EKONOMICKÁ UNIVERZITA V BRATISLAVE
PODNIKOVOHOSPODÁRSKA FAKULTA
SO SÍDLOM V KOŠICIACH

Evidenčné číslo: 107007/I/2023/36119984580092420

INFORMAČNÝ SYSTÉM A POŽIADAVKY NA JEHO OCHRANU

Diplomová práca

2023 **Bc. Andrea Ješková**

EKONOMICKÁ UNIVERZITA V BRATISLAVE
PODNIKOVOHOSPODÁRSKA FAKULTA
SO SÍDLOM V KOŠICIACH

INFORMAČNÝ SYSTÉM A POŽIADAVKY NA JEHO OCHRANU

Diplomová práca

Študijný program:	finančné riadenie podniku
Študijný odbor:	ekonómia a manažment
Školiace pracovisko:	Katedra ekonómie a manažmentu
Vedúci záverečnej práce:	Ing. Jaroslav Dugas, PhD.

Košice 2023 **Bc. Andrea Ješková**

Ekonomická univerzita v Bratislave
Podnikovohospodárska fakulta so sídlom v Košiciach

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta:	Bc. Andrea Ješková
Študijný program:	finančné riadenie podniku (Jednoodborové štúdium, inžiniersky II. st., denná forma)
Študijný odbor:	ekonómia a manažment
Typ záverečnej práce:	Inžinierska záverečná práca
Jazyk záverečnej práce:	slovenský
Sekundárny jazyk:	anglický

Názov: Informačný systém a požiadavky na jeho ochranu

Anotácia: Kritickým faktorom úspechu každého podniku je, aby jeho manažment zabezpečil primerané zdroje na podporu ochrany svojho informačného systému. V dnešnej dobe len premyslený komplexný program informačnej bezpečnosti zabezpečí ochranu informačného systému a to prostredníctvom vrstvených technických a netechnických prvkov ochrany a kontroly. Hlavným cieľom záverečnej práce je návrh a následná implementácia programu informačnej bezpečnosti v konkrétnom slovenskom podniku.

Vedúci:	Ing. Jaroslav Dugas, PhD.
Katedra:	KM PHF - Katedra manažmentu
Dátum zadania:	14.10.2021

Dátum schválenia: 31.05.2022 prof. Ing. Bohuslava Mihalčová, PhD.

vedúci katedry

Čestné vyhlásenie

Čestne vyhlasujem, že som túto záverečnú prácu vypracovala samostatne a všetky použité zdroje boli citované a uvádzané v súlade s pravidlami citovania.

Dátum: .....

(podpis študenta)

Poďakovanie

Chcem sa poďakovať pánovi Ing. Jaroslavovi Dugasovi, PhD., za odborné rady a pomoc pri vypracovaní mojej diplomovej práce.

ABSTRAKT

JEŠKOVÁ, Andrea: Informačný systém a požiadavky na jeho ochranu – Ekonomická univerzita v Bratislave. Podnikovohospodárska fakulta so sídlom v Košiciach; Katedra ekonómie a manažmentu. – Vedúci záverečnej práce: Ing. Jaroslav Dugas, PhD.. – Košice: PHF EU, 2023, počet strán 52.

Cieľom záverečnej práce je: Hlavným cieľom záverečnej práce je návrh a následná implementácia programu informačnej bezpečnosti v konkrétnom slovenskom podniku. Práca je rozdelená do 5 kapitol. Obsahuje 3 obrázky, 3 grafy a 8 tabuliek. Prvá kapitola je venovaná teoretickej časti, kde sú vymedzené pojmy: informačný systém a informačná bezpečnosť. V ďalšej časti sa charakterizuje sledovaný podnik a metódy použité pri tvorbe práce. V predposlednej kapitole je rozpracovaná problematika kybernetickej bezpečnosti na Slovensku a vytvorený program informačnej bezpečnosti pre sledovaný podnik. Posledná kapitola obsahuje zhodnotenie a návrhy spojene s informačnou bezpečnosťou pre daný podnik.

Kľúčové slová:

informačný systém, informačná bezpečnosť, implementácia, manažment,

ABSTRACT

JEŠKOVÁ, Andrea: Information system and its security requirements - University of Economics in Bratislava. Faculty of Business with headquarters in Košice; Department of Economics and Management. - Supervisor: Ing. Jaroslav Dugas, PhD. - Košice: PHF EU, 2023, 52 pages.

The main goal of this thesis is to design and subsequently implement an information security program in a specific Slovak company. The work is divided into 5 chapters, containing 3 images, 3 graphs, and 8 tables. The first chapter is dedicated to the theoretical part, where the terms "information system" and "information security" are defined. The following chapter characterizes the observed company and methods used in the work. The third chapter elaborates on the issue of cyber security in Slovakia and the information security program developed for the observed company. The last chapter contains an evaluation and proposals related to information security for the given company.

Keywords:

information system, information security, implementation, management.

OBSAH

Zoznam ilustrácií a zoznam tabuliek

Úvod

V dnešnej dobe s narastajúcim významom informačných technológií a s rozširovaním oblastí, kde sa využívajú, sa stáva nevyhnutným zabezpečiť informačné systémy a ich dáta pred rôznymi hrozbami. Správne zabezpečenie informačného systému pred neoprávneným prístupom, zneužitím alebo poškodením je kľúčové pre úspešné fungovanie organizácií a spoločností.

V prípade narušenia bezpečnosti informačného systému môže dôjsť k finančným stratám, porušeniu zákona a reputačným problémom. Preto je dôležité, aby organizácie mali vysoko kvalitný program informačnej bezpečnosti, ktorý zabezpečí, že súčasné bezpečnostné riziká sú minimalizované a že súčasný stav je kontrolovaný.

Pre firmy je dôležité zabezpečiť informačnú bezpečnosť, pretože informácie patria medzi najcennejšie zdroje a aktíva spoločnosti. V súčasnosti firmy využívajú množstvo informačných systémov na správu a uchovávanie dôležitých informácií. K tomu môžu použiť rôzne metódy a nástroje na zabezpečenie bezpečnosti, ako sú napríklad firewally, antivírusové programy, šifrovanie dát alebo pravidelné zálohovanie údajov. Okrem technických opatrení je však nevyhnutné aj dodržiavať pravidlá a procesy pre správu informačnej bezpečnosti a poskytovať dostatočné školenia pre zamestnancov, aby boli informačne gramotní a vedeli správne zachádzať s citlivými informáciami.

V súčasnosti sú informačné systémy základným nástrojom pre mnoho spoločností a organizácií. Umožňujú im rýchlejšie a presnejšie rozhodovanie, zvýšenie produktivity a konkurencieschopnosti. Sú však tiež spojené s rizikami a bezpečnostnými hrozbami, pretože môžu obsahovať dôležité a citlivé informácie. Preto je dôležité zabezpečiť primeranú ochranu informačných systémov a údajov v nich uložených.

Predkladaná diplomová práca sa zameriava na informačné systémy a ich ochranu. V teoretickej časti práce sme popísali rôzne typy informačných systémov. Druhá časť teoretickej časti sa zaoberá problematikou informačnej bezpečnosti, kde sme využili domácu a zahraničnú literatúru na priblíženie kybernetických hrozieb, ktorým čelia podniky v súčasnosti, a popísali sme moderné modely ochrany dát v podnikovom prostredí.

V nasledujúcej časti sme opísali cieľ záverečnej práce spolu s čiastkovými cieľmi. V časti práce s názvom „ Metodika práce a metódy skúmania“ sme načrtli metódy využité

v práci, a uviedli sme charakteristiku spolu s potrebnými informáciami o sledovanej spoločnosti, ktorá na účely tejto práce bola spoločnosť Panel Team s.r.o.

V praktickej časti našej práce sme využili dostupné informácie a štatistiky na vytvorenie trojročného prehľadu o kybernetickej bezpečnosti na Slovensku. Následne sme sa zamerali na vytvorenie programu informačnej bezpečnosti pre sledovanú spoločnosť Panel Team s.r.o., čo bolo základným cieľom nášho výskumu.

Celková záverečná práca je aktuálna a zdôrazňuje význam ochrany informačných systémov v podnikovom prostredí.

1 Súčasný stav riešenej problematiky doma a v zahraničí

V prvej teoretickej časti diplomovej práce si priblížime informačné systémy, informačnú bezpečnosť, kybernetickú bezpečnosť a súčasné modely ochrany dát v podniku.

1.1 Informačné systémy

Informačný systém je súbor vzájomne prepojených komponentov, ktoré spolupracujú pri zhromažďovaní, spracovávaní, uchovávaní a šírení informácií. Tieto informácie podporujú základné obchodné operácie, vykazovanie a vizualizáciu údajov, analýzu údajov, rozhodovanie, komunikáciu a koordináciu v rámci organizácie. Dobre navrhnutý informačný systém obsahuje určitú formu mechanizmu spätnej väzby na monitorovanie a riadenie jeho prevádzky. Táto spätná väzba zaisťuje, že systém naďalej funguje efektívne. (Stair, 2020)

Janošcová (2014) definuje informačný systém ako komplex ľudských zdrojov, technických prostriedkov a metód, ktoré umožňujú zber, prenos a spracovanie dát s cieľom poskytnúť užívateľom informácie. Jeho úlohou je systematicky získavať, spracovávať, uchovávať a poskytovať informácie potrebné pre riadenie organizácie. Kvalitný a spoľahlivý informačný systém je nevyhnutný pre úspešné fungovanie každej organizácie, umožňuje rýchle a efektívne rozhodovanie sa a pružné získavanie, prenos a spracovanie informácií.

Jednotlivci a organizácie používajú každý deň počítačové informačné systémy na vykonávanie širokého spektra pracovných úloh. Zahŕňa to spracovanie základných transakcií potrebných na prevádzkovanie podniku (napr. zaznamenávanie zákazníckych objednávok a platieb) a komunikáciu s kolegami zamestnancami, zákazníkmi, obchodnými partnermi a inými zdrojmi. (Stair, 2020)

1.1.1 Typy informačných systémov

Zahraničný autori rozlišujú niekoľko základných typov IS v podnikoch. Ide o tieto typy IS:

- **Výkonný systém podpory** - pomáha vedúcim pracovníkom na najvyššej úrovni plánovať a kontrolovať pracovný tok a robiť obchodné rozhodnutia. Je veľmi

podobný manažérskemu informačnému systému. Patrí sem systém na podporu exekutívy (Executive Support Systems – ESS)

- **Manažérsky informačný systém** – Manažérsky informačný systém (MIS) je automatizovaný systém, ktorý poskytuje manažérom podporu pri rôznych procesoch, ktoré boli predtým vykonávané ručne. Tieto procesy zahŕňajú sledovanie a analýzu výkonnosti podniku, prijímanie obchodných rozhodnutí, tvorbu obchodného plánu a definovanie pracovného toku. MIS tiež poskytuje spätnú väzbu manažérom pomocou analýzy úloh a zodpovedností. Okrem MIS existujú aj systémy na podporu rozhodovania (Decision Support Systems – DSS), ktoré poskytujú rozšírenú funkcionalitu pre analýzu a rozhodovanie.
- **Systém práce so znalosťami** – Organizácie implementujú rôzne systémy riadenia znalostí, aby zabezpečili neustály tok nových a aktualizovaných znalostí pre ich procesy. Medzi takéto systémy patria napríklad znalostné pracovné systémy (Knowledge Work Systems - KWS) a systémy na automatizáciu kancelárie (Office Automation Systems - OAS).
- **Systém na podporu rozhodovania** - Systém na podporu rozhodovania (Decision Support System – DSS) je informačný systém, ktorý umožňuje automatizovať rozhodovanie a riešenie problémov v podniku pomocou analýzy obchodných údajov a iných súvisiacich informácií. Jeho použitie je najužitočnejšie v situáciách, kedy podnik čelí nepriaznivým podmienkam. DSS sa často používa na zhromažďovanie informácií týkajúcich sa príjmov, predaja alebo zásob a nachádza uplatnenie v rôznych odvetviach. Je to obľúbený informačný systém, ktorý sa využíva na zlepšenie kvality rozhodovania v podniku.
- **Systém spracovania transakcií** - Systém spracovania transakcií (Transaction Processing Systems – TPS), automatizuje proces zhromažďovania, úpravy a vyhľadávania transakcií. Zvláštnosťou tohto typu informačného systému je, že zvyšuje výkonnosť, spoľahlivosť a konzistentnosť obchodných transakcií. Pomáha podnikom vykonávať každodenné operácie. (Emeritus, 2022)

1.1.2 Databáza

Cieľom mnohých informačných systémov je transformovať údaje na informácie s cieľom generovať poznatky, ktoré možno použiť na rozhodovanie. Na tento účel musí byť

systém schopný prijímať údaje, zasadzovať ich do kontextu a poskytovať nástroje na agregáciu a analýzu. Databáza je navrhnutá práve na takýto účel, pričom ju možno charakterizovať ako organizovanú zbierku súvisiacich informácií. (Bourgeois, 2019)

Údajová základňa

Pre riadenie a rozhodovanie v organizácii je dôležité mať aktuálnu a prístupnú údajovú základňu, ktorá obsahuje uložené údaje. Je nevyhnutné umožniť používateľom a manažérom prístup k týmto dátam, aby mohli efektívne vyhľadávať a prezentovať informácie. Údajová základňa by mala byť pružná, jednoduchá a účinná, aby umožnila rýchle a presné rozhodovanie a riadenie. Priamy prístup k údajom z údajovej základne by mal byť k dispozícii pre manažérov a používateľov, ktorí ich potrebujú pre svoju riadiacu a rozhodovaciu činnosť.

Autori Kokles a Romanová (2018) rozdeľujú vývojové etapy údajovej základne do nasledovných generácii:

1. generácia (1950-1960) - údaje sú zaznamenávané v sekvenčných súboroch tvorených postupnosťou viet uložených na magnetických páskach. Typické je dávkové spracovanie úloh.
2. generácia (1960-1965) - využíva SRBD založený na súboroch s priamym prístupom, ktoré sú uložené na magnetických diskoch. Umožňuje aj interaktívne spracovanie úloh.
3. generácia (1965-1975) - predstavuje začiatok integrovaného systému riadenia bázy dát, poskytuje nezávislosť logickej a fyzickej štruktúry dát. Používateľ pracuje s dátami na základe podschémy, ktorá predstavuje podmnožinu schémy dát daného databázového systému. Základom sú hierarchické a sieťové modely dát.
4. generácia (1975-1990) je založená na relačnom modeli dát Vzťahy medzi údajmi sú vyjadrené pomocou relácií, orientácia pre využívanie databázových systémov bežným používateľom. Patrí sem tiež vytváranie distribuovaných báz dát, ktorých aplikácie podnietil rozvoj počítačových sietí a využívanie textových databáz.
5. generácia (1990- doteraz) - vývoj a postupné zavádzanie do praxe objektovo orientovaných databázových systémov - údaje nie sú uložené vo forme súborov ani relácií, ale predmetom spracovania sú objekty, ktoré obsahujú potrebné informácie. Okrem svojho stavu si objekt pamätá aj svoje správanie.

1.1.3 Databázové modely

Databázy môžu byť organizované mnohými rôznymi spôsobmi, a preto majú mnoho podôb. Rozlišujeme 3 základné databázové modely (Kokles, Romanová, 2018):

1. Hierarchický
2. Sieťový
3. Relačný

Hierarchický model

Pre hierarchické modelovanie je typická práca so stromami. Vzťahy v strome fungujú na princípe nadriadenosti a podriadenosti. Vzťah možno definovať ako, 1:N. Koreňový segment sa nachádza na vrchole hierarchie. Každý nadriadený prvok môže mať 0 až N podriadených prvkov, pričom každý podriadený prvok môže mať len jeden nadriadený prvok. Pri hierarchickom modely sa kladie dôraz na navrhovanie jednotlivých stromov a na definovanie nadväznosti medzi stromami.

Sieťový model

Predstavuje variant hierarchického modelu. Sieťový model okrem vzťahu 1:N umožňuje použiť aj vzťah M:N. Na realizáciu tohto modelu sa využíva veľké množstvo ukazovateľov a aktualizácia zvykne byť náročná.

Relačný model

Najprepracovanejší model v ktorom sú všetky údaje uložené v dvojrozmerných tabuľkách nazývaných relácie. Jednu z hlavných výhod predstavuje flexibilita (ľahká modifikácia tabuliek a ľahké prepájanie tabuliek medzi sebou).

Obľúbenými príkladmi relačných databáz podľa autora Bourgeoisa (2019), sú Microsoft Access, MySQL a Oracle. Relačná databáza je databáza, v ktorej sú údaje usporiadané do jednej alebo viacerých tabuliek. Každá tabuľka má množinu polí, ktoré definujú povahu údajov uložených v tabuľke. Záznam je jedna inštancia množiny polí v tabuľke.

1.2 Informačná bezpečnosť

Bezpečnosť je možné charakterizovať ako ochrana. Cieľom bezpečnosti je ochrana pred osobami, ktoré môžu úmyselne škodiť/ubližovať. Dosiahnutie primeranej úrovne zabezpečenia pre organizáciu si vyžaduje mnohostranný systém. Úspešná organizácia by mala mať zavedených viacero vrstiev zabezpečenia, aby boli chránené operácie, fyzická infraštruktúra, ľudia, funkcie, komunikácia a informácie. (Whitman, 2018)

Až donedávna bola hlavným zameraním informačnej bezpečnosti ochrana IT systémov, ktoré spracúvajú a uchovávajú veľkú väčšinu informácií, a nie samotných informácií. Tento prístup je však zameraný na technológiu a je príliš úzky na to, aby dosiahol úroveň integrácie, procesného zabezpečenia a celkovej bezpečnosti, ktorá je teraz potrebná. (Brotby, 2008)

Informačná bezpečnosť zastáva širší názor, že informácie a poznatky na nich založené musia byť primerane chránené. Informačná bezpečnosť sa zaoberá celým radom rizík, výhod a procesov spojených so všetkými informačnými zdrojmi. Ukázalo sa, že s informáciami sa musí zaobchádzať s rovnakou starostlivosťou a obozretnosťou ako s inými kritickými organizačnými zdrojmi. Keďže sa organizácie snažia zostať konkurencieschopné v globálnej ekonomike, neustále existuje tlak na znižovanie nákladov prostredníctvom automatizácie a nasadzovania väčšieho množstva informačných systémov. Manažment sa tiež musí vysporiadať s množstvom nových a existujúcich zákonov a nariadení, ktoré vyžadujú dodržiavanie a vyššiu úroveň zodpovednosti. (Brotby, 2008)

Pri informačnej bezpečnosti hovoríme o bezpečnosti pri manipulácií s informáciami, pričom sa kladie veľký dôraz na požiadavky, ako je dôvernosť, integrita, dostupnosť, autentickosť a užitočnosť informácií. Potrebnú mieru informačnej bezpečnosti IS môžeme podľa Janošcovej (2014) dosiahnuť kombináciou niekoľkých vrstiev ochrany:

Fyzickou ochranou

Za fyzickú bezpečnosť považujeme ochranu fyzického prístupu ku zdrojom danej organizácie. Princíp tejto ochrany je postavený na inštalácií a prevádzkovaní monitorovacích a zabezpečovacích zariadení. Pri tomto druhu ochrany ide predovšetkým o včasné zistenie pokusu o prienik ako aj samotné odradenie o daný pokus.

Logickou ochranou

Logická ochrana predstavuje hardvérové a softvérové riešenia, ktoré realizujú funkcie presadzujúce bezpečnosť. Patrí sem kódovanie, šifrovanie, zálohovanie a archiváciu dát, čiže prostriedky na zabezpečenie prístupu a na bezpečný prenos dát

Komunikačnou ochranou

Komunikačná bezpečnosť zahŕňa ochranu šifrovacích kľúčov a ich distribúciu.

Organizačnými a legislatívnymi opatreniami.

Organizačná úroveň bezpečnosti zahŕňa súbor opatrení, smerníc, nariadení a pokynov, ktoré majú za cieľ zabezpečiť bezpečnosť organizácie a jej cieľov. Dôležitým prvkom je dodržiavanie legislatívnych opatrení, a v prípade ich porušenia, aj príslušné sankcie. Pre organizácie je kľúčové zaviesť bezpečnostnú politiku a vytvoriť skupinu pre bezpečnostný manažment, ktorá bude zodpovedná za riadenie a monitorovanie bezpečnostných opatrení.

Typy bezpečnostných politík

Podľa Nextech (2023), rozpoznávame tri typy základného filozofického prístupu k bezpečnostnej politike využívania IS:

- Opatrná politika – zlatá stredná cesta. Všetko je zakázané, okrem tých aktivít, ktoré sú explicitne povolené
- Liberálna politika je opak paranoje, teda čo nie je zakázané, je povolené. Ľudia by sa mali riadiť rozumnými pravidlami, ktoré ich neobmedzujú pri práci, ale každý má iba oprávnenia, ktoré nevyhnutne potrebuje pri svojej práci.
- Anarchia – absolútny chaos, keď si vo firme každý robí, čo chce. Anarchia môže vládnuť buď v celej firme, alebo len od určitej úrovne (napr. stredný technický manažment, prípadne paradoxne IT oddelenie, hlavne programátori). Administrátor nezvláda správu siete a manažmentu nezáleží na používaní informačných technológií.

Prístup organizácií k ochrane informačných zdrojov

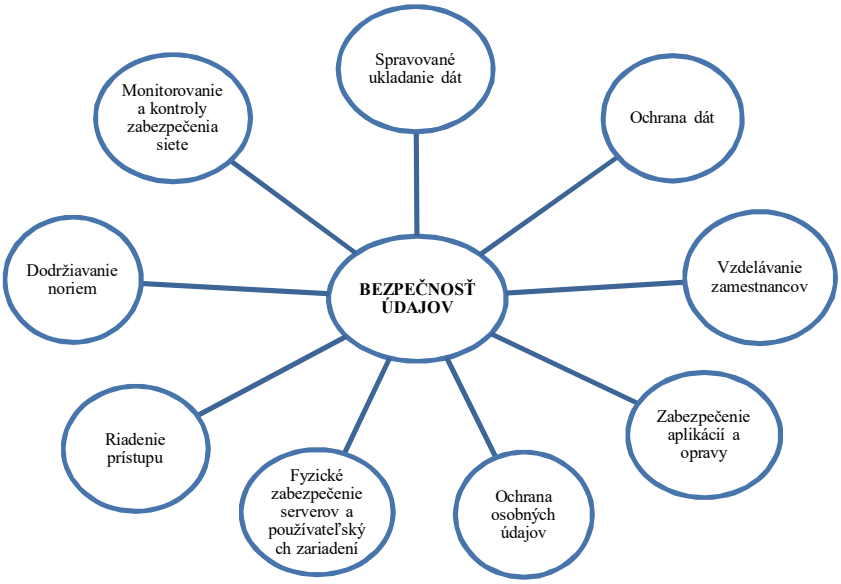
V skutočnosti je bezpečnosť záležitosťou každého v organizácii. Jednou z hlavných povinností každého obozretného CIO, ako aj funkčných manažérov, ktorí kontrolujú informačné zdroje je organizácia vhodného obranného systému. (Rainer, 2021)

Potenciálne hrozby spojené s ochranou informácií (Rainer, 2022):

- Výpočtové zdroje môžu byť umiestnené na mnohých miestach.
- Mnoho jednotlivcov kontroluje alebo má prístup k informačným aktívam.
- Počítačové siete môžu byť umiestnené mimo organizácie, čo sťažuje ich ochranu.
- Rýchle technologické zmeny spôsobujú, že niektoré ovládacie prvky sú zastarané hneď po ich inštalácii.
- Mnoho počítačových zločinov je dlho neodhalených, takže je ťažké poučiť sa zo skúseností.
- Ľudia majú tendenciu porušovať bezpečnostné postupy, pretože postupy sú nepohodlné.
- Množstvo počítačových znalostí potrebných na vykonanie počítača je zvyčajne minimálne. V skutočnosti sa potenciálny zločinec môže naučiť hacking zadarmo z internetu.
- Náklady na predchádzanie nebezpečenstvám môžu byť veľmi vysoké. Preto si väčšina organizácií jednoducho nemôže dovoliť aby sa chránili pred všetkými možnými nebezpečenstvami.
- Je ťažké vykonať zdôvodnenie nákladov a prínosov pre kontroly predtým, ako dôjde k útoku, pretože je ťažké posúdiť vplyv hypotetického útoku.

Okrem problémov uvedených vyššie je ďalším dôvodom, prečo je ťažké chrániť informačné zdroje to, že odvetvie online obchodu nie je zvlášť ochotné inštalovať ochranné opatrenia, ktoré by sťažili alebo skomplikovali dokončenie transakcií. Ako jeden príklad by obchodníci mohli požadovať heslá alebo osobné identifikačné čísla pre všetky transakcie kreditnými kartami. Tieto požiadavky však môžu ľudí odradiť od nakupovania online. Pre spoločnosti vydávajúce kreditné karty je lacnejšie zablokovať ukradnutú kreditnú kartu a ísť ďalej, ako investovať čas a peniaze do stíhania páchateľov. (Rainer, 2022)

Komponenty stratégie zabezpečenia údajov



Obrázok 1 Komponenty stratégie zabezpečenia údajov

Zdroj: TechTarget, 2022

Komplexná stratégia zabezpečenia údajov zahŕňa ľudí, procesy a technológie. Zavedenie vhodných kontrol a politík je rovnako otázkou organizačnej kultúry, ako aj nasadenia správnej sady nástrojov. To znamená, že informačná bezpečnosť je prioritou vo všetkých oblastiach podniku. (IBM, 2021)

Fyzické zabezpečenie serverov a používateľských zariadení - bez ohľadu na to, či sú údaje uložené lokálne, v podnikovom dátovom centre alebo vo verejnom cloude, je potrebné zabezpečiť, aby boli zariadenia zabezpečené proti votrelcom a mali primerané protipožiarne opatrenia a kontroly klímy. Poskytovateľ cloudu prevezme zodpovednosť za tieto ochranné opatrenia vo vašom mene. (Flowii, 2018)

Zálohy - udržiavanie použiteľných, dôkladne otestovaných záložných kópií všetkých dôležitých údajov je základnou súčasťou každej robustnej stratégie zabezpečenia údajov. Okrem toho by všetky zálohy mali podliehať rovnakým fyzickým a logickým bezpečnostným kontrolám, ktoré riadia prístup k primárnym databázam a základným systémom. (IBM, 2021)

Pohyb dát - jedným z najdôležitejších krokov k účinnej ochrane údajov je presne vedieť, ktoré údaje sa uchovávajú a kde. Presnou identifikáciou životného cyklu svojich údajov a

bezpečnostných rizík, ktoré sú s ním spojené, môžu spoločnosti prijímať informované rozhodnutia týkajúce sa opatrení, ktoré potrebujú na ich ochranu. (Coos, 2021)

Správa a kontrola prístupu - princíp „najmenej privilegovaného prístupu“ by sa mal dodržiavať v celom IT prostredí podniku. To znamená poskytnúť prístup k databáze, sieti a správcovskému účtu čo najmenšiemu počtu ľudí a iba tým, ktorí to nevyhnutne potrebujú na vykonávanie svojich úloh. (IBM, 2021)

Vzdelávanie zamestnancov - nutnosť, aby boli zamestnanci informovaní o nariadeniach a dodržiavaní predpisov a osvedčených bezpečnostných postupoch. Organizácie poskytujú školenia a jasné pokyny pre tých, ktorí prichádzajú do kontaktu s najcitlivejšími typmi údajov. (Coos, 2021)

Monitorovanie a kontroly zabezpečenia siete a koncových bodov - implementácia komplexného balíka nástrojov a platforiem na správu, detekciu a odozvu v lokálnom prostredí a cloudových platformách môže zmierniť riziká a znížiť pravdepodobnosť narušenia. (IBM, 2021)

1.2.1 Kybernetické hrozby

Botnet – botnety sú vytvorené s účelom zväčšiť, automatizovať a zrýchliť schopnosti hackerov vykonávať rozsiahlejšie útoky. I keď jedna osoba alebo aj malý tím hackerov môže vykonať iba obmedzený počet akcií na svojich lokálnych zariadeniach, za nízku cenu a s trochou času môžu získať množstvo ďalších zariadení, ktoré môžu použiť na efektívnejšie operácie. Bot-veliteľ vedie skupinu infikovaných zariadení pomocou vzdialených príkazov. Po zhromaždení botov veliteľ použije programovanie príkazov na riadenie ich ďalších akcií. Osoba alebo skupina, ktorá má kontrolu nad botnetom, ho môže buď sami vytvoriť, alebo prevádzkovať ako prenájom. (Kaspersky, 2023)

Za najčastejšie typy útokov botnetmi Greenlee (2021) považuje:

- **Útok hrubou silou** - keď útočník nevie cieľové heslá, zvolí siútok hrubou silou. Táto metóda útoku využíva rýchlu a opakovanú techniku hádania hesiel. Počas tohto útoku malware priamo komunikuje s postihnutou službou a získava v reálnom čase spätnú väzbu k pokusom o heslo. Útok pomocou hrubej sily môže využiť aj ukradnuté prihlasovacie údaje alebo osobne identifikovateľné informácie.
- **Spam a phishing** - útočníci často používajú emailový spam na phishing kampane, ktoré sú navrhnuté tak, aby oklamali zamestnancov a donútili ich zdieľať citlivé

informácie alebo prihlasovacie údaje. Ďalším cieľom phishing útokov je získanie prístupu k ďalším zariadeniam a rozšírenie botnetu. Preto je dôležité byť opatrný pri spracovaní e-mailov a v prípade podozrivého obsahu nekliknúť na odkazy alebo neposkytovať citlivé informácie, ktoré môžu byť využité na získanie prístupu k zariadeniam. Je tiež odporúčané používať rôzne bezpečnostné opatrenia, ako sú antivírusové programy a firewall-y, aby sa minimalizovalo riziko útoku.

- **Zariadenie Bricking** - útočníci môžu nasadiť bota na útok, ktorý sa skladá z viacerých fáz a vedie k nefunkčnosti zariadenia. Tento typ útoku je často nazývaný "bricking attack", pri ktorom je zariadenie infikované malwarom, ktorý zmaže jeho obsah a spôsobí, že prestane fungovať a stane sa nepoužiteľným. Útočníci môžu týmto spôsobom odstrániť dôkazy o hlavnom útoku alebo získať kontrolu nad ďalšími zariadeniami, ktoré sú súčasťou botnetu.

DoS (Denial of service) - sú útoky, ktoré majú za cieľ znemožniť alebo obmedziť prístup k nejakej službe alebo systému. Ide o útoky, ktoré sa snažia zaplniť komunikačné kanály a zdroje cieľového systému tak, aby bol nedostupný pre legitímnych používateľov. Tieto útoky môžu byť veľmi nebezpečné a môžu spôsobiť vážne finančné straty a poškodenie reputácie cieľovej organizácie. Najnebezpečnejším typom DoS útokov je distribuovaný DoS (DDoS), ktorý sa tiež nazýva koordinovaný útok, pri ktorom sa použije veľké množstvo skompromitovaných strojov na vykonanie DoS útoku. (Mahmoud, 2019)

Firma môže utrpieť rôzne škody, ktoré sa môžu prejaviť v podobe veľkých hospodárskych strát z dôvodu výpadkov služieb, výroby a predaja, poškodenia imidžu na trhu a strate zákazníkov. V oblasti národnej bezpečnosti môže mať tieto škody rozsiahle účinky, ako napríklad nemožnosť udržania verejnej dopravy. (Enzenhofer, 2019)

Malvér (malicious software) - je škodlivý softvér, ktorý nesťahuje škodlivé súbory ani nezapisujú žiadny obsah na disk. Útočník využíva zraniteľnosť aplikácie na vloženie škodlivého kódu priamo do hlavnej pamäte. Útočník môže tiež využiť dôveryhodné a široko používané aplikácie, ako sú kancelárske alebo administratívne nástroje Microsoftu, ktoré sú natívne pre operačný systém Windows, ako napríklad PowerShell. (Kumar, 2020)

Väčšinu typov malvéru možno klasifikovať podľa Cyberark (2023), do jednej z nasledujúcich kategórií:

- **Vírus -** po spustení sa počítačový vírus môže šíriť tým, že upravuje iné programy a vkladá svoj škodlivý kód. Ide o jeden z mála typov malvéru, ktorý dokáže

infikovať ďalšie súbory a predstavuje jednu z najnáročnejších hrozieb na odstránenie.

- **Červ** - je schopný replikácie bez interakcie koncového používateľa a môže rýchlo infikovať celé siete šírením z jedného počítača na ďalšie.
- **Trójsky kôň** - je jedným z najťažších typov malvéru na odhalenie, pretože sa maskuje ako legitímny program. Obsahuje škodlivý kód a pokyny, ktoré môžu fungovať nepovšimnuté, keďže sa javia ako neškodné. Často sa využíva na vniknutie ďalších typov malvéru do systému.
- **Hybridný malvér** - súčasný malvér často kombinuje rôzne typy škodlivého softvéru, čím vznikajú hybridné hrozby. Príkladom môžu byť tzv. "boti", ktoré sa najskôr prezentujú ako trójsky kôň a následne sa správajú ako červ. Sú často používané na cielenie na jednotlivých používateľov v rámci rozsiahleho kybernetického útoku, ktorý sa šíri po celej sieti.
- **Spyware** - sleduje koncového používateľa bez jeho vedomia, zhromažďuje prihlasovacie údaje, heslá, históriu prehliadania a iné informácie.
- **Ransomware** - infikuje zariadenia, šifruje súbory a drží potrebný dešifrovací kľúč ako rukojemníka, kým obeť nezaplatí výkupné. Útoky ransomvéru zamerané na podniky a vládne organizácie sa stávajú čoraz častejšími a niektoré organizácie sú ochotné platiť útočníkom milióny, aby obnovili kritické systémy. Medzi najznámejšie rodiny ransomvéru patria Cryptolocker, Petya a Loky.

1.2.2 Modely ochrany dát v podniku

Požiadavky na ochranu dát v spoločnostiach sa stávajú čoraz zložitejšie. Mnohé zo spoločností potrebujú chrániť iné kategórie údajov nad rámec informácií o zákazníkoch, ako sú duševné vlastníctvo a finančné údaje. Za efektívne spôsoby ochrany údajov v organizácii a zabezpečenia podnikových údajov možno považovať:

Architektúra nulovej dôvery (Zero Trust)

Na riešenie externých bezpečnostných hrozieb veľké spoločnosti nasadzujú a pravidelne aktualizujú základné opatrenia, ako je dvojfaktorová autentifikácia, brány firewall a antimalvérové riešenia. Zachádzajú tiež ešte ďalej implementáciou

pokročilejších stratégií, ako sú možnosti modulu Trusted Platform Module (TPM), a prijatím architektúry nulovej dôvery (Zero Trust). (Microsoft, 2023)

Táto architektúra navrhuje nový spôsob riešenia kybernetickej bezpečnosti: „nikdy neverte, vždy overujte.“ Zaisťuje, že používatelia, zariadenia a sieťová prevádzka sú pri prístupe k dôveryhodným zdrojom overení a podliehajú pravidlám najmenších privilégií. Týmto spôsobom, ak sa jeden počítač nakazí, útočníkom sa zabráni v bočnom pohybe po sieti. (Coos, 2021)

Detekcia a odozva koncového bodu a rozšírená detekcia a odozva

Detekcia a odozva koncového bodu (EDR - Endpoint Detection and Response), je integrované riešenie zabezpečenia koncového bodu, ktoré kombinuje nepretržité monitorovanie a zber údajov koncového bodu v reálnom čase s automatickými funkciami odozvy a analýzy založenej na pravidlách. (Trellix, 2023)

EDR je neoddeliteľnou súčasťou kompletnej informačnej bezpečnosti. Nie je to antivírusový softvér , ale môže mať antivírusové funkcie alebo môže používať údaje z iného antivírusového produktu. Antivírusový softvér je primárne zodpovedný za ochranu pred známym škodlivým softvérom, zatiaľ čo dobre vykonaný program ochrany a odozvy koncových bodov nájde nové zneužitia počas ich spustenia a zisťuje škodlivú aktivitu útočníka počas aktívneho incidentu. To umožňuje EDR detekovať bezsúborové malvérové útoky a útočníkov pomocou ukradnutých poverení, ktoré samotný tradičný antivírus nezastaví. (Wright, 2021)

Keďže útočníci neustále aktualizujú svoje metódy a schopnosti, tradičné ochranné systémy môžu zaostať. EDR kombinuje údaje a analýzu správania, vďaka čomu sú účinné proti vznikajúcim hrozbám a aktívnym útokom, ako sú:

- nový malvér;
- ransomvér ;
- pokročilé perzistentné hrozby (APT).

Rozšírená detekcia a odozva

Rozšírená detekcia a odozva (XDR - Extended Detection and Response), predstavuje vyvinutý bezpečnostný systém, ktorý rozširuje funkcie tradičných bezpečnostných nástrojov, ako sú EDR. Predstavuje automatickú koreláciu širšej škály údajov vrátane e-mailov, koncových bodov, serverov, cloudových pracovných zaťažení a sietí naprieč viacerými vrstvami zabezpečenia. Rozšírené riešenia detekcie a odozvy zisťujú hrozby rýchlejšie kontrolou rôznych vrstiev údajov, čím sa zlepšujú časy vyšetrovania a odozvy prostredníctvom analýzy zabezpečenia. (Sapphire, 2022)

Systém XDR funguje v troch základných krokoch:

1. Analýza údajov
2. Detekcia hrozieb
3. Reakcia na útok

Tabuľka 1 Porovnanie EDR a XDR

	EDR	**XDR**
Rozsah	Koncové body a hostitelia.	Koncové body, hostitelia, sieť a prenos medzi zariadeniami
Zámer	Zameranie na ochranu koncových bodov a prístupových oblastí. Ide o infiltráciu, monitorovanie a zmierňovanie, hodnotenie zraniteľnosti, varovanie a reakciu.	Viditeľnosť/transparentnosť na viacerých úrovniach zabezpečenia (sieť, koncový bod, aplikácie), detekcia známych a neznámych hrozieb, monitorovanie, hodnotenie zraniteľnosti, varovanie a reakcia,
Metódy	Detekcia škodlivého správania, analýza TTP, analýza indikátora kompromisu (IoC), podpisy a strojové učenie.	Strojové učenie, identifikácia taktiky, techník a postupov útočníka (TTP), detekcia anomálií, detekcia škodlivého správania a analýza indikátorov kompromisu (IoC).

Zdroj: Sapphire, 2022

2 Cieľ práce

Diplomová práca *Informačný systém a požiadavky na jeho ochranu* sa v teoretickej časti práce zaoberá priblížením pojmov ako je informačný systém a informačná bezpečnosť. Prvá kapitole ďalej obsahuje charakteristiku komponentov stratégie zabezpečenia údajov a modely ochrany dát v podnikoch.

Hlavným cieľom diplomovej práce je návrh a následná implementácia programu informačnej bezpečnosti v konkrétnom slovenskom podniku.

Realizáciu hlavného cieľa záverečnej práce dosiahneme pomocou čiastkových cieľov, ktorými sú preštudovanie a vymedzenie aktuálnych pojmov, získanie relevantných informácií o sledovanom podniku a následný návrh programu informačnej bezpečnosti.

V časti práce s názvom metodika práce a metódy skúmania si popíšeme metódy použité pri tvorbe záverečnej práce, pričom táto kapitola bude obsahovať aj bližšiu charakteristiku vybranej spoločnosti a interných procesov v nej.

Praktická časť práce bude slúžiť na priblíženie kybernetickej bezpečnosti na Slovensku a riešenie problému s nedostačujúcim systémom vo vybranej spoločnosti. Základným cieľom tejto kapitoly bude návrh programu informačnej bezpečnosti v konkrétnom slovenskom podniku.

3 Metodika práce a metódy skúmania

V tretej kapitole si priblížime metódy a spôsoby získavania údajov a pracovné postupy pri tvorbe záverečnej práce. Popíšeme základné informácie o skúmanej spoločnosti, ktorou je Panel Team s.r.o. a v nasledujúcich podkapitolách sa zameriame na terajšiu štruktúru podniku, znázornenie mapy procesov, ako aj na stav informačného systému a technológií.

Metódy využívané v diplomovej práci sú nasledovné:

Literárna rešerš - Ide o zbieranie potrebných faktov a poznatkov z literatúry a iných zdrojov. V práci budeme využívať čo najnovšie informácie, ktoré budeme čerpať zväčša z internetových zdrojov, ktoré podporíme vhodne zvolenou literatúrou.

Syntéza - je proces, pri ktorom sa spoja rôzne časti problému do jedného celku. Cieľom je zistiť, ako tieto časti spolu súvisia a aké sú dôležité vzájomné súvislosti medzi nimi. V práci budeme skúmať, ako jednotlivé časti ovplyvňujú celkové pôsobenie spoločnosti.

Analógia - založená na metóde pozorovania, ktorá sa zameriava na hľadanie spoločných charakteristík medzi rôznymi objektmi alebo udalosťami. V práci sa budeme venovať hľadaniu spoločných čŕt pomocou analógie, zameriame sa na informačný systém spoločnosti a zahraničné riešenia.

Porovnávanie - proces, ktorý sa zameriava na posúdenie podobných alebo odlišných charakteristík medzi dvoma alebo viacerými objektmi alebo javmi.

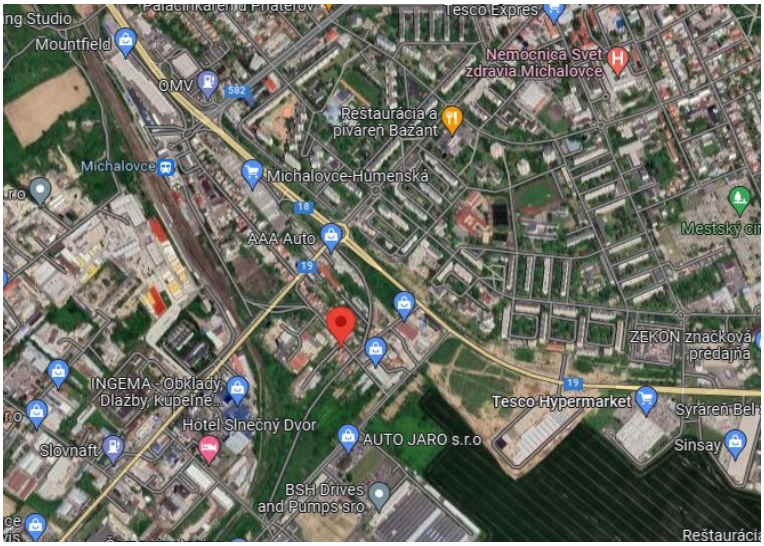
Analýza – zameriava sa na rozklad alebo rozbor skúmaného predmetu alebo javu na menšie časti. V našej práci budeme dôkladnejšie preskúmať teoretické základy pomocou analýzy.

Hodnotenie rizika – táto metóda pozostáva z identifikácie potenciálnych hrozieb a zraniteľností, ktoré by mohli ohroziť informačnú bezpečnosť spoločnosti. V práci si vytvoríme škálu a následne podľa nej budeme hodnotiť riziká.

3.1 Charakteristika spoločnosti Panel Team s.r.o.

Panel Team je spoločnosť zameraná na predaj sendvičových panelov a ich príslušenstva. Sendvičový panel je moderný materiál, ktorý sa používa v dnešnom stavebnom priemysle čoraz viac. Spoločnosť svoju obchodnú činnosť na trhu začala v roku 2017.

Cieľom spoločnosti je prinášať zákazníkom viac ako bežná obchodná spoločnosť. Ide predovšetkým o: vzájomnú dôveru, korektné obchodné vzťahy, vysokú úroveň služieb a kvalifikované poradenstvo.



Obrázok 2 Zobrazenie sídla spoločnosti na mape

Zdroj: Panel Team, 2023

5 pilierov spoločnosti:

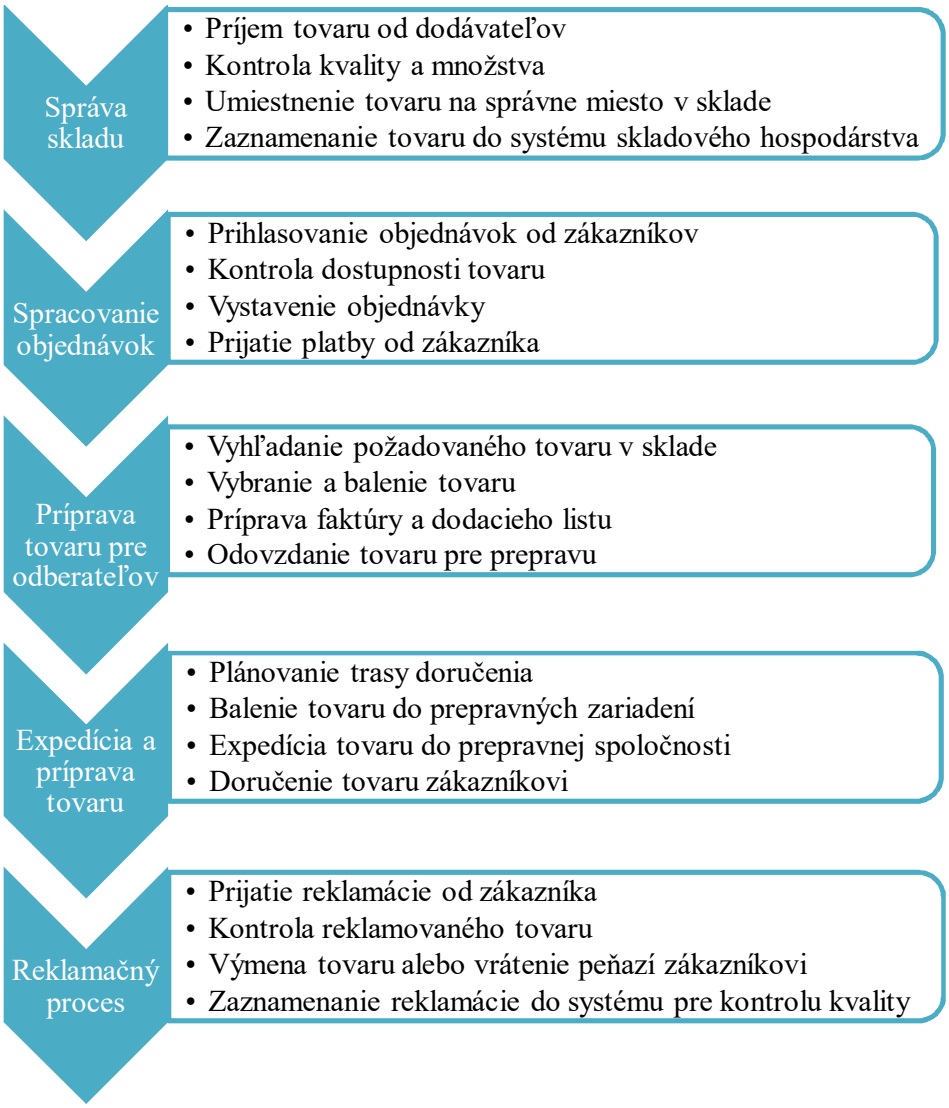
1. Konkurencieschopné služby - predaj, výroba
2. Posilnenie konkurencieschopnosti zákazníka
3. Rozvoj vzťahov so zákazníkmi
4. Najlepší nákup = priamy predaj
5. Optimalizované skladovanie

Obrázok 3 Logo spoločnosti

Zdroj: Panel Team, 2023

V súčasnosti sa spoločnosť zaoberá predajom a dopravou hutníckeho materiálu, pričom jej produkty sa vyznačujú vysokou kvalitou. Skladové zásoby a rozmanitosť sortimentu, ako aj možnosť doručenia na miesto určenia umožňuje spoločnosti uspokojiť aj náročnejšie požiadavky firiem a zákazníkov. Vlastný rozvoz pomáha šetriť drahocenný čas a prostriedky zákazníkov. Spoločnosť má sortiment skladom, čo jej umožňuje okamžite vyhovieť požiadavkám zákazníkov.

Procesy v spoločnosti



3.2 Informačný systém a informačné technológie v podniku

Informačné systémy a informačné technológie v sledovanom podniku predstavujú rôzne softvérové a hardvérové nástroje, ktoré slúžia na zlepšenie správy informácií a procesov v rámci podniku. Pomocou týchto nástrojov vie podnik zefektívniť svoje operácie a dosiahnuť lepšie výsledky prostredníctvom rýchlejšej a efektívnejšej správy informácií.

Informačné systémy a technológie v podniku:

Systém riadenia skladu: pomocou tohto systému môže firma spravovať svoje skladové zásoby a sledovať pohyb tovaru v reálnom čase. Takýto systém môže pomôcť minimalizovať zásobovacie chyby a zvýšiť efektivitu. Podnik využíva: *Systémy plánovania zdrojov podniku (ERP).*

CRM systém: systém riadenia vzťahov s klientmi (CRM) môže pomôcť firme udržiavať informácie o zákazníkoch, zákazníckych zmluvách a histórii nákupov. Toto môže pomôcť pri správe vzťahov so zákazníkmi a zvýšiť ich spokojnosť. Ide o: *Hubspot CRM*

Cloudové riešenia: umožňujú firme ukladať a zdieľať údaje online a v reálnom čase, čím pomáhajú zvýšiť efektivitu a produktivitu práce. V podniku sa využíva *Google Cloud..*

Analýza dát: analytické nástroje umožňujú firme zhromažďovať, spracovávať a analyzovať dáta o svojom obchode, ktoré môžu pomôcť pri rozhodovaní a zvyšovaní efektívnosti. Ide o: *Google Analytics*

Digitálny marketing: umožňuje malým podnikom zvyšovať povedomie o svojich produktoch a službách a získavať nových zákazníkov cez rôzne online platformy a kanály. Ide o tieto typy: *Facebook, Instagram, Pay-per-click, Google AdWords*

3.3 Nevýhody súčasného riešenia

Prostredníctvom podnikových údajov sme identifikovali nasledujúce nevýhody v riadení informačnej bezpečnosti v podniku:

Obmedzený prístup k odborným znalostiam - nedostatočný prístup k odborným znalostiam a skúsenostiam v oblasti informačnej bezpečnosti, čo vedie k nedostatočnému riešeniu bezpečnostných hrozieb.

Potreba vyššej špecializácie personálu na informačnú bezpečnosť - V niektorých prípadoch môže byť potrebné zamestnať špecializovaného personálu na implementáciu a správu bezpečnostných opatrení, čo je finančne nákladné.

Zraniteľnosť voči vnútorným hrozbám - nedostačujúce politiky v rámci interných záležitosti, môže dôjsť ku zneužívaniu dôvernosti alebo krádeži citlivých informácií zo strany zamestnancov alebo bývalých zamestnancov.

Časová náročnosť - implementácia a udržiavanie bezpečnostných opatrení je pre podnik časovo náročné, čo ovplyvňuje schopnosť venovať sa iným dôležitým oblastiam podnikania.

Zložitosť a technická náročnosť - niektoré bezpečnostné opatrenia predstavujú ťažkosti pri implementácií a správe, a vyžadujú si technickú odbornosť a skúsenosti.

4 Výsledky práce

Štvrtá kapitola bude venovaná výsledkom práce, ktoré sme získali prostredníctvom dostupných a zhromaždených informácií. Priblížime si kybernetickú bezpečnosť na Slovensku a navrhneme program informačnej bezpečnosti pre vybranú spoločnosť.

4.1 Kybernetická bezpečnosť na Slovensku

Kybernetický bezpečnostný incident sa označuje ako akákoľvek udalosť, ktorá spôsobí negatívny vplyv na kybernetickú bezpečnosť, a to buď preto, že došlo k narušeniu siete a informačného systému, porušeniu bezpečnostnej politiky alebo nedodržaniu záväznej metodiky. (NBU, 2022)

Hackeri, ktorí sa zamýšľajú nad útokom na podniky na podnikovej úrovni, sú motivovaní väčšími možnosťami zisku a preto venujú viac času a úsilia na plánovanie a vykonávanie útokov. Mohli by tráviť mesiace testovaním svojich metód a hľadaním zraniteľností, prípadne dokonca spolupracovať s inými hackermi, aby dosiahli svoj cieľ.

Za roky 2019, 2020 a 2021 Národné centrum kybernetickej bezpečnosti SK-CERT sledovalo slovenský kybernetický priestor a systematicky zhromažďovalo informácie o kybernetických bezpečnostných incidentoch. Informácie boli získané zo vlastných detekcií, povinných a dobrovoľných hlásení prevádzkovateľov základných a digitálnych služieb, ako aj od partnerov a partnerských organizácií.

Na základe získaných dát za dostupné roky možno vytvoriť ucelený pohľad na počet detegovaných (nahlásených) a riešených incidentov podľa jednotlivých kategórií.

Tabuľka č. 2 predstavuje počet detegovaných a riešených incidentov za dostupné roky (2019, 2020, 2021) a kybernetické incidenty, ktoré boli rozdelené do 5 kategórii a to: nedostupnosť (DoS, DDoS), botnet, pokus o prienik, škodlivý kód a získavanie informácií.

Z údajov v tabuľke je možné konštatovať, že najviac detegovaných incidentov obsahuje kategória „získavanie informácií“, pričom počet nahlásených incidentov má rastúcu tendenciu. Počet riešených incidentov je tiež rastúci, no nedostačujúci pre túto kategóriu, pretože počet riešených incidentov v roku 2021 predstavuje iba 0,3 %.

Kategória s najlepším pomerov detegovaných a riešených incidentov predstavuje „pokus o prienik“, kde percento riešených incidentov predstavuje v roku 2021 31%.

V kategórií „nedostupnosť“ možno sledovať značný nárast incidentov. Z roku 2020 na rok 2021 počet incidentov stúpol o 93 865. Najviac riešených incidentov bolo zaznamenaných v roku 2019, čo predstavovalo 15%.

Tabuľka 2 Počet detegovaných a riešených incidentov podľa typu za roky 2019-2021

	Nedostupnosť (DoS,DDoS)		Botnet		Pokus o prienik		Škodlivý kód		Získavanie informácií	
	Detegované	Riešené	D	R	D	R	D	R	D	R
2021	98 092	81	60 693	4	10 870	3 401	17 191	433	431 788	1 339
2020	4 227	121	73 133	10	7 032	1 216	1 441	446	221 836	1 164
2019	6 231	931	80 375	3 628	45 385	1 529	3 483	520	296 782	797

Zdroj: Vlastné spracovanie

V nasledujúcom grafe č. 1 možno sledovať detegované incidenty za sledované roky (2019, 2020, 2021), rozdelené podľa počtu výskytu z časového hľadiska pre každý mesiac.

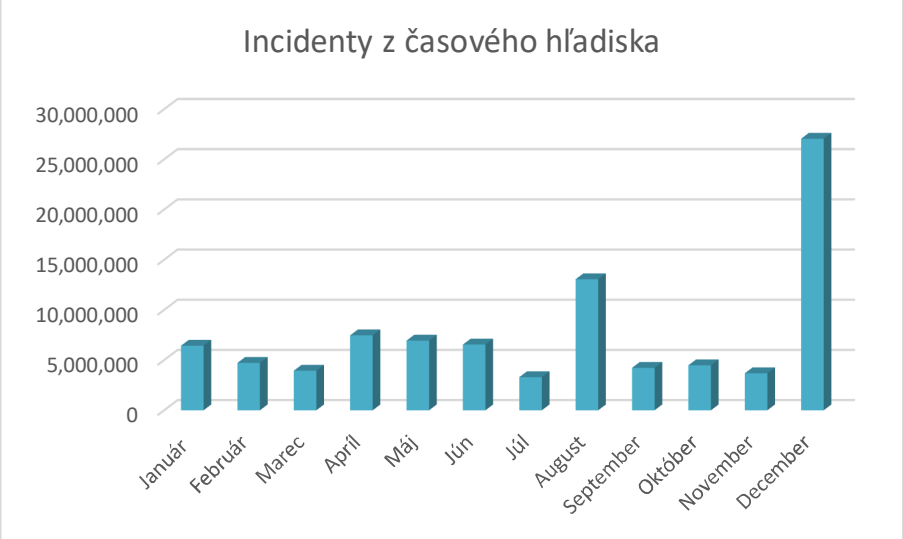
Z grafu možno konštatovať, že najvyšší počet incidentov za všetky roky bol zaznamenaný v mesiaci december (27 062 282). Mesiac s najnižším počtom detegovaných incidentov je júl (3 302 772). Výraznejším mesiacom je aj august kde bolo zaznamenaných 13 059 401 incidentov. Zvyšné mesiace možno rozdeliť do 3 skupín:

1. skupina do 4 miliónov incidentov (Marec, November),

2. skupina do 5 miliónov (Február, September, Október),

3. skupina do 7,5 miliónov (Apríl, Máj, Jún)

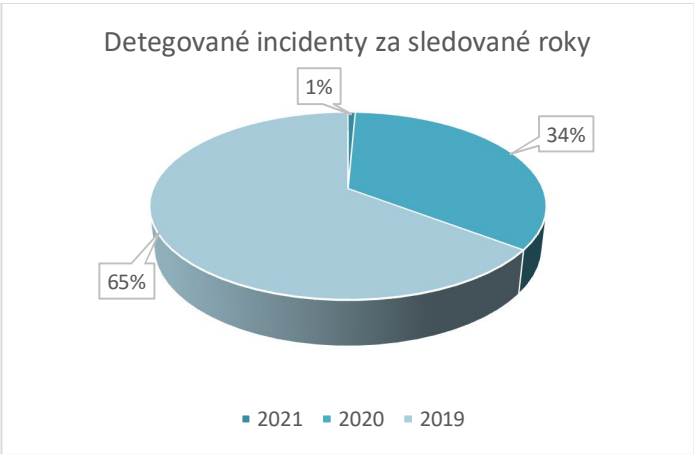
Graf 1 Rozdelenie detegovaných incidentov z časového hľadiska za sledované roky 2019-2021



Zdroj: Vlastné spracovanie

Graf č. 2 predstavuje kumulatívnu sumu detegovaných incidentov za sledované roky (2019, 2020, 2021). Celkový počet detegovaných incidentov za 3 roky predstavoval sumu 91 886 017. Z grafu možno vidieť, že rok s najvyšším počtom incidentov bol rok 2019 (59 455 329). Počet incidentov v ďalších dvoch nasledujúcom rokoch klesal, čo predstavuje pozitívny jav. V roku 2021 počet incidentov tvoril iba 1%, čo predstavuje sumu 654 517.

Graf 2 Detegované incidenty za roky 2019-2021



Zdroj: Vlastné spracovanie

4.2 Program informačnej bezpečnosti

Procesy a mechanizmy, ktoré tvoria program informačnej bezpečnosti (PIB), zahŕňajú technické, administratívne a fyzické zabezpečenia. Ich úlohou je ochrániť bezpečnosť a funkčnosť organizácie pred možnými rizikami a zamedziť neoprávnenému prístupu k jej údajom. Účinný bezpečnostný program pomáha organizácii zabezpečiť dôvernosť, integritu a dostupnosť informácií o klientoch a zákazníkoch, ako aj súkromných údajov organizácie prostredníctvom účinných postupov a kontrol zabezpečenia. (Tam, 2021)

Základné kroky pri tvorbe programu informačnej bezpečnosti:

1. Identifikácia a vymedzenie kľúčových informácií pre podnik
2. Hodnotenie rizík
3. Vytvorenie politík a postupov
4. Vzdelávanie zamestnancov
5. Implementácia bezpečnostných technológií
6. Kontrola a hodnotenie

1. Identifikácia kľúčových informácií

Sledovaný podnik môžeme zaradiť medzi malé podniky, čo znamená, že si musí určiť, ktoré informácie majú chrániť ako prvé, keďže zdroje sú obmedzené. Kľúčové informácie, ktoré by mal sledovaný podnik identifikovať a chrániť, predstavujú :

- Zákaznícke dáta - to zahŕňa osobné informácie ako mená, adresy, telefónne čísla, e-mailové adresy a údaje o kreditných kartách. Pre sledovaný podnik je ochrana týchto údajov dôležitá aby sa predišlo krádeži identít a udržala sa dôvera zákazníkov.
- Údaje o podnikových operáciách - ide predovšetkým o interné plány, podnikové stratégie, marketingové údaje a iné podnikové informácie. Ochranou základných podnikových prvkov možno docieliť zabráneniu neoprávnenej manipulácií.
- Finančné údaje: - ide o detaily účtov, faktúry, bankové údaje a daňové priznania. Ochrana týchto údajov je potrebná pre udržanie finančnej stability.

- Duševné vlastníctvo - predstavuje patenty, know-how podniku, obchodnú značku, autorské práva, obchodné tajomstvá a iné vlastnícke informácie. Ochranou týchto údajov možno zaistiť konkurenčnú výhodu.
- Údaje o zamestnancoch - ide o osobné informácie ako mená, adresy, telefónne čísla, e-mailové adresy, čísla sociálneho zabezpečenia a bankové údaje. Podnik ochranou týchto údajov zaisťuje súkromie zamestnancov a zabraňuje možnej krádeži identity.

2. Hodnotenie rizík

Pre hodnotenie rizika v podniku sme vytvorili v tabuľke číslo 3 škálu hodnotenia. Na základe toho sme v tabuľke číslo 4 vybrali 6 najpravdepodobnejších rizík, ktoré by mohli spoločnosť ohroziť a rozdelili sme ich na externé a interné. Pre každé riziko sme popísali jeho obsah a priradili sme závažnosť a pravdepodobnosť výskytu. Výsledkom bol výpočet celkového rizika.

Z výpočtu celkového rizika možno vidieť, že interné hrozby predstavujú stredné a vysoké riziko, pričom externé hrozby predstavujú nevýznamné a nízke riziko pre podnik. Najvyššia hodnota celkového rizika je 12 a prislúcha kategórií nebezpečenstva: *„Zneužitie zariadení“*.

Tabuľka 3 Škála pre hodnotenie rizika

Hodnotenie rizika závažnosť		**Hodnotenie rizika pravdepodobnosť**		**Celkové riziko (závažnosť x pravdepodobnosť)**		
1.	Žiadne alebo minimálne straty	1.	Vysoko nepravdepodobné	1-2	Nie je významné	Sledovať
2.	Straty vyžadujúce si pozornosť	2.	Nepravdepodobné	3-5	Nízke	Prijateľné (snažiť sa o zníženie)
3.	Straty, pri ktorých dochádza k pozastaveniu pracovného postupu	3.	Možné	6-10	Stredné	Znížiť a riadiť
4.	Veľké straty spôsobené rozsiahlymi škodami	4.	Pravdepodobné	11-25	Vysoké	
5.	Straty spôsobené v dôsledku celkového zlyhania	5.	Veľmi pravdepodobné			

Zdroj: Vlastné spracovanie

Tabuľka 4 Hodnotenie rizík

	Nebezpečenstvo	Aké hrozí riziko	Závažnosť	Pravdepodobnosť	Celkové riziko (závažnosť x pravdepodobnosť)
Externé hrozby	Kybernetický útok	škodlivý softvér, ktorý môže byť nainštalovaný na zariadeniach zamestnancov alebo serveroch podniku	3	2	**6**
	Fyzické hrozby	prírodné katastrofy (záplavy, požiare),výpadky energie	2	2	**4**
	Zákonné požiadavky	nutnosť sprístupnenia informácií vládnym orgánom alebo iným inštitúciám	1	1	**1**
Interné hrozby	Zneužitie právomoci	prístup zamestnancov k informáciám, ktoré by nemali byť sprístupnené	3	3	**9**
	Nesprávne používanie zariadení	nesprávne používanie softvéru, ľahostajné správanie pri manipulácií s citlivými informáciami	3	3	**9**
	Zneužitie zariadení	nadpriemerné používanie firemných zariadení na osobné (súkromné) účely	3	4	**12**

Zdroj: Vlastné spracovanie

3. Vytvorenie politík a postupov

Program informačnej bezpečnosti obsahuje politiky, postupy a opatrenia, ktoré má spoločnosť prijať a dodržiavať, aby zabezpečila ochranu svojich informácií a zabezpečila súlad so zákonnými a regulačnými požiadavkami týkajúcimi sa informačnej bezpečnosti.

Vytvorenie politík a postupov v spoločnosti, ktorá sa orientuje na hutnícky materiál, môže pomôcť zabezpečiť efektívne fungovanie podniku a zlepšiť jeho výkonnosť.

Politiky a postupy, ktoré by mali byť súčasťou sledovaného podniku sú:

- Zabezpečenie prístupu k informáciám - ktorí zamestnanci alebo oddelenia majú prístup k citlivým informáciám týkajúcim sa obchodných transakcií a finančných údajov.
- Bezpečnosť siete a systémov: politiky a postupy na zabezpečenie bezpečnosti siete a systémov spoločnosti. Toto môže zahŕňať pravidelné aktualizácie softvéru a

hardvéru, zabezpečenie, že siete sú chránené pred neoprávneným prístupom a ochranu pred vírusmi a malvérom,

- Ochrana citlivých informácií: politiky a postupy na zabezpečenie ochrany citlivých informácií. Toto môže zahŕňať šifrovanie citlivých dát, fyzickú ochranu citlivých dokumentov a zabezpečenie, že citlivé informácie sú zdieľané len s oprávnenými osobami a organizáciami,
- Politiky a postupy pri vzniku incidentov: postupy a politiky na správu incidentov. Toto môže zahŕňať postupy na identifikáciu, hodnotenie a správu incidentov, ako aj na obnovu z dôsledkov incidentov.

4. Vzdelávanie zamestnancov

Vzdelávanie zamestnancov zahŕňa poskytovanie školení a výcviku, ktoré pomáhajú zamestnancom zlepšovať ich zručnosti, znalosti a schopnosti, aby mohli účinne vykonávať svoje práce. Tento proces zahŕňa školenie v oblasti bezpečnosti a ochrany zdravia pri práci, informačnej bezpečnosti, právnych predpisov a regulácií, ako aj rozvoj konkrétnych technických zručností potrebných pre prácu v organizácii. Zvyšovanie informačnej gramotnosti a povedomia o informačnej bezpečnosti je kľúčovým prístupom pri vzdelávaní zamestnancov. To zahŕňa oboznamovanie zamestnancov s základnými princípmi informačnej bezpečnosti a konkrétnymi hrozbami, ktoré môžu ovplyvniť ich prácu. Tieto aktivity majú kľúčový vplyv na zlepšenie výkonu a výsledkov organizácie.

Pri výber konkrétnych typov školení je potrebné dbať na potreby podniku a zamestnancov, ich pozície a zodpovednosti v organizácii. Je dôležité, aby organizácia mala prehľad o tom, ktoré školenia by mali byť prioritou a aby ich poskytla zamestnancom pravidelne a systematicky.

Pre sledovaný podnik sme vybrali základné typy školení, ktoré sa zameriavajú na rôzne aspekty informačnej bezpečnosti a technických zručností. Ide o tieto typy:

- Školenie zabezpečenia pracovného miesta: ide o školenia zamerané na to, ako zabezpečiť pracovné miesto a ochrániť citlivé informácie pred prístupom neoprávnených osôb.

- Školenia týkajúce sa zdieľania informácií: prínosom tohto školenia je vzdelávanie zamestnancov na účely toho, ako zdieľať informácie v organizácii a s tretími stranami, pričom sa zachováva bezpečnosť a súkromie.
- Školenia o phishingu a podvodoch: výsledkom tohto školenia je oboznámenie zamestnancov s rôznymi scenármi kybernetických útokov, pričom zamestnancom umožňujú lepšie identifikovať phishingové útoky a iné podvody
- Školenia o právnych predpisoch a reguláciách: tieto školenia sa zameriavajú na dodržiavanie právnych predpisov a regulácií týkajúcich sa ochrany údajov a informačnej bezpečnosti.
- Školenia v technických zručnostiach: tento druh školení sa zameriava na vývoj zručností v softvérovej a hardvérovej technológii, sieťovej bezpečnosti a databázových systémoch.

5. Implementácia bezpečnostných technológií

Implementácia bezpečnostných technológií závisí od konkrétnych potrieb a cieľov každého podniku. Pre zvolený podnik sme si vybrali priblížiť softvérové riešenia, ktoré podniku zabezpečia ochranu pred hrozbami a zefektívnenie podnikových procesov.

V tabuľkách číslo 5 a 6 sú zobrazené vybrané softvérové riešenia pre skúmaný podnik. Zvolili sme si základné kategórie, pričom sme pri výbere brali ohľad na veľkosť, zameranie a vlastnosti podniku.

Pre každú kategóriu sme vytvorili subkategóriu, kde sme vybrali 5 najvhodnejších riešení pre sledovaný podnik ide o tieto kategórie: pre kategóriu Financie sme si zvolili účtovníctvo, pre Správu vzťahov sme vybrali správu vzťahov so zákazníkmi (CRM-Customer relationship management), pre kategóriu Podniková inteligencia BI (Bussiness Inteligence), sme vybrali správu skladu, ďalšiu kategóriu tvoria Ľudské zdroje a poslednou kategóriou je Bezpečnosť kde sme si zvolili softvérové riešenia pre antivírus a pre XDR.

Účtovníctvo

Existuje množstvo softvérových riešení pre účtovníctvo, ktoré môžu byť použité v podniku, no je potrebné zosúladiť funkcie, cenu, použiteľnosť a prispôsobiteľnosť

konkrétnym potrebám podniku. Tieto riešenia môžu pomôcť automatizovať množstvo úloh v účtovníctve a zlepšiť efektivitu práce.

Pre sledovaný podnik sú nevyhnutné softvérové riešenia, ktoré obsahujú funkcie pre riadenie faktúr, výdavkov, výpočet miezd a sledovanie zásob. Okrem toho by softvérové riešenia pre účtovníctvo mali byť kompatibilné s legislatívnymi požiadavkami a zákonnými normami. Musia byť schopné generovať potrebné dokumenty a správy v súlade s týmito požiadavkami, ako napríklad daňové priznania, odpočty DPH, závierky a podobne.

Správa vzťahov so zákazníkmi

Pre správu vzťahov so zákazníkmi by požadovaný softvér mal obsahovať vstavané bezpečnostné funkcie, ako sú napríklad autentifikácia a autorizácia používateľov, šifrovanie dát, zálohovanie a obnovenie dát a podobne. Okrem toho by mal umožňovať nastavenie rôznych úrovní prístupových práv pre rôzne používateľské role a funkcie.

Ďalším dôležitým prvkom je sledovanie a monitorovanie aktivít používateľov, aby sa mohli identifikovať akékoľvek nezvyčajné aktivity alebo pokusy o neoprávnený prístup k citlivým informáciám. Softvér by mal umožňovať aj správu prístupových práv a povolení pre tretie strany, ako sú napríklad externí poskytovatelia služieb.

Podniková inteligencia – Správa skladu

Softvérové riešenia pre podnikovú inteligenciu pre správu skladu predstavujú dôležitý nástroj, ktorý by podniku uľahčil a zefektívnil získať a analyzovať dáta týkajúce sa skladových zásob a zásobovania. Tieto riešenia poskytujú informácie o pohybe tovaru, množstve zásob na sklade, predajoch a objednávkach, pričom pomáhajú optimalizovať procesy skladovania a zásobovania.

Softvérové riešenia pre správu skladu sú dôležitým nástrojom pre podniky, ktoré sa zameriavajú na zlepšenie efektívnosti svojho obchodného procesu a zvýšenie ziskov.

Ľudské zdroje

Softvérové riešenia pre správu ľudských zdrojov sú navrhnuté na automatizáciu a zlepšenie rôznych aspektov riadenia zamestnancov v organizácii. Tieto riešenia zvyčajne poskytujú nástroje na správu personálnych údajov, plánovanie ľudských zdrojov, monitorovanie výkonnosti, hodnotenie zamestnancov, výber a nábor zamestnancov, tréning a rozvoj a ďalšie funkcie, ktoré pomáhajú spravovať a optimalizovať pracovnú silu v organizácii.

Z pohľadu informačnej bezpečnosti je dôležité, aby tieto softvérové riešenia boli bezpečné a chránili citlivé údaje zamestnancov, ako sú osobné údaje, údaje o platoch a výkonnosti. Softvérové riešenia musia byť v súlade s legislatívnymi požiadavkami týkajúcimi sa ochrany osobných údajov a musia byť chránené pred rôznymi typmi kybernetických hrozieb.

Bezpečnosť

Softvérové riešenia sú kľúčové z hľadiska bezpečnosti, keďže zabezpečujú ochranu informácií a údajov v organizácii a dodržiavanie príslušných bezpečnostných noriem a predpisov. Tieto riešenia môžu zahŕňať rôzne nástroje a technológie, ako sú firewally, antivírusové programy, softvérové nástroje na detekciu a prevenciu hrozieb, správu prístupových práv, monitorovanie sietí a systémov, zálohovacie a obnovovacie nástroje a ďalšie.

Okrem toho musia byť tieto softvérové riešenia schopné monitorovať a kontrolovať prístup k informáciám, a to nielen zvnútra organizácie, ale aj zvonka. Pre sledovaný podnik je teda potrebné zamerať sa na tieto aspekty bezpečnosti:

- Identifikácia a autentifikácia používateľov,
- Antivírusová ochrana,
- Firewall,
- Zálohovanie a obnova dát.

Tabuľka 5 Navrhované softvérové riešenia pre vybraný podnik

Softvérové riešenia		
Financie	**Správa vzťahov**	**Podniková inteligencia (BI)**
Účtovníctvo	***Správa vzťahov so zákazníkmi (CRM)***	***Správa skladu***
Accounting SEED	4Degrees	AppRise
Bench Accounting	Affinity	FishBowl
BigTime	amoCRM	Zangerine
Elorus	AutoRaptor	Snapfulfil
ValueSoft	BigContacts	GOIS PRO

Zdroj: Vlastné spracovanie

Tabuľka 6 Navrhované softvérové riešenia pre vybraný podnik (pokračovanie)

Softvérové riešenia		
Ľudské zdroje	**Bezpečnosť**	
Ľudské zdroje	***Antivírus***	***XDR***
15Five	ADrive	Crashplan
Aurora Training Advantage	Barracuda Networks	Curricula
BerniePortal	Codeproof	DeviceLink
Bob	Avast	DollyDrive
ConnecTeam	Eset	Idrive

Zdroj: Vlastné spracovanie

6. Kontrola a hodnotenie

Je dôležité, aby kontroly a hodnotenia bezpečnosti informačných systémov v podniku prebiehali pravidelne a systematicky. Kontrola sa zameriava na overovanie, či sú implementované bezpečnostné politiky a postupy dodržiavané, a či sú príslušné bezpečnostné opatrenia efektívne. Dôležité je tiež zabezpečiť, aby bola bezpečnostná politika podniku aktualizovaná a prispôsobená aktuálnym rizikám.

Za vhodné formy kontroly informačnej bezpečnosti pre sledovaný podnik pokladáme tieto formy:

- Interná kontrola - je proces, ktorým sa zabezpečuje, že podnik riadi svoje operácie v súlade s internými politikami a postupmi. Táto kontrola môže byť vykonávaná internými odborníkmi na kontrolu alebo kontrolórmi v podniku.

- Externá kontrola - vykonáva sa nezávislými odborníkmi, ktorí nie sú zamestnancami podniku. Táto kontrola môže byť vykonávaná externými audítormi alebo bezpečnostnými odborníkmi.
- Penetračné testovanie - ide o formu kontroly, ktorá sa snaží zistiť, či existujú v informačnom systéme neoprávnené prístupy. Táto kontrola je vykonávaná bezpečnostnými odborníkmi, ktorí sa snažia prekonať bezpečnostné opatrenia a získať neoprávnený prístup do systému.
- Monitorovanie a sledovanie - pomáha podniku sledovať používanie informačného systému a zaznamenávať udalosti, ktoré by mohli naznačovať bezpečnostné riziká. Táto kontrola môže byť vykonávaná pomocou softvérových nástrojov alebo manuálne.

5 Diskusia

V poslednej kapitole záverečnej práce sa zameriavame na zhrnutie poznatkov a výsledkov, ktoré sme dosiahli v oblasti informačných systémov a požiadaviek na ich ochranu. Taktiež predstavíme návrhy na zlepšenie celkovej bezpečnosti vybraných procesov pre skúmanú spoločnosť.

Aktuálny stav kybernetickej bezpečnosti na Slovensku:

S využitím dostupných správ o vývoji kybernetickej bezpečnosti na Slovensku sme v našej práci sledovali vývoj v posledných troch rokoch (2019, 2020, 2021). Z rozsiahlych údajov týkajúcich sa tohto problému sme sa rozhodli priblížiť počet detegovaných a riešených incidentov podľa ich typu. Pre naše závery sme sa zameriavali na kategórie nedostupnosti (DoS, DDoS), botnet, pokusy o prienik, škodlivý kód a získavanie informácií. Výsledkom našej analýzy je zistenie, že kategória, ktorá zaznamenala najvyšší pomer riešených incidentov voči detegovaným, bola kategória "pokus o prienik". Pre rok 2021 sme zistili, že percento riešených incidentov v tejto kategórii predstavovalo hodnotu 31%.

Ďalej sme graficky zobrazili detegované incidenty za sledované roky rozdelené podľa počtu výskytov z časového hľadiska pre každý mesiac. Mesiac s najvyšším počtom incidentov bol december (27 062 282). Naopak, mesiac júl zaznamenal najnižší počet detegovaných incidentov (3 302 772). Ďalšie mesiace sme rozdelili do troch skupín, a to nasledovne:

1. skupina do 4 miliónov incidentov (Marec, November),
2. skupina do 5 miliónov (Február, September, Október),
3. skupina do 7,5 miliónov (Apríl, Máj, Jún)

Následne sme vypočítali kumulatívnu sumu za každý rok ohľadom detegovaných incidentov. Z výpočtov sme dospeli k záveru, že kybernetická bezpečnosť na Slovensku sa zlepšuje a zaznamenáva klesajúcu tendenciu, čo predstavuje pozitívny vývoj.

Program informačnej bezpečnosti pre spoločnosť Panel Team s.r.o.:

V druhej časti výsledkov práce sme sa venovali programu informačnej bezpečnosti, kde sme rozpracovali 6 základných krokov s prihliadnutím na aktuálny stav a zameranie sledovanej spoločnosti.

V prvom kroku sme identifikovali kľúčové informácie pre podnik. Keďže sledovaná spoločnosť patrí medzi malé podniky, je potrebné brať ohľad na správne vymedzenie najpodstatnejších informácií, ktoré sú:

- Zákaznícke dáta,
- Údaje o podnikových operáciách,
- Finančné údaje,
- Duševné vlastníctvo,
- Údaje o zamestnancoch.

V druhom kroku sme hodnotili riziko. Pred samotným hodnotením sme si vytvorili škálu, pomocou ktorej sme následne hodnotili riziká, ktoré hrozia podniku v oblasti informačnej bezpečnosti. Rizika sme si rozdelili na interné a externé a priraďovali sme závažnosť a pravdepodobnosť každému riziku. Výsledkom bolo celkové riziko, ktoré sme dostali súčinom závažnosti a pravdepodobnosti. Najvyššiu hodnotu sme zaznamenali pre riziko "Zneužitie zariadení", kde hodnota predstavuje sumu 12 z celkových možných 25.

V treťom kroku sme priblížili politiky a postupy na zabezpečenie bezpečnosti informácií v podniku. Spolu s podnikovými údajmi od sledovanej spoločnosti sme popísali najvýznamnejšie z nich a to sú:

- Zabezpečenie prístupu k informáciám,
- Bezpečnosť siete a systémov,
- Ochrana citlivých informácií,
- Politiky a postupy pri vzniku incidentov.

V štvrtom kroku sme sa venovali vzdelávaniu zamestnancov a popísali sme dôležitosť neustáleho vzdelávania sa v oblasti informačnej bezpečnosti. Pre sledovaný podnik sme následne navrhli päť typov školení, ktoré považujeme za vhodné na minimalizáciu chýb v tejto oblasti.

Piaty krok bol zameraný na implementáciu bezpečnostných technológií. Pre podnik sme si vybrali priblížiť softvérové riešenia. Podľa veľkosti a zamerania podniku sme

následne vybrali 5 kategórií (financie, správa vzťahov, podniková inteligencia, správa skladu, ľudské zdroje a bezpečnosť) a vytvorili sme tabuľky s najvhodnejšími riešeniami.

V poslednom šiestom kroku sme popísali kontrolu a hodnotenie, kde sme za vhodné formy kontroly v podniku určili tieto:

- Interná kontrola,
- Externá kontrola,
- Penetračné testovanie,
- Monitorovanie a sledovanie.

Návrhy a odporúčania pre podnik Panel Team s.r.o.:

Z výsledkov hodnotenia rizika vidíme, že hodnoty v rozmedzí 6 až 10 a 11 až 25 predstavujú stredné a vysoké riziko. Tieto hodnoty patria do rovnakej kategórie, konkrétne "Zníženie a riadenie". Preto sa prvotne zameriame na návrhy a odporúčania pre túto kategóriu.

Zneužitie právomoci (jedná sa o prístup zamestnancov k informáciám, ktoré by nemali byť sprístupnené)

- Hlavným krokom pre zníženie tohto rizika vidíme vo vytýčení každej pozície v podniku a s tým spojených úloh a právomoci.

Nesprávne používanie zariadení (ide o nesprávne používanie softvéru, ľahostajné správanie pri manipulácií s citlivými informáciami)

- Podnik by mal zabezpečiť pravidelnosť a aktuálnosť svojich podnikových systémov, čo je možné dosiahnuť prostredníctvom vzdelávania a školenia zamestnancov. Pri správnom a efektívnom nastavení školení by sa dalo predchádzať časovým stratám a s tým spojeným stratám v podniku.

Zneužitie zariadení (súvisí s nadpriemerným používaním firemných zariadení na osobné (súkromné) účely)

- Zneužitie zariadení predstavuje najzávažnejšie riziko v našom celkovom hodnotení. Je tomu tak, pretože v dnešnej dobe sa stále viac procesov automatizuje alebo

poloautomatizuje a na riadenie sa využívajú počítačové programy. Pre výkon svojej práce zamestnanci potrebujú telefón, tablet alebo počítač čoraz častejšie.

Návrhy pre zníženie rizika sú nasledovné:

- Podnik by mal zabezpečiť, aby zamestnanci mali prístup len k programom a rozhraniu potrebným pre výkon svojej práce.
- Podnik by mal zvážiť poskytnutie alternatív pre zamestnancov, ako sú napríklad osobné zariadenia, aby sa minimalizovalo používanie firemných zariadení na osobné účely.

Pre ďalšie odporúčania by sme dali do pozornosti vzdelávanie a školenie zamestnancov. Za efektívne riešenie vo vzdelávaní zamestnancov pokladáme kombináciu skupinového a individuálneho školenia. Kombinácia môže byť výhodná, pretože umožňuje prispôsobenie sa potrebám každého jednotlivca a maximalizuje efektivitu výučby. Za hlavné výhody pokladáme:

- Personalizované školenie (prispôsobené potrebám jednotlivca)
- Interakcia (skupinová diskusia)
- Flexibilita (kombinácia umožňuje prispôsobiť sa potrebám a preferenciám jednotlivca)
- Motivácia: (pri učení sa od iných v skupine)

Tabuľka 7 Odporúčané školenia a kurzy v oblasti informačnej bezpečnosti

Názov školenia	Časová náročnosť	Suma
Základy informačnej bezpečnosti	1 deň	384 €
Prehľad kybernetickej bezpečnosti	1 deň	280 €
Základy kybernetickej bezpečnosti	1 deň	320 €

Zdroj: Vlastné spracovanie

Kurzy zabezpečuje Kompetenčné a certifikačné centrum kybernetickej bezpečnosti.

V poslednom návrhu sa zameriavame na komparáciu cloudového riešenia, ktoré momentálne podnik využíva, a riešenia, ktoré sme navrhli. Pre porovnanie sme využili nasledovné kritéria: veľkosť úložiska, náklady na používanie, rýchlosť nahrávania a podporu. Pri porovnávaní údajov sme zistili, že v každom kritériu je súčasné riešenie horšie ako navrhované, s výnimkou nahrávania, ktoré je pri oboch riešeniach rovnaké.

Tabuľka 8 Komparácia súčasného a navrhovaného cloudového riešenia

	Úložisko €/GB	Náklady na používanie		Rýchlosť nahrávania MB/s	Podpora	
		Nahrávanie	Sťahovanie		Mesačné náklady	Doba odozvy
Google Cloud	0,0166/1	Zadarmo	0,094 €	1,2	150 €	<6 hodín
Backblaze	0,0042/1	Zadarmo	0,045€	1,5	130 €	<2 hodiny

Zdroj: Vlastné spracovanie

Záver

V závere našej diplomovej práce sme zhrnuli body, ktorým sme sa venovali, a priblížili sme výsledky z praktickej časti, v rámci ktorej sme navrhli odporúčania pre sledovanú spoločnosť.

V teoretickej časti sme sa venujeme vymedzeniu pojmov informačný systém a informačná bezpečnosť, typom informačných systémov a databázovým modelom, ako aj kybernetickým hrozbám a moderným modelom ochrany dát v podniku.

Druhá kapitola sa zameriava na hlavný cieľ práce s menšími čiastkovými cieľmi.

V tretej kapitole sme opísali metodiku práce a metódy skúmania a detailne sme načrtli procesy a informačné systémy a technológie využívané v sledovanej spoločnosti.

V praktickej časti sme sa prv venovali kybernetickej bezpečnosti na Slovensku. Prostredníctvom dostupných údajov sme mohli sledovať vývoj za tri roky (2019, 2020, 2021). Vybrali sme si priblížiť počet detegovaných a riešených incidentov podľa typu. Najviac detegovaných incidentov obsahovala kategória „získavanie informácií“, pričom počet nahlásených incidentov má za sledované roky rastúcu tendenciu. Možno konštatovať, že kategória, ktorá zaznamenala najvyšší pomer riešených incidentov voči detegovaným, bola kategória "pokus o prienik". Pre rok 2021 sme zistili, že percento riešených incidentov v tejto kategórii predstavovalo hodnotu 31%. Následne sme graficky zobrazili počet detegovaných incidentov rozdelených z časového hľadiska podľa mesiacov. Kde najvýraznejší mesiac bol december s počtom detegovaných incidentov (27 062 282). Ďalej sme zobrazili kumulatívnu sumu za každý sledovaný rok a dospeli sme k záveru, že kybernetická bezpečnosť na Slovensku sa zlepšuje a zaznamenáva klesajúcu tendenciu, čo predstavuje pozitívny vývoj.

V druhej časti programu informačnej bezpečnosti pre podnik Panel Team s.r.o. sme sa venovali hodnoteniu rizika. Na začiatku sme si vytvorili škálu pre hodnotenie rizika, aby sme mohli následne vyhodnotiť najväčšie hrozby pre zabezpečenie informačnej bezpečnosti podniku. Tieto hrozby sme následne zhrnuli v tabuľke najviac pravdepodobných rizík, ktoré by mohli byť pre podnik ohrozením.

V tretej časti sme rozpracovali postupy a politiky, ktoré by mali byť súčasťou sledovaného podniku. Tieto politiky zahŕňajú pravidlá pre používanie zariadení v podniku, prístupové práva k informáciám, zálohovanie dát a ďalšie aspekty, ktoré súvisia s ochranou informácií.

V štvrtej časti sme sa zameriavali na vzdelávanie a školenie zamestnancov. Navrhli a priblížili sme najvhodnejšie typy školení v oblasti informačnej bezpečnosti pre sledovaný podnik.

V piatej časti sme sa venovali implementácii bezpečnostných technológií pre podnik. Zameriavali sme sa najmä na softvérové riešenia, ktoré môžu zabezpečiť ochranu pred hrozbami a zefektívniť podnikové procesy.

V poslednej časti sme opísali najvhodnejšie formy kontroly a hodnotenia programu informačnej bezpečnosti pre sledovaný podnik. Tieto kontroly a hodnotenia by mali byť súčasťou pravidelných auditov, ktoré by mali zabezpečiť, že program informačnej bezpečnosti je aktuálny a účinný.

Posledná kapitola našej záverečnej je diskusia, kde sme sa venovali zhrnutiu dosiahnutých poznatkov z praktickej časti a následným návrhom na zlepšenie informačnej bezpečnosti v sledovanom podniku.

Ako objekty pre stanovenie návrhov pre zlepšenie informačnej bezpečnosti v podniku sme si vybrali vytvoriť návrhy pre nami najviac rizikové faktory, ktoré by v podniku mohli nastať, pričom sme uviedli odporúčané typy školení a porovnali súčasné cloudové riešenie a nami odporúčané.

Bibliografické zdroje

BOURGEOIS, D., et al. 2019. *Information Systems for Business and Beyond*. Textbook 1. Saylor Academy. [Online]. [Dátum: 08. 02. 2023]. Dostupné na: https://digitalcommons.biola.edu/open-textbooks/1/

BROTBY, W. 2008. *Information security governance: guidance for information security managers*. ISBN 978-1-933284-73-6. [Online]. [Dátum: 15. 02. 2023]. Dostupné na: http://www.csun.edu/~yz73352/657/sent-0710/InfoSec-Guidance-for-Mgrs-Research-21May08.pdf

COOS, A. 2022. *5 Ways Large Enterprises Protect their Data*. [Online]. [Dátum: 01.02. 2023]. Dostupné na: 5 Ways Big Companies Protect their Data | Endpoint Protector

CYBERARK. 2023. *Malvérové útoky*. [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://www.cyberark.com/

EMERITUS. 2022. *6 typov informačných systémov a ich aplikácií*. [Online]. [Dátum: 20. 03. 2023]. Dostupné na: https://emeritus.org/in/learn/the-6-types-of-information-systems-and-their-applications/

ENZENHOFER, W. 2019. *Sprievodca kyber-bezpečnosťou pre výrobné podniky* [Online]. [Dátum: 10. 04. 2023]. Dostupné na: Sprievodca_kyber_bezpecnostou_2019.pdf (industry4um.sk)

FLOWII, 2018. *Zásady bezpečnosti internetových aplikácií.* [Online]. [Dátum: 20. 03. 2023]. Dostupné na: https://www.flowii.com/sk/blog/zasady-bezpecnosti-internetovych-aplikacii

GREENLEE, M. 2021. *What Is a Botnet Attack?* [Online]. [Dátum: 20. 04. 2023]. Dostupné na: https://securityintelligence.com/articles/what-is-botnet-attack/

IBM, 2021. *Why is data security important?*. [Online]. [Dátum: 15. 02. 2023]. Dostupné na: https://www.ibm.com/topics/data-security

JANOŠCOVÁ, R. 2014. *Princípy informačnej bezpečnosti.* [Online]. [Dátum: 01. 02. 2023]. Dostupné na: https://www.researchgate.net/publication/281098287_Principy_informacnej_bezpecnosti

KASPERSKY, 2023. *What is a Botnet.* [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://usa.kaspersky.com/resource-center/threats/botnet-attacks

KOKLES, M., ROMANOVÁ, A. 2018. *Informatika*. [2. vyd.]. Bratislava: Sprint dva, Economics. ISBN 978-80-89710-40-9.

KUMAR, S. 2020. *An emerging threat Fileless malware.* [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0043-x

LAUDON, K., LAUDON, J., 2014. *Management Information Systems*. 13th edition, ISBN: 978-0-13-305069-1. [Online]. [Dátum: 08. 02. 2023]. Dostupné na: https://pressbooks.pub/bus206/chapter/chapter-1/#return-footnote-25-3

MAHMOUD, M. 2019. *Modeling and control of Cyber-Physical Systems subject to cyber attacks.* 101-115s., ISSN 0925-2312

MICROSOFT, 2022. *Trusted Platform Module Technology Overview.* [Online]. [Dátum: 15. 03. 2023]. Dostupné na: https://learn.microsoft.com/en-us/windows/security/information-protection/tpm/trusted-platform-module-overview

MONEY, 2022. *Vzdelávanie a rozvoj zamestnancov. Koho, kedy a ako vzdelávať?* [Dátum: 10. 04. 2023]. Dostupné na: https://www.money.sk/dane-a-uctovnictvo/vzdelavanie-a-rozvoj-zamestnancov-koho-kedy-a-ako-vzdelavat/

NBU, 2020. *Správa o kybernetickej bezpečnosti v Slovenskej republike za rok 2019.* [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-SR-2019.pdf

NBU, 2021. *Správa o kybernetickej bezpečnosti v Slovenskej republike za rok 2020.* [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Sprava-o-kybernetickej-bezpecnosti-2020.pdf

NBU, 2022. *Správa o kybernetickej bezpečnosti v Slovenskej republike za rok 2021*. [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://www.nbu.gov.sk/wp-content/uploads/urad/Vyrocne_spravy/Sprava-o-KB-SR-2021.pdf

NBU, 2023. *Hlásenie kybernetických bezpečnostných incidentov*. [Online]. [Dátum: 10. 04. 2023]. Dostupné na: https://www.nbu.gov.sk/kyberneticka-bezpecnost/hlasenie-kybernetickych-bezpecnostnych-incidentov/index.html

NEXTECH, 2023. *Kybernetická bezpečnosť pre firmy*. [Online]. [Dátum: 10. 04. 2023]. Dostupné na: Kyber Bezpecnost v2.indd (nextech.sk)

PANEL TEAM, 2023. *O spoločnosti*. [Online]. [Dátum: 20. 03. 2023]. Dostupné na: https://www.panelteam.sk/

RAINER, R. K., PRINCE, B. 2022. *Introduction to information systems supporting and transforming business.* Anglicko : John Wiley & Sons, Inc, Hoboken, NJ, 2022. 978-1-119-76146-4. [Online]. [Dátum: 12. 02. 2023]. Introduction to Information Systems - R. Kelly Rainer, Brad Prince - Knihy Google

SHERRER, K. 2023. *How to Choose the Best HR Software.* [Online]. [Dátum: 22. 04. 2023]. Dostupné na: https://technologyadvice.com/blog/human-resources/how-to-choose-hr-software/

STAIR, R., REYNOLDS, G., 2017. *Principles of Information Systems*. 13. Boston: Cengage Learning. [Online]. [Dátum: 08. 02. 2023]. ISBN 9781-3059-7177-6. Dostupné na:https://books.google.sk/books/about/Principles_of_Information_Systems.html?id=j0VjwAEACAAJ&redir_esc=y

TAM, F. 2021. *6 Steps to Help Implement a Cost-Effective Information Security Program***.** [Online]. [Dátum: 15. 04. 2023]. Dostupné na: https://www.mossadams.com/articles/2021/08/cost-effective-information-security-program#information-security-program

TECHNOLOGY ADVICE, 2023. *Software categories*. [Dátum: 20. 04. 2023]. Dostupné na: https://technologyadvice.com/browse-categories/

TRELLIX, 2022. *What Is Endpoint Detection and Response*. [Online]. [Dátum: 15. 03. 2023]. Dostupné na: What Is Endpoint Detection and Response? | EDR Security | Trellix

WHITMAN, M., MATTORD, H. 2018. *Principles of Information Security*. 6th. Edition. [Online]. [Dátum: 01. 03. 2023]. ISBN: 978-1-337-10206-3. Dostupné na: Principles of Information Security - Michael E. Whitman, Herbert J. Mattord - Google Knihy

WRIGHT, G. 2022. *Endpoint detection and response (EDR).* [Online]. [Dátum: 15. 03. 2023]. Dostupné na: https://www.techtarget.com/searchsecurity/definition/endpoint-detection-and-response-EDR