále vznikať určite riziká, ktoré musia byť neustále monitorované. Túto problematiku rozoberieme v nasledujúcej kapitole.

1.2 Riziká informačnej bezpečnosti

Je jasné, že informačná bezpečnosť má dopad na celú organizáciu. Tieto dopady nepôsobia len na určité IT oddelenie v podniku, ktoré sa snaží aplikovať rôzne informačné technológie ako sú napríklad firewally. Dopady pôsobia na celú obchodnú likviditu podniku. Podľa doterajších skúseností, najväčšia frekvencia narušení informačnej bezpečnosti prichádza z vonkajšieho prostredia. Existujú však ukazovatele, ktoré naznačujú že najrizikovejšie a najviac nákladne útoky pochádzajú zvnútra organizácie.

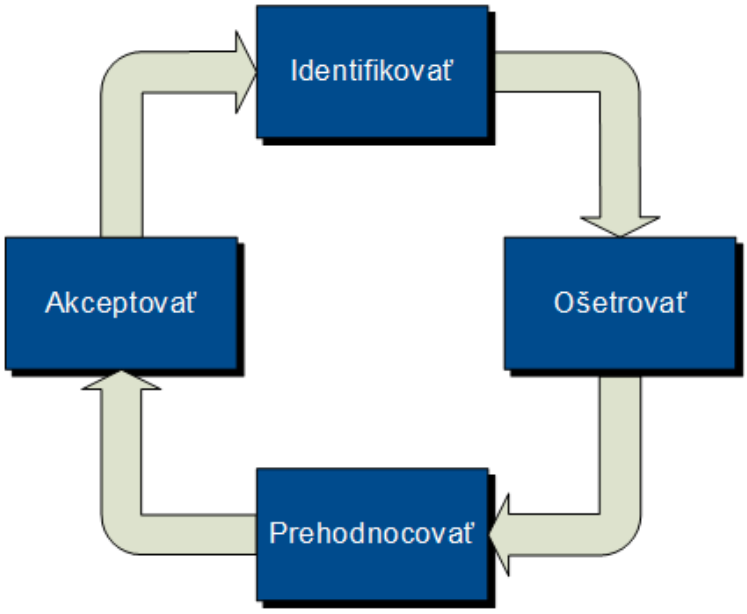
Čo je to riziko definuje autor S. Filip ako „určitý stupeň ohrozenia. Ide o pravdepodobnosť nastávania a dôsledok vzniku určitej udalosti.“[15]

Podľa Hubbarda je riziko „potencionálna strata, katastrofa alebo iná nežiadúca udalosť rôznej veľkosti, ktorá môže byť určená pravdepodobnosťou.“[16]

Riziko je možnosť utrpenia škody alebo straty. Vzťahuje sa na situáciu, v ktorej by osoba mohla urobiť niečo nežiaduce alebo prirodzená udalosť by mohla spôsobiť nežiaduci výsledok, ktorý má negatívny vplyv alebo následok. Prvým krokom pri riadení rizika je pochopiť, aké sú riziká vo vzťahu k poslaniu organizácie a jej kľúčovým aktívam. Toto

[15]FILIP, Stanislav – ŠIMÁK, Ladislav – KOVÁČ, Marián. Manažment rizika. Bratislava: Sprint dva, 2011. s. 28, ISBN 978-80-89393-49-7
[16]HUBBARD, W. Douglas. The failure of risk management: Why it's broken and how to fix it. 2 edition. John Wiley & Sons, 2020. s. 9, ISBN 978-1-119-52203-4

pochopenie sa dosiahne vykonaním komplexného hodnotenia rizík s cieľom identifikovať riziká organizácie. Keď sú tieto riziká identifikované, pracovníci organizácie sa musia rozhodnúť, ako ich riešiť. Riadenie rizík je neustály proces identifikácie rizík a implementácie plánov na ich riešenie[17].



Obrázok 1 Demingov cyklus procesu rizika

Zdroj: Bojňanský, J. - Polák, M. Riadenie rizík v informačnej bezpečnosti [online]. In: Bezpečnosť a manažment 2020: zborník vedeckých prác z konferencie. Trnava : AlumniPress, 2020, s. 42-47 [cit. 2023-04-28]. ISSN 2585-7714. Dostupné na: https://preventista.sk/info/riadenie-rizik-v-informacnej-bezpecnosti/

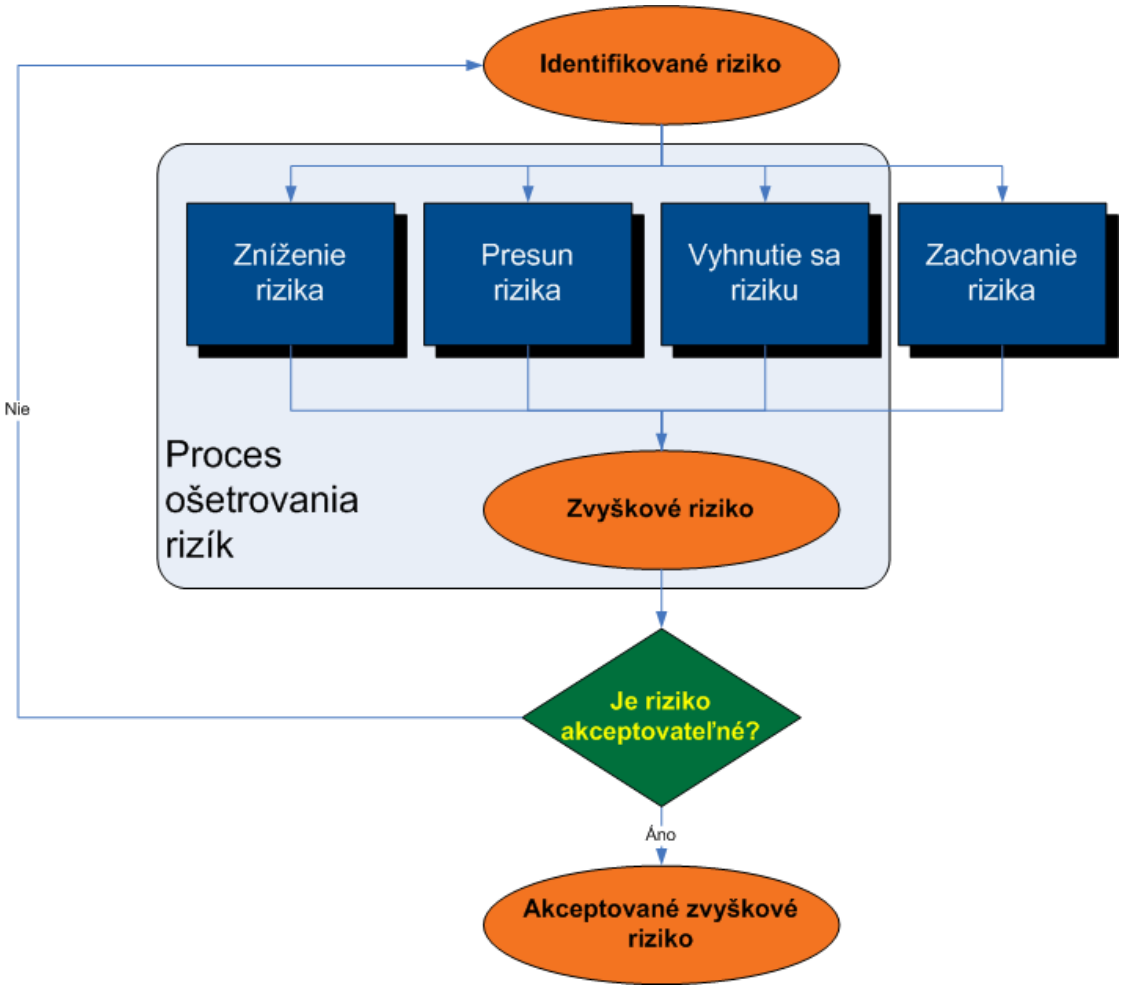
Obrázok znázorňuje Demingov cyklus riadenia IT rizika, ktorý zobrazuje nepretržitý proces správy informačných rizík založenom na štyroch fázach:

- Plánovanie- v tomto kroku sa stanovia ciele a cieľové parametre, určia sa metódy na dosiahnutie týchto cieľov, vyberie sa tím, ktorý bude pracovať na projektov a stanovia sa merateľné ukazovatele výkonu.
- Vykonávanie- plánované akcie a projekty sa uskutočnia. Tím pracuje na zlepšovaní procesov a dosahovaní stanovených cieľov.

[17]ALBERTS, Christopher– DOROFEE Audrey. Managing Information Security Risks: The OCTAVESM Approach [online]. In: Information Security Management Handbook. Boca Raton, FL: CRC Press, 2013, 6. vydanie., kap 14, s. 1-28 [cit. 2023-04-28]. ISBN 0-321-11886-3. Dostupné na: https://books.google.sk/books?hl=en&lr=&id=EGInzsKcG_8C&oi=fnd&pg=PR15&dq=Managing+Information+Security+Risks:+The+OCTAVESM+Approach&ots=qGcU2vGjt6&sig=VyXkLwNKp2PY-Lizp_Tc87mZtzM&redir_esc=y#v=onepage&q=Managing%20Information%20Security%20Risks%3A%20The%20OCTAVESM%20Approach&f=false.

- Kontrolovať- v tomto kroku sa zhromaždia údaje a informácie o dosiahnutom výsledku. Tieto údaje sa porovnajú s cieľmi a parametrami, ktoré boli stanovené v prvom kroku.
- Pôsobenie- na základe získaných poznatkov a údajov sa prijmú opatrenia na zlepšenie procesov a dosiahnutie lepších výsledkov. Tieto opatrenia sa implementujú a celý cyklus sa opakuje.

Riadenie rizík je proces, ktorý identifikuje spôsoby, ako znížiť alebo eliminovať hrozby, ktoré predstavujú potenciálne riziká. Po zhodnotení rizika by sa mal zvoliť najefektívnejší plán liečby rizika, aby sa riziko znížilo na prijateľnú úroveň. Táto metóda by sa mala použiť, pretože umožní výrazné zníženie rizika pri relatívne nízkych nákladoch. Plány liečby rizík zahŕňajú výber a implementáciu rôznych opatrení na zníženie rizika. Takéto opatrenia by mohli zahŕňať vypracovanie pohotovostných plánov pre prípad neočakávaných udalostí, implementáciu procesov na zníženie expozície alebo nákup poistných zmlúv na pokrytie určitých typov strát. Tieto protiopatrenia je možné zaradiť do jednej z kategórií v nasledujúcom obrázku, ktorý znázorňuje ošetrovanie rizika.



Obrázok 2 Ošetrovanie rizika

Zdroj: Preventista.sk - Konštantinides, D. Riadenie rizík v informačnej bezpečnosti [online]. In: Preventista.sk. Bratislava: Preventista, 2021 [cit. 28.04.2023]. Dostupné na: https://preventista.sk/info/riadenie-rizik-v-informacnej-bezpecnosti/

Obrázok znázorňuje ako sa ošetruje riziko v informačnom prostredí. Proces ošetrenia rizík v informačnom prostredí sa zvyčajne skladá z nasledujúcich krokov:

1. Identifikácia rizík: Prvým krokom je identifikácia rizík, ktoré by mohli narušiť bezpečnosť a dôvernosť informačného prostredia. Riziká môžu byť vnútorné (napr. zlým správaním zamestnancov) alebo vonkajšie (napr. útokom hackerov). Je potrebné vyhodnotiť, aké riziká sú najpravdepodobnejšie a aké by mohli mať najzávažnejšie následky.
2. Analýza rizík: Po identifikácii rizík sa vykonáva analýza, ktorá zahrnuje zhodnotenie ich vážnosti, pravdepodobnosti výskytu a dôsledkov. Na základe tejto analýzy sa určia prioritné oblasti, na ktoré by sa mal zamerať ďalší postup.
3. Plánovanie ošetrenia rizík: Na základe identifikácie a analýzy rizík sa pripraví plán, ako by sa tieto riziká mohli ošetriť. Plán by mal zahrňovať rôzne opatrenia, ktoré by

mohli znížiť pravdepodobnosť vzniku rizika a minimalizovať jeho následky. Medzi opatrenia môžu patriť zvýšenie bezpečnosti hesiel, implementácia firemnej politiky v oblasti ochrany súkromia a dát, zabezpečenie prístupu k informáciám len pre oprávnené osoby a podobne.

4. Implementácia plánu: Po pripravení plánu ošetrenia rizík nasleduje jeho implementácia. To zahŕňa implementáciu rôznych opatrení, ktoré boli navrhnuté v predchádzajúcom kroku.
5. Monitorovanie a hodnotenie: Monitorovanie a hodnotenie sú kritické prvky procesu ošetrenia rizík. Musí sa pravidelne kontrolovať, či sú implementované opatrenia účinné a či sú všetky riziká pod kontrolou. Ak sa zistia nové riziká alebo sa zistí, že existujúce opatrenia nie sú účinné, je potrebné vykonať opätovnú analýzu a zopakovať proces.

Celý proces ošetrenia rizík v informačnom prostredí musí byť riadenej a systematický, aby sa zabezpečila ochrana informácií. Podnik by mal postupovať k riadeniu informačných rizík čo najkomplexnejšie a mal by nastaviť taký postup, ktorý by čo najkomplexnejšie zahŕňal informácie o hrozbách. Tento postup by mal počítať s celou organizáciou vrátane personálu, či už informačného oddelenia alebo obchodného. Implementáciou týchto riešení založených na praxi naprieč oddelením informačných technológií a obchodnými líniami môže organizácia začať inštitucionalizovať osvedčené bezpečnostné postupy a urobiť z nich súčasť spôsobu, akým organizácia bežne podniká.

Faktory spôsobujúce riziká sa delia na vonkajšie (externé riziká), takže také, ktoré vznikajú v externom okolo podniku. Podnik nevie ovplyvniť externé rizika a jediné čo môže spraviť, je to, že sa pripraví a včasne na tieto riziká zareaguje. Po externých rizikách nasledujú vnútorné (interné) riziká, vznikajúce vo vnútri organizácie. Tieto riziká je organizácia schopná ovplyvniť a zvládnuť. [18]

[18] BELAN, Ľubomír. Bezpečnostné riziká [online] In: 19. Medzinárodná vedecká konferencia: Riešenie krízových situácií v špecifickom prostredí, Žilina, 2014, s. 8 [cit. 2022-26-01]. Dostupné na: <http://fbiw.uniza.sk/rks/2014/articles/Belan_Belan.pdf>

1.2.1 Ľudské faktory

Ľudské faktory, ktoré predstavujú riziká informačnej bezpečnosti podniku sa viažu na situácie, kedy ľudská chyba ma za následok narušenie údajov alebo bezpečnosti informačných systémov a technológií. Tieto narušenia predstavujú neväčšie riziká a hrozby pre organizácie.

Obsahom tejto kapitoly je priblíženie informácií o súvislostiach medzi typmi incidentov narušenia údajov na základe vzťahu ľudských faktorov k piatim typom incidentov narušenia údajov.

Spoločnosti, chrániace sa proti útokom z externého prostredia, cítia potrebu zabezpečenia, hlavne z dôvodov ochrany množstva údajov a alokujú všetky dostupné zdroje na zabezpečenie týchto dôležitých informačných aktív podniku. Avšak často zabúdajú koncentrovať prostriedky na najzraniteľnejšiu časť informačnej bezpečnosti, a tou je samotný zamestnanec. Útočníci vedia, že ľudia môžu byť najslabším článkom aj v najlepšej prepracovanej informačnej bezpečnosti, a preto investujú veľa úsilia na detekciu čo i najmenšieho ľudského zaváhania alebo neopatrnosti. Uskutočnilo sa mnoho výskumov, ktoré naznačujú ľudské správanie malo na informačnú bezpečnosť negatívny vplyv. Podľa výskumu M. Alotaibiho a spol. „je podstatný kultúrny faktor, teda ľudský faktor, ktorý je pozitívne spojený s ochotou zamestnanca dodržiavať stanovene bezpečnostné postupy.“ [19]

V každej organizácii môže existovať firemná kultúra bez ohľadu na to, či si to zamestnanci uvedomujú alebo nie. Kultúra nemusí byť len organizačná ale aj národná, regionálna a náboženstvo. Štúdie realizované väčšinou na západnej kultúre a ázijskej kultúre naznačujú, že západné organizačné kultúry sú viac individualistické, zatiaľ čo ázijské organizačné kultúry sú skôr kolektívne.[20]

Ďalším ľudským faktorom, ktorý ovplyvňuje informačnú bezpečnosť je osobnosť zamestnanca. Na tento faktor bol tiež uskutočnený výskum na 120 respondentoch, ktorý skúmal vzťahy medzi piatimi osobnostnými črtami (otvorenosť, ústretovosť, extraverzia, svedomitosť, neurotizmus) a dodržiavaním bezpečnostných nariadení. Výskum preukázal, že ústretoví a svedomití používatelia predstavujú najmenšie riziko. Naopak, účastníci, ktorí

[19]ALOTAIBI, Mutlaq – FURNELL, Steven, - CLARKE, Nathan. Information security policies: A review of challenges and influencing factors. [online] *2016 11th International Conference for internet Technology and Secured Transactions (ICITST)*. IEEE, 2016. [cit. 2022-26-01]. Dostupné na: https://ieeexplore.ieee.org/abstract/document/7856729
[20]CROSSLER, Robert E. Future directions for behavioral information security research. [online] *computers & security* 32 (2013): 90-101. [cit. 2022-26-01]. Dostupné na: https://www.sciencedirect.com/science/article/pii/S0167404812001460

boli viac extrovertní a neurotickí, majú často tendenciu porušovať politiku informačnej bezpečnosti.[21]

Z týchto prieskumov vyplynulo, že podniky zaoberajúce sa tým ako vnímajú používatelia informačnú bezpečnosť, tak následne sa aj odráža chybovosť ľudského faktora. Menšia chybovosť sa rovná väčšej informačnej bezpečnosti. Ak používatelia majú jasný obraz o stratégií informačnej bezpečnosti, tým je pozitívnejší vplyv na ochranu informácií. Bezpečnosť je determinovaná viacerými ľudskými faktormi ako informovanosť, znalosti, kontrolovateľnosť, závažnosť správania a rozhodovania. Preto možno považovať za znalosti o konkrétnej doméne a ako takí zamestnanci by mali byť informovaní o najnovších vzorcoch hrozieb a následných bezpečnostných požiadavkách.

Zaujímavé je aj tvrdenie, že medzi ľudské faktory ovplyvňujúce bezpečnosť je aj pohlavie. Veľký počet výskumov sa prikláňa k tvrdeniu, že až 94% interných incidentov majú na svedomí muži, ale niektoré štúdie toto tvrdenie nepodporujú a hovoria, že pomer pohlaví zodpovedných za interné útoky je 50/50 a početná mužská prevaha je len následok početnejšieho mužského zastúpenia v informatickom sektore, ale nedeterminuje sklon k útoku podľa faktoru pohlavie. [22]

Veľmi dôležitá je spokojnosť zamestnanca v podniku, lebo ak je zamestnanec spokojný, tak aj tendencia porušiť informačné zásady bude nižšia. Niektoré štúdie skúmali vzťah medzi spokojnosťou s prácou a konformitou zamestnancov. Empiricky podporili tvrdenie, že spokojnosť s prácou má pozitívny vplyv na dodržiavanie bezpečnostnej politiky. Ich príklady skúmali vplyv pracovnej spokojnosti na rozhodnutia používateľov o dodržiavaní politiky informačnej bezpečnosti a vo svojom teoretickom výskumnom modeli predpokladali, že spokojnosť je pozitívne spojená so zámerom zhody s bezpečnosťou. Výskumný model bol testovaný na 223 účastníkoch prieskumu a výsledky naznačili, že spokojnosť s prácou prispieva k dodržiavaniu bezpečnostnej politiky. Výsledok ďalej zistil silný vzťah medzi zámerom používateľov prispôsobiť sa informačnej bezpečnosti a spokojnosťou s prácou.[23]

---

[21]SHROPSHIRE, Jordan – WARKENTIN, Merrill JOHNSTON, Allen – SCHMIDT, Mark. Personality and IT security: An application of the five-factor model. [online] *AMCIS 2006 Proceedings* (2006): s. 415. [cit. 2022-26-01] Dostupné na: https://aisel.aisnet.org/amcis2006/415/

[22]HANLEY, Michael – DEAN, Tyler - SCHROEDER, Will. *An analysis of technical observations in insider theft of intellectual property cases*. [online] CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST, 2011. [cit. 2022-26-01]. Dostupné na: https://apps.dtic.mil/sti/citations/ADA549391

[23]JOHN, D'Arcy - HOVAV, Anat - GALLETTA, Dennis. User awareness of security countermeasures and its impact on information systems misuse: [online] A deterrence approach." *Information systems research* 20.1 (2009): s 79-98. [cit. 2022-26-01]. Dostupné na: https://pubsonline.informs.org/doi/10.1287/isre.1070.0160

Ako posledný faktor, ktorý môže ovplyvniť informačnú bezpečnosť podniku je tzv. technologická demokracia. Tento pojem podľa C. Collwilla sú „systémy a aplikácie, ktoré sa používajú v práci a doma, sa v priebehu rokov zblížili a prepojili. Aplikácie, ktoré sa používajú v domácom prostredí, sa teraz používajú aj v podnikových systémoch, čo potenciálne predstavuje výzvu pre súčasný stav používania technológií v mnohých organizáciách.“[24] Zamestnanci necítia nebezpečenstvo, keď na zefektívnenie svojej práce prepájajú kontá medzi domácim a podnikovým prostredím. Tieto požiadavky na používanie rôznej škály aplikácií bez rozdielu pracovného alebo domovského prostredia, vedú k zmesi prostredí v ktorom je podnik zraniteľný.

Prostredníctvom nasledujúcich opatrení organizácie dokážu zredukovať risk ohrozenia informačnej bezpečnosti: [25]

- zvyšovanie povedomia zamestnancov o informačnej bezpečnosti organizácie
- zlepšovanie a kontrolovanie používateľských návykov,
- efektívny manažment správy hesiel,
- prijať ošetrenia proti strate alebo krádeži zariadení ako : inštalácia bezpečnostného softvéru na prenosné alebo mobilné zariadenia, monitorovanie správania používateľov, stanovenie jasných a stručných pravidiel používania prenosných alebo mobilných zariadení, šifrovanie a zníženie viditeľnosti do zariadení, ktoré majú prístup do organizačnej siete, segmentácia údajov a softvéru v používateľských zariadeniach, ktoré sú súčasťou organizačnej siete,
- neoprávnený prístup alebo zverejnenie by malo mať jasnú stratégiu riadenia prístupu k kritickým a dôverným informáciám.

Ľudské faktory sú najväčším rizikom pre informačnú bezpečnosť podniku, pretože dokáže byť narušená aj pri najprísnejšom zabezpečení, prostredníctvom interného zásahu. Ak sú ľudia súčasťou procesu ochrany informácií, musí byť vždy zohľadnený ľudský faktor v návrh a implementácií informačno-bezpečnostnej stratégií. Tieto faktory ďalej nasledujú technické faktory, ktoré ak nie sú nakonfigurované, organizácia je veľmi zraniteľná voči externým útokom.

[24]COLWILL, Carl. Human factors in information security: The insider threat–Who can you trust these days? [online] Information *security technical report*. 2009, s. 186-196. [cit. 2022-26-01]. Dostupné na: https://www.sciencedirect.com/science/article/abs/pii/S1363412710000051

[25]LARTEY, Kwesi Hughes. – LI, Meng – BOTCHEY, Francis – QIN, Zhen. Human factor, a critical weak point in the information security of an organization's internet of things [online]. Heliyon, Volume 7, Issue 3, 2021, ISSN 2405-8440, [cit. 2022-26-01]. Dostupné na: https://www.sciencedirect.com/science/article/pii/S2405844021006253

1.2.2 Technické a fyzické faktory

Informačno-bezpečnostné ciele je nemožné dosiahnuť prostredníctvom stratégie, ktorá sa zameriava iba na technickú úroveň stratégie. Je potrebná vyvážená úroveň sociálneho a technického prístupu, ktorý kladie dôležitosť ako sociálno-organizačnej stránke, tak aj v maximálnej možnej miere zdôrazňuje potrebnosť efektívnej bezpečnostnej technológií.

Pri presadzovaní svojich stratégií riadenia rizík musia byť manažéri bezpečnosti zruční v uplatňovaní technológie, ako aj v uplatňovaní mechanizmov organizačnej integrácie a sociálneho zosúladenia, aby sa zabezpečilo, že bezpečnosť informácií je v súlade s obchodnou organizáciou a kultúrou. Vyvážený sociálno-technický prístup povedie k zosúladeniu, ktoré je kľúčové pre uľahčenie konvergentných zámerov, v zdieľanom chápaní a v koordinovaných postupoch medzi informačnou bezpečnosťou a inými organizačnými zložkami. úrovne organizácie na vzájomné posilňovanie poslania, plánov a cieľov informačnej bezpečnosti s podnikom[26].

Technické faktory informačnej bezpečnosti sa vťahujú ako na ochranu personálu, tak aj na hardvéry, softvéry. Pri opise technologických procesov sa vyskytujú pojmy ako ohrozenie alebo riziko. Tieto pojmy na prvý pohľad možno znejú rovnako ale majú odlišný význam.

„**Ohrozenie** je aktívna vlastnosť objektu spôsobiť negatívny jav; je to možnosť aktivovať nebezpečenstvo v konkrétnom čase a priestore, resp. zdroj možného zranenia alebo poškodenia zdravia; tiež označenie všetkých faktorov, ktoré môžu spôsobiť negatívny jav,

Riziko je kvantitatívne a kvalitatívne vyjadrenie ohrozenia, stupeň alebo miera ohrozenia; je to pravdepodobnosť vzniku negatívneho javu a jeho dôsledok, alebo tiež kombinácia pravdepodobnosti a rozsahu možného zranenia alebo poškodenia zdravia v nebezpečnej situácii.“ [27]

Analýzou vzťahu rizika a ohrozenia musíme rozlišovať prostredie, v ktorom sa tieto pojmy používajú. V technických (technologických) procesoch je ohrozenie chápané ako aktivované nebezpečenstvo, ako vývojové štádium nebezpečenstva a riziko predstavuje

[26]AGNES, Hui Chan – VIRGIL, Gligor. Information Security: 5th International Conference, ISC 2002, Sao Paulo, Brazil, September 30 – October 2, 2002: Proceedings ISBN: 9783540442707
[27] ŠIMÁK, Ladislav. Krízový manažment vo verejnej správe. Žilina, 2001. s. 39. ISBN: 80-88829-13-5

mieru, resp. potenciál ohrozenia, je reálnym vyjadrením ohrozenia. Tieto technologické ohrozenia pre technické komponenty, môžeme zhrnúť do siedmych hlavných bodov: [28]

- zlyhanie (výpadok) komponentu,
- chybná činnosť komponentu,
- neštandardné, neočakávané správanie komponentu,
- nekompatibilita súčasne používaných zariadení,
- logická chyba komponentu,
- skrytá chyba komponentu,
- preťaženie komponentu.

Ďalej existuje mnoho úrovní technických rizík komponentov, ktoré môžu ohroziť informačnú bezpečnosť organizácie. Po "offline" rizikách, sa vyskytujú riziká technického charakteru aj vo virtuálnom priestore a tie musia byť technologicky správne nastavené a aktualizované. Ak by nejestvovali ľudské faktory snažiace sa ovplyvniť informačnú bezpečnosť organizácie, nebolo by potreba neustále zvyšovať úsilie v kybernetickej bezpečnosti. Neväčšie technické riziká online priestoru môžeme identifikovať ako problém so zraniteľnosťou, ktorý je asi najrozšírenejším technickým rizikom organizácií. Pri nesprávne nastavených hardvérových a softvérových nástrojoch, útočník môže skrz dobre navrhnuté červy a vírusy prelomiť obrannú líniu systému.

Okrem technických rizík existujú aj fyzické riziká. Rámec fyzickej bezpečnosti sa skladá z troch hlavných komponentov: kontrola prístupu , dohľad a testovanie. Úspech programu fyzickej bezpečnosti organizácie možno často pripísať tomu, ako dobre je každý z týchto komponentov implementovaný, vylepšený a udržiavaný.[29]

- Kontrola prístupu je dôležitým opatrením na maximalizáciu fyzickej bezpečnosti. Zahŕňa používanie fyzických bariér, ako sú zámky, ploty, steny, dvere a ID skenery, ako aj sofistikovanejšie metódy, ako sú mikročipy NFC vložené pod kožu. Tieto kontroly prístupu pôsobia ako odstrašujúce prostriedky

[28]BARTEK, Alojz. Bezpečnostné prostredie a faktory bezpečnosti [online]. 1. vydanie. Žilina: Strix et SSŽP, 13. september 2018. s. 8. [cit. 2022-26-01]. ISBN 978-80-89753-27-7. Dostupné na: https://www.sszp.eu/wp-content/uploads/2018_conference_IBP__p-75__BartekA_Bezpe%C4%8Dnostn%C3%A9_prostredie_f4e.pdf
[29]PELTIER, Thomas. Information Security Risk Analysis [online]. 2. vydanie. Boca Raton: CRC Press, 2005, [cit. 2022-26-01]. ISBN 0-8493-3346-6. Dostupné na: https://books.google.sk/books?hl=en&lr=&id=n8Z1RDjEKa0C&oi=fnd&pg=PR7&dq=information+security+risks&ots=Sajot89E0Y&sig=2hX8IvOLfGa9D5bUl1VWDu856No&redir_esc=y#v=onepage&q=information%20security%20risks&f=false

pred vstupom zločincov, pomáhajú overovať totožnosť jednotlivcov vstupujúcich do zariadení a vychádzajúcich z nich a zvyšujú čas, ktorý musia organizácie reagovať na potenciálne hrozby.

- Dohľad je dôležitým komponentom fyzickej bezpečnosti, ktorý používajú organizácie na monitorovanie aktivity v reálnych lokalitách a zariadeniach. Tento typ zabezpečenia zvyčajne zahŕňa kamery, hliadkovú stráž, tepelné senzory a oznamovacie systémy. Kamery sú obzvlášť cenné, pretože dokážu zaznamenať kriminálne správanie a môžu byť použité na odstrašenie potenciálnych hrozieb.
- Testovanie fyzickej bezpečnosti je nevyhnutné pre každú organizáciu. Požiarne cvičenia sú kľúčovou zložkou, ktorá pomáha koordinovať veľké skupiny a precvičovať úlohy a zodpovednosti. Testovanie by sa malo vykonávať pravidelne, aby sa zabezpečilo, že zásady a postupy budú účinné. Správne testovanie pomáha identifikovať a reagovať na hrozby a zabrániť incidentu. Zabezpečuje tiež jednotu organizácie a minimalizuje pravdepodobnosť chýb. Testovanie je dôležitým preventívnym opatrením a nástrojom reakcie, ktorý by všetky organizácie mali brať vážne.

Fyzická bezpečnosť môže mať mnoho podôb a podôb. Stratégie, bariéry a techniky, ktoré organizácie používajú na podporu všeobecnej bezpečnosti fyzických informačných technológií, sa výrazne líšia od tých, ktoré sa používajú na zabezpečenie fyzickej bezpečnosti informácií.

1.3 Manažment informačnej bezpečnosti v podniku

Manažment informačnej bezpečnosti sa skladá z dvoch častí. Čo je informačná bezpečnosť sme si už zhrnuli v prvej kapitole. Druhá časť je manažment.

„Mimoriadne významným subsystémom organizácie je manažment, ktorý zodpovedá za usmerňovanie a koordinovanie ostatných subsystémov. Práve manažment má s nimi a prostredníctvom nich dosahovať ciele organizácie v meniacom sa prostredí. Jeho úlohou je zabezpečiť plnenie cieľov pri efektívnom používaní obmedzených zdrojov.“[30]

Sedlák ďalej definuje manažment ako „interdisciplinárny vedný odbor a patrí medzi praxeologické disciplíny. Zaoberá sa riadením ako cieľavedomou činnosťou ľudí a jeho

[30]SEDLÁK, Mikuláš. Základy manažmentu. Wolters Kluwer (Iura Edition), 2012, 330 s. ISBN 9788080784553.

poslaním je vytvoriť metodológiu riadenia s dôrazom na dosiahnutie efektívnosti tejto činnosti vo vzťahu k vopred určenému cieľu.“[31]

Informačná bezpečnosť ako taká, sa za posledné desaťročia rozšírila do každej organizačnej zložky podnikov. Z počiatočnej technickej iniciatívy, tiež označovanej ako IT bezpečnosť sa začala vyvíjať do nových foriem výziev pre podniky. Počiatočná výzva chrániť dôležite informačné aktíva podniku sa pretransformovali do výzvy ponúknuť podniku obchodné výhody voči konkurencií a uľahčovať kontrolovanie zdieľaných informácií a riadenie rizík v rizikových podmienkach podnikového prostredia. Tento vývoj znamená, že informačná bezpečnosť ako koncept, sa rozvinul do šírky aj hĺbky.

Manažment informačnej bezpečnosti opisuje skupina zahraničných autorov ako „proces správy ľudí, politík a programov s cieľom zabezpečiť kontinuitu operácií pri zachovaní strategického súladu s organizačným poslaním“.[32] V ideálnom prípade by sa aktivity riadenia informačnej bezpečnosti mali riadiť organizačnými cieľmi, aby sa na bezpečnosť nevynakladali zbytočné zdroje. „Historicky sa riadenie informačnej bezpečnosti zaoberalo výlučne zavedením technických a fyzických kontrol. Avšak rastúce používanie, hodnota a závislosť od počítačových systémov na podporu operácií v reálnom svete zvýšili dôležitosť začlenenia procesných a organizačných otázok do riadenia bezpečnostných rizík.“[33]

Ďalšia citácia uvádza, že informačný manažment je „disciplína pri vytváraní kompromisov v nepretržitej činnosti: kontroly v systéme verzus kontroly v prostredí, kontrola bezpečnosti verzus pohodlie a produktivita zákazníka, silné kontroly verzus implementácia a administratívne náklady atď..“[34]

V skratke teda môžeme definovať manažment informačnej bezpečnosti ako manažment, ktorý rieši problémy súvisiace s informačnou bezpečnosťou. Ako pri každom druhu manažmentu aj pri manažmente informačnej bezpečnosti je potrebné zaviesť určitý systém riadenia bezpečnosti. Tento systém je definovaný ako „systém riadenia informačnej

[31]SEDLÁK, Mikuláš. Základy manažmentu, Bratislava : Edičné stredisko EU , 1994. - 253 s, 1. vyd. ISBN: 80-225-0591-9.

[32]CAZEMIER, Jacques – OVERBEEK, Paul– PETERS, Louk. Security Management (IT Infrastructure Library Series), UK: Stationery Office, 1. január 2000, 124 s. ISBN 978-0113300143.

[33]BLAKELY, Bob – MCDERMOTT, Ellen – GEER, Dan. Information Security is Information Risk Management, Proceedings of the 2001 Workshop on New Security Paradigms [online]. (Cloudcroft, NM, Sept. 10-13), New York: ACM Press, s. 97-104. [cit. 2022-26-01]. Dostupné na: https://www.nspw.org/papers/2001/nspw2001-blakley.pdf

[34]ABRAMS, M. – JAJODIA, S. – PODELL, H.. Information Security: An Integrated Collection of Essays. 1. vydanie. IEEE Computer Society Press, Los Alamitos, CA, USA, 1995. s .98-99. ISBN 978-0-7923-7389-6.

bezpečnosti (ang. Information Management System, ISMS), používaný na vytvorenie a udržiavanie bezpečného informačného prostredia. Bezpečnostný systém musí riešiť implementáciu a údržbu procesov a postupov na riadenie bezpečnosti informačných technológií. Tieto akcie zahŕňajú identifikáciu potrieb informačnej bezpečnosti, implementáciu stratégií na splnenie týchto potrieb, meranie výsledkov a zlepšovanie stratégií ochrany a systému riadenia informačnej bezpečnosti v priebehu času.“[35]

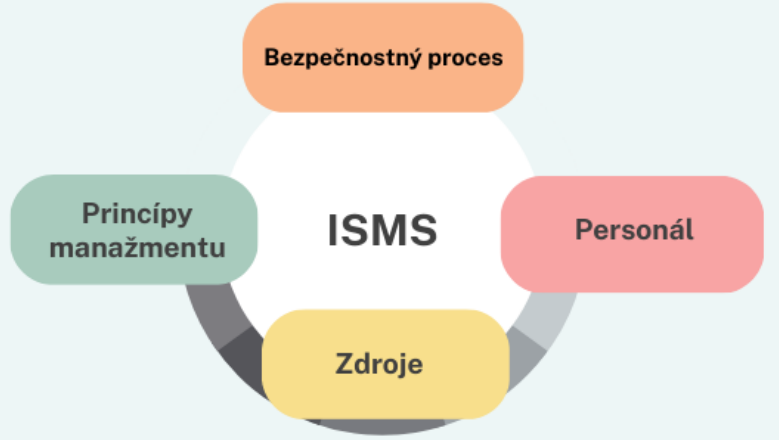
Treba pamätať na to, že manažment informačnej bezpečnosti nie je iba výhradne manažérskeho charakteru ale aj technického. Tieto skutočnosti treba kombinovať v správnej miere a zvažovať ich na najvyššej úrovni riadenia pri príprave stratégií s akými sa pristupuje k politike informačnej bezpečnosti podniku.

1.3.1 Bezpečnostná politika podniku

Všetky politiky, ktoré zahŕňa systém riadenia bezpečnosti v podniku sa týkajú riadenia s cieľom dosahovať ciele. Bezpečnostná politika by mala špecifikovať nástroje a metódy, použiteľné pre strategické manažovanie úloh informačnej bezpečnosti ako plánovanie, adaptácia, implementácia, dohľad a zlepšovanie. Základne komponenty informačného systému bezpečnosti sú:

- Zásady riadenia
- Zdroje
- Personál
- Proces informačnej bezpečnosti

[35]ELOFF, Jan – ELOFF, Mariki. Information Security Management – A New Paradigm [online]. 1. vyd. s. 130-136. [cit. 2022-26-01]. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf



Obrázok 3 Komponenty systému riadenia informačnej bezpečnosti (ISMS)
Zdroj: Vlastné spracovanie podľa: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

Správna kombinácia a integrácia prvkov manažmentu informačnej bezpečnosti je zobrazená na obrázku 3. Obrázok zobrazuje komponenty manažmentu informačnej bezpečnosti.

Obrázok 4 Stratégia informačnej bezpečnosti ako centrálny komponent ISMS
Zdroj: Vlastné spracovanie podľa: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

Organizácia informačnej bezpečnosti a bezpečnostná politika sú nástroje, ktoré manažment používa na implementáciu svojej bezpečnostnej stratégie. Obrázok 4 znázorňuje stratégiu informačnej bezpečnosti ako centrálny komponent systému riadenia informačnej bezpečnosti (ISMS).

Obrázok 5 Implementácia stratégie informačnej bezpečnosti pomocou politiky informačnej bezpečnosti a organizácia pre bezpečnosť informácií

Zdroj: Vlastné spracovanie podľa: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

Obrázok 5 zobrazuje implementáciu stratégie bezpečnosti pomocou politiky informačnej bezpečnosti a organizácie informačnej bezpečnosti. Ústredné body bezpečnostnej stratégie sú zdokumentované v politike informačnej bezpečnosti. Politika informačnej bezpečnosti má prvoradý význam, pretože obsahuje vizuálny záznam záväzku riadiacej úrovne k svojej stratégii.[36]

Dynamika politiky informačnej bezpečnosti, ktorú aplikuje manažment sa rozdeľuje do štyroch bodov: [37]

- plánovanie,
- implementácia plánu a realizácia projektu,
- kontrola a monitorovanie výkonnosti dosiahnutie cieľov,
- odstránenie zistených nedostatkov a optimalizácia menších nedostatkov.

[36]BSI. BS 100-1:2013. Information technology. IT baseline protection. Part 1: Overview and concepts [online]. Berlin : Federal Office for Information Security, 2013 [cit. 2023-03-22]. Dostupné na: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile

[37]ASHENDEN, Debi. Information Security management: A human challenge? [online]. Department of Informatics & Sensors, Cranfield University, Seindon SN6 8LA, UK, 2008. s. 195-201. [cit. 2023-03-22]. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/spring2014/paper1.pdf

Vďaka politike informačnej bezpečnosti, ktorú uplatňuje manažment, je možná konfigurácia zdrojov pre riadenie informačnej bezpečnosti, ktoré ma organizácia k dispozícií. Ak je politika správne orientovaná na opakovateľný a kontrolovateľný prístup, tak jej význam môžeme zhrnúť do niekoľkých výhod plynúcich pre podnik:

- je možné zdôvodniť požiadavky na rozpočet a zdroje a poskytuje logicky prehľad na podporu rozhodovania vyššieho manažmentu,
- širšie organizačné príspevky na informačnú bezpečnosť sa preukážu v efektívnosti podnikania, dosahovania súladu s predpismi, ochrany značky, reputácie, v správe a spracúvaní vlastných informácií atď.
- zapojenie rozhodovacích orgánov do formulovania obchodných aspektov informačnej bezpečnosti.
- systematický prístup k analýze a zaobchádzaniu s informačnými rizikami, k implementácii bezpečnostných kontrol, k meraniam, monitorovaniu a preskúmaniu týchto kontrol.
- postupy a kontrolná pozíciu, ktorá umožňuje inteligentnú diskusiu s akcionármi a regulačnými orgánmi
- napokon prispieva k pokračujúcemu rozvoju informačnej bezpečnosti ako profesie.

Význam politiky v podniku, ktorú uplatňuje manažment informačnej bezpečnosti je, že táto úroveň riadenia v podniku zohráva dôležitú úlohu, pokiaľ ide o informačnú bezpečnosť. Zodpovedá za celkovú úroveň informačnej bezpečnosti, integruje informačnú bezpečnosť do všetkých procesov a projektov. Prostredníctvom implementácií manažment informačnej bezpečnosti aktívne iniciuje, riadi a dohliada na bezpečnostný proces, stanovuje dosiahnuteľné ciele, porovnáva náklady na bezpečnosť. Zabezpečuje tým správne využívanie dostupných zdrojov a vážnosť informačnej bezpečnosti, ktoré sú ale ovplyvňované rôznymi normami a predpismi.

1.3.2 Výzvy manažmentu informačnej bezpečnosti

Po opísaní hlavného významu manažmentu informačnej bezpečnosti podniku, sa v tejto kapitole pozrieme na výzvy riadenia informačnej bezpečnosti. Už bolo spomenuté, že správna konfigurácia štruktúry informačných procesov s rozhodovacími organmi v podniku je kriticky dôležitá. V kapitole 1.3.2. sa zameriame na výzvy, vyplývajúce z konfigurácií štruktúr, procesov, hraníc a ako jedna z najdôležitejších výziev, správna konfigurácia vzťahov.

Štrukturálne, procesné a hraničné výzvy pre manažment informačnej bezpečnosti v 21. storočí, znamená nutnosť adaptácie podniku v stále sa meniacom podnikateľskom prostredí. Pomyselné hranice, čo kedysi existovali sa vplyvom globalizácie strácajú, a preto by sa nemala bezpečnosť riešiť individuálne, ale prostredníctvom partnerstiev a externých vzťahov. Ako následok týchto aliancií môže byť vytvorenie plochejších organizačných štruktúr, ktoré si vyžadujú decentralizáciu dôvery a rozhoduje sa o riziku na nižšej, individuálnej úrovni. Tieto problémy ďalej komplikuje aj potreba integrovať rôzne tímy a rôznych jednotlivcov.

Na prevádzkovej úrovni je riadenie manažmentu informačnej bezpečnosti sťažené nedostatkom odborných znalostí a neustále sa meniacou obchodnou dynamikou (fúzie, akvizície, atď.). Na udržanie rizika informácií na prijateľnej úrovni musia organizácie často zvýšiť konektivitu a byť flexibilné pri používaní nových technológií. To by mohlo zahŕňať zdieľanie údajov so zákazníkmi a zainteresovanými stranami v rámci hodnotového reťazca.

Výzvy ľudských faktorov sú asi najväčšou výzvou manažmentu informačnej bezpečnosti. Ako sme už uviedli v kapitole 1.2.1. ľudské faktory zohrávajú v informačnej bezpečnosti najzásadnejšiu rolu. „Hovorí sa, že hackeri trávia viacej času zvažovaním ľudských výziev ako odborníci na informačnú bezpečnosť.“[38] V nasledujúcej časti rozoberieme, prečo je ťažké riadiť ľudí v kontexte informačnej bezpečnosti a aké zručnosti by mali manažéri pre informačnú bezpečnosť rozvíjať.

1. Zmena organizačnej kultúry: „výskumníci už nejaký čas poukazujú, že riadenie informačnej bezpečnosti je viac než len o zámkoch a kľúčoch a musí súvisieť so sociálnym zoskupením a správaním.“[39] Výskumníci zdôrazňujú potrebu,

[38] ADAMS, Anne – SASSE, Angela. Users are not the Enemy [online]. Communications of the ACM. December 1999, s. 40-46. [cit. 2023-03-22]. Dostupné na: https://www.researchgate.net/publication/220427273_Users_Are_Not_the_Enemy
[39]DHILLON, Gurpreet – BACKHOUSE, James. Current directions in IS security research: towards socio-organizational perspectives [online]. Information Systems Journal, 20 december 2001, s. 127-153. [cit. 2023-03-22]. Dostupné na: https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2575.2001.00099.x

lepšie pochopiť sociálne a ľudské aspekty organizácií. Ľudia sú ovplyvniteľný vo svojej konzistentnosti správania a aj vo svojich pocitoch. Tento mix organizačnej úlohy a osobnej identity formuje organizačnú kultúru. Koncoví používatelia nemusia mať správne nastavené hodnoty na nakladanie s informáciami, čo mohlo prispieť k incidentom pri manipulácii s údajmi. Je jasné, že organizačná kultúra má v týchto prípadoch veľkú úlohu. Hoci je možné zmeniť pozorovateľné správanie, je nepravdepodobné, že sa manažment informačnej bezpečnosti, dokáže dostať pod kožu jednotlivca, aby zmenili jeho postoje a vnímanie. Technológia a procesy nemusia postačovať na ochranu informácií a zabezpečenie správneho spracovania údajov.

2. Rozvoj osobnosti manažéra informačnej bezpečnosti je veľmi podstatný faktor ako predchádzať riziku úniku informácií z interného prostredia podniku. Nie je fér viniť z bezpečnostných problémov výlučne koncového používateľa, pretože správne riadenie bezpečnosti si vyžaduje zapojenie procesov a aj ľudí v rámci organizácie. Manažéri informačnej bezpečnosti môžu mať technické vzdelanie, ktoré ich vedie k tomu, aby robili rozhodnutia s veľmi malým ohľadom na zamestnancov. Na rozvoj účinných bezpečnostných postupov je preto potrebná kolektívna akcia všetkých zúčastnených. „Manažéri informačnej bezpečnosti by sa stále viac mali pokúšať nahradiť prístup k riadeniu kolegiálnejším štýlom. To znamená byť videný ako pomoc koncovým používateľom a diskutovať a preberať rozhodnutia o širších otázkach riadenia informačnej bezpečnosti aj s nižšou úrovňou riadenia. Bohužiaľ, výskum ukázal, že to tak nie je.“ [40] Manažéri informačnej bezpečnosti zápasia s úlohou zaujatia postoja medzi kontrolným alebo kolaboratívnym postojom. Pri druhom postoji je väčšia možnosť výskytu chýb ale na druhej strane, manažér dokáže odhaliť nespokojnosť alebo nové nápady zamestnancov.
3. Efektívna komunikácia je nástroj na zabezpečenie správneho využitia zdrojov na udržanie informačnej bezpečnosti. Závisí od toho, ako sú zmeny riadené a ako sú odkomunikované s ľuďmi, ktorý s nimi prichádzajú do kontaktu v rámci spoločnosti. Medzi neefektívnu komunikáciu môžeme označiť aj snahu

[40]ASHENDEN, Debi. Information Security management: A human challenge? [online]. Department of Informatics & Sensors, Cranfield University, Seindon SN6 8LA, UK, 2008. s. 195-201. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/spring2014/paper1.pdf

manažérov informačnej bezpečnosti, snažiacich sa ovplyvniť a prinútiť manažérov na vrcholnej úrovni, aby pochopili dôležitosť témy ako je informačná bezpečnosť v podniku. Často sa považuje za technickú záležitosť a je delegovaná a aj riadená iba technickým personálom. To má nepriaznivý vplyv, pretože sa tým vymyká z oblasti podnikania. Najnovšie trendy teraz vyžadujú, aby tí, ktorí sú na vrchole, venovali pozornosť informačnej bezpečnosti, a aby si organizácie ako celok, začali uvedomovať nevyhnutnosť riadenia informačnej bezpečnosti. Stále však existuje veľa organizácií, v ktorých je informačná bezpečnosť čisto technickou oblasťou, a dokonca aj v tých, ktoré ju berú vážne, stále existuje priepasť medzi manažmentom a technickým oddelením informačnej bezpečnosti. [41]

Na záver môžeme zhrnúť, že manažment informačnej bezpečnosti je komplexná oblasť a čelí mnohým ľudským výzvam, ktoré je potrebné riešiť, aby sa zabezpečil úspech organizácie. Tieto výzvy sa týkajú riadenia jednotlivcov a ich identity, ako aj riadenia zdrojov a vzťahov. Aby boli manažéri informačnej bezpečnosti úspešní, musia rozvíjať svoje komunikačné schopnosti a stať sa bojovníkmi za zmenu, aby vytvorili efektívnejšiu identitu manažéra informačnej bezpečnosti. To im umožní lepšie riadiť zdroje a vzťahy potrebné na dosiahnutie cieľov informačnej bezpečnosti a v konečnom dôsledku prispieť k úspechu organizácie.

[41]ASHENDEN, Debi. Information Security management: A human challenge? [online]. Department of Informatics & Sensors, Cranfield University, Seindon SN6 8LA, UK, 2008. s. 195-201. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/spring2014/paper1.pdf.pdf

2 Cieľ práce

Cieľom tejto práce je posúdiť zavedené normy informačnej bezpečnosti v podniku a realizovateľnosť implementácie novej smernice o informačnej bezpečnosti NIS2 (The Network and Information Security) v rámci spoločnosti. Táto norma zavádza nové bezpečnostné požiadavky pre organizácie zamerané na zlepšenie odolnosti a bezpečnosti sieťových a informačných systémov v celej Európskej únií. Tento cieľ praktickej časti diplomovej práce, bude pozostávať zo zhodnotenia vplyvu normy NIS2 na praktiky informačnej bezpečnosti v malej organizácií. Konkrétne na zmenu existujúcich, už zavedených noriem informačnej bezpečnosti tak, aby boli v súlade s novou normou NIS2. Je nevyhnutné posúdiť potencionálne prínosy, náklady a výzvy implementácie novej normy v rámci podniku. Účelom zmeny a doplnenia starých noriem na novú normu NIS2 je zlepšiť postupy v oblasti bezpečnosti informácií a zlepšiť schopnosť organizácií chrániť citlivé údaje. Ciele implementácie normy zahŕňajú zvýšenie bezpečnosti informačného systému, zabezpečenie súladu s predpismi, ochranu kritickej infraštruktúry, zlepšenie schopnosti reakcie na incidenty a zvýšenie dôvery zákazníkov. Dosiahnutím cieľov môžu organizácie zmierniť riziká kybernetických útokov a zaistiť bezpečnosť a súkromie svojich údajov. Ako čiastkové ciele sme určili:

1. Analyzovať existujúce postupy informačnej bezpečnosti: na implementáciu normy NIS2 je nevyhnutné najprv pochopiť súčasné praktiky informačnej bezpečnosti v danej organizácii. Bude vykonaná komplexná analýza existujúcich postupov podniku v oblasti bezpečnosti informácií vrátane riadenia rizík, hlásenia incidentov a bezpečnostných požiadaviek pre kritickú infraštruktúru. Táto analýza identifikuje potenciálne riziká a slabé miesta, ktoré by mohli ovplyvniť bezpečnosť informačných systémov a údajov pre implementáciu smernice NIS 2.
2. Vytvorenie implementčného rámca: na základe zistení analýzy sa vyvinie prispôsobený rámec, ktorý zosúladí súčasné zavedené postupy informačnej bezpečnosti s normou NIS2. Tento rámec bude zahŕňať vývoj a implementáciu nových bezpečnostných kontrol na zmiernenie identifikovaných rizík a slabých miest. Rámec bude navrhnutý tak, aby vyhovoval špecifickým potrebám malej organizácie a zároveň zabezpečil súlad s normou NIS2.
3. Implementácia nového rámca: Ďalší čiastkový cieľ práce bude zahŕňať implementáciu nového rámca. To bude zahŕňať školenie zamestnancov o nových

praktikách informačnej bezpečnosti, aktualizáciu zásad a postupov a implementáciu nových bezpečnostných kontrol.

V skratke je účelom práce analyzovať existujúce praktiky informačnej bezpečnosti v organizácií, vytvoriť prispôsobený rámec, implementovať nový rámec a vyhodnotiť jeho účinnosť. Výsledky tohto výskumu pomôžu pri vývoji nových zásad a postupov na zlepšenie pozície podniku v oblasti bezpečnosti informácií a lepšiu ochranu údajov klientov organizácie. Metódy a pracovné postupy, ktoré boli v tejto práci uplatnené, sú prezentované v nasledujúcej kapitole.

3 Metodika práce a metódy skúmania

Táto kapitola popisuje metodiku a metódy skúmania, ktoré budú použité v rámci diplomovej práce. Kapitola sa skladá z troch podkapitol, ktoré zahŕňajú charakteristiku objektu skúmania, použité metódy a pracovné postupy a spôsoby získavania údajov a ich zdroje.

3.1 Charakteristika objektu skúmania

V kapitole 3.1 sa zameriame na charakteristiku objektu skúmania, teda na podnik, ktorým sa v našej diplomovej práci zaoberáme. V súlade s podmienkou anonymity firmy, nebudeme spomínať jej názov. Avšak, môžeme využiť informácie dostupné na finančnej analýze z portálu Finstat.sk, ktoré nám poskytujú pomerne podrobný obraz o podniku.

Na základe dostupných informácií sa jedná o podnik pôsobiaci v oblasti konzultačných a stavebných služieb v sektore verejného obstarávania. Podnik zamestnáva 15 zamestnancov a je založený v právnej forme podnikania s.r.o.. Podnik podľa finančných ukazovateľov vykazuje stabilný a rastúci trend v posledných rokoch, s celkovými tržbami dosahujúcimi približne 150 000 EUR v roku 2019, 250 000 EUR v roku 2020 a v roku 2022 170 000 EUR.

Vzhľadom na oblasť pôsobenia, teda konzultačné a stavebné služby v sektore verejného obstarávania, tak objektom našej analýzy bude predovšetkým informačný systém podniku a jeho prevádzkové a bezpečnostné opatrenia. Tento informačný systém je pre podnik kritický a je potrebné mu venovať dostatočnú pozornosť v oblasti informačnej bezpečnosti.

Organizácia spadá do triedy malých podnikov, preto implementácia novej smernice nemusí byť až tak potrebná, lebo táto smernica sa uplatňuje na stredné a veľké podniky. Avšak, spoločnosť spolupracuje so štátnou správou na kriticky dôležitých projektoch pre štát, ako diaľnice, tunely, verejné budovy. Taktiež, prichádza do styku s utajovanými informáciami pri súdnych sporoch, kde ako konzultačná firma zastupuje štát ako objednávateľa, proti zhotoviteľom. Preto podnik spadá pod pôsobenie spomínanej smernice podľa článku 2, odseku 2 smernice NIS 2 body:

a) služby poskytujú: ii) poskytovatelia dôveryhodných služieb;

b) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv.

Na základe tejto charakteristiky podniku a jeho činnosti budeme v nasledujúcich podkapitolách popisovať použité metódy a postupy, ako aj spôsoby získavania údajov, potrebných na náš výskum v oblasti informačnej bezpečnosti.

3.2 Použitie metódy a pracovné postupy

Pri realizácii tejto diplomovej práce boli použité metódy a pracovné postupy, ktoré umožnili efektívne dosiahnuť hlavný ale aj stanovené čiastkové ciele. Zmixovali sme kombináciu kvantitatívnych a kvalitatívnych metód skúmania. Kvantitatívne metódy budú použité na zhromaždenie štatistických údajov o používaní informačných technológií, zabezpečení a ochrany informácií v rámci spoločnosti. Kvalitatívne metódy budú použité na zhromaždenie podrobných informácií o fungovaní spoločnosti, vnútorných procesoch a postupoch.

V prvom rade sme sa zamerali na zhromaždenie relevantnej literatúry a zdrojov, ktoré sa týkajú implementácie informačnej bezpečnosti v podnikoch a noriem, ktoré sú s tým spojené.

Veľmi dôležitá metóda, ktorá bola použitá, bola analýza súčasnej infraštruktúry podniku v oblasti informačnej bezpečnosti. Táto analýza zahŕňala skúmanie aktuálnej konfigurácie sieťových zariadení, skúmanie zabezpečenia fyzických zariadení a podobne.

Následne sme použili metódu komparatívnej analýzy, ktorá umožnila porovnať staré normy, ktoré sú zavedené v podniku, s novou normou NIS 2. Táto metóda nám umožnila identifikovať oblasti, ktoré vyžadujú aktualizáciu a doplnenie na základe nových požiadaviek smernice NIS 2.

3.3 Spôsoby získavania údajov a ich zdroje

V tejto kapitole sú uvedené spôsoby získavania údajov a ich zdroje v súvislosti s predmetom skúmania, konzultačnou a stavebnou spoločnosťou v oblasti informačnej bezpečnosti.

Hlavnými zdrojmi údajov boli rozhovory s kľúčovými zamestnancami a manažmentom spoločnosti. Tieto rozhovory boli realizované osobne v rámci spoločnosti vďaka tomu, že jeden z autorov je zamestnancom firmy. Rozhovory boli štruktúrované a zamerané na nasledovné témy:

- organizačná štruktúra a riadenie informačnej bezpečnosti v spoločnosti,
- identifikácia kritických oblastí informačnej bezpečnosti a ich riešenie,

- procesy správy rizík a riešenie incidentov v oblasti informačnej bezpečnosti,
- plánovanie a realizácia bezpečnostných opatrení,
- zabezpečenie dodržiavania bezpečnostných požiadaviek a noriem v spoločnosti.

Okrem rozhovorov boli využité aj interné dokumenty spoločnosti, ako napríklad politiky a postupy v oblasti informačnej bezpečnosti a dokumentácia o plnení požiadaviek normy ISO 27001. Tieto dokumenty boli poskytnuté manažmentom spoločnosti na požiadanie a slúžili ako dôležitý zdroj informácií o fungovaní systému informačnej bezpečnosti v spoločnosti.

Bola vykonaná aj analýza existujúcich bezpečnostných opatrení a technológií v spoločnosti, ako aj skúmanie informácií o bezpečnostných incidentoch v minulosti.

Všetky získané údaje boli spracované a analyzované s cieľom identifikovať nedostatky v oblasti informačnej bezpečnosti a navrhnúť vhodné opatrenia na zlepšenie a zabezpečenie súladu s požiadavkami normy NIS 2.

4 Výsledky práce

V tejto kapitole praktickej časti diplomovej práce sa zameriame na to, aké informačné normy existujú v Slovenskej a republike ale aj eurozóne. Popíšeme presný popis konkrétnych krokov, ktoré sme vykonali v rámci implementácie novej smernice NIS 2 do malého podniku. V predchádzajúcich kapitolách sme sa zameriavali na teoretické aspekty, ktoré sa týkajú informačnej bezpečnosti a jej smernicami. V tejto časti diplomovej práce sa ale zaoberáme praktickou stránkou tejto témy a popisujeme, ako sme postupovali pri implementácií novoprijatej smernice do reálneho prostredia malého podniku.

Ďalej predstavíme výsledky analýzy súčasného stavu informačnej bezpečnosti podniku a identifikáciu požiadaviek, ktoré vykonáme v prvých krokoch projektu. Hlavným zameraním bude správne zhodnotenie existujúcich postupov a systémov na riadenie informačnej bezpečnosti v malom podniku, ako aj analýzu zákonov a smerníc, ktoré sa týkajú informačnej bezpečnosti a ich porovnanie s novými požiadavkami uplatňujúcich sa na novu normu NIS 2. Následne opíšeme opatrenia, ktoré sme navrhli a implementovali v malom podniku na zlepšenie ochrany informácií a zabezpečenie súladu s novými požiadavkami.

V tejto kapitole budeme taktiež prezentovať konkrétne výsledky projektu a ukážeme, ako sme pomocou vhodných opatrení zabezpečili ochranu informácií a súlad s novými požiadavkami smernice NIS 2 v malom podniku. Tieto výsledky môžu byť nápomocné aj pre iné malé a stredné podniky, ktoré sa chystajú implementovať novú smernicu NIS 2, podľa posledného platného návrhu Európskej komisie, schválenia Európskym parlamentom a prijatím radou EÚ.

4.1 Informačná bezpečnosť v SR a EÚ

Informačná bezpečnosť sa dotýka každého kľúčového odvetvia v Slovenskej republike alebo v Európskej únií, či sa už jedná konkrétne o dopravu, energetiku, zdravotníctvo a financie. Tieto odvetvia sa každým rokom stávajú závislejšie na digitálnych technológiách. Tie síce prinášajú so sebou mnohé príležitosti a výhody, zároveň je hospodárstvo vystavené kybernetickým hrozbám. Útoky na informačnú bezpečnosť eurozóny sa neustále zvyšujú a tento trend bude ďalej pokračovať, keďže do konca roka 2025 bude na celom svete pripojených až 41 miliardy zariadení. Európska únia novými smernicami a nariadeniami neustále posilňuje odolnosť EÚ voči informačným hrozbám. Hlavnou úlohou týchto

smerníc a ich aktualizácií je zabezpečenie kybernetickej bezpečnosti, aby všetky subjekty mohli využívať digitálne nástroje v čo najväčšej miere bez obmedzení. V nasledujúcej kapitole si rozoberieme čo sú štandardy informačnej bezpečnosti a na čo slúžia.

4.1.1 Štandardy informačnej bezpečnosti pre manažment v podniku

Všeobecnou definíciou pre štandardu informačnej bezpečnosti, zverejnenej na slovenskom portáli informatizácia.sk je „štandardy sú nástrojom pre zavádzanie a udržiavanie interoperability informačných systémov a využívania informačno-komunikačných technológií.“[42]

V zmysle pôvodného znenia zákona č. 275/2006 Z. z. o informačných systémoch verejnej správy sú štandardy definované nasledovne: „Štandardom je súbor pravidiel spojených s vytváraním, rozvojom a využívaním informačných systémov verejnej správy, ktorý obsahuje charakteristiky, metódy, postupy a podmienky, najmä pokiaľ ide o bezpečnosť a integrovateľnosť s inými informačnými systémami. Štandardy musia byť otvorené a technologicky neutrálne."[43]

Štandardy sú pravidlá, ktoré musia zo zákona spĺňať všetky informačné systémy verejnej správy (IS VS). IS VS sú napr. rôzne registre, systémy slúžiace na zabezpečenie výkonu verejnej správy atď. Štandardy nie sú iba technické normy (napr. STN), ale aj rôzne smernice, postupy a podobne.[44]

Normy predstavujú konsenzus súčasných osvedčených postupov a poskytujú organizáciám vzor na vybudovanie a implementáciu systému riadenia informačnej bezpečnosti. To im umožňuje riadiť riziká a určiť úlohy potrebné na vybudovanie bezpečnosti. Keďže mnohé informačné nástroje používané v organizáciách sú štandardné, je efektívnejšie používať rovnaké štandardizované bezpečnostné opatrenia ako vytvárať nové. Organizácie môžu prijať opatrenia, ktoré zodpovedajú štandardu, alebo ich zlepšiť, prípadne nahradiť vhodnejšími a aktuálnejšími opatreniami.

[42]Národný projekt Informatizácia spoločnosti. Výnos Úradu pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky č. 596/2010-54 o štandardoch informačnej bezpečnosti v informačných systémoch verejnej správy [online]. Bratislava: ÚNMZ SR, 4 septembra 2007. [cit. 28.4.2023]. Dostupné na: http://www.informatizacia.sk/standardy-is-vs/596s#vynos_STD

[43] Zbierka zákonov o informačných systémoch verejnej správy č.275/2006. [cit. 28.4.2023]. Dostupné na: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2006/275/20151101.html

[44]BÍRO, Peter. Štandardy rýchlo a ľahko. [online]. Mnisterstvo financií Slovenskej republiky, 29 september 2014. [cit. 28.4.2023]. Dostupné na: http://www.informatizacia.sk/standardy-rychlo-a-lahko/5586s#STD_info

Je nevyhnutné, aby informačný systém riadenia podniku zostal aktuálny s meniacim sa rýchlym prostredím a aby nebol zastaraný. V mnohých spoločnostiach zamestnanci najprv dodržiavajú bezpečnostné nariadenia a predpisy, keď sú prvýkrát implementované. Postupom času sa ne zabúda a stále menej a menej sa zameriava na dodržiavanie pravidiel. Napríklad spoločnosť mohla zaviesť účinnú politiku klasifikácie informácií pred niekoľkými rokmi, ale odvtedy sa vyskytli externé a interné zmeny, ktoré spôsobili, že politika je zastaraná. Aby k podobnej situácii pri ochrane informačných technológií nedošlo, je potrebné politiku priebežne aktualizovať a prispôsobovať meniacim sa podmienkam.

V posledných rokoch sa EÚ zamerala na kybernetickú bezpečnosť prostredníctvom vytvárania a zlepšovania nových nariadení a smerníc. Ich cieľom je zvýšiť možnosti kybernetickej bezpečnosti a spoluprácu medzi organizáciami a krajinami a tiež zaviesť súbor noriem, ktoré bude musieť každý členský štát EÚ uplatňovať na bezpečné obchodovanie v rámci jednotného digitálneho trhu.

Zvýšená prísnosť v oblasti ochrany a integrity údajov, má za cieľ zlepšiť zdieľanie údajov a digitálnu komunikáciu cez hranice v EÚ, aby menej podnikov bolo zasiahnutých únikmi údajov a kybernetickými útokmi. Na štandardy, ktoré upravujú informačnú bezpečnosť v Európskej únií sa pozrieme v nasledujúcej kapitole.

4.1.2 Informačná bezpečnosť v eurozóne

Vzhľadom na to, že dopyt po kybernetickej bezpečnosti naďalej rastie, tak Európska únia sa ju rozhodla v posledných rokoch postaviť do popredia. Meniaca sa povaha bezpečnostných hrozieb núti Európsku úniu čeliť roztrieštenému prístupu k otázkam bezpečnosti. Kybernetické a hybridné útoky sú v EÚ čoraz bežnejšie a hoci rozsah problému je ťažké merať, jednotlivé inštitúcie by mali začať podnikať kroky na zvýšenie ich odolnosti.

Cieľom novej verzie kybernetickej bezpečnosti EÚ od Európskej komisie a Európskej služby pre vonkajšiu činnosť je zabezpečiť odolnosť Európy voči kybernetickým hrozbám a zabezpečiť občanom prístup k spoľahlivým digitálnym službám a nástrojom. Prijatie stratégie kybernetickej bezpečnosti Radou v marci 2021 dokazuje strategický význam kybernetickej bezpečnosti pre vytvorenie digitálnej, zelenej a odolnej Európy. Na dosiahnutie strategickej autonómie sa EÚ snaží využiť svoje vlastné rozhodnutia v oblasti kybernetickej bezpečnosti na podporu svojho vedúceho postavenia a kapacity v oblasti digitálnych technológií. Krajiny z EÚ zastávajú majoritnú skupinu v celosvetovom indexe informačnej bezpečnosti štátov (18 z 20 štátov). Odhaduje sa, že trh má hodnotu viac ako

130 miliónov EUR a rastie tempom 17 % ročne. S viac ako 60 000 spoločnosťami a 660 odbornými centrami v tejto oblasti na celom kontinente je EÚ odhodlaná poskytovať svojim občanom najlepšiu možnú kybernetickú bezpečnosť. [45]

Európska komisia zverejnila svoj plán na vytvorenie otvoreného, bezpečného a chráneného kybernetického priestoru. Stanovilo sa v ňom päť základných priorít: zvýšenie odolnosti voči kybernetickým útokom, výrazné zníženie počítačovej kriminality, vytvorenie politík a kapacít kybernetickej obrany, podpora priemyselných a technologických zdrojov pre kybernetickú bezpečnosť a presadzovanie konzistentnej medzinárodnej kybernetickej stratégie pre Európsku úniu.[46]

Na lepšej informačnej bezpečnosti pôsobí mnoho komunít a organizácií ako:[47,48,49]

- ENISA (agentúra EÚ pre kybernetickú bezpečnosť)- zodpovedá za pomoc pri ochrane kybernetickej bezpečnosti EÚ. Ponúkajú pomoc členským štátom, organizáciám EÚ a podnikom v oblastiach, ako je napríklad prijatie smernice o bezpečnosti sietí a informácií.
- ISACs (Centrá zdieľania informácií a analýzy)- komisia uprednostňuje ďalší rozvoj ISAC na úrovni EÚ a na vnútroštátnej úrovni a aj v koordinácii s ENISA.
- JRC (Spoločné výskumné centrum)- pracuje na zlepšení kybernetickej bezpečnosti. Na tento účel vyvinula taxonómiu kybernetickej bezpečnosti s cieľom štandardizovať terminológiu a získať prehľad o schopnostiach EÚ. Nedávno tiež zverejnila správu „Kybernetická bezpečnosť – naša digitálna kotva“, ktorá načrtáva históriu a súčasné postavenie EÚ v oblasti kybernetickej bezpečnosti.
- CSIRTs/CERTs- tímy spolupracujú na úrovni EÚ pri riešení incidentov a rizík kybernetickej bezpečnosti a spolupracujú so súkromným sektorom. Všetci

[45] CONSORTIUM. Cybersecurity: Resilience, deterrence and defence: Building strong cybersecurity for the EU [online]. Brussels: Council of the European Union, 2017 [cit. 2023-04-28]. Dostupné na: https://www.consilium.europa.eu/sk/policies/cybersecurity/#resilience
[46] ZDRAVEC, M. - FERKOVÁ, T. EU stratégia informačnej bezpečnosti [online]. In: iTAPA 2019. Bratislava: NASES, 2019, s. 1-11 [cit. 2023-04-28]. Dostupné na: https://www.itapa.sk/eu-strategia-informacnej-bezpecnosti/
[47]EUROPEAN UNION AGENCY FOR CYBERSECURITY. European Cybersecurity Competence Centre and Network: New EU-funded project to support the cyber community. [online]. In: News. European Union Agency for Cybersecurity [cit. 2023-04-28]. Dostupné na: https://cybersecurity-centre.europa.eu/news/european-cybersecurity-competence-centre-and-network-new-eu-funded-project-support-cyber-community-2022-12-20_en
[48] EUROPEAN COMMISSION. Cybersecurity policies [online]. Digital Single Market. [cit. 2023-04-28]. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
[49] CyberSec4Europe. Our community [online]. [cit. 2023-04-28]. Dostupné na: https://cybersec4europe.eu/our-community/

prevádzkovatelia základných služieb a poskytovatelia digitálnych služieb musia mať prístup k určeným CSIRT.

- ECSO (Európska organizácia pre kybernetickú bezpečnosť)- založené v roku 2016, je verejno-súkromné partnerstvo medzi Európskou komisiou a 250 členmi z odvetvia kybernetickej bezpečnosti, výskumných a akademických inštitúcií, verejného sektora a priemyslu na strane dopytu. Vydáva odporúčania a pomáha rozvíjať európsku komunitu kybernetickej bezpečnosti.

Aktivity EÚ v informačnej bezpečnosti sa zameriavajú aj na rôzne politiky ako počítačová kriminalita, kybernetická diplomacia, kybernetická obrana a budovanie kybernetických kapacít v tretích krajinách.

Európska únia sa tiež snaží presadzovať dosiahnutie spoločnej stratégie pre informačnú bezpečnosť. Túto agendu ma pod krídlami organizácia ENISA (european union agency for cybersecurity)- agentúra Európskej únie pre kybernetickú bezpečnosť „je zameraná na dosiahnutie vysokej spoločnej úrovne kybernetickej bezpečnosti v celej Európe. Agentúra Európskej únie pre kybernetickú bezpečnosť, založená v roku 2004 a posilnená zákonom EÚ o kybernetickej bezpečnosti, prispieva ku kybernetickej politike EÚ, zvyšuje dôveryhodnosť produktov, služieb a procesov IKT prostredníctvom certifikačných schém kybernetickej bezpečnosti, spolupracuje s členskými štátmi a orgánmi EÚ a pomáha Európe. pripraviť sa na kybernetické výzvy zajtrajška. Prostredníctvom zdieľania znalostí, budovania kapacít a zvyšovania informovanosti agentúra spolupracuje so svojimi kľúčovými zainteresovanými stranami na posilnení dôvery v prepojenú ekonomiku, na posilnení odolnosti infraštruktúry Únie a v konečnom dôsledku na udržaní digitálnej bezpečnosti európskej spoločnosti a občanov.“

ENISA sa snaží udržiavať a zvyšovať súdržnosť kybernetickej bezpečnosti skrz jednotné kybernetické zabezpečenie. Túto snahu podporujú aj ďalšie organizácie ako CEN, CENELEC, ETSI a aj ISO. ENISA podporuje bezpečnú štandardizáciu s cieľom zabezpečiť konzistentnosť a dôveru v digitálne produkty a služby a monitoruje európsky trh s kybernetickou bezpečnosťou s cieľom identifikovať príležitosti na posilnenie ochrany. Zvoláva pracovné skupiny na posúdenie a podporu väčšej bezpečnostnej súdržnosti v Európe a aj mimo nej.[50]

[50]EUROPEAN UNION AGENCY FOR CYBERSECURITY. Mapping and Prioritisation of European ICT Security and Privacy Research and Innovation [online]. In: ENISA. Athens : ENISA, 2020 [cit. 2023-04-28]. Dostupné na: https://www.enisa.europa.eu/topics/standards.

Existuje viacero štandardov z ktorých vychádza informačná bezpečnosť európskej únie:[51,52]

- **Common Criteria** spomenuté už v kapitole 1.1.2. je štandardný rámec na hodnotenie bezpečnosti produktu, ktorý sa hodnotí na základe vopred definovaných požiadaviek na bezpečnosť a zabezpečenie. Úrovne zabezpečenia sa pohybujú od 1 do 7.[53]
- **OWASP ASVS** je open source komunitou vyvinutý rámec, ktorý overuje technické bezpečnostné kontroly v softvérových produktoch a procesoch ich vývoja. Definuje úrovne zrelosti na posúdenie bezpečnostného profilu systému, určenie potrebných bezpečnostných požiadaviek a poskytnutie prípadov použitia, ako je školenie, referencie a pokyny pre automatizáciu.[54]
- **ISO/IEC 27034** je viacdielna, usmerňujúca medzinárodná norma zameraná na bezpečnosť aplikácií. Každá z jeho početných častí podrobne popisuje, ako by sa mala dosiahnuť softvérová bezpečnosť. Najrelevantnejšie z nich sú:

  27034-3: proces riadenia bezpečnosti aplikácie;

  27034-4: validácia a overenie (ešte bude zverejnené);

  27034-5: dátová štruktúra protokolov a bezpečnostných kontrol aplikácií; 27034-7: rámec predikcie záruky.[55]
- **BSIMM** (verzia 2018) je komerčná iniciatíva, ktorá využíva prístup zdola nahor, začínajúc identifikáciou aktivít úspešných softvérových spoločností. Načrtáva kontroly, ktoré možno merať pre úrovne zrelosti, ktoré sa zvyšujú so zvyšujúcou sa úrovňou.[56]

---

[51] CEN/CENELEC. Cybersecurity – Baseline security recommendations for Internet of Things (IoT) in the context of critical information infrastructures. [online]. In: CEN-CENELEC. Brussels: CEN-CENELEC Management Centre, 2017, CWA 17133:2017(E), s. 41. [cit. 2023-04-28]. Dostupné na: https://standards.cencenelec.eu/BPCEN/2307986.pdf

[52]JANOŠČOVÁ, Renáta. Standardy informačnej bezpečnosti [online]. In: Manažment informačnej bezpečnosti: Podnikový prístup. Bratislava: Vydavateľstvo EKONÓM, 2015, s. 17-32 [cit. 2023-04-28]. ISBN 978-80-225-4114-7. Dostupné na: https://www.researchgate.net/profile/Renata-Janoscova/publication/281098237_Standardy_informacnej_bezpecnosti/links/55ddbc8f08aeaa26af0f137a/Standardy-informacnej-bezpecnosti.pdf

[53] COMMON CRITERIA RECOGNITION ARRANGEMENT. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [online]. 2017. [cit. 2023-04-28]. Dostupné na: https://www.commoncriteriaportal.org/

[54] OWASP Foundation. OWASP Application Security Verification Standard (ASVS) Project. [online]. In: OWASP. [cit. 2023-04-28]. Dostupné na: https://owasp.org/www-project-application-security-verification-standard/

[56] SYNOPSYS. Building Security In Maturity Model (BSIMM): The Software Security Framework. [online]. In: Synopsys Software Integrity. Mountain View, CA: Synopsys, 2021, Version 12, 1-82 [cit. 2023-05-02]. Dostupné na: https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html

- **Microsoft SDL** je dobre známy bezpečný vývojový rámec, ktorý pokrýva školenie, požiadavky, návrh, implementáciu, overovanie, vydanie a odozvu.

Ako je názorne zobrazené vyššie existuje mnoho štandardov súvisiacich s informačnou a softvérovou bezpečnosťou. V tejto práci však budeme zameriavať pozornosť na konkrétne jednu smernicu, ktorá ako prvá znamenala prvé celoúnijné legislatívne opatrenie na zintenzívnenie spolupráce medzi členskými štátmi v dôležitej oblasti kybernetickej bezpečnosti.

Smernica NIS platná v celej EÚ bola zavedená v roku 2016 s cieľom posilniť spoluprácu medzi členskými štátmi v oblasti kybernetickej bezpečnosti. Uložila bezpečnostné požiadavky na prevádzkovateľov základných služieb (energetika, doprava, zdravotná starostlivosť, financie) a poskytovateľov digitálnych služieb (online trhy, vyhľadávače, cloud). V reakcii na meniace sa prostredie hrozieb a digitálnu transformáciu vyvolanú pandémiou COVID-19 Európska komisia v decembri 2020 navrhla aktualizovanú smernicu NIS (NIS2). Rada a Európsky parlament dosiahli predbežnú dohodu o nových opatreniach v máji 2022. Aké zmeny a povinnosti budú platiť prijatím tejto novej smernice sa dozvieme v praktickej časti diplomovej práce. V nasledujúcej kapitole si povieme niečo o Slovenskej úprave informačnej bezpečnosti, pretože práve prostredníctvom použitia komparatívnej metódy medzi Európskou a Slovenskou legislatívou vieme určiť, čo smernica NIS 2 prináša.

4.1.3 Informačná bezpečnosť v Slovenskej republike.

Bezpečnostnú politiku, ktorú sme si rozobrali v kapitole 1.3.1, môžeme považovať za dokument, ktorý je základom pre bezpečnostné riešenie podniku ale môže sa uplatňovať aj na štátne inštitúcie. V bezpečnostnej politike sa definujú operácie podniku v bezpečnostnej sfére a to isté aj na úrovni štátu. Slovenská republika uplatňuje viacero predpisov a zákonov ovplyvňujúcich tvorbu politiky, súvisiacou s bezpečnosťou informácií a to:

- zákon č. 211/2000 Z.z. o slobodnom prístupe,
- zákon č. 215/2004 Z. z. o ochrane utajovaných skutočností,
- zákon č. 428/2002 Z.z. o ochrane osobných údajov,
- zákon č. 215/2002 Z. z. o elektronickom podpise, • Obchodný zákonník č. 513/1991 Zb.

Inštitúcie, pôsobiace v Slovenskej republike na ochranu počítačovej bezpečnosti:[57,58]

Národný bezpečnostný úrad (NBÚ) - je ústredný orgán štátnej správy Slovenskej republiky pre ochranu utajovaných skutočností, šifrovú službu, kybernetickú bezpečnosť a dôveryhodné služby.

Komisia pre kybernetickú bezpečnosť je stály odborný poradný orgán riaditeľa Národného bezpečnostného úradu pre uplatňovanie štátnej politiky v oblasti kybernetickej bezpečnosti v Slovenskej republike.

ÚPV SR pre investície a informatizáciu /Sekcia riadenia informatizácie zabezpečuje v oblasti informatizácie spoločnosti centrálne riadenie informatizácie spoločnosti 80 a tvorbu politiky jednotného digitálneho trhu, rozhodovanie o využívaní finančných zdrojov vo verejnej správe pre informačné technológie, centrálnu architektúru integrovaného informačného systému verejnej správy a koordináciu plnenia úloh v oblasti informatizácie spoločnosti. Jeho činnosť upravuje Zák. č. 275/2006 Z. z. o ISVS. Vykonáva koordináciu a riadenie aktivít pre zaistenie počítačovej bezpečnosti

MV SR vykonáva v zmysle Zák. č. 45/2011 Z.z. o kritickej infraštruktúre štátnu správu na úseku kritickej infraštruktúry spolu s Vládou SR a MH SR. Výkonnými zložkami v oblasti kritickej infraštruktúry sú odpovedajúce sektory MH SR, MDV SR, MF SR, MZ SR, MŽP SR.

Špecifické postavenie pri ochrane počítačovej bezpečnosti má **MO SR** upravené zák. č. 319/2002 Z.z. o obrane SR, zák. č. 321/2002 Z.z. o ozbrojených silách SR a unesením Vlády SR č.120/2007 - Koncepcia kritickej infraštruktúry v SR a spôsob jej ochrany a obrany.

Nové štandardy alebo úpravu starších zabezpečuje Komisia pre štandardizáciu informačných systémov verejnej správy. Táto komisia je poradným orgánom odborníkov z verejnej správy, súkromného a akademického sektora, zriadeným Ministerstvom financií Slovenskej republiky. Pracuje na a schvaľuje všetky normy vydané vyhláškou pred legislatívnym schválením.

[57] BELÁŇOVÁ, Benita. Vývoj informačnej bezpečnosti v Slovenskej republike – výsledky prieskumu 2006-2017. Aktuálne výzvy prevencie počítačovej kriminality [online]. In: Konferencia inovatívneho manažmentu (KIM) 2018, Piešťany, Slovenská republika, 21. marec 2018. s. 17-23. [cit. 2023-04-28]. Dostupné na: https://www.akademiapz.sk/sites/default/files/KIM/ZBORN%C3%8DK%2021.3.2018%20WEB_0.PDF#page=17

[58] BÍRO, Peter. NÁRODNÝ PORTÁL INFORMATIZÁCIE. Štandardy IS VS: Verzia 5.9.6S [online]. In: Informatizácia. Bratislava: Národné centrum pre informatizáciu, 2018 [cit. 2023-04-28]. Dostupné na: http://www.informatizacia.sk/standardy-is-vs/596s.

V Slovenskej republike sa zvyšuje záujem o informačnej bezpečnosti a kybernetike vo verejnom ako ja súkromnom sektore. Vláda SR a jej inštitúcie podnikajú viaceré kroky na riešenie hrozieb informačnej bezpečnosti v online priestore napr. zriadenie Národnej rady pre kybernetickú bezpečnosť, zavedenie zákona o kybernetickej bezpečnosti alebo zvýšenou iniciatívou informovať verejnosť o informačných hrozbách prostredníctvom kampaní ako napríklad Mesiac kybernetickej bezpečnosti. Na Slovensku platia mnohé normy a štandardy, ktoré sa budú musieť inovovať alebo kompletne nahradiť novými štandardami z dielne Európskej únie. To aké zmeny prinesie nová legislatíva a čo to bude znamenať našu podnikateľskú jednotku si rozoberieme v ďalšej časti diplomovej práce.

4.2 Identifikácia požiadaviek podniku na informačnú bezpečnosť

Identifikácia požiadaviek je prvým krokom v procese nahradenia starých smerníc o informačnej bezpečnosti a implementácie novej smernice NIS 2 do malého podniku. Tento krok je kritický pre úspešné plánovanie a úspešnú realizáciu projektu. Zahŕňa identifikáciu existujúcich postupov, opatrení a systémov na riadenie informačnej bezpečnosti v podniku, analýzu existujúcich smerníc, ktoré sú momentálne implementované v organizácií a identifikáciu oblastí, ktoré vyžadujú aktualizáciu a doplnenie na základe nových požiadaviek smernice NIS 2.

V prvom kroku je dôležité identifikovať existujúce postupy a systémy na riadenie informačnej bezpečnosti v organizácií. To znamená, že je potrebné preskúmať existujúce procesy a postupy na zabezpečenie ochrany informácií v malom podniku, ako aj všetky existujúce systémy a nástroje, ktoré sa používajú na riadenie informačnej bezpečnosti. Takéto preskúmanie, by malo zahrňovať aj posúdenie existujúcich politík, stratégií a plánov na riadenie informačnej bezpečnosti.

Druhým krokom je analýza existujúcich zákonov a smerníc, ktoré sú momentálne implementované v podniku. V tomto kroku by sa mali identifikovať všetky relevantné zákony a smernice, ktoré sa týkajú informačnej bezpečnosti a sú aktuálne implementované. Tieto zákony a smernice by mali byť analyzované a porovnané s požiadavkami smernice NIS 2. Tento proces umožní určiť, aké zmeny a doplnenia budú potrebné na dosiahnutie súladu s novými požiadavkami.

V poslednom kroku identifikujeme oblasti, ktoré vyžadujú aktualizáciu a doplnenie na základe nových požiadaviek smernice NIS 2. V tomto kroku by mali byť preskúmané všetky oblasti malého podniku, ktoré sú zahrnuté do smernice NIS 2, ako napríklad oblasť

identifikácie a hodnotenia rizík, zabezpečenie prevádzky kritických služieb alebo ochrana pred kybernetickými útokmi. Po identifikácii týchto oblastí by mali byť stanovené nové ciele, postupy a opatrenia na zlepšenie informačnej bezpečnosti v podniku.

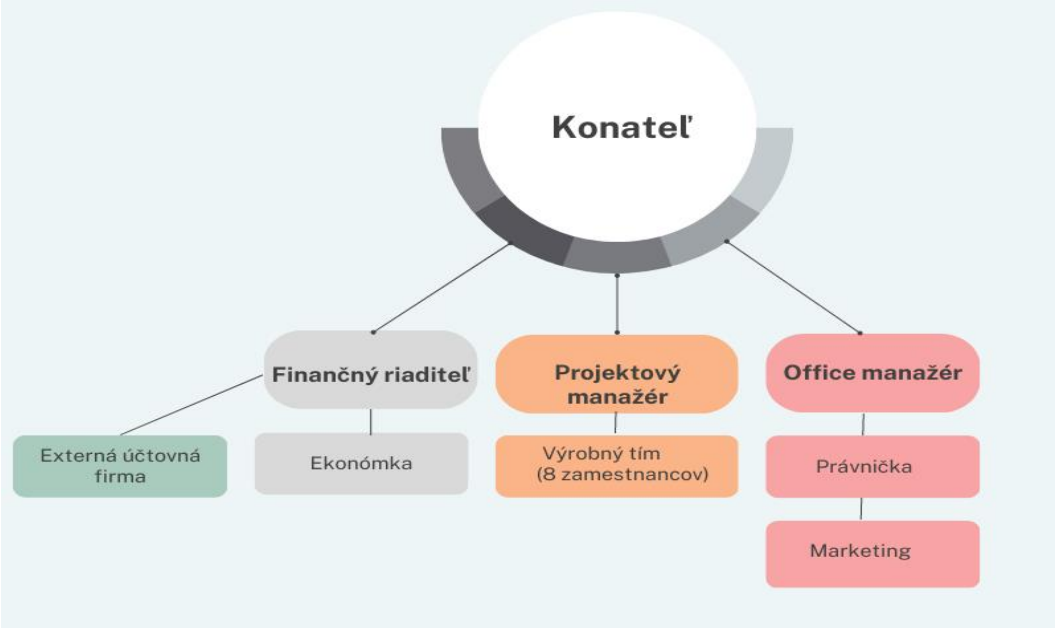
4.2.1 Identifikácia existujúcich postupov a systémov na riadenie informačnej bezpečnosti v malom podniku

Pri implementácií novej smernice do podniku je táto kapitola veľmi dôležitá v rámci diplomovej práce, z dôvodu zhodnotenia súčasného stavu riadenia informačnej bezpečnosti a identifikácií potencionálnych oblastí zlepšenia.

Na identifikáciu existujúcich postupov a systémov sme začali analýzou súčasných procesov riadenia informačnej bezpečnosti v malom podniku. Táto analýza zahŕňala posúdenie existujúcich bezpečnostných politík, postupov, procesov a technológií. Ďalej sme analyzovali existujúce riziká a hrozby, ktorým malý podnik čelí v oblasti informačnej bezpečnosti.

Po zhodnotení súčasného stavu sme prešli k porovnaniu existujúcich postupov a systémov s požiadavkami novej smernice NIS 2. Táto analýza nám pomohla identifikovať oblasti, ktoré je potrebné zlepšiť alebo doplniť v súčasných postupoch a systémoch, aby sme zabezpečili súlad s novými požiadavkami.

Pre správne pochopenie fungovania informačnej bezpečnosti v podniku je nutné predstaviť organizačnú štruktúru, ktorá sa vyznámným podielom podiela na bezpečnosti podniku v informačnom sektore.



Obrázok 6 Organizačná štruktúra podniku
Zdroj: Vlastné spracovanie podľa organizačnej štruktúry podniku

- **Konateľ**- osoba, ktorá zastupuje a riadi firmu, taktiež nesie zodpovednosť za riadenie spoločnosti. V tomto prípade je konateľ aj majiteľ jedna osoba. Jeho povinnosti zahŕňajú dohľad nad činnosťou firmy, riadenie podnikateľskej činnosti a rozhodovanie o dôležitých záležitostiach spoločnosti.
- **Finančný riaditeľ**- je zodpovedný za finančné riadenie a kontrolu vo firme a zabezpečenie toho, aby bola spoločnosť schopná plniť svoje finančné záväzky. Jeho povinnosti zahŕňajú zabezpečenie správneho vedenia účtovníctva, ktorú poskytuje externá firma, výrobu a predkladanie finančných správ, monitorovanie finančných tokov, plánovanie a riadenie rozpočtu a zabezpečenie účinného zdaňovania. Finančný riaditeľ taktiež pôsobí vo firme ako osoba, ktorá zodpovedá za obchod a získavanie zákaziek od rôznych klientov a ich presvedčenie využitia služieb podniku.
- **Ekonómka-** má za úlohu spravovať a monitorovať finančné zdroje spoločnosti. Jej povinnosti zahŕňajú vypracovanie rozpočtu, sledovanie vývoja finančnej situácie, zabezpečenie účtovníctva a splnenie všetkých finančných povinností voči štátu a iným subjektom. Ekonómka finančného riaditeľa tiež pomáha pri tvorbe obchodnej stratégie, financovaní projektov a investícií spoločnosti.
- **Externá účtovná firma**- je profesionálna spoločnosť, ktorá poskytuje účtovné služby pre iné firmy. V tomto konkrétnom podniku má povinnosť

zabezpečovať vedenie účtovníctva, vypracúvať daňové priznania, vykazovať dane a iné povinnosti spojené s účtovníctvom. Taktiež môže poskytnúť poradenstvo v otázkach daní, účtovníctva a finančnej správy spoločnosti.

- **Projektový manažér-** Projektový manažér je zodpovedný za koordináciu, plánovanie a riadenie projektov vo firme, ktorá sa zameriava na stavebné práce vo verejnom sektore. Jeho hlavnou úlohou je zabezpečiť, aby boli projekty dokončené včas, v rámci rozpočtu a s požadovanou kvalitou. Projektový manažér je zodpovedný za stanovenie cieľov projektu, plánovanie, pridelenie zdrojov a koordináciu práce tímu, vrátane podriadených stavebných inžinierov a pracovníkov výroby. Okrem toho je tiež zodpovedný aby boli dodržané všetky regulačné, právne a normové požiadavky.
- **Výrobný tím-** v stavebno-konzultačnej firme pre verejné zákazky zodpovedá za realizáciu stavebných projektov a zabezpečenie kvality a časového plnenia pracovných úloh. Jeho povinnosťami sú plánovanie a koordinácia výrobných procesov, riadenie pracovníkov, dohľad nad bezpečnosťou a kvalitou práce, riadenie zdrojov a zabezpečenie dodávok a materiálov potrebných pre realizáciu projektov. Výrobný tím tiež spolupracuje s projektovým manažérom a stavebným inžinierom na plánovaní a sledovaní pokroku projektov a zabezpečuje komunikáciu s klientom.
- **Office manažér-** osoba, ktorá je zodpovedná za koordináciu administratívnych a organizačných úloh vo firme. Povinnosti zahŕňajú plánovanie, koordináciu a monitorovanie práce tímu, vedenie účtovníctva, prípravu dokumentácie pre zákazníkov a zabezpečenie účinného fungovania firmy.
- **Právnička-** má za úlohu zabezpečiť, aby spoločnosť dodržiavala všetky právne predpisy a zákony súvisiace s verejnými zákazkami. Jej povinnosťou je tiež zabezpečiť, aby všetky zmluvy boli v súlade s právnymi predpismi a aby spoločnosť mala správne dokumenty na účely verejných súťaží. Okrem toho je jej úlohou poskytovať právne poradenstvo pre riešenie sporov a konfliktov súvisiacich s verejnými zákazkami.
- **Marketing-** osoba zodpovedná za propagáciu a predaj výrobkov alebo služieb spoločnosti. Povinnosti zahŕňajú plánovanie a realizáciu marketingových kampaní, zabezpečenie propagácie firmy a služieb, budovanie a udržiavanie

vzťahov so zákazníkmi, prípravu marketingových materiálov a účasť na verejných súťažiach a podujatiach. Musí byť schopný identifikovať potreby zákazníkov a vytvárať stratégie na zvýšenie povesti spoločnosti a zvyšovanie predaja.

Analýza súčasných procesov riadenia informačnej bezpečnosti v malom podniku ukázala, že spoločnosť má základné opatrenia na ochranu dát, ale je tu veľký priestor na zlepšenie. Zistilo sa, že spoločnosť za svoju existenciu spolupracovala s viacerými externými dodávateľmi, ktorý čiastkovo, no nie komplexne nastavili základné parametre informačnej bezpečnosti.

Tabuľka 1 Zavedené postupy informačnej bezpečnosti podniku

Zavedené postupy informačnej bezpečnosti podniku
1. Zabezpečený prístup do firemnej siete s použitím užívateľských mien a hesiel.
2. Unikátne heslo pre každého zamestnanca pre prístup do svojho počítačového zariadenia
3. Spolupráca s externými dodávateľmi informačnej bezpečnosti
4. Antivírusový software nainštalovaný na všetkých pracovných stanovištiach a serveroch
5. Pravidelné zálohovanie dát na cloudových serveroch
6. Čipové karty zabezpečujúce prístup do kancelárií
7. Dostupnosť firemných informácií len pre zamestnancov s príslušnými oprávneniami.
8. Jednotná, uzavretá sieť
9. Nárazové školenie zamestnancov
10. Vstupné školenie nových zamestnancov
11. Správca siete: Finančný riaditeľ

Zdroj: Vlastné spracovanie

Tabuľka 1 prezentuje súčasné zavedené opatrenia informačnej bezpečnosti malého podniku. Napriek tomu bolo odhalené, že spoločnosť nemá stanovenú žiadnu bezpečnostnú politiku, ktorá by obsahovala postupy a zásady pre správu a ochranu informácií. Taktiež nie je implementovaná žiadna prísna autentifikačná metóda pre prístup k citlivým informáciám a existuje len okrajové školenie pre zamestnancov týkajúce sa ochrany informácií. V nasledujúcich bodoch konkrétnejšie opíšeme postupy informačnej bezpečnosti podniku.

1. Zabezpečený prístup do firemnej siete s použitím užívateľských mien a hesiel je bezpečnostná opatrenie, ktoré zaisťuje, že iba oprávnení zamestnanci alebo osoby s autorizovaným prístupom majú prístup k firemnej sieti. Každý užívateľ v spoločnosti má svoje unikátne užívateľské meno a heslo. Tieto prihlasovacie údaje sú uložené v zabezpečenej databáze na serveri a sú chránené proti neoprávnenému prístupu. Pri prihlásení do firemnej siete sa užívateľ musí najskôr overiť pomocou svojho

užívateľského mena a hesla. Po overení je užívateľovi pridelený prístup k jeho oprávneným sieťovým zdrojom, ako sú zdieľané priečinky, tlačiarne, aplikácie a podobne. Takýto zabezpečený prístup pomáha minimalizovať riziko neoprávneného prístupu k firemnej sieti a jej citlivým dátam. Zároveň umožňuje správcovi siete monitorovať a sledovať prístupové práva užívateľov a prevádzku siete ako celku.

2. Unikátne heslo pre každého zamestnanca je súčasťou opatrení informačnej bezpečnosti. Každý zamestnanec musí mať svoje vlastné heslo, ktoré mu umožní prístup do jeho počítačového zariadenia. Heslo musí byť unikátne a pozná ho iba on zodpovedný vedúci pracovník, ktorý ho potrebuje pre správu podnikových zariadení.
3. Spolupráca s externými dodávateľmi informačnej bezpečnosti kľúčová pre zabezpečenie aspoň minimálnej ochrany dát a sietí podniku a pomáha podniku zabezpečiť dodržiavanie noriem a zákonov v oblasti informačnej bezpečnosti. Avšak, spolupráca nie je konštantná a podnik viacej krát zmenil dodávateľa informačných služieb, čo bráni nastaveniu ucelenej informačno-bezpečnostnej politiky pre podnik.
4. V podnikovom prostredí sú zvyčajne nainštalované verzie antivírusového softvéru ESET na všetkých pracovných stanovištiach a serveroch. Tento software môže byť riadený centrálne pomocou správcovského panelu, ktorý umožňuje administrátorovi sledovať stav ochrany a aktualizovať softvér na všetkých zariadeniach naraz. Okrem toho, antivírusový software od ESET umožňuje správu a kontrolu prístupových práv, aby bolo zabezpečené, že iba oprávnení používatelia majú prístup k dôležitým dátam a informáciám.
5. Spoločnosť používa na skladovanie a predovšetkým uchovávanie svojich dát pravidelné zálohovanie dát na cloudových serveroch pomocou služby OneDrive. Tento proces zabezpečuje, že dôležité údaje sú chránené a k dispozícii v prípade výpadku alebo stratu údajov. Konkrétny spôsob využitia OneDrive pre zálohovanie dát podnik uplatňuje nasledovne:
    - Vytvorenie účtu OneDrive pre podnik a jednotlivých zamestnancov a pripojenie k svojmu operačnému systému a aplikáciám.
    - Nastavenie automatického zálohovania dát z vybraných zariadení a súborov do OneDrive.

- Prispôsobenie nastavení zálohovania podľa potrieb podniku, napríklad nastavenie časových intervalov alebo výber konkrétnych súborov na zálohovanie.

V prípade, že dôjde k výpadku alebo straty dát, podnik môže ľahko obnoviť svoje údaje z OneDrive. To zabezpečuje, že podnik nebude mať problémy s obnovením svojich dôležitých údajov a bude schopný pokračovať v prevádzke bez veľkých prerušení. Okrem toho OneDrive umožňuje zdieľanie dát medzi rôznymi zariadeniami a používateľmi v podniku, čo zlepšuje spoluprácu a produktivitu. OneDrive tiež poskytuje rôzne bezpečnostné funkcie, ktoré pomáhajú chrániť údaje podniku, napríklad dvojfaktorové overenie a šifrovanie dát.

Norma NIS 2 obsahuje nové a prísnejšie požiadavky na zálohovanie a obnovu dát, testovanie a dokumentovanie týchto postupov. Ak sú súčasné postupy zálohovania a obnovy dát v podniku nekompatibilné s požiadavkami normy NIS 2, môže to znamenať, že v prípade výpadku alebo útoku na informačné systémy podniku nebude možné dosiahnuť dostatočnú rýchlosť obnovy, alebo nebude možné zabezpečiť úplnú obnovu dát. Okrem toho, ak sú súčasné postupy zálohovania a obnovy dát v podniku nekompatibilné s požiadavkami normy NIS 2, môže to viesť k neúspešnej certifikácii podniku podľa normy NIS 2, čo môže mať negatívny vplyv na dôveryhodnosť podniku.

6. Proces zaistenia kancelárskych priestorov čipovými kartami zabezpečuje, že len oprávnení zamestnanci majú prístup do určitých kancelárií alebo priestorov, čo pomáha chrániť podnikové aktíva a zabezpečiť bezpečnosť zamestnancov a zákazníkov.
7. Opatrenia o informačnej bezpečnosti, ktoré zabezpečujú dostupnosť firemných informácií len pre zamestnancov s príslušnými oprávneniami, sa nazývajú opatrenia na riadenie prístupu k informáciám. Kontrola prístupu k informáciám je pravidelne monitorovaná a aktualizovaná finančným riaditeľom v závislosti na potrebách a zmenách v organizácii, čo by rozhodne nemalo patriť do jeho kompetencií.
8. Jednotná uzavretá sieť LAN zvyčajne znamená, že všetky zariadenia a užívatelia, ktorí sa pripájajú k sieti, patria do jednej organizácie alebo firmy. Konkrétne nastavenia siete a ich hierarchia sa nám nepodarila zistiť v dôsledku neposkytnutia informácií podnikom.

9. Nárazové školenie zamestnancov je súčasťou bezpečnostného úsilia podniku a absolvujú ho všetci zamestnanci, ktorí majú prístup k citlivým informáciám alebo ktorí sú vystavení riziku kybernetických útokov. Po absolvovaní nárazového školenia by mali byť zamestnanci schopní rozpoznať a oznámiť podozrivé aktivity, ako sú phishingové e-maily, snaženia o získanie citlivých informácií a iné potenciálne nebezpečné situácie, ktorým však zamestnanci aj po absolvovaní školení nekladú zvýšenú pozornosť.
10. Celkovo vstupné školenie v podniku pre nových zamestnancov v tomto prípade nie je účinným opatrením pre zabezpečenie citlivých informácií podniku. Týka sa predovšetkým informácií o virtuálnych procesoch podniku a všeobecných informácií. Svojím podpisom na dotazník nový zamestnanec súhlasí s informačnou politikou podniku, ktorá však nie je nastavená a tiež súhlasí s ochranou osobných údajov.
11. Ako prvý a aj posledný kontakt s informačnou bezpečnosťou zabezpečuje finančný riaditeľ. Táto úloha bola mu bola zverená konateľom v začiatkoch firmy, vďaka jeho nadšeniu a skúsenosťami v informačnom sektore. Postupne ako sa podnik rozrastá, je potrebné zabezpečovať náročnejšie informatické operácie na ktoré si podnik skrz finančného riaditeľa najíma externých konzultantov. Pre svoju vyťaženosť, ale aj v tomto štádiu firmy nekompetentnosť nie je vhodné aby finančný riaditeľ ďalej vykonával správcu informačných aktív podniku.

Na základe identifikácie poskytnutých existujúcich postupov a systémov na riadenie informačnej bezpečnosti v malom podniku, možno konštatovať, že súčasné opatrenia sú dôležitými prvkami pre ochranu informácií. Avšak, neexistuje žiadna ucelená politika ochrany pred kybernetickými hrozbami a zneužitím informácií, a preto je nevyhnutné, aby podnik zmenil a vylepšil bezpečnostné opatrenia v kybernetickom priestore.

Je dôležité zdôrazniť, že malé podniky sú často zraniteľnejšie vzhľadom na obmedzené finančné a ľudské zdroje, a preto by mali byť oveľa opatrnejšie pri ochrane informácií. Vzhľadom na to, že všetky súčasné opatrenia sú vedené a riadené finančným riaditeľom, môže to byť pre podnik nevýhodou, pretože existuje riziko, že ostatní zamestnanci nemajú potrebné vedomosti a zručnosti na riadenie informačnej bezpečnosti alebo dokonca aj sám správca informačných technológií, teda finančný riaditeľ. Vďaka identifikovaným informačným postupom v oblasti informačnej bezpečnosti, dokážeme

definovať nedostatky týchto postupov a navrhnúť zlepšenia, ktoré budú smerovať k lepšej ochrane údajov. Tieto návrhy si rozoberieme v kapitole 4.1.3..

4.2.2 Analyzovanie existujúcich zákonov a smerníc, ktoré sú momentálne implementované v podniku

Analyzovaná firma, ktorá pôsobí vo verejnom sektore, musí dodržiavať rôzne informačné štandardy a normy, ktoré zabezpečujú bezpečnosť a ochranu informácií. Niektoré z týchto štandardov sú:

Tabuľka 2 Akreditačné normy používané podnikom

Certifikačné normy	
1	ISO/IEC 2701
2	GDPR
3	PCI-DSS

Zdroj: Vlastná tvorba spracované podľa interných materiálov podniku

1. ISO/IEC 27001: Tento štandard sa zaoberá riadením informačnej bezpečnosti a zabezpečuje, že sú dodržiavané procesy pre identifikáciu, hodnotenie a riadenie rizík v oblasti informačnej bezpečnosti.
2. GDPR (Všeobecné nariadenie o ochrane údajov): Toto nariadenie stanovuje požiadavky na spracovanie osobných údajov a zabezpečuje, že sú tieto údaje spracované v súlade s požiadavkami na ochranu súkromia.
3. PCI-DSS (Payment Card Industry Data Security Standard): Tento štandard sa týka zabezpečenia platobných kariet a zabezpečuje, že karty sú spracované v súlade s bezpečnostnými požiadavkami a pravidlami.

Je dôležité, aby stavebno-konzultačná firma mala jasne definované požiadavky na informačnú bezpečnosť a aby tieto požiadavky boli súčasťou firemnej kultúry a procesov. To zabezpečí, že firma bude schopná splniť požiadavky verejných zákaziek a bude konkurencieschopná na trhu.

Okrem informačných štandardov a noriem, podnik musí dodržiavať aj rôzne zákony a nariadenia súvisiace so svojou stavebnou činnosťou. Niektoré z týchto zákonov môžu zahŕňať:

1. Zákon o stavebnom poriadku: Tento zákon určuje pravidlá pre stavebné práce vrátane požiadaviek na stavebné povolenia a schvaľovanie projektov.

2. Zákon o ochrane prírody a krajiny: Tento zákon sa týka ochrany prírody a krajiny v rámci stavebnej činnosti a zabezpečuje, že sú dodržiavané požiadavky na ochranu životného prostredia.
3. Zákon o verejnom obstarávaní: Tento zákon upravuje verejné obstarávanie a zabezpečuje, že procesy sú transparentné, otvorené a spravodlivé pre všetkých zúčastnených.
4. Zákon o pracovnom práve: Tento zákon určuje požiadavky na pracovné podmienky, pracovné vzťahy a sociálne zabezpečenie zamestnancov.
5. Zákon o zodpovednosti za škodu: Tento zákon sa týka zodpovednosti za škody spôsobené v rámci stavebnej činnosti a zabezpečuje, že zodpovednosť za škodu bude spravodlivo rozdelená.
6. Zákon o ochrane spotrebiteľa: Tento zákon sa týka ochrany práv spotrebiteľov v rámci stavebných služieb a zabezpečuje, že spotrebitelia budú chránení pred nekalými praktikami.

Je dôležité, aby stavebná konzultačná firma mala jasne definované požiadavky na dodržiavanie týchto zákonov a aby tieto požiadavky boli súčasťou firemnej kultúry a procesov. To zabezpečuje zamestnaná právnička, že firma bude schopná poskytovať kvalitné služby a bude konkurencieschopná na trhu.

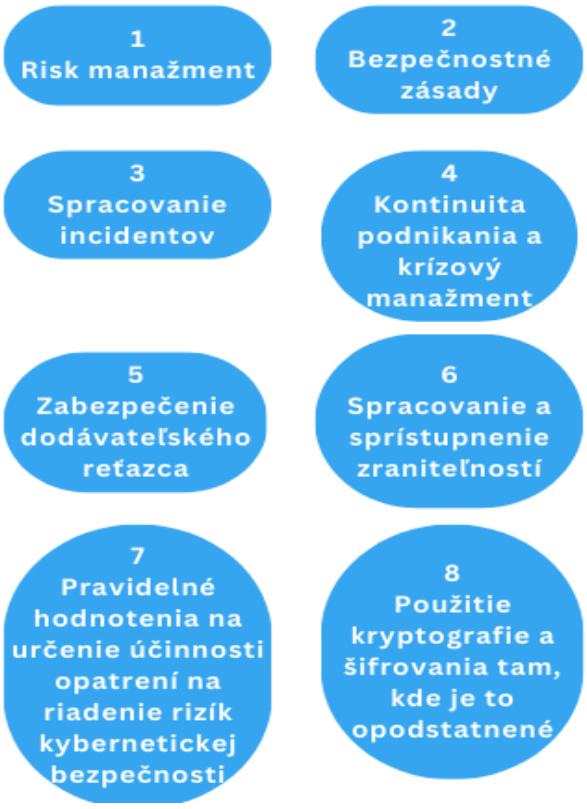
4.2.3 Smernica NIS 2

V roku 2016 Európska únia schválila smernicu NIS týkajúcu sa bezpečnosti sietí a informačných systémov, ktorá sa týkala oblasti IT a kybernetickej bezpečnosti, ako aj prevádzkovateľov základných služieb. Teraz Európska únia posilňuje tento rámec s novou smernicou NIS2, ktorá zvyšuje bezpečnosť sietí a informačných systémov v celej Únii. Cieľom nového právneho rámca je zvýšiť odolnosť organizácií proti kybernetickým hrozbám v celej EÚ, aby sa mohli lepšie brániť rizikám digitalizácie a závislosti kritickej infraštruktúry na digitálnych technológiách. To znamená, že mnohé firmy budú musieť prijať nové technické a prevádzkové opatrenia na ochranu svojich systémov a údajov.

Dňa 27.12.2022 bola zverejnená Smernica NIS II v Úradnom vestníku Európskej únie pod číslom 2022/2555. Táto smernica, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148, sa zaoberá zabezpečením vysokej úrovne kybernetickej bezpečnosti v celej EÚ. Nadobudla účinnosť 16.01.2023 a

členské štáty, vrátane Slovenskej republiky, majú do 17.10.2024 čas na prijatie a uverejnenie opatrení potrebných na dosiahnutie súladu so Smernicou NIS II. Tieto opatrenia sa musia uplatňovať od 18.10.2024. Zrušenie Smernice NIS bude účinné od tohto dátumu. Vzhľadom na tieto termíny majú členské štáty a povinné osoby dostatok času na prípravu a plnenie povinností vyplývajúcich z novej legislatívy týkajúcej sa kybernetickej bezpečnosti.[59]

NIS2 presne nešpecifikuje, aké nástroje a technológie kybernetickej bezpečnosti musia byť implementované. Navrhuje však rámec toho, ako by manažment mal postupovať v oblasti rizika a kybernetickej bezpečnosti, a to:



Obrázok 7 Rámec kybernetickej bezpečnosti navrhovaný normou NIS2
Zdroj: Vlastná tvorba podľa https://www.tricent.com/blog/nis2

Požiadavky na kybernetickú bezpečnosť NIS2 je možné riešiť pomocou tradičných systémov riadenia informačnej bezpečnosti, ako je ISO 27001 alebo ich ekvivalent. NIS2 nariaďuje, aby bol manažment zodpovedný za rôzne praktiky kybernetickej bezpečnosti, vrátane vykonávania hodnotení rizík kybernetickej bezpečnosti, implementácie technických

[59]BCH. Národný informačný systém pre biologickú diverzitu (NIS) [online]. In: Biodiverzita.sk: portál o biodiverzite na Slovensku. Bratislava: Biologické centrum SAV, 2015-2023 [cit. 2023-04-29]. Dostupné na: https://www.bch.sk/nis-2

a organizačných bezpečnostných opatrení, poskytovania školení a programov riadenia rizík a riadneho riadenia rizík.

Nepreukázanie súladu môže mať za následok sankcie vo výške najmenej 10 miliónov EUR alebo 2 % ročných príjmov dodávateľa. Podobne ako v prípade GDPR má NIS2 národné dozorné orgány zodpovedné za schvaľovanie opatrení na riadenie rizík kybernetickej bezpečnosti, dohľad nad ich implementáciou a zabezpečenie poskytovania príslušných školení na hodnotenie a zmierňovanie rizík kybernetickej bezpečnosti. Z hľadiska kybernetickej bezpečnosti poskytuje NIS2 organizáciám opodstatnenie, aby vyčlenili dodatočné zdroje na riadenie rizík, bezpečnostné technológie a školenia zamestnancov.[60]

Norma NIS2 bola vydaná 13. mája 2022. Členské štáty EÚ však dostali 21 mesiacov na presadenie NIS2 do vnútroštátneho práva. V dôsledku toho bude NIS2 plne účinná do roku 2024.

Ochrana kritickej infraštruktúry: smernica NIS2 nahradila pôvodnú smernicu o kybernetickej bezpečnosti z roku 2016 a rozšírila jej pôsobnosť na kritické odvetvia, vrátane energetiky, dopravy, bankovníctva a vody. Kriticky dôležité podniky budú musieť prijať technické a prevádzkové opatrenia na riešenie incidentov a zabezpečenie dodávateľského reťazca, až po plánovanie krízového riadenia. Pri porušení smernice hrozia pokuty a pozastavenie certifikácie. Európska sieť styčných organizácií pre kybernetické krízy, EU-CyCLONe, bude umožňovať spoluprácu medzi vnútroštátnymi agentúrami.

V prípade bezpečnostného incidentu musia byť kriticky dôležité subjekty povinné poskytnúť prvotné oznámenie do 24 hodín a podrobnejšie informácie do 72 hodín. Za nedodržanie smernice NIS2 hrozia pokuty a pozastavenie certifikácie, ako aj osobná zodpovednosť vedúcich pozícií podľa vnútroštátnych právnych predpisov.[61]

Smernica NIS II sa vzťahuje na všetky osoby s povinnosťou podľa súčasného zákona o kybernetickej bezpečnosti, vrátane prevádzkovateľov základnej a digitálnej služby, aj tých, ktorí sa ešte nehlásili na Národný bezpečnostný úrad. Táto smernica však prináša nový

[60] WULFF, Frank. Tricent – NIS2: What is it and How Will it Affect You? [online]. In: Tricent Blog: Insights and News for the Utilities Industry. 12 december 2022, [cit. 2023-05-01]. Dostupné na: https://www.tricent.com/blog/nis2

[61]ESET, Bezpečné vo firemne. Nová európska smernica NIS2 – potrebný základ pre spoločnú kybernetickú bezpečnosť [online]. In: Eset. 9. január 2023, [cit. 2023-04-25]. Dostupné na: https://bezpecnevofirme.eset.com/sk/firemna-bezpecnost/nova-europska-smernica-nis2-potrebny-zaklad-pre-spolocnu-kyberneticku-bezpecnost/

rozsah povinných osôb, ktoré zahŕňajú nové sektory a podsektory podľa zákona o kybernetickej bezpečnosti.

Norma NIS 2 sa sťahuje na nasledujúce odvetvia:[62,63]

Tabuľka 3 Subjekty na ktoré sa sťahuje norma NIS 2

Bankovníctvo	Sektor bankovníctva je regulovaný nariadením digit. prevádzkovej odolnosti finančného sektora.
Digitálna infraštruktúra	Poskytovatelia výmenných uzlov internetu (tzv. IXP), cloud computingu, dátového centra, služieb vytvárajúcich dôveru, elektronických komunikácií, CDN služieb, registrov TLD, služieb systému doménových mien (DNS), s výnimkou poskytovateľov root name serverov.
Doprava	• Komerční letecký prepravcovia, riadiace orgány letísk, prevádzkovatelia kontroly riadenia leteckej premávky • Prevádzkovateľ železničných tratí a dopravca využívajúci tieto trate • Cestné orgány zodpovedné za plánovanie, kontrolu a správu ciest spadajúcich do ich územnej pôsobnosti.
Energetika	Prevádzkovatelia distribučnej a prenosovej sústavy, výrobcovia a predajcovia elektrickej energie, nominovaní organizátori trhu s elektrikou, prevádzkovatelia dobíjacích staníc spolu s poskytovateľmi elektromobily.
Infraštruktúra fin. trhov	Sektor infraštruktúry finančných trhov je regulovaný nariadením digitálnej prevádzkovej odolnosti finančného sektora.
Odpadové vody	Subjekty zhromažďujúce, vypúšťajúce alebo upravujúce mestské alebo priemyslové odpadové vody alebo splašky, avšak okrem tých, pre ktoré ide o vedľajšiu činnosť k ich hlavnej činnosti.
Pitná voda	Dodávatelia a distribútori vody určenej pre ľudskú spotrebu.
Poskytovatelia riadených služieb	Dodávatelia a distribútori vody určenej pre ľudskú spotrebu, avšak okrem tých, pre ktoré ide o vedľajšiu činnosť k ich hlavnej činnosti zaoberajúcej sa distribúciou iných služieb.
Verejná správa	Ústredné orgány štátnej správy, verejná správa na regionálnej úrovni, súdy, štátne zastupiteľstvá a ďalšie inštitúcie významné pre chod štátu.
Zdravotníctvo	Poskytovatelia zdravotnej starostlivosti (nemocnice a ďalšie), subjekty vykonávajúce výskum a vývoj liečivých výrobkov a prípravkov, výrobci základných farmaceutických prípravkov.
Služby uvedené v prílohe II NIS2	Subjekty poskytujúce služby uvedené v prílohe I a splňujúce podmienku „stredný podnik" a subjekty poskytujúce služby uvedené v prílohe II a splňujúce podmienku „veľký podnik" a „stredný podnik" podľa odporúčaní Komisie (EÚ) 2003/361/EC budú regulované v režime „important" (nižšie nároky z hľadiska bezpečnostných opatrení), ak nebude stanovené zvláštnymi kritériami inak.
Chemický priemysel	Subjekty poskytujúce služby v chemickom priemysle, t. j. výrobcovia, distribútori, vrátane maloobchodníkov, ktorí skladujú a uvádzajú na trh chemickú látku alebo predmet
Odpadové hospodárstvo	Subjekty poskytujúce službu nakladania s odpadmi, t. j. zariadenia pre nakladanie s odpadmi, obchodníci, sprostredkovatelia, dopravci podľa zákona č. 79/2015 Z. z.,

[62]EUR-Lex Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 z 12. októbra 2022 [online]. In: Úradný vestník Európskej únie. Brusel: Európska únia, 2022, [Cit. 2023-04-27]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32022L2555.

[63] TOPPRIVACY. NIS2 – Povinne regulované služby [online]. In: Topprivacy.sk. [cit. 2023-04-28]. Dostupné na: https://www.topprivacy.sk/userfiles/file/NIS2_Topprivacy%20-%20povinne%20regulovan%c3%a9%20slu%c5%beby.pdf

	okrem tých, pre ktoré nakladanie s odpadmi nie je ich hlavnou ekonomickou činnosťou
Poštové služby	Subjekty poskytujúce poštové služby, t. j. výber, triedenie, prepravu a dodanie poštových zásielok, vrátane prevádzkovateľov kuriérskych služieb.
Potravinárstvo	Potravinárske subjekty, ktoré sa zaoberajú veľkoobchodnou distribúciou a priemyselnou výrobou alebo spracovaním.
Výroba	Výroba zdravotníckych a diagnostických zdravotníckych prostriedkov, počítačov, elektronických a optických prístrojov, elektrických zariadení, strojov a zariadení, motorových vozidiel (okrem motocyklov), prívesov a návesov a ostatných dopravných prostriedkov a zariadení
Výskum	Výskumné organizácie, s výnimkou vzdelávacích inštitúcií, ktorých hlavným cieľom je vykonávať aplikovaný výskum alebo experimentálny vývoj s ohľadom na využitie výsledkov tohto výskumu pre komerčné účely

Zdroj: vlastné spracovanie podľa TOPPRIVACY. NIS2 - Povinne regulované služby [online]. In: Topprivacy.sk. [cit. 2023-04-28]. Dostupné na: https://www.topprivacy.sk/userfiles/file/NIS2_Topprivacy%20-%20povinne%20regulovan%c3%a9%20slu%c5%beby.pdf.

4.2.4 Identifikácia oblastí informačnej bezpečnosti, ktoré vyžadujú aktualizáciu a doplnenie na základe nových požiadaviek smernice NIS 2

V tejto kapitole sa aj zameriame na identifikáciu konkrétnych oblastí, ktoré vyžadujú aktualizáciu a doplnenie na základe nových požiadaviek smernice NIS2, konkrétne v súvislosti so starými normami ISO/IEC 2701, GDPR.

ISO/IEC 27001: Implementácia smernice NIS2 bude mať vplyv na mnohé oblasti informačnej bezpečnosti, ktoré sú už pokryté normou ISO/IEC 27001. Nová smernica zavádza prísnejšie požiadavky na identifikáciu a riadenie rizík, plánovanie krízového riadenia, zlepšenie riadenia a správu dodávateľského reťazca. Podnik bude musieť aktualizovať svoje súčasné politiky a postupy, aby zodpovedali novým požiadavkám smernice NIS2.

GDPR: Smernica NIS2 obsahuje aj požiadavky na ochranu osobných údajov, ktoré môžu mať vplyv na oblasti informačnej bezpečnosti pokryté GDPR. Podnik bude musieť zvážiť, ako zabezpečí dodržiavanie nových požiadaviek smernice NIS2 v súvislosti s ochranou osobných údajov a ako ich integruje do svojich súčasných postupov ochrany údajov.

Tieto dve normy je teda potrebné aktualizovať hlavne v súvislosti s normou NIS 2 a to konkrétne riadenie a monitorovanie prístupu k informáciám. Staré normy, ako ISO/IEC 27001 a GDPR, ustanovujú zásady na zabezpečenie ochrany dát a obmedzenie prístupu k nim len pre autorizované osoby. Keďže náš skúmaný podnik, pôsobí prevažne vo verejnom sektore, tak obmedzenie a ochrana dát je kritická. To zahŕňa aj riadenie prístupov tretích

strán, ktoré majú prístup k informáciám podniku napríklad štátna správa. Norma NIS 2 tiež poskytuje pokyny na monitorovanie prístupu k informáciám a na zabezpečenie, že iba oprávnené osoby majú prístup k citlivým informáciám.

Ďalšou oblasťou, ktorá by mohla vyžadovať aktualizáciu na základe normy NIS 2, je zálohovanie a obnova dát. Norma NIS 2 ustanovuje požiadavky na zálohovanie a obnovu dát s cieľom minimalizovať straty dát v prípade havárie alebo iného incidentu. Staré normy, ako ISO/IEC 27001, ustanovujú zásady na zabezpečenie zálohovania a obnovy dát, ale norma NIS 2 poskytuje podrobnejšie pokyny a príklady na minimalizovanie straty dát.

Zameriame sa aj na zavedenú normu v podniku PCI-DSS. Norma je dôležitá pre ochranu informácií v podniku, ale na základe nových požiadaviek NIS2 by mohli vyžadovať aktualizáciu a doplnenie.

NIS2 vyžaduje, aby organizácie mali jasný plán prevencie kybernetických útokov, ktorý by zahŕňal aj plán obnovy. Implementácia nových požiadaviek NIS2 by mohla tiež vyžadovať aktualizáciu politiky riadenia hesiel, riadenie prístupu a ďalších bezpečnostných opatrení. Pri implementácii NIS2 by sa mohlo zvažovať, ako by sa tieto nové požiadavky dali zahrnúť do existujúcich procesov ISO, GDPR a PCI-DSS, aby sa zabezpečilo, že nová norma je plne integrovaná a aby sa minimalizovali neefektívne dvojité práce. Rovnako by sa mohlo zvažovať, či by bolo lepšie nahradiť existujúce normy novou normou NIS2 alebo pokračovať v používaní súčasných noriem a doplniť ich o nové požiadavky.

Ďalšie vec, ktorú treba aktualizovať, je oblasť zálohovania a obnovy dát. Nová norma NIS 2 obsahuje požiadavky na zálohovanie a obnovu dát a tiež na testovanie a dokumentovanie týchto postupov. To je veľmi dôležité pre zabezpečenie rýchlej obnovy v prípade výpadku alebo útoku na informačné systémy podniku. Tieto požiadavky by mohli mať vplyv na súčasné postupy zálohovania a obnovy dát, ktoré sú už v podniku zavedené.

V neposlednom rade, nová norma NIS 2 môže mať vplyv na oblasť monitorovania a detekcie bezpečnostných incidentov. Smernica NIS 2 zahŕňa požiadavky na monitorovanie informačných systémov na detekciu možných hrozieb. To môže znamenať aktualizáciu súčasných nástrojov na monitorovanie informačných systémov alebo zavedenie nových nástrojov na detekciu hrozieb. Podnik by mohol investovať do nových nástrojov a procesov na zabezpečenie efektívneho monitorovania a detekcie hrozieb.

Výsledkom implementácie smernice NIS2 by malo byť zlepšenie celkovej úrovne informačnej bezpečnosti v podniku. Podnik by mal mať jasný a dobre definovaný postup na

správu incidentov a zraniteľností a mala by byť zavedená aj systematická kontrola a hodnotenie bezpečnosti informačných systémov. To by mohlo pomôcť minimalizovať riziká spojené s kybernetickými hrozbami a ochrániť podnik pred vysokými nákladmi.

4.3 Návrh a implementácia nových riešení informačnej bezpečnosti

V tejto kapitole sa budeme venovať tvorbe a aplikácií nových riešení informačnej bezpečnosti. Informačná bezpečnosť je nevyhnutná, ako sme už spomínali v predchádzajúcich kapitolách a preto je nevyhnutné neustále sa prispôsobovať novým hrozbám a zdokonaľovať súčasné riešenia implementované v podniku. Návrh a realizácia nových bezpečnostných opatrení, ktoré zabezpečia ochranu informačných aktív podniku, budú hlavnými témami tejto kapitoly.

Posúdime nebezpečenstvá a ohrozenia, ktoré v súčasnosti existujú, a následne navrhneme vhodné protiopatrenia. Prejdeme si aj to, ako sa tieto opatrenia skutočne zavádzajú do praxe a zhodnotíme ich úspešnosť.

Náplňou tejto kapitoly je poskytnúť prehľad aplikovaných, moderných riešení informačnej bezpečnosti v reálnom podniku a ukázať, ako môžu mať aj drobné úpravy významný vplyv.

Návrh nových riešení, ktoré zodpovedajú požiadavkám smernice NIS 2

Táto časť sa zameriava na navrhovanie nových riešení informačnej bezpečnosti, ktoré spĺňajú požiadavky smernice NIS 2. Zanalyzujeme hlavné rozdiely medzi súčasnými implementovanými normami v podniku a navrhovanou smernicou NIS 2.

ISO 27001: táto norma zohráva pri monitorovaní informačnej bezpečnosti veľmi dôležitú úlohu. Preskúmava, udržiava a zlepšuje informačnú bezpečnosť podniku. Funguje ako celkový riadiaci a kontrolný rámec pre riadenie rizík informačnej bezpečnosti organizácie. Hlavným cieľom tejto normy je zvyčajne zaviesť, navrhnúť, implementovať a riadiť efektívnu informačnú bezpečnosť. Tento proces vedie k celému radu výhod pre organizáciu, ktoré však môže smernica NIS 2 rozšíriť a doplniť. [64]

[64] Osborne, M. - Ryan, P. Information Security Challenge and Breach Effectiveness: Qualitative Research Findings. In: Journal of Computer Information Systems: Spring 2014, Vol. 54, Issue 3, s. 29-38. [cit. 2023-04-28]. Dostupné na: https://d1wqtxts1xzle7.cloudfront.net/38094740/36585913256483-libre.pdf?1436081591=&response-content-disposition=inline%3B+filename%3DInformation_Security_Challenge_and_Breac.pdf&Expires=1682683171&Signature=DgFbAoHdrkVV2KK4SdBH67t1BAIU0nyY~zXTTEV-T1lSYRhRTi9FlgLIUrJqJ9JRBagwLXTp957WIxdalyATBHtkt37HGuMO3av8yA4szIwsEHvkVe2jnpbiMLVQsWdOvaEeaHG5xvEIOQQwTa~tIi7ldS7fJVnxh429GGEgn0eJVZxatS9OOIl~~RBnbbkTaoqba8kMjykea9oUBpcKFnimELRvxjJjYXWI27jEkkU6Qsis4XNpFX7~kH6M-6zdmpn6RK4OEUKV-

V nasledujúcej tabuľke je prehľad odlišností, ktoré dané normy pokrývajú v podnikových oblastiach, ktoré sme si identifikovali v predchádzajúcej kapitole.

Tabuľka 4 Rozdiely noriem v oblasti identifikácie a riadenia rizík

Zálohovanie a obnova dát	
Norma ISO 27001	**Norma NIS 2**
Norma ISO 27001 poskytuje rámcovú štruktúru pre zabezpečenie informačnej bezpečnosti a rieši problematiku riadenia rizík v súvislosti s informačnou bezpečnosťou.	Smernica NIS 2 sa zameriava na posilnenie ochrany kľúčových digitálnych služieb a infraštruktúr v Európskej únii.
V rámci normy ISO 27001 existuje požiadavka na plánovanie zálohovania a obnovy dát, ktorá zahŕňa plánovanie zálohovania, testovanie obnovy a dokumentáciu týchto postupov.	NIS 2 obsahuje požiadavky na zálohovanie a obnovu dát pre kritické digitálne služby a infraštruktúry, aby sa minimalizovali vplyvy v prípade incidentov v oblasti kybernetickej bezpečnosti.
Norma ISO 27001 poskytuje podrobné pokyny a postupy pre zálohovanie a obnovu dát, vrátane kritérií pre zálohovacie a obnovovacie procesy, testovanie obnovy a pravidelnú údržbu.	Smernica NIS 2 uvádza, že poskytovatelia kritických digitálnych služieb a infraštruktúr by mali mať vypracovaný plán obnovy, ktorý zahŕňa pravidelné testovanie obnovy, a to na základe rizikového manažmentu.
ISO 27001 zahŕňa aj požiadavky na zabezpečenie ochrany dát, zálohovanie a obnova dát v prípade havárií a krízového riadenia.	NIS 2 má tiež požiadavky na kybernetickú bezpečnosť a krízové riadenie pre kritické digitálne služby a infraštruktúry.
Riadenie a monitorovanie prístupu k informáciám	
Norma ISO 27001	**Norma NIS2**
Vymedzuje požiadavky pre riadenie informačnej bezpečnosti všeobecne a týka sa všetkých typov organizácií.	Vymedzuje základné požiadavky na riadenie prístupu k informáciám, ktoré majú byť splnené organizáciami, ktoré zabezpečujú kritické služby a digitálne služby.
Zameriava sa na riadenie informačnej bezpečnosti všeobecne a poskytuje ucelený rámec pre riadenie prístupu k informáciám, ktorý zahŕňa aj ďalšie aspekty, ako sú napríklad prístupové práva a riadenie identít.	Zameriava sa na zabezpečenie prístupu k informáciám v súvislosti s kritickými a digitálnymi službami a kladie dôraz na základné požiadavky, ako sú napríklad autentifikácia a autorizácia používateľov.
Tiež obsahuje požiadavky na monitorovanie a sledovanie informačnej bezpečnosti, ale neposkytuje špecifické požiadavky pre monitorovanie prístupu k informáciám.	Stanovuje požiadavky na monitorovanie a sledovanie prístupu k informáciám s cieľom odhaliť a riešiť bezpečnostné incidenty.
Identifikácia a riadenie rizík	

zNbKkcQPEqlfCKQ0Pgkc0R38RNkorkk8902bpFOtXTjkmPnO6o7BwjBLyXvUw2OM4a6eZS38w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA

Norma ISO 27001	Norma NIS2
Poskytuje všeobecné zásady pre riadenie bezpečnosti informácií a podporuje identifikáciu a riadenie rizík.	Sústreďuje sa priamo na riziká, ktorým čelia poskytovatelia digitálnych služieb a zabezpečovateľské služby.
Všeobecný rámec pre riadenie rizík, ktorý obsahuje prvky, ako sú hodnotenie rizík, riadenie rizík a monitorovanie rizík.	Presný postup na identifikáciu a hodnotenie rizík
Odporúčania na vytvorenie bezpečnostnej politiky, vytvorenie postupov na riadenie rizík a vykonávanie interných a externých auditov bezpečnosti informácií.	Presné požiadavky na identifikáciu, hodnotenie a riadenie rizík a zabezpečenie pravidelného hodnotenia a aktualizácie opatrení na riadenie rizík.
Široký rámec pre riadenie bezpečnosti informácií, ktorý sa môže použiť pre rôzne organizácie a odvetvia.	Zameriava sa na poskytovateľov digitálnych služieb.
Monitorovanie bezpečnostných incidentov	
Norma ISO 27001	**Norma NIS2**
Neuvádza žiadne presné požiadavky na monitorovanie bezpečnostných incidentov, ale spomína na to, že organizácia by mala mať vytvorený proces na identifikáciu a klasifikáciu bezpečnostných incidentov	Norma NIS 2 vyžaduje, aby organizácie monitorovali svoje siete a služby v reálnom čase, aby identifikovali a vyriešili bezpečnostné incidenty.
Pri implementácii ISO 27001 je organizácia schopná navrhnúť a implementovať vlastné riešenia, ktoré najlepšie vyhovujú jej potrebám a zdrojom.	Norma NIS 2 obsahuje presné požiadavky na monitorovanie bezpečnostných incidentov a vyžaduje, aby organizácie mali vytvorený plán monitorovania, aby boli schopné identifikovať a vyriešiť bezpečnostné incidenty.

Zdroj: Vlastné spracovanie

Tabuľka zobrazuje porovnanie implementovanej normy ISO 27001 v skúmanom podniku a novej normy NIS 2 v identifikovaných oblastiach, ktoré prejdú implementáciou nových riešení.

GDPR- rozširuje rozsah ochrany údajov, takže každá osoba alebo organizácia, ktorá zhromažďuje a spracúva informácie o občanoch EÚ, musí dodržiavať GDPR bez ohľadu na to, kde sídli alebo kde sú údaje uložené. Cloudové úložisko nie je výnimkou. Rozšírila sa aj definícia osobných údajov. Uvádza, že osobné údaje zahŕňajú informácie, ktoré môžu priamo alebo nepriamo identifikovať jednotlivca.

V nasledujúcej tabuľke je vypracované porovnanie noriem GDPR a NIS 2.

Tabuľka 5 Rozdiely noriem v oblasti identifikácie a riadenia rizík.

Rozsah ochrany	
GDPR	**Norma NIS2**
Zameriava sa na ochranu osobných údajov a zabezpečenie ich správneho spracovania.	Norma NIS 2 sa zameriava na identifikáciu, hodnotenie a riadenie rizík v oblasti kybernetickej bezpečnosti.
Použitie	
GDPR	**Norma NIS2**
Vzťahuje na všetky spoločnosti, ktoré spracúvajú osobné údaje občanov EÚ.	Vzťahuje na kritické digitálne služby a iné subjekty, ktoré poskytujú digitálne služby alebo využívajú digitálne nástroje na riadenie kritických oblastí.
Požiadavky	
GDPR	**Norma NIS2**
Obsahuje prísne požiadavky na ochranu osobných údajov, ako napríklad nahlásenie porušenia dát, zavedenie opatrení technickej a organizačnej ochrany a ochranu súkromia.	Obsahuje požiadavky na identifikáciu rizík, zavedenie bezpečnostných opatrení a implementáciu bezpečnostných štandardov.
Penále	
GDPR	**Norma NIS2**
GDPR ukladá prísne sankcie za porušenie ochrany osobných údajov, ktoré môžu byť až do výšky 4 % celkového obratu spoločnosti alebo 20 miliónov eur, podľa toho, čo je vyššie.	Norma NIS 2 ukladá sankcie za porušenie kybernetickej bezpečnosti, ktoré môžu byť až do výšky 2 % ročného obratu, alebo 10 miliónov eur, podľa toho, čo je vyššie.

Zdroj: Vlastné spracovanie

V predchádzajúcej tabuľke je zobrazený rozsah použitia GDPR a smernice NIS 2. je zjavné, že nová smernica nedokáže nahradiť aplikovanú normu GDPR, ktorá zodpovedá za ochranu osobných údajov, avšak aplikáciou NIS 2, dokážeme rozšíriť informačnú ochranu citlivých aktív podniku. Tým sa zvýši celková kybernetická bezpečnosť podniku.

Vykonali sme komparatívnu analýzu implementovaných smerníc v podniku, konkrétne tých, ktoré sa týkajú informačnej bezpečnosti. V organizácií pôsobí smernica ISO 27001 a pravidlá ochrany osobných údajov, ktoré upravuje GDPR. Po vykonaní komparatívnej analýzy implementovaných noriem v podniku a novej smernice NIS 2, sme boli schopní identifikovať oblasti, nepokryté súčasnými normami. Tieto oblasti, budú doplnené rozšírenou verziou normy o informačnej bezpečnosti NIS 2.

V nasledujúcej kapitole Diskusia, prezentujeme sumár návrhov a opatrení, nevyhnutné pre implementáciu štandardov a nariadení. Tieto návrhy by mal podnik zvážiť a zakomponovať do svojej informačnej stratégie ochrany voči kybernetickým útokom.

Smernica NIS 2 rozširuje pôsobnosť a dosah informačnej bezpečnosti až na štátnu úroveň. Každý podnik, ktorý pôsobí pre alebo vo verejnom sektore musí tieto nové nariadenia dodržiavať v prípade ak spadá do skupín uvedených v prílohe 1.

5 Diskusia

V tejto kapitole si predstavíme, ako by podnik mohol implementovať pravidlá a postupy smernice NIS 2. Na úvod, je potrebné vysvetliť prečo podnik spadá pod vplyv tejto smernice. Skúmaný podnik zamestnáva 15 zamestnancov, čo znamená, že je radený do kategórie malých podnikov. Nová norma upravuje podľa článku 2, rozsah pôsobností, odsek 1, iba stredné podniky alebo podniky, ktoré presahujú limity stredného podniku, teda veľké podniky. Organizácia, na ktorú sme vypracúvali implementáciu novej smernice, však spadá do kategórie, kde veľkosť firmy nehrá významnú rolu, vďaka pôsobeniu vo verejno-stavebnom sektore, predovšetkým, konzultácia a výstavba pozemných komunikácií ako diaľnice a iné významne stavebné diela pre štát. Uplatňujeme teda článok 2, odsek 2, konkrétne body:[65]

a) služby poskytujú: ii) poskytovatelia dôveryhodných služieb;

b) narušenie služby poskytovanej subjektom by mohlo vyvolať významné systémové riziko, najmä v odvetviach, v ktorých by takéto narušenie mohlo mať cezhraničný vplyv;

Na základe komparatívnej analýzy legislatívnej úpravy informačnej bezpečnosti v európskom priestore sme navrhli niekoľko odporúčaní pre podnik, ktoré by mohli pomôcť pri implementácii smernice NIS 2. Tieto odporúčania sú zhrnuté v tabuľke nižšie.

Tabuľka 6 Prehľad navrhovaných opatrení v súlade so smernicou NIS 2

Návrh implementácie riešení smernice NIS 2	
Návrh číslo:	**Zálohovanie ochrana a obnova dát**
1	Posilnenie súčasnej ochrany kľúčových služieb, ktoré podnik poskytuje pre verejný sektor a to predovšetkým, voči štátnym organizáciám.
2	Vytvorenie bezpečnejšieho zálohovania a obnovy dát na minimalizáciu vplyvov, ak je narušená kritická infraštruktúra.
3	Vypracovať plán obnovy, zahŕňajúci pravidelné testovanie obnovy s využitím rizikového manažmentu.

[65]SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022:o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

4	Implementovať požiadavky novej smernice NIS 2 na kybernetickú bezpečnosť a krízové riadenie pre digitálne služby infraštruktúry.
Riadenie a monitorovanie prístupu k informáciám	
5	Zadefinovanie základných otázok a požiadaviek pre správne riadenie prístupu k informáciám.
6	Dôkladné zabezpečenie prístupu k informáciám a digitálnej infraštruktúry, podľa nariadení smernice NIS 2.
7	Prijatie požiadaviek na monitorovanie a sledovanie prístupu k informáciám na odhalenie bezpečnostných hrozieb a incidentov.
Identifikácia a riadenie rizík	
8	Vytvoriť presný postup identifikácie a hodnotenia rizika
9	Zabezpečenie pravidelného hodnotenia a aktualizácie informačných systémov.
Ostatné	
10	Vytvorenie riadenia oznamovacích povinností, podľa nariadení smernice NIS 2.
11	Zlepšenie zabezpečenia mobilných zariadení poskytovaných podnikom pre svojich zamestnancov.
12	Zlepšené a pravidelné školenia zamestnancov
13	Vytvorenie komplexnej politiky informačnej bezpečnosti.

Zdroj: vlastné spracovanie

Novoprijatou smernicou NIS 2 sa podnikom, spadajúcich pod vplyv tejto smernice, ukladajú nové povinnosti v oblasti ochrany a zálohovania kľúčových digitálnych služieb, dát a infraštruktúr v Európskej únií a mnoho ďalšieho. Po analýze súčasných nariadení smernice NIS 2, navrhujeme nasledujúce riešenia na úspešnú implementáciu požiadaviek tejto smernice:[66]

Návrh č. 1: Posilnenie súčasnej ochrany kľúčových služieb, ktoré podnik poskytuje pre verejný sektor a do predovšetkým voči štátnym organizáciám.

- Podľa odseku 109 všeobecných nariadení smernice Európskeho parlamentu sa subjektom ukladá povinnosť udržiavať presné databázy údajov pre poskytovanie zákonného prístupu nadriadenými európskymi inštitúciami. Podnik takýmito

[66]SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022: o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

databázami nedisponuje, čo znamená, že organizácia nemá čo preukázať nadriadeným orgánom a mal by pristúpiť k ich tvorbe.

- Táto norma v odseku 83, všeobecných nariadení prikazuje subjektom, poskytujúcich kritické služby, aby mali zaistenú svoju informačnú bezpečnosť a bezpečnosť sietí internými pracovníkmi, alebo externými dodávateľmi. Zvýraznené je kontinuálne zabezpečovanie pred kybernetickými hrozbami, no v našom prípade podnik túto povinnosť nesplňuje. Informačná bezpečnosť je zaistená finančným riaditeľom, ktorý nemá dostatočné schopnosti ani čas, na implementáciu a sledovanie dodržiavania nových pravidiel. Preto navrhujeme aby firma prijala nového interného zamestnanca, alebo externý subjekt, ktorý bude vykonávať údržbu týchto sietí.
- Podnik spadá pod sektor poskytovateľov dôveryhodných služieb a preto sa mu nariaďuje zaradenie pod rozsah pôsobností a spolupráce s jednotkami CSIRT a rozsah smerníc, ktoré ovplyvňuje a to nariadenie (EÚ) 2016/679 a smernica 2002/58/ES. CSIRT je skupina IT profesionálov, ktorí poskytujú organizácii služby a podporu v súvislosti s hodnotením, riadením a prevenciou núdzových situácií súvisiacich s kybernetickou bezpečnosťou, ako aj koordináciou úsilia v oblasti reakcie na incidenty .[67] Organizácia by pre to mala prijať opatrenie na implementáciu rámca, v ktorom by mohol CSIRT pôsobiť.

Návrh č. 2: Vytvorenie bezpečnejšieho zálohovania a obnovy dát na minimalizáciu vplyvov, ak je narušená kritická infraštruktúra.

- Pravidlá smernice ukladajú presné postupy zavádzania a využívania služieb cloud computingu a to: „digitálne služby, ktoré umožňujú správu na požiadanie a vzdialený širokopásmový prístup ku škálovateľnému a pružnému súboru zdieľateľných počítačových zdrojov, a to aj ak sa tieto zdroje nachádzajú na viacerých miestach. Počítačové zdroje zahŕňajú zdroje, ako sú siete, servery alebo iná infraštruktúra, operačné systémy, softvér, úložiská, aplikácie a služby. Modely služieb cloud computingu zahŕňajú okrem iného infraštruktúru ako službu (IaaS), platformu ako službu (PaaS), softvér ako službu (SaaS) a sieť ako službu (NaaS). Modely zavádzania cloud computingu by mali zahŕňať súkromný, komunitný, verejný a

[67] TECHTARGET. Computer Security Incident Response Team (CSIRT) [online]. In: WhatIs.com [cit. 2023-04-29]. Dostupné na: https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT.

hybridný cloud..“[68] Z manažérskeho hľadiska, odporúčame podniku implementáciu všetkých potrebných nástrojov zálohy dát.

- Článok 27, odsek 1, registra subjektov ukladá povinnosť subjektu používať zálohovacie služby ako cloud, poskytovateľov zálohových služieb, atď., iba registrované v zozname vytvoreným agentúrou ENISA. Navrhujeme, aby kompetentní zamestnanci preštudovali tento register a zvážili nové možnosti využívania cloudových zariadení, ktoré musia byť takto registrované. V našom prípade podnik používa cloudové služby od spoločnosti Google, ktorá spadá do tohto registra, navrhujeme však aby spoločnosť zvolila dvojstupňové zabezpečenie svojich informačných aktív, použitím ešte jedného zálohového centra, spomínaného v predchádzajúcom bode.

Návrh č. 3: Vypracovať plán obnovy, zahŕňajúci pravidelné testovanie obnovy s využitím rizikového manažmentu.

- NIS 2 vyžaduje, aby organizácie mali plány zálohovania, vykonávali cvičenia a školili všetky relevantné strany. Odporúčame aby skúmaná organizácia identifikovala svoje najvýznamnejšie slabé miesta, lebo aktualizovaná smernica od nej vyžaduje, aby zaviedla jasné postupy na predchádzanie útokom a dohodla sa na metódach detekcie potenciálnych incidentov. Výsledkom by mal byť plán reakcie a obnovy na incidenty.

Návrh č. 4: Implementovať požiadavky novej smernice NIS 2 na kybernetickú bezpečnosť a krízové riadenie pre digitálne služby infraštruktúry.

- V dôsledku rozdielnych požiadaviek na kybernetickú bezpečnosť v jednotlivých štátoch Európskej únie, norma NIS 2 prichádza s jednotenými pravidlami na požiadavky informačnej bezpečnosti. Skúmaný podnik má uplatnené požiadavky na informačnú bezpečnosť normou ISO 27001. Táto norma, však nesplňuje nové nariadenie o aktívnej kybernetickej ochrane organizácie alebo štátu. V článku 57 sa hovorí, že „aktívna kybernetická ochrana je aktívna prevencia, odhaľovanie, monitorovanie, analýza a zmierňovanie narušení bezpečnosti siete v spojení s využitím spôsobilostí nasadených v zasiahnutej sieti a mimo nej, a nie reaktívne

[68]SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022: o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

reagovanie. Mohla by zahŕňať poskytovanie bezplatných služieb alebo nástrojov určitým subjektom zo strany členských štátov, a to vrátane samoobslužných kontrol, detekčných nástrojov a služieb odstraňovania.“ Preto navrhujeme, aby podnik využil bezplatné služby štátnych organov a uplatnil nástroje aktívnej kybernetickej ochrane, ktorá sa zakladá jednotnom úsilí celej Európskej únie uplatňovať prevenciu, odhaľovanie, riešenie a blokovanie útokov voči informačným systémom.

Návrh č. 5: Zadefinovanie základných otázok a požiadaviek pre správne riadenie prístupu k informáciám.

- Podnik nemá jasne zadefinovanú hierarchiu prístupu k informáciám. Odporúčame, aby boli identifikované stupne dôležitosti a citlivosti informácií a následne podľa pozície alebo oprávnenosti zamestnanca, bol udelený prístup k ním.

Návrh č. 6: Dôkladné zabezpečenie prístupu k informáciám a digitálnej infraštruktúry, podľa nariadení smernice NIS 2.

- Smernica NIS 2 špecifikuje v odseku 98 požiadavky na zaistenie informačných sietí a komunikačných služieb. Presadzuje podporu používania šifrovacích technológií a to konkrétne šifrovanie bez medzi fáz, kartografia, segmentácia označovanie, politika prístupu a automatizované rozhodnutia o prístupe. Podnik nemá zavedenú ani jednu z menovaných metód. Je potrebné, aby si spoločnosť najala certifikovaného odborníka alebo firmu na zavedenie vyššie spomínaných postupov do organizácie.

Návrh č. 7: Prijatie požiadaviek na monitorovanie a sledovanie prístupu k informáciám na odhalenie bezpečnostných hrozieb a incidentov.

- V odseku 44 smernice NIS 2 sa hovorí, že subjekt, teda náš podnik, má jednotke CSIRT proaktívne oznamovať organizačné riziká a kritické zraniteľnosti. Táto jednotka by mala byť schopná monitorovať aktíva subjektu a preto, by podnik mal umožniť toto monitorovanie pre lepšiu informačnú bezpečnosť.
- Odporúčame aby podnik aplikoval do svojej kybernetickej ochrany politiky kybernetickej hygieny. Tieto postupy obsahujú podľa novej smernice, odsek 49: „základy pre ochranu infraštruktúry sietí a informačných systémov, bezpečnosť hardvéru, softvéru a online aplikácií a ochranu obchodných údajov alebo údajov o koncových používateľoch, na ktoré sa subjekty spoliehajú. Politiky kybernetickej hygieny zahŕňajúce spoločný základný súbor postupov vrátane aktualizácií softvéru a hardvéru, zmeny hesiel, riadenia nových inštalácií, obmedzenia prístupových účtov

na úrovni správcu a zálohovania údajov umožňujú proaktívny rámec pripravenosti a celkovej bezpečnosti a ochrany v prípade incidentov alebo kybernetických hrozieb.“[69]

Návrh č. 8: Vytvoriť presný postup identifikácie a hodnotenia rizika.

- Organizácia nemá vytvorený ani aplikovaný žiadny ucelený postup na odhalenie rizika. V smernici NIS 2 sa špecifikuje, čo by tento postup mal obsahovať, a to: „opatrenia by mali zahŕňať opatrenia na identifikáciu rizika incidentov, opatrenia na predchádzanie incidentom, ich odhaľovanie, reakciu na ne a zotavenie sa z nich, ako aj opatrenia na zmiernenie ich vplyvu. Bezpečnosť sietí a informačných systémov by mala zahŕňať bezpečnosť uchovávaných, prenášaných a spracúvaných údajov.“[70] Tieto postupy odporúčame vytvoriť a mohli by byť súčasťou opatrení na riadenie kybernetických rizík.
- Ako treba mať zabezpečenú informačnú bezpečnosť, tak isto treba uplatniť prístup na identifikáciu všetkých možných rizík a nie len v kybernetickom priestore. Odstavec 79 smernice NIS 2 hovorí, že „fyzické prostredie informačných systémov, treba chrániť pred udalosťami, ako je krádež, požiar, povodeň, výpadok telekomunikácie alebo elektrickej energie, alebo pred neoprávneným fyzickým prístupom, poškodením alebo zásahom.“[71] Tieto nariadenia sa odvolávajú na normu ISO 27000, kde sú definované. Navrhujeme aby podnik implementoval do svojej politiky aj smernicu IS 27000, ktorá výrazne prispeje k ochrane informačných aktív.

Návrh č. 9: Zabezpečenie pravidelného hodnotenia a aktualizácie informačných systémov.

- Navrhujeme aby v súlade s politikou kybernetickej hygieny, ktorú predpisuje novo implementovaná smernica, podnik pristúpil k pravidelnej kontrole a aktualizácií svojich softvérov, hardvérov, hesiel, zálohovania a kontrole prístupu podľa odstavca 49.

[69]SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022: o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

[70]SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022: o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2)

[71] SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022: o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

Návrh č. 10: Vytvorenie riadenia oznamovacích povinností, podľa nariadení smernice NIS 2.

- Prijatím tejto smernice sa podnik zaväzuje plniť oznamovanie incidentov, ktoré ohrozili alebo ohrozujú informačnú bezpečnosť organizácie alebo štátu. Tieto povinnosti sú:
    a) Oznamovacia povinnosť incidentov: Ak podnik utrpí kybernetický incident, musí o ňom informovať príslušný národný orgán do 24 hodín od zistenia incidentu.
    b) Oznamovacia povinnosť kritických incidentov: Ak podnik utrpí kritický incident, ktorý má vplyv na poskytovanie kritických služieb, musí o ňom informovať príslušný národný orgán do jednej hodiny od zistenia incidentu.
    c) Oznamovacia povinnosť zraniteľností: Ak podnik objaví zraniteľnosť, ktorá má vplyv na jeho informačné systémy alebo služby, musí o nej informovať príslušný národný orgán do 24 hodín od zistenia zraniteľnosti.

Návrh č. 11: Zlepšenie zabezpečenia mobilných zariadení poskytovaných podnikom pre svojich zamestnancov.

- Podnik by mal zabezpečiť svoje mobilné zariadenia a aplikácie, aby sa predišlo útokom na mobilné zariadenia a zabezpečila sa dostatočná ochrana zdieľaných informácií. To môže byť dosiahnuté pomocou pravidelných aktualizácií a monitorovania.

Návrh č. 12: Zlepšené a pravidelné školenia zamestnancov.

- Zlepšené školenia svojich zamestnancov v oblasti kybernetickej bezpečnosti a informačnej bezpečnosti. To zahŕňa výučbu správneho používania hesiel, rozpoznávania phishingových útokov a oboznamovanie zamestnancov s postupmi pri hlásení bezpečnostných incidentov.

Návrh č. 13: Vytvorenie komplexnej politiky informačnej bezpečnosti.

- Ako posledný návrh predstavujeme zavedenie komplexnej firemnej politiky o informačnej bezpečnosti. Podnik nemá prijatú a aplikovanú žiadnu politiku, ktorá upravuje všetky oblasti informačnej bezpečnosti. Navrhujeme, aby kompetentní pracovníci po preštudovaní prezentovaných návrhov, zhodnotili ich prínos pre kybernetickú bezpečnosť podniku a vytvorili súhrnný a prehľadný postup krokov

a nariadení v ktorom sa pokryje každý jeden aspekt aplikovaných smerníc o informačnej bezpečnosti ako NIS 2, ISO 27000, ISO 27001, GDPR.

V predošlej kapitole sme taktiež porovnávali a skúmali **GDPR** a smernicu NIS 2. Hodnotíme, že GDPR a NIS 2 sú odlišné smernice, ktoré sa zameriavajú na rozličné aspekty informačnej bezpečnosti. GDPR sa zameriava na ochranu osobných údajov a zabezpečenie ich správneho spracovania, zatiaľ čo NIS 2 sa zameriava na ochranu kritických informačných systémov a sietí v kľúčových odvetviach. Preto nie je možné navrhnúť, že by bolo vhodné nahradiť GDPR novou smernicou NIS 2. Obidve smernice majú svoje miesto v legislatívnom rámci pre informačnú bezpečnosť podniku, a ich správna implementácia je dôležitá pre ochranu cenných informačných aktív podnikov.

Všeobecné ekonomické zhodnotenie implementácie smernice NIS 2 do podniku

Ak sa podnik rozhodne pre implementáciu riešení, ktoré sú navrhované vyššie, je potrebné, aby sme vymenovali aspoň základné faktory ovplyvňujúce ekonomickú návratnosť tejto investície. Tieto faktory sme zhrnuli v tabuľke č. 7:

Tabuľka 7 Všeobecné zhodnotenie implementácie smernice NIS2

Náklady na implementáciu a dodržiavanie smernice	Zavedenie smernice NIS 2 si vyžaduje určité náklady na implementáciu a dodržiavanie jej požiadaviek. V prípade malého podniku môžu tieto náklady tvoriť podstatnú časť ich rozpočtu (aspoň 10%).
Zvýšenie bezpečnosti informačných systémov	Ak podnik pristúpi k implementácií novej smernice, tak to by mohlo pomôcť zvýšiť bezpečnosť informačných systémov v malom podniku. Toto by mohlo znížiť riziko straty údajov a poškodenia systémov, čo by mohlo viesť k zníženiu nákladov na obnovu alebo opravu.
Zvýšené požiadavky na odbornosť a zručnosti	NIS 2 môže vyžadovať, aby malý podnik mal odborne zručný personál alebo aby najal externých odborníkov na zabezpečenie požiadaviek smernice. Toto môže byť ďalším nákladom pre podnik.
Vplyv na konkurencieschopnosť	Táto smernica môže mať vplyv na konkurencieschopnosť malého podniku. Podniky, ktoré nebudú schopné zabezpečiť požiadavky smernice, môžu byť v nevýhode voči konkurencii. Na druhej strane, ak sa podarí zabezpečiť vysokú úroveň bezpečnosti a ochrany údajov, môže to zvýšiť dôveru zákazníkov v podnik a viesť k zlepšeniu konkurencieschopnosti.
Právne náklady	NIS 2 môže zvýšiť právne náklady malého podniku. Podnik bude musieť zabezpečiť, aby dodržiaval všetky právne požiadavky, ktoré súvisia so smernicou, a aby sa vyhýbal potenciálnym sankciám a pokutám.

Zdroj: Vlastné spracovanie

Tieto faktory je potrebné podrobne zhodnotiť a aj vplyv zavedenia smernice NIS 2 na celkový rozpočet a prevádzku malého podniku. Malo by sa zohľadniť aj potenciálne zvýšenie dôvery zákazníkov v ochranu ich osobných údajov a dôvernosť informácií. To by mohlo mať priaznivý vplyv na obrat a celkovú výkonnosť podniku. Okrem toho, by mal malý podnik zvážiť aj možnosti financovania zavedenia smernice NIS 2. Existujú rôzne možnosti, ako získať finančné prostriedky na zavedenie smernice, ako napríklad štátne dotácie, zmeny v rozpočte alebo úvery. Je dôležité zvážiť, aké sú tieto možnosti pre náš konkrétny skúmaný podnik jeho manažmentom a aké sú ich budúce náklady. Nakoniec, pri ekonomickom zhodnotení zavedenia smernice NIS 2 do malého podniku by mal byť zohľadnený aj dlhodobý efekt zvýšenej ochrany informačných systémov a dát. Toto by mohlo viesť k zníženiu nákladov na obnovu a opravu systémov v budúcnosti.

Pri zavedení smernice NIS 2 do tohto konkrétneho podniku, ktorý pôsobí vo verejnom sektore ako stavebno-konzultačný subjekt, by sa muselo zohľadniť množstvo faktorov, ktoré by ovplyvňovali celkové náklady a prínosy. Medzi tieto faktory patria napríklad veľkosť a zložitosť informačných systémov, množstvo a typy dát, ktoré sú spracovávané, rizikové faktory a množstvo potrebných opatrení na ochranu a zabezpečenie informačných systémov, ktoré by na základe našich odporúčaní už implementovali informační experti. Ceny za ich služby, rozsah a kvalita implementovaných systémov, ktoré navrhnú sa môže líšiť. Preto konkrétne finančno-ekonomické zhodnotenie nechávame na manažmente podniku, aby sa podľa cenových ponúk, rozhodli bez riešenie, ktoré bude najviac vyhovovať ich potrebám a rozpočtu.

Vzhľadom na stále rastúce hrozby a riziká v oblasti informačnej bezpečnosti je kľúčové, aby sa podniky držali smernice NIS 2 a zabezpečili účinnú ochranu svojich informačných aktív. Naše odporúčania môžu pomôcť podniku pri implementácii tejto smernice a zabezpečiť, aby jeho informačné aktíva boli chránené pred potenciálnymi hrozbami.

Záver

Ochrana informácií nikdy v kybernetickom priestore nikdy nebola dôležitejšia ako dnes. Európska únia prijala mnohé opatrenia, aby zabránila útokom na digitálne aktíva štátov alebo podnikov. S cieľom lepšie chrániť Európanov a organizácie pred kybernetickými hrozbami, európsky parlament prijal a schválil novu smernicu NIS 2. Tieto pravidlá majú pomôcť integrovať vyššiu úroveň informačného zabezpečenia a týmto zabezpečeniam, sme sa v tejto diplomovej práci venovali.

Cieľom tejto diplomovej práce bolo posúdiť zavedené normy informačnej bezpečnosti v podniku a realizovateľnosť implementácie novej smernice o informačnej bezpečnosti NIS2 v rámci spoločnost, s vyústením do konkrétnych odporúčaní pre podnik. Vymedzili sme odporúčané pravidlá pre manažment informačnej bezpečnosti podniku a na základe komparatívnej analýzy legislatívnej úpravy informačnej bezpečnosti v európskom priestore, sme navrhli sumár odporúčaní pre podnik zohľadňujúci výsledky tejto analýzy. Tento cieľ sa nám podarilo splniť.

Čiastkové ciele, ktoré sme si zvolili sa nám tiež podarilo splniť. Prvý cieľ pozostával z analýzy existujúcich postupov informačnej bezpečnosti. Na základe analýzy sme identifikovali hlavné prvky manažmentu informačnej bezpečnosti, ako sú politiky, procesy, technológie a školenie zamestnancov. Zohľadnili sme požiadavky európskych smerníc, ako napríklad smernicu NIS 2.

Druhý čiastkový cieľ bolo vytvorenie prispôsobivého rámca. V tomto rámci sme zhrnuli politiky informačnej bezpečnosti, použité v podniku. Analyzovali sme implementované smernice ako ISO 27001, GDP. Následne sme zisťovali ich dosah na informačnú bezpečnosť podniku. Novú smernicu NIS 2 sme komparatívnou analýzou porovnali s implementovanými normami.

Posledný čiastkový cieľ pozostával s implementácie nového rámca. Ako implementáciu pravidiel sme si zvolili sumár odporúčaní pre podnik. V rámci odporúčaných pravidiel sme zdôraznili význam riadenia rizík a zabezpečenia dôvernosti, integrity a dostupnosti informácií. Taktiež sme navrhli riešenia pre monitorovanie informačnej bezpečnosti, zabezpečenie dostupnosti informačného systému, zlepšenie zabezpečenia mobilných zariadení a zabezpečenie zmlúv s tretími stranami.

Výsledky tejto diplomovej práce by mali byť pre podniky prínosom pri zabezpečovaní ich informačnej bezpečnosti a mali by im pomôcť implementovať

bezpečnostné opatrenia a štandardy v malom podnik v súlade s legislatívnou úpravou v európskom priestore. Informačná bezpečnosť je dôležitou súčasťou podnikovej stratégie a jej zabezpečenie by malo byť na najvyššej úrovni.

Zoznam použitej literatúry

Literárne zdroje:

1. CALDER, Alan. A Business Guide To Information Security: How to Protect your company is IT Assets Reduce Risks and Understand the Law. Kogan Page Published, 2005. s.136. ISBN 0-7949-4395-2.
2. SIVÁK, Rudolf. 2011. Slovník znalostnej ekonomiky. Bratislava: Sprint 2. s.119. ISBN 978-80-89393.
3. KOSTRECOVÁ, Eva. Informačná bezpečnosť. 1. vyd. Bratislava: Slovenská technická univerzita v Nakladateľstvo STU, 2013. s. 7, ISBN 978-80-227-3927-6
4. FILIP, Stanislav – ŠIMÁK, Ladislav, KOVÁČ, Marián. Manažment rizika. Bratislava: Sprint dva, 2011. s. 28, ISBN 978-80-89393-49-7.
5. HUBBARD, W. Douglas. The failure of risk management: Why it's broken and how to fix it. 2 edition. John Wiley & Sons, 2020. s. 9, ISBN 978-1-119-52203-4.
6. AGNES, Hui Chan - VIRGIL, Gligor. Information Security : 5th International Conference, ISC 2002, Sao Paulo, Brazil, September 30-October 2, 2002: Proceedings ISBN: 9783540442707.
7. ŠIMÁK, Ladislav. Krízový manažment vo verejnej správe. Žilina, 2001. s. 39. ISBN: 80-88829-13-5.
8. SEDLÁK, Mikuláš. Základy manažmentu. Wolters Kluwer (Iura Edition), 2012, 330 s. ISBN 9788080784553.
9. SEDLÁK, Mikuláš. Základy manažmentu, Bratislava : Edičné stredisko EU , 1994. - 253 s, 1. vyd. ISBN: 80-225-0591-9.
10. CAZEMIER, Jacques – OVERBEEK, Paul– PETERS, Louk. Security Management (IT Infrastructure Library Series), UK: Stationery Office, 1. január 2000, 124 s. ISBN 978-0113300143.
11. ABRAMS, M. – JAJODIA, S. – PODELL, H.. Information Security: An Integrated Collection of Essays. 1. vydanie. IEEE Computer Society Press, Los Alamitos, CA, USA, 1995. s .98-99. ISBN 978-0-7923-7389-6.
12. SMERNICA EURÓPSKEHO PARLAMENTU A RADY (EÚ) 2022/2555: 14. december 2022:o opatreniach na zabezpečenie vysokej spoločnej úrovne kybernetickej bezpečnosti v Únii, ktorou sa mení nariadenie (EÚ) č. 910/2014 a smernica (EÚ) 2018/1972 a zrušuje smernica (EÚ) 2016/1148 (smernica NIS 2).

Elektronické zdroje

1. WHITMAN, Michael E., HERBERT J. Mattord. Management of information security. Cengage Learning, [Online] 2013. [Cit. 2023-04-28] Dostupné na: https://books.google.sk/books?hl=en&lr=&id=naB0AgAAQBAJ&oi=fnd&pg=PP1&dq=Information+security+&ots=yB5EUqZ27S&sig=mQl_rG3x5MnuY4R13NpRNt7E-aQ&redir_esc=y#v=onepage&q=Information%20security&f=false
2. Meservy, K. - A brief history of information security. The Circuit: The Official Newsletter of the IEEE Computer Society of the IEEE Circuits and Systems Society. [online] New York: IEEE, June 2013, Vol. 25, No. 2, pp. 23-27 [cit. 2023-04-28]. ISSN 1059-7043. Dostupné na: https://blog.mesltd.ca/a-history-of-information-security-from-past-to-present
3. DE LEEUW, K. - BALEN, R. The History of Information Security: A Comprehensive Handbook. [online] In: Handbook of Information and Communication Security. Amsterdam: Elsevier, 2010, p. 1-28 [cit. 2023-05-01]. ISBN 978-0-444-51608-4. Dostupné na: https://www.elsevier.com/books/the-history-of-information-security/de-leeuw/978-0-444-51608-4
4. DQs Global – Blogová sekcia. Ciele ochrany informačnej bezpečnosti a ich význam [online]. In: DQs Global: Blog. Bratislava: DQs Global, 2019 [citované 2023-04-28]. Dostupné na: https://www.dqsglobal.com/sk-sk/blog/ciele-ochrany-informacnej-bezpecnosti-a-ich-vyznam
5. BOOTH, Wayne C. - COLOMB, Gregory G. - WILLIAMS, Joseph M. The Craft of Research: Fourth Edition [online]. Chicago : The University of Chicago Press, 2016, 4. vydanie, 320 s. [cit. 2023-05-01]. ISBN 978-0226239873. Dostupné na: http://common.books24x7.com.proxy.cityu.edu/toc.aspx?bookid=30815
6. ONLINEMANIPAL - Information Security in Digital Transformation [online]. In: Manipal ProLearn. Manipal, 2021 [cit. 2023-04-28]. Dostupné na: https://www.onlinemanipal.com/blogs/information-security-in-digtial-transformation.
7. RANUM, Marcus J. - KUMAR, Ravi - SCHNEIER, Bruce. Critical Infrastructure Security. [online] In: Elsevier Science & Technology Books: Computer Science. San Diego: Elsevier, 2003, 1st edition, 284 pages [cit. 2023-05-01]. Dostupné na: https://www.elsevier.com/books/critical-infrastructure-security/ranum/978-0-12-514031-2
8. COMPTON, J. SLOAN, L. What Are Information Security Criteria? In: Computerworld: [online]. IDG Communications, Inc., 2012 [cit. 2023-04-28]. Dostupné na: https://www.computerworld.com/article/2500941/what-are-information-security-criteria.html.
9. NIST Special Publication 800-14 Revision 2. (2013). Addressing the Cybersecurity Risk to Critical Infrastructure: NIST Framework. [online]. National Institute of Standards and Technology. [cit. 2023-04-28]. Dostupné na: https://csrc.nist.gov/publications/detail/sp/800-14/rev-2/final.
10. DOD85 - Department of Defense Trusted Computer System Evaluation Criteria. [online]. In: Proceedings of the 21st National Information Systems Security Conference. Washington D.C.: National Institute of Standards and Technology, 1998, s. 13-15 [cit. 2023-04-28]. Dostupné na:

https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf.

11. KOLLÁR, Miroslav – RUSKO, Vojtech. "BEZPEČNOSTNÉ MANAŽÉRSTVO A SYSTÉM INFORMAČNEJ BEZPEČNOSTI." [online]. s. 148–149 [cit. 2023-04-28] ISBN 978-80-89281-85-5 Online dostupné na: https://www.sszp.eu/wp-content/uploads/2012_konf_MaZP_B11__Rusko-Kollar.pdf
12. ALBERTS, Christopher – DOROFEE Audrey. Managing Information Security Risks: The OCTAVESM Approach [online]. In: Information Security Management Handbook. Boca Raton, FL: CRC Press, 2013, 6. vydanie., kap 14, s. 1-28 [cit. 2023-04-28]. ISBN 0-321-11886-3. Dostupné na: https://books.google.sk/books?hl=en&lr=&id=EGInzsKcG_8C&oi=fnd&pg=PR15&dq=Managing+Information+Security+Risks:+The+OCTAVESM+Approach&ots=qGcU2vGjt6&sig=VyXkLwNKp2PY-Lizp_Tc87mZtzM&redir_esc=y#v=onepage&q=Managing%20Information%20Security%20Risks%3A%20The%20OCTAVESM%20Approach&f=false.
13. BELAN, Ľubomír. Bezpečnostné riziká [online] In: 19. Medzinárodná vedecká konferencia: Riešenie krízových situácií v špecifickom prostredí, Žilina, 2014, s. 8 [cit. 2022-26-01]. Dostupné na: <http://fbiw.uniza.sk/rks/2014/articles/Belan_Belan.pdf>
14. ALOTAIBI, Mutlaq. – FURNELL, Steven, - CLARKE, Nathan. "Information security policies: A review of challenges and influencing factors." [online] 2016 11th International Conference for internet Technology and Secured Transactions (ICITST). IEEE, 2016. [cit. 2022-26-01] Dostupné na: https://ieeexplore.ieee.org/abstract/document/7856729
15. CROSSLER, Robert E., Future directions for behavioral information security research. [online] computers & security 32 (2013): 90-101. [cit. 2022-26-01] Dostupné na: https://www.sciencedirect.com/science/article/pii/S0167404812001460
16. SHROPSHIRE, Jordan. – WARKENTIN, Merrill. JOHNSTON, Allen. – SCHMIDT, Mark. Personality and IT security: An application of the five-factor model. [online] AMCIS 2006 Proceedings (2006): s. 415. [cit. 2022-26-01] Dostupné na: https://aisel.aisnet.org/amcis2006/415/
17. JOHN, D'Arcy. - HOVAV, Anat. - GALLETTA, Dennis. User awareness of security countermeasures and its impact on information systems misuse: [online] A deterrence approach." Information systems research 20.1 (2009): s 79-98. [cit. 2022-26-01] Dostupné na: https://pubsonline.informs.org/doi/10.1287/isre.1070.0160
18. COLWILL, Carl. Human factors in information security: The insider threat–Who can you trust these days? [online] Information security technical report . 2009, s. 186-196. [cit. 2022-26-01]. Dostupné na: https://www.sciencedirect.com/science/article/abs/pii/S1363412710000051
19. LARTEY, Kwesi Hughes. – LI, Meng. – BOTCHEY, Francis. – QIN, Zhen. Human factor, a critical weak point in the information security of an organization's internet of things [online]. Heliyon, Volume 7, Issue 3, 2021, ISSN 2405-8440, [cit. 2022-26-01]. Dostupné na: https://www.sciencedirect.com/science/article/pii/S2405844021006253

20. BARTEK, Alojz. Bezpečnostné prostredie a faktory bezpečnosti [online]. 1. vydanie. Žilina: Strix et SSŽP, 13. september 2018. s. 8. [cit. 2022-26-01]. ISBN 978-80-89753-27-7. Dostupné na: https://www.sszp.eu/wp-content/uploads/2018_conference_IBP__p-75__BartekA_Bezpe%C4%8Dnostn%C3%A9_prostredie_f4e.pdf
21. PELTIER, Thomas. Information Security Risk Analysis [online]. 2. vydanie. Boca Raton: CRC Press, 2005, [cit. 2022-26-01]. ISBN 0-8493-3346-6. Dostupné na: https://books.google.sk/books?hl=en&lr=&id=n8Z1RDjEKa0C&oi=fnd&pg=PR7&dq=information+security+risks&ots=Sajot89E0Y&sig=2hX8IvOLfGa9D5bUl1VWDu856No&redir_esc=y#v=onepage&q=information%20security%20risks&f=false
22. BLAKELY, Bob – MCDERMOTT, Ellen – GEER, Dan. Information Security is Information Risk Management, Proceedings of the 2001 Workshop on New Security Paradigms [online]. (Cloudcroft, NM, Sept. 10-13), New York: ACM Press, s. 97-104. [cit. 2022-26-01]. Dostupné na: https://www.nspw.org/papers/2001/nspw2001-blakley.pdf
23. ELOFF, Jan – ELOFF, Mariki. Information Security Management – A New Paradigm [online]. 1. vyd. s. 130-136. [cit. 2022-26-01]. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/SecManParadigm2.pdf
24. BSI. BS 100-1:2013. Information technology. IT baseline protection. Part 1: Overview and concepts [online]. Berlin : Federal Office for Information Security, 2013 [cit. 2023-03-22]. Dostupné na: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.pdf?__blob=publicationFile
25. ASHENDEN, Debi. Information Security management: A human challenge? [online]. Department of Informatics & Sensors, Cranfield University, Seindon SN6 8LA, UK, 2008. s. 195-201. Dostupné na: http://www.sis.pitt.edu/jjoshi/courses/is2621/spring2014/paper1.pdf
26. DHILLON, Gurpreet – BACKHOUSE, James. Current directions in IS security research: towards socio-organizational perspectives [online]. Information Systems Journal, 20 december 2001, s. 127-153. [cit. 2023-03-22]. Dostupné na: https://onlinelibrary.wiley.com/doi/abs/10.1046/j.1365-2575.2001.00099.x
27. BÍRO, Peter. Štandardy rýchlo a ľahko. [online]. Mnisterstvo financií Slovenskej republiky, 29 september 2014. [cit. 28.4.2023]. Dostupné na: http://www.informatizacia.sk/standardy-rychlo-a-lahko/5586s#STD_info
28. CONSORTIUM. Cybersecurity: Resilience, deterrence and defence: Building strong cybersecurity for the EU [online]. Brussels: Council of the European Union, 2017 [cit. 2023-04-28]. Dostupné na: https://www.consilium.europa.eu/sk/policies/cybersecurity/#resilience
29. ZDRAVEC, M. - FERKOVÁ, T. EU stratégia informačnej bezpečnosti [online]. In: iTAPA 2019. Bratislava: NASES, 2019, s. 1-11 [cit. 2023-04-28]. Dostupné na: https://www.itapa.sk/eu-strategia-informacnej-bezpecnosti/
30. EUROPEAN UNION AGENCY FOR CYBERSECURITY. European Cybersecurity Competence Centre and Network: New EU-funded project to support the cyber community. [online]. In: News.

European Union Agency for Cybersecurity [cit. 2023-04-28]. Dostupné na: https://cybersecurity-centre.europa.eu/news/european-cybersecurity-competence-centre-and-network-new-eu-funded-project-support-cyber-community-2022-12-20_en

31. EUROPEAN COMMISSION. Cybersecurity policies [online]. Digital Single Market. [cit. 2023-04-28]. Dostupné na: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies
32. CyberSec4Europe. Our community [online]. [cit. 2023-04-28]. Dostupné na: https://cybersec4europe.eu/our-community/
33. EUROPEAN UNION AGENCY FOR CYBERSECURITY. Mapping and Prioritisation of European ICT Security and Privacy Research and Innovation [online]. In: ENISA. Athens : ENISA, 2020 [cit. 2023-04-28]. Dostupné na: https://www.enisa.europa.eu/topics/standards.
34. CEN/CENELEC. Cybersecurity – Baseline security recommendations for Internet of Things (IoT) in the context of critical information infrastructures. [online]. In: CEN-CENELEC. Brussels: CEN-CENELEC Management Centre, 2017, CWA 17133:2017(E), s. 41. [cit. 28 Apr 2023]. Dostupné na: https://standards.cencenelec.eu/BPCEN/2307986.pdf
35. JANOŠČOVÁ, Renáta. Standardy informačnej bezpečnosti [online]. In: Manažment informačnej bezpečnosti: Podnikový prístup. Bratislava: Vydavateľstvo EKONÓM, 2015, s. 17-32 [citované 28.4.2023]. ISBN 978-80-225-4114-7. Dostupné na: https://www.researchgate.net/profile/Renata-Janoscova/publication/281098237_Standardy_informacnej_bezpecnosti/links/55ddbc8f08aeaa26af0f137a/Standardy-informacnej-bezpecnosti.pdf
36. COMMON CRITERIA RECOGNITION ARRANGEMENT. Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5 [online]. 2017. [cit. 28 Apr. 2023]. Dostupné na: https://www.commoncriteriaportal.org/
37. OWASP Foundation. OWASP Application Security Verification Standard (ASVS) Project. [online]. In: OWASP. [cit. 2023-04-28]. Dostupné na: https://owasp.org/www-project-application-security-verification-standard/
38. SYNOPSYS. Building Security In Maturity Model (BSIMM): The Software Security Framework. [online]. In: Synopsys Software Integrity. Mountain View, CA: Synopsys, 2021, Version 12, 1-82 [cit. 2023-05-02]. Dostupné na: https://www.synopsys.com/software-integrity/software-security-services/bsimm-maturity-model.html
39. BELÁŇOVÁ, Benita. Vývoj informačnej bezpečnosti v Slovenskej republike – výsledky prieskumu 2006-2017. Aktuálne výzvy prevencie počítačovej kriminality [online]. In: Konferencia inovatívneho manažmentu (KIM) 2018, Piešťany, Slovenská republika, 21. marec 2018. s. 17-23. [cit. 2023-04-28]. Dostupné na: https://www.akademiapz.sk/sites/default/files/KIM/ZBORN%C3%8DK%2021.3.2018%20WEB_0.PDF#page=17
40. BÍRO, Peter. NÁRODNÝ PORTÁL INFORMATIZÁCIE. Štandardy IS VS: Verzia 5.9.6S [online]. In: Informatizácia. Bratislava: Národné centrum pre informatizáciu, 2018 [cit. 2023-04-28]. Dostupné na: http://www.informatizacia.sk/standardy-is-vs/596s.

41. BCH. Národný informačný systém pre biologickú diverzitu (NIS) [online]. In: Biodiverzita.sk: portál o biodiverzite na Slovensku. Bratislava: Biologické centrum SAV, 2015-2023 [cit. 2023-04-29]. Dostupné na: https://www.bch.sk/nis-2
42. LFF, Frank. Tricent – NIS2: What is it and How Will it Affect You? [online]. In: Tricent Blog: Insights and News for the Utilities Industry. 12 december 2022, [cit. 2023-05-01]. Dostupné na: https://www.tricent.com/blog/nis2
43. ESET, Bezpečné vo firemne. Nová európska smernica NIS2 – potrebný základ pre spoločnú kybernetickú bezpečnosť [online]. In: Eset. 9. január 2023, [cit. 2023-04-25]. Dostupné na: https://bezpecnevofirme.eset.com/sk/firemna-bezpecnost/nova-europska-smernica-nis2-potrebny-zaklad-pre-spolocnu-kyberneticku-bezpecnost/
44. EUR-Lex Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 z 12. októbra 2022 [online]. In: Úradný vestník Európskej únie. Brusel: Európska únia, 2022, [Cit. 2023-04-27]. Dostupné na: https://eur-lex.europa.eu/legal-content/SK/TXT/PDF/?uri=CELEX:32022L2555.
45. TOPPRIVACY. NIS2 – Povinne regulované služby [online]. In: Topprivacy.sk. [cit. 2023-04-28]. Dostupné na: https://www.topprivacy.sk/userfiles/file/NIS2_Topprivacy%20-%20povinne%20regulovan%c3%a9%20slu%c5%beby.pdf
46. Osborne, M. - Ryan, P. Information Security Challenge and Breach Effectiveness: Qualitative Research Findings. In: Journal of Computer Information Systems: Spring 2014, Vol. 54, Issue 3, s. 29-38. [cit. 2023-04-28]. Dostupné na: https://d1wqtxts1xzle7.cloudfront.net/38094740/36585913256483-libre.pdf?1436081591=&response-content-disposition=inline%3B+filename%3DInformation_Security_Challenge_and_Breac.pdf&Expires=1682683171&Signature=DgFbAoHdrkVV2KK4SdBH67t1BAIU0nyY~zXTTEV-T1lSYRhRTi9FlgLIUrJqJ9JRBagwLXTp957WIxdalyATBHtkt37HGuMO3av8yA4szIwsEHvkVe2jnpbiMLVQsWdOvaEeaHG5xvEIOQQwTa~tIi7ldS7fJVnxh429GGEgn0eJVZxatS9OOIl~~RBnbbkTaoqba8kMjykea9oUBpcKFnimELRvxjJjYXWI27jEkkU6Qsis4XNpFX7~kH6M-6zdmpn6RK4OEUKV-zNbKkcQPEqlfCKQ0Pgkc0R38RNkorkk8902bpFOtXTjkmPnO6o7BwjBLyXvUw2OM4a6eZS38w__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
47. TECHTARGET. Computer Security Incident Response Team (CSIRT) [online]. In: WhatIs.com [cit. 2023-04-29]. Dostupné na: https://www.techtarget.com/whatis/definition/Computer-Security-Incident-Response-Team-CSIRT.