Dopady kybernetických hrozieb na vybranú organizáciu

Bc. Ján Štofan

Diplomová práce
2020

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav elektroniky a měření

Akademický rok: 2019/2020

ZADÁNÍ DIPLOMOVÉ PRÁCE
(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Bc. Ján Štofan**
Osobní číslo:	**A18572**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**Kombinovaná**
Téma práce:	**Dopady kybernetických hrozeb na vybranou organizaci**
Téma práce anglicky:	**The Impacts of Cyber Threats on a Selected Organisation**

Zásady pro vypracování

1. Analyzujte organizace, jejich účel, cílovou funkci, strukturu a aktiva. Vytvořte jejich vhodnou typologii, použitelnou k řešení dopadů kybernetických hrozeb.
2. Pojednejte o kybernetické bezpečnosti v podmínkách organizace. Zaměřte se na hrozby, scénář průběhu bezpečnostní situace a jejich dopady na aktiva a organizaci.
3. Analyzujte možné způsoby oceňování hmotných a nehmotných aktiv. Zaměřte se na oceňování výpadků, způsobených kybernetickými hrozbami.
4. Vytvořte model dvou hypotetických organizací, na nichž budete hodnotit dopady kybernetických hrozeb. Na základě analýzy rizik stanovte pořadí nebezpečnosti kybernetických hrozeb. Pro tři nejhorší hrozby zpracujte scénář vývoje bezpečnostní situace a dopadů na hypotetické organizace.
5. S pomocí vhodného postupu oceňte výši dopadů jednotlivých narušení bezpečnosti, způsobených třemi nejhoršími kybernetickými hrozbami. Ocenění proveďte po jednotlivých fázích vývoje.

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

Seznam doporučené literatury:

1. SVAČINA, Pavel. Oceňování nehmotných aktiv. Praha: Ekopress, 2010. ISBN 978-80-86929-62-0.
2. ČERMÁK, Miroslav. Řízení informačních rizik v praxi. Brno: Tribun EU, 2009. ISBN 978-80-7399-731-1.
3. LUKÁŠ, Luděk. Teorie bezpečnosti I. Zlín: Radim Bačuvčík ? VeRBuM, 2017. ISBN 978-80-87500-89-7.
4. LUKÁŠ, Luděk. Bezpečnostní technologie, systémy a management V. Zlín: Radim Bačuvčík ? VeRBuM, 2015. ISBN 978-80-87500-67-5.
5. ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. Vybrané aspekty kybernetické bezpečnosti. Pardubice: Univerzita Pardubice, 2015. Monografia. ISBN 978-80-7395-953-1.
6. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
7. ČEJKOVÁ, Viktória a Dana MARTINOVIČOVÁ. Poistenie rizík malých a stredných podnikov. Bratislava: Wolters Kluwer (Iura Edition), 2013. ISBN 978-80-80786-72-4.
8. PAVLÍK, Lukáš. Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti. Dizertačná práca. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019. Školiteľ dizertačnej práce doc. Ing. Luděk Lukáš, CSc.

Vedoucí diplomové práce: **doc. Ing. Luděk Lukáš, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **9. prosince 2019**
Termín odevzdání diplomové práce: **29. května 2020**

doc. Mgr. Milan Adámek, Ph.D.
děkan

Ing. Milan Navrátil, Ph.D.
ředitel ústavu

Ve Zlíně dne 9. prosince 2019

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

Ján Štofan, v. r.
podpis diplomanta

ABSTRAKT

Diplomová práca sa venuje kybernetickej bezpečnosti z pohľadu organizácií. Analyzuje a identifikuje problematické oblasti, potenciálne kybernetické hrozby, možné dopady kybernetických hrozieb na aktíva organizácií s vplyvom na ich činnosť. Pomocou vhodného postupu oceňuje výšku dopadov vybraných kybernetických hrozieb na hypotetické organizácie.

Kľúčové slova: organizácia, kybernetická bezpečnosť, aktíva, hrozba, riziko, dopad, ocenenie,

ABSTRACT

The Master's thesis deals with cyber security from the perspective of organizations. Analyzes and identifies problem areas, potential cyber threats, possible impacts of cyber threats on the assets of organization with an impact on their activities. Using an appropriate procedure, it evaluates the amount of impact of selected cyber threats on hypothetical organizations.

Keywords: organization, cyber security, assets, threat, risk, impact, valuation,

POĎAKOVANIE

Na tomto mieste by som sa rád poďakoval vedúcemu mojej diplomovej práce, *doc. Ing. Luďkovi LUKÁŠOVI, CSc.* za neoceniteľné odborné rady, vecné pripomienky a vedenie pri vypracovaní mojej diplomovej práce.

Prehlasujem, že odovzdaná verzia diplomovej práce a verzia elektronická nahraná do IS/STAG sú totožné.

OBSAH

ÚVOD

V počiatkoch internetu nikto nemohol vedieť, aká raz táto sieť bude veľká. V súčasnej dobe je každodennou súčasťou našich životov. Využívame ho na platenie účtov, nakupujeme cez neho, hľadáme rôzne informácie, hráme hry a sme v kontakte s blízkymi. V počítačoch však o nás zostáva uložených veľké množstvo osobných údajov, ktoré tam uchovávame vedome, ale aj také, o ktorých ani len netušíme, že ich náš počítač ukladá pre ďalšie využitie v budúcnosti. Ak sa k takým údajom dostane niekto nepovolaný, hrozí nám nebezpečenstvo v podobe napríklad krádeže identity a následného zneužitia našich osobných údajov pre nelegálnu činnosť, napadnutie počítača škodlivým softvérom, alebo zneužitia informácií ako konkurenčnú výhodu.

Oblasť kybernetickej bezpečnosti vo svete prešla v posledných rokoch dynamickým rozvojom, ktorý ovplyvnil podobu existujúcich regulačných mechanizmov. Pojem kybernetickej bezpečnosti, alebo kyberbezpečnosti sa skladá z prefixu kyber, ktorý vyjadruje vzťah pojmu k informačným a komunikačným technológiám, resp. ku kybernetickému priestoru a pojmu bezpečnosť. Za bezpečnosť sa dá v ideálnom prípade považovať absencia hrozieb. Avšak takúto absolútnu bezpečnosť v praxi nie je možné dosiahnuť. Preto pri zaisťovaní bezpečnosti ide predovšetkým o minimalizáciu rizík vyplývajúcich z týchto hrozieb pre objekt bezpečnosti a jeho záujmy. Tieto riziká by súčasne mali byť minimalizované prostredníctvom takých právnych, organizačných, technických a vzdelávacích opatrení, ktoré v čo najširšej miere umožňujú výkon základných práv a slobôd. Kybernetická kriminalita predstavuje veľké riziko pre našu spoločnosť a je veľmi odolná voči tradičným metódam prevencie. Na rozdiel od tradičnej kriminality, ktorá síce ovplyvňuje celú spoločnosť, má však omnoho menej priamych obetí, kybernetická kriminalita zasahuje do života takmer všetkých subjektov.

Cieľom diplomovej práce je na základe spracovania teoretických východísk skúmanej problematiky kybernetickej bezpečnosti spracovať analýzu v tejto oblasti, identifikovať problematické oblasti, potenciálne hrozby, možné dopady kybernetických hrozieb a pomocou vhodného postupu oceniť výšku dopadu kybernetických hrozieb na hypotetické organizácie.

V teoretickej časti diplomovej práce sa zameriame na organizácie, kde si popíšeme ich zameranie, štruktúru, typológiu a aktíva. V ďalšej časti si ozrejmíme základne pojmy a oblasti informačnej bezpečnosti so zameraním na kybernetickú bezpečnosť z pohľadu

organizácií a teoretickú časť ukončíme kapitolou o oceňovaní nehmotných aktív podnikov a organizácií. V nej si popíšeme základne pojmy oceňovania nehmotných aktív, základné prístupy oceňovania a nakoniec aj metódy oceňovania nehmotného majetku a nehmotných aktív podnikov a organizácií.

V praktickej časti diplomovej práce si vymodelujeme dve hypotetické organizácie, v ktorých zanalyzujeme stav kybernetickej bezpečnosti a prípadných kybernetických hrozieb, ktoré ohrozujú kybernetickú bezpečnosť v týchto organizáciách. Zameriame sa na hrozby a priebeh bezpečnostnej situácie a ich dopady na hypotetické organizácie. Vyhodnotíme kybernetické hrozby ohrozujúce hypotetické organizácie a pre vybrané tri najnebezpečnejšie hrozby z pohľadu kybernetickej bezpečnosti zanalyzujeme a popíšeme priebeh vývoja bezpečnostnej situácie v organizácii a podľa vhodného, už známeho postupu ocením výšku dopadov jednotlivých kybernetických hrozieb na tieto organizácie.

I. TEORETICKÁ ČASŤ

1 TEORETICKÉ VÝCHODISKA SKÚMANEJ PROBLEMATIKY

K tomu, aby sme naplnili hlavný cieľ práce, si na základe pomocných cieľov, teda najmä teoretického vymedzenia pojmov, definujeme, charakterizujeme a rozdelíme organizácie, ktoré v spoločnosti pôsobia. Môže ísť o výrobnú aj nevýrobnú sféru, o súkromné a verejné organizácie a iné. Charakterizujeme si rôznorodosť ich organizačných štruktúr, cieľovú funkciu a aktíva organizácií.

1.1 Organizácie a ich ciele

Organizáciou, podnikom, firmou, alebo spoločnosťou, sa vo všeobecnosti označuje zoskupenie ľudí a prostriedkov na formálnych, alebo neformálnych základoch, ktorá sa vytvára za určitým účelom, resp. za plnením určitých spoločenských cieľov. Rôzne organizácie majú rôzne ciele. Najhlavnejším cieľom organizácií, alebo podnikov v podnikateľskej (súkromnej) sfére je svojou činnosťou na voľnom trhu generovať zisk výrobou tovaru, predajom tovaru, alebo služieb. Tento zisk potom ďalej slúži na vlastný rozvoj organizácie, alebo priamo vlastníkom organizácie.

Organizácie v neziskovom sektore zase svojou činnosťou poskytujú všeobecne prospešné služby. Hlavný rozdiel medzi organizáciou v neziskovom sektore a podnikateľskom sektore je ten, že nezisková organizácia nesmie svoj finančný príjem použiť na nič iné ako na zabezpečenie všeobecne prospešných služieb, ktoré sama poskytuje. Cieľom organizácií v neziskovom sektore je poskytovať všeobecne prospešné služby hlavne v sociálnej oblasti, oblasti ochrany ľudských práv, rozvoja vzdelávania a vedy, oblasti ochrany životného prostredia a mnoho ďalších. Mnohé ciele organizácií v neziskovom sektore sa prekrývajú aj s cieľmi organizácií vo verejnom sektore.

Verejný sektor tvoria organizácie, ktoré sú priamo financované zo štátneho rozpočtu formou príspevkov, alebo ich rozpočet je priamo určený v štátnom rozpočte. Zriaďovateľom organizácií vo verejnom sektore je štát, alebo samospráva. Cieľom organizácií vo verejnom sektore je poskytovať obyvateľstvu služby, ktoré zo samotnej podstaty fungovania štátu vyplývajú, a ktoré sa nedajú delegovať na súkromné organizácie. Ako príklad uvediem oblasť bezpečnosti (armáda, polícia, súdy), oblasť školstva, oblasť verejného zdravotníctva, oblasť medzinárodnej spolupráce a mnoho ďalších.

1.2 Organizačná štruktúra organizácií

Organizačná štruktúra je organizovaný systém, v ktorom je práca rozdelená, zoskupená a koordinovaná. Keď manažéri formujú a menia svoju organizačnú štruktúru, vykonávajú projektovanie organizácie, čo je proces rozhodovania o šiestich kľúčových prvkoch:

- špecializácia práce,
- rozdelenie organizácie do oddelení (útvarov),
- reťazec príkazov,
- rozmer kontroly,
- centralizácia a decentralizácia,
- formalizácia.[1]

Organizačná štruktúra predstavuje v inštitúcii kostru, ktorá umožňuje plniť jej plánované ciele. Manažér, resp. organizátor volí základnú formu, podľa ktorej je štruktúra vytváraná.[2] Vyjadruje usporiadanie stupňov, organizáciu rozdeľuje po stránke vertikálnej aj horizontálnej, určuje obsah činnosti útvaru a jednotlivé väzby medzi útvarmi organizácie. Organizačná štruktúra sa znázorňuje sa organizačnou schémou.

Medzi základné charakteristiky klasifikácie organizačných štruktúr patria:

- uplatňovanie rozhodovacích právomocí medzi organizačnými jednotkami štruktúry,
- udržovanie činností, ktoré tvoria hlavnú obsahovú náplň organizačných jednotiek.[1]

Organizačné štruktúry organizácií delíme podľa niekoľkých hľadísk. Za základné delenie považujeme delenie na hierarchické, adhokratické a ostatné. Vychádzajúc zo základného delenia organizačných štruktúr, ďalej delíme organizácie na:

Hierarchické

- podľa počtu stupňov riadenia a útvarov
    - vysoké (strmé),
    - široké (ploché).
- podľa rozhodovacích právomocí
    - líniové,

    - štábne,
    - líniovo-štábne.
- podľa činností
    - projektové,
    - výrobkové,
    - divizionálne,
    - hybridné,
    - funkčné.
- podľa združovania činností
    - zákazníkov,
    - procesov,
    - riadenia,
    - oblastí.

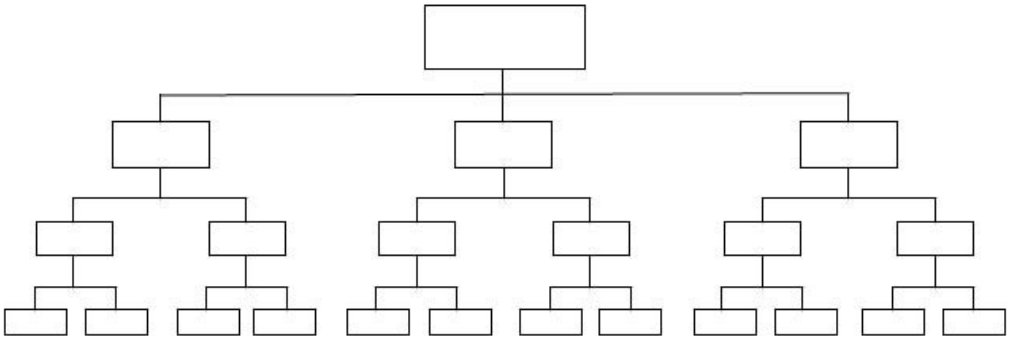
Adhokratické – účelovo neorganizované

- paralelné,
- maticové,
- sieťové.

Ostatné

- voľné a strategické aliancie,
- strategické obchodné jednotky,
- fraktály.

Vysoké organizačné štruktúry znamenajú, že medzi radovými pracovníkmi a vrcholovým vedením je veľa riadiacich úrovní. Každý vedúci pracovník má obmedzený počet podriadených. Typickým príkladom môže byť armáda, alebo veľké štátne a výrobné organizácie.



Obrázok 1 Schéma vysokej organizačnej štruktúry [1]

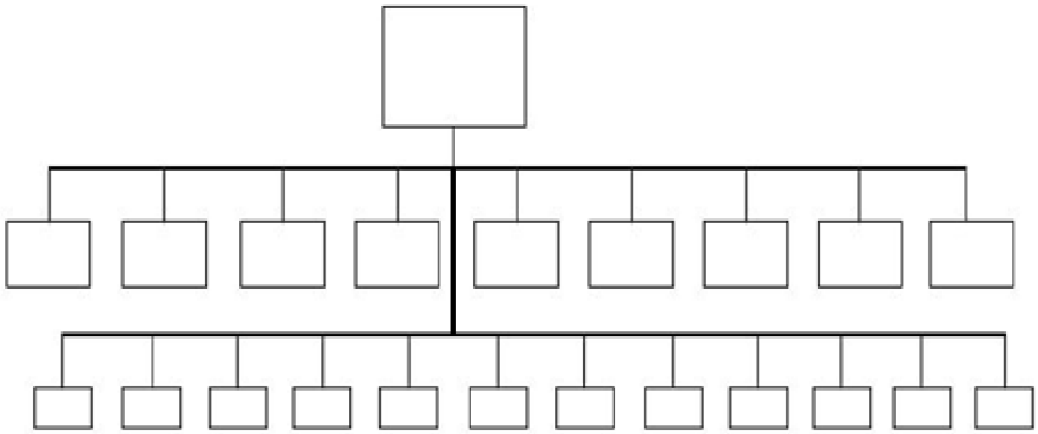
Výhody:

- úzka kontrola a vedenie,
- rýchla komunikácia medzi podriadenými a vedúcimi pracovníkmi.

Nevýhody:

- tendencia vedúcich pracovníkov angažovať sa v práci podriadených,
- vysoký počet organizačných úrovní, na základe ktorého potom vzniká komunikačný šum,
- vyššie náklady spojené s vyšším počtom organizačných úrovní.

Široké (ploché) organizačné štruktúry sú typické malým počtom riadiacich úrovní a veľkým počtom podriadených. Príkladom môže byť napríklad univerzita, kde rektor riadi dekanov jednotlivých fakúlt, tí potom riadia vedúcich jednotlivých odborných katedier, ktorým sú priamo podriadení jednotliví odborní pedagógovia. [1]



Obrázok 2 Schéma širokej organizačnej štruktúry [1]

Výhody:

- vedúci sú nútení delegovať právomoci,
- musí byť k dispozícii jasná taktika a stratégia,
- podriadení musia byť starostlivo vybraní a manažéri musia byť kvalitní.

Nevýhody:

- preťažení vedúci majú tendenciu k odďaľovaniu rozhodnutí,
- riziko, že vedúci stratí prehľad,
- toto rozpätie vyžaduje mimoriadne kvalitných manažérov.

V líniovej organizačnej štruktúre sú jednotlivé útvary organizácie usporiadané podľa činnosti do líniovej štruktúry. Na vrchole je iba jeden vedúci, ktorý dáva príkazy priamo podriadeným na nižších stupňoch.

Výhody:

- jasná podriadenosť a nadriadenosť,
- jasné určenie povinnosti a vzťahov,
- spoločné riadenie,
- efektívnejší spôsob organizovania.

Nevýhody:

- možná centralizácia riadenia,
- väčšie nároky na riadiacich pracovníkov,
- možná nižšia kvalita rozhodovania.

V líniovo-štábnej organizačnej štruktúre sa k líniovému riadeniu pridávajú aj podporné útvary – štáby, ktoré ale nemajú rozhodovaciu právomoc. Slúžia na podporu pri kvalifikovanom rozhodovaní líniového vedúceho prípravou a analýzou podkladov. Združujú sa v nich špecialisti a odborníci z rôznych oblastí.

Výhody:

- ľahšie rozhodovanie,
- rozhodnutia na základe odborných analýz,
- vyššia kvalita riadenia.

Nevýhody:

- obchádzanie líniových vedúcich,
- viacej štábnych útvarov.

Organizačné úrovne vytvárame preto, že manažér je schopný efektívne riadiť len obmedzený počet osôb. Zároveň si musíme uvedomiť, že organizačné úrovne sú drahé. Čím vyšší počet organizačných úrovní, tým rastú aj náklady na riadenie v organizácii.

1.3 Aktíva organizácií

Aktívami organizácie nazývame všetko, t.j. akýkoľvek hmotný a nehmotný majetok v organizácii, ktorý organizácia považuje za životne dôležitý a významný, a u ktorého sa predpokladá, že z neho bude mať organizácia v budúcnosti ekonomický osoh v podobe ekonomického zisku. Medzi aktíva môžeme zaradiť aj človeka, ktorý svojou prácou a umom naplňuje spoločenské ciele organizácií. Preto je dôležité, aby organizácie svoje aktíva chránili a zaisťovali ich bezpečnosť.

Aktívami rozumieme:

- nehnuteľný majetok – budovy,
- hnuteľný majetok – stroje, výrobné linky, autá,
- goodwill – dobré meno organizácie, výrobku, služby,
- know-how – špecifické výrobne poznatky, vedomosti,
- informačné aktíva – informácie, dáta,
- hardvérové aktíva – technické prostriedky – hardvér (PC),
- softvérové aktíva – technické prostriedky – softvér,
- služby poskytované prostredníctvom informačných systémov.

Pre účely našej práce nás budú určite najviac zaujímať informačné aktíva. Informačné aktíva sú zariadenia, programy a informácie, na ktorých závisí chod firmy alebo organizácie. Predovšetkým ide o dáta v informačných systémoch, dokumentoch spoločnosti a ich zálohách. Súpis informačných aktív je základným kameňom efektívneho riadenia nákladov na ich ochranu.

Informačné aktíva sa identifikujú analýzou aktív, pri ktorej špecialisti na informačné technológie (IT) spoločne so zástupcami organizácií označia prostriedky a informácie dôležité pre hladký chod organizácie. Každé takéto aktívum je potom popísané a klasifikované. Následne je spracovaný návrh zabezpečenia aktíva a určená osoba zodpovedná za realizáciu navrhnutých opatrení. Prednostne sú zvyčajne zabezpečované aktíva s najvyššou stanovenú hodnotou. Len spoľahlivý súpis informačných aktív umožňuje ich efektívnu ochranu. Bez znalosti aktív, kľúčových hodnôt organizácie, nie je možné určiť efektívne náklady na ich ochranu.

Spôsoby, akými môže organizácia oceňovať svoje hmotné a nehmotné aktíva bližšie špecifikujeme v kapitole 3.

1.4 Typológia organizácií

Typológiu organizácií môžeme rozlišovať na základe viacerých hľadísk. Z hľadiska toho ako organizácie hospodária a ako sú financované ich rozdeľujeme na verejný (prvý) sektor, podnikateľský (druhý) sektor a neziskový (tretí) sektor. Podľa formy vlastníctva

rozdeľujeme organizácie na súkromné, municipálne a štátne. Z pohľadu členstva v nich sa organizácie delia na dobrovoľné, donucovacie a utilitárne – užitočné organizácie. Z pohľadu veľkosti organizácie delíme na malé, stredné a veľké. Hranice sektorov súkromného, verejného a neziskového sa vzájomne prekrývajú. To znamená, že v jednotlivých častiach verejného, podnikateľského a neziskového sektora pôsobia inštitúcie, ktoré až na výnimky uspokojujú potreby na neziskovom, aj na ziskovom princípe (realizujú čisté verejné statky).

1.4.1 Verejný sektor (prvý sektor)

Verejný sektor je časť národnej ekonomiky, v ktorej sa vo verejnom záujme realizujú verejné služby. Organizácie patriace do verejného sektora sú financované z verejných rozpočtov, sú riadené a spravované verejnou správou, rozhoduje sa o nich verejnou voľbou a podliehajú verejnej kontrole.[3] V organizáciách vo vlastníctve štátu je vlastníkom štát, alebo aspoň jeho časti, o majetku rozhoduje výkonná zložka, vláda prostredníctvom svojich organizačných zložiek. Existencia a definícia verejného sektoru je z ekonomického pohľadu spojená so vstupom štátu do ekonomických vzťahov, so štátnymi netrhovými aktivitami v rámci zmiešanej ekonomiky. Aj napriek tomu hovoríme o štáte 21. storočia, kedy došlo k prelivu, teda decentralizácii týchto aktivít a funkcií aj na územnú samosprávu. [4]

Subjekty vo verejnom sektore

Subjekty, ktoré pôsobia vo verejnom sektore môžeme rozlíšiť podľa viacerých hľadísk.

- *na základe právnej formy*

Rozpočtové organizácie

Rozpočtové organizácie sú právnické osoby v pôsobnosti štátu, vyšších územných celkov alebo obcí a sú zriadené zákonom, resp. rozhodnutím ich zriaďovateľa. Sú zriadené Zákonom o rozpočtových pravidlách verejnej správy. Úlohou rozpočtových organizácií je zabezpečovať rôzne funkcie štátu. podstatou rozpočtových organizácií je najmä to, že sú napojené na štátny rozpočet rozpočtom, to znamená, že všetky príjmy plynú do štátneho rozpočtu, ale aj všetky výdavky sú realizované zo štátneho rozpočtu.[5] Ako príklad môžeme uviesť Akadémiu Policajného zboru v SR.

Príspevkové organizácie

Príspevkové organizácie sú taktiež právnickými osobami štátu, vyššieho územného celku alebo obce, avšak sú na štátny rozpočet alebo na rozpočet zriaďovateľa napojené

príspevkom. Svoje príjmy využívajú na pokrytie svojich nákladov. Ich príjmy sú väčšinou ale nepostačujúce, preto sú odkázané na príspevky z rozpočtu. Typickým znakom príspevkových organizácií je fakt, že vlastnia majetok a hospodária samostatne.[5] Ako príklad môžeme uviesť Akadémiu Policajného zboru v SR.

Verejnoprávne organizácie

Aj verejnoprávne organizácie sú právnické osoby štátu a sú zriadené Zákonom o nakladaní s majetkom verejnoprávnych inštitúcií. Tieto sa od ostatných odlišujú tým, že sú finančne oddelené od štátneho rozpočtu. Sami disponujú v oblasti ekonomickej, obchodnej, finančnej aj výrobnej politiky. Zákon im umožňuje dosahovať príjmy, zostavujú si svoj vlastný rozpočet.[6] Patria sem napríklad Rozhlas a televízia alebo Sociálna poisťovňa.

Štátne podniky

Štátne podniky sú právnické osoby štátu zriadené Zákonom o štátnom podniku. Ich zakladateľom je ústredný orgán štátnej správy a ich predmet činnosti je záväzne daný v ich zakladateľskej listine. Svoje výdavky si hradia z príjmov z vlastnej činnosti, ale všetky ich majetkové práva sú vo vlastníctve štátu. Štátne podniky sú vo svojej výhradnej pôsobnosti avšak o všetkých zmenách rozhoduje vláda a za činnosť štátneho podniku zodpovedá riaditeľ.[7] Príkladom štátneho podniku sú napríklad Lesy Slovenskej republiky.

Akciové spoločnosti vo verejnom sektore

Ich zakladateľom je štátny orgán, t. j. ministerstvo a spolumajiteľom je štát a sú zriadené na podnikanie s cieľom uspokojiť záujmy štátu. vznikajú zakladateľskou listinou alebo zmluvou. Príkladom takejto spoločnosti je napríklad Slovenská pošta alebo Tipos, národná lotériová spoločnosť.

Neziskové organizácie

Posledným typom organizácií v rámci tohto členenia sú neziskové organizácie. Taktiež ide o právnické osoby štátu, ktoré poskytujú špecifické služby ale nevykonávajú podnikateľskú činnosť a sú zriadené Zákonom o neziskových organizáciách poskytujúcich všeobecne prospešné služby. Hospodária so svojim majetkom, prípadne s majetkom štátu alebo územnej samosprávy. Štátny rozpočet im môže poskytnúť dotáciu.[8] Hovoríme napríklad o nadáciách alebo občianskych združeniach.

- *na základe štruktúry potrieb*

Z hľadiska štruktúry potrieb spoločnosti, môžeme rozdeliť organizácie podľa ich druhu. Ide o:

  - spoločenské potreby (ochrana občanov, ochrana majetku, bezpečnosť),
  - rozvoj človeka (vzdelávanie, sociálne služby, zdravotníctvo),
  - poznávanie a informácie (veda a výskum),
  - technická infraštruktúra (vodné a odpadové hospodárstvo, energetika, kanalizácia a čistenie, doprava),
  - existenčné istoty (sociálna politika štátu, podpora zamestnanosti),
  - privátne statky (lesníctvo a rybolov, bývanie).

- *z hľadiska infraštruktúry*

Organizácie výrobnej infraštruktúry

Organizácie vyrábajúce produkty pre nákladnú a osobnú dopravu, produkty pre obchod, spracovateľský priemysel, drobné prevádzkové výroby a podobne.

Organizácie nevýrobnej infraštruktúry

Organizácie, ktoré patria do nevýrobnej infraštruktúry sa pohybujú v oblasti dopravy, informačných technológií, sociálnom odvetví, ekonomickej sféry.

1.4.2 Podnikateľský sektor (druhý sektor)

Pri súkromných organizáciách je vlastník plne kompetentný rozhodovať o svojom majetku, resp. o majetku organizácie. Tvoria ho podnikajúce fyzické a právnické osoby, ktoré podnikajú na trhu s tovarom, alebo službami a výsledkom ich podnikateľskej činnosti je tvorba zisku. Právnické osoby sú osoby založené v medziach práva podľa Obchodného zákonníka a majú pridelené identifikačné číslo organizácie. Vznikajú písomnou zmluvou, zakladacou listinou, alebo podľa osobitných zákonov.

Subjekty v podnikateľskom sektore

- *z hľadiska právnej úpravy podnikania fyzických osôb*

Fyzická osoba podnikajúca na základe živnostenského oprávnenia

Pri tomto type podnikania podniká fyzická osoba samostatne na základe živnostenského oprávnenia. Rozsah činnosti upravuje živnostenský zákon. Fyzická osoba podnikajúca na základe živnostenského oprávnenia vykonáva činnosť vo svojom mene a na vlastnú zodpovednosť.

Združenie fyzických osôb

Táto forma podnikania umožňuje minimálne dvom fyzickým osobám spojiť sa v združení a spoločne vykonávať činnosť k naplneniu cieľa združenia. Združenie ako také nemá právny základ a preto nemôže vystupovať ako samostatné pred úradmi. Výhodou podnikateľskej činnosti fyzických osôb v združení je, že pre účastníkov neplatí zákaz konkurencie a združenie sa nemusí registrovať v nijakej evidencii.

- *z hľadiska právnej úpravy podnikania právnických osôb*

Spoločnosť s ručením obmedzeným

Spoločnosť s ručením obmedzeným je kapitálovou spoločnosťou, ktorú môže založiť jedna osoba zakladacou listinou, alebo niekoľko osôb spoločenskou zmluvou. Základné imanie spoločnosti s ručením obmedzeným je tvorené vkladom zakladateľa, alebo vkladmi jednotlivých spoločníkov. Spoločníci ručia za záväzky spoločnosti obmedzene, do výšky vkladu. V mene spoločnosti vystupuje konateľ.

Akciová spoločnosť

Akciová spoločnosť je kapitálovou spoločnosťou, kde akcionár, alebo akcionári neručia za záväzky spoločnosti a základné imanie akciovej spoločnosti je získavané predajom akcií medzi väčší počet akcionárov. Zisk akciovej spoločnosti sa delí na základe podielu vlastnených akcií. Zakladá sa pri jednej osobe zakladateľskou listinou, alebo pri viacerých osobách zakladateľskou zmluvou. Akciovú spoločnosť riadi predstavenstvo, kontroluje ho dozorná rada a o dôležitých rozhodnutiach hlasuje valné zhromaždenie akcionárov ako najvyšší orgán akciovej spoločnosti.

Verejná obchodná spoločnosť

Verejná obchodná spoločnosť je osobná obchodná spoločnosť, kde minimálne dve osoby, môže byť fyzická, alebo právnická, vykonávajú podnikateľskú činnosť spoločne pod jedným obchodným menom. Za záväzky spoločnosti ručia spoločníci celým svojím majetkom. Verejná obchodná spoločnosť má právny základ a musí vykonávať iba podnikateľskú činnosť. Zakladá sa spoločenskou zmluvou a riadiť ju môžu všetci spoločníci, alebo podľa dohody v spoločenskej zmluve. Platí zákaz konkurencie.

Komanditná spoločnosť

Komanditná spoločnosť je spoločnosť, ktorú zakladajú minimálne dvaja spoločníci - komplementári a komandisti. Komplementári ručia za záväzky spoločnosti celým svojím majetkom a komandisti ručia za záväzky spoločnosti, iba do výšky svojho kapitálového vkladu. Komanditná spoločnosť sa zakladá spoločenskou zmluvou, kde sa určuje okrem iného aj delenie zisku. Riadenie spoločnosti vykonávajú komplementári a komandisti zasahujú do riadenia spoločnosti iba veľmi obmedzene.

1.4.3 Neziskový sektor (tretí sektor)

Všeobecne môžeme povedať, že subjekty v neziskovom sektore nie sú motivované ziskom, ale ich cieľom je dosiahnutie úžitkov vyplývajúcich z realizácie určitého poslania. Podrobnejšie o neziskových organizáciách som sa venoval vyššie v bode 1.4.1, odstavec Neziskové organizácie. Z pohľadu neziskových organizácií sa verejný a neziskový sektor vo veľkej časti prelínajú.

V úvodnej kapitole sme sa venovali organizáciám, ktoré pôsobia v Slovenskej republike. Ozrejmili sme si ciele, ktoré organizácie napĺňajú, resp. na aký účel tie, ktoré organizácie vznikajú. Venovali sme sa organizačným štruktúram organizácií a aktívam, ktorými môžu jednotlivé organizácie disponovať. V závere sme rozdelili organizácie podľa ich typov.

2 KYBERNETICKÁ BEZPEČNOSŤ

Pre objasnenie kybernetickej bezpečnosti je nutné najprv vysvetliť aj pojem informačná bezpečnosť, ktorej súčasťou kybernetická bezpečnosť je. Všeobecne informačná bezpečnosť predstavuje ochranu akýchkoľvek informácií pred širokým spektrom možných hrozieb vo všetkých ich formách a po celý ich životný cyklus. Táto ochrana teda pokrýva časť vzniku, spracovania, prenosu, uchovania a samozrejme aj likvidáciu či znehodnotenie informácie. Z pohľadu informačnej bezpečnosti sú informácie chránené bez ohľadu na ich umiestnenie a formu. Môžu teda byť umiestnené v informačnom systéme, vytlačené na papieri alebo môžu byť odovzdávané ústne. Kybernetická bezpečnosť sa oproti informačnej bezpečnosti zaoberá bezpečnosťou informácií vytváraných, prenášaných, uchovávaných a likvidovaných čisto len v digitálnej podobe. S informáciami môže byť nakladané rôznym spôsobom. Pre ich ochranu je dôležité si stanoviť niekoľko základných otázok:

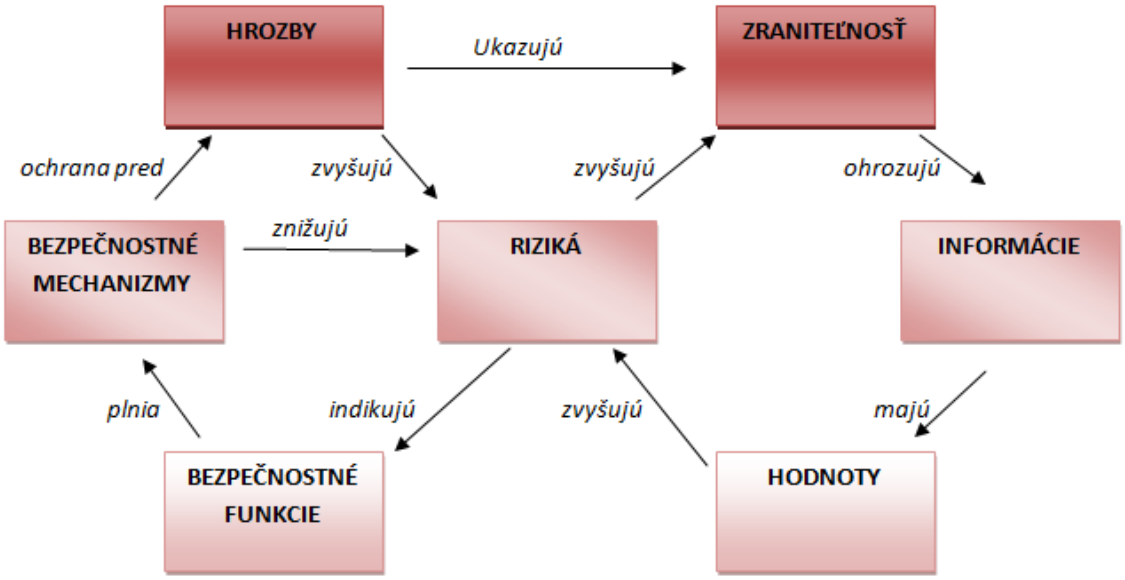
- čo chrániť,
- prečo informáciu chrániť,
- kedy chrániť,
- proti akým hrozbám informáciu chrániť,
- akým spôsobom informáciu chrániť.[9]

V tejto kapitole je dôležité rozlíšiť pojmy z oblasti kybernetickej bezpečnosti, kybernetického priestoru a hrozieb, informačných a komunikačných technológií a dokumenty, ktoré túto oblasť upravujú. Pozrieme sa na túto problematiku z legislatívneho hľadiska, ale aj z pohľadu rôznych odborníkov. Čerpať budeme najmä z platnej legislatívy, prijatých dokumentov, odborných článkov, publikácií a periodík.

2.1 Informačná bezpečnosť v podmienkach organizácie

Základný koncept zabezpečenia bezpečnosti predstavujú vzťahy medzi aktívami organizácie, hrozbami, ktoré na nich môžu potenciálne pôsobiť, možnú zraniteľnosť aktív reálnymi hrozbami, dopady reálnych hrozieb na tento majetok a možnosťami ochrany aktív organizácie formou protiopatrení.[10]

Obrázok číslo 3 zachytáva, akým spôsobom sú ovplyvnené všetky prvky informačnej bezpečnosti, teda čím sú bezpečnostné riziká posilňované či naopak oslabované.[9]



Obrázok 3 Prvky informačnej bezpečnosti [9]

Každá, či už veľká, alebo malá, súkromná, alebo verejná organizácia v dnešnej dobe pracuje s informáciami, ktoré pre jednotlivé organizácie tvoria veľmi dôležité a hodnotné aktívum. Informácie v digitálnej podobe jednotlivý pracovníci organizácií spracovávajú na informačných prostriedkoch, ktoré tvoria informačný systém organizácie. Okrem fyzických zariadení (hardvér), tvorí informačný systém organizácie aj programové vybavenie (softvér), ktorý slúži na vytváranie, spracovanie a ukladanie informácií v digitalizovanej podobe. V dnešnej dobe patrí využívanie informácií a z nich pochádzajúcich poznatkov ku kľúčovým vlastnostiam organizácie pri úspešnom pôsobení na voľnom trhu. S efektívnym využívaním informačných systémov a zvyšovaním konkurencieschopnosti organizácií sa zvyšujú aj požiadavky na ochranu informačných systémov a dát v nich uložených. Každé napadnutie, alebo poškodenie informačného systému spôsobuje škody s negatívnym dopadom na organizáciu. Cielené útoky na informačné technológie (IT) sú celosvetovým fenoménom a ich vplyv spôsobuje rozsiahle ekonomické škody vo verejnom aj súkromnom sektore. Súčasne sú schopné vyvolať negatívne politické dôsledky, a to ako v národnom meradle, tak aj v globálnom rozsahu.[11] Rôzne organizácie používajú

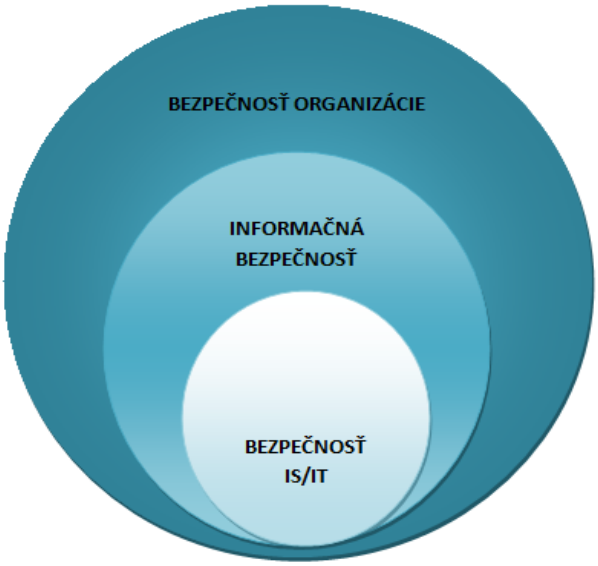
informačné systémy s odlišnými funkciami a na rôzne účely. Preto aj útoky a spôsoby napadnutia informačných systémov sa líšia.

Vplyvy hrozieb na aktíva môžu mať rôznorodý charakter. Od okamžitého efektu vo forme bezprostrednej finančnej straty (napríklad zničenie počítača) až po efekty, ktoré nie sú na prvý pohľad zrejmé a objavujú sa postupne (napríklad strata dobrej povesti organizácie alebo pravidelný únik informácií z nej). Vplyvy všetkých hrozieb sa následne prevádzajú na finančné hodnoty.[12]

Úrovne bezpečnosti informácií

Vývoj bezpečnosti informácií a jej systému riadenia nemá príliš dlhú tradíciu. Jeho intenzívna potreba začala vznikať v čase, keď sa lokálne počítače začali prepájať do počítačových sietí a významnejšie sa rozšírili komunikačné kanály medzi počítačmi rôznych právnych subjektov a organizácií.

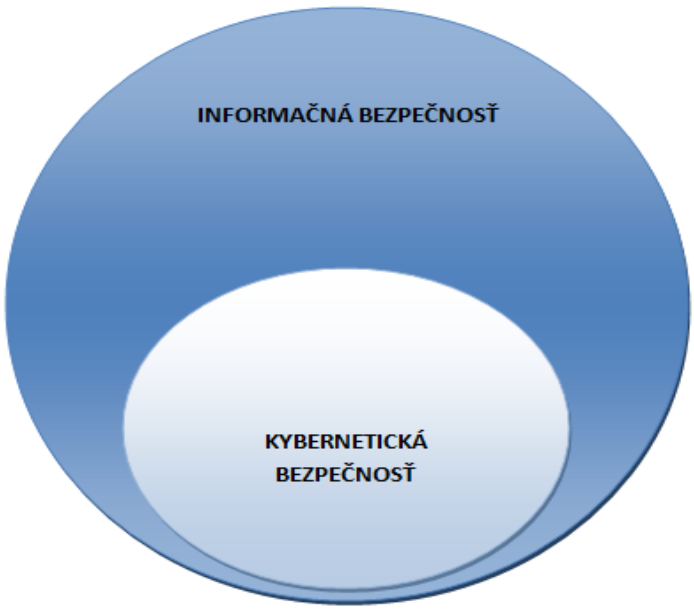
V súvislosti s termínom bezpečnosti informácií je nutné spomenúť ešte ďalšie pojmy, a to bezpečnosť organizácie a bezpečnosť informačných systémov (IS), informačných a komunikačných technológií (ICT), ktorých vzťah vidíme na obrázku číslo 4.[13]



Obrázok 4 Vzťah bezpečností v organizácii [13]

Kategórie bezpečností v organizácii

- **bezpečnosť organizácie** je balík komplexných opatrení a jej súčasťou je zabezpečenie bezpečnosti objektov a majetku, ako je stráženie prístupov do objektov, strážna služba, zabezpečenie dodávok energií, ekonomických prostriedkov potrebných na zabezpečenie chodu organizácie a pod. Niektoré jej činnosti napomáhajú zároveň aj zabezpečeniu bezpečnosti informačného systému ako napríklad kontrola oprávnenia fyzického prístupu do budov. Jej súčasťou je aj informačná bezpečnosť,
- **informačná bezpečnosť** je multidisciplinárny odbor, ktorý rieši problematiku ochrany dát a informácií pred narušením ich integrity, dostupnosti a dôvernosti počas celého životného cyklu, tzn. ich vzniku, spracovania, ukladania, prenosu a likvidácie. Informačná bezpečnosť sa všeobecne zaoberá informáciami a ochranou informácií nech už sú vo fyzickej, alebo elektronickej forme,[14]
- **bezpečnosť informačných systémov, informačných a komunikačných technológií** má za úlohu chrániť len tie aktíva, ktoré sú súčasťou informačného systému organizácie. Preto je táto bezpečnosť relatívne najužšou oblasťou riadenia bezpečnosti.[12]
-



Obrázok 5 Vzťah informačnej a kybernetickej bezpečnosti [15]

Zaistenie bezpečnosti v organizáciách je nutné riešiť vo viacerých komplexných rovinách. Z tohto pohľadu je potrebné prijať a aplikovať opatrenia nie len z oblasti informačnej bezpečnosti, ale aj z bezpečnosti fyzickej, administratívnej, personálnej, ekonomickej a v neposlednom rade aj bezpečnosti energetickej. Realizáciou bezpečnostných opatrení v kľúčových oblastiach znížime riziko pôsobenia hrozieb na aktíva organizácií na prijateľné minimum.

Do realizovania bezpečnostných opatrení zahrňujeme oblasti

- bezpečnostnú politiku - definuje základné pravidlá bezpečnosti informácií a vyjadruje podporu vedením organizácie,
- riadenie aktív - predstavuje udržiavanie prehľadu o existujúcich aktívach organizácie a stanovenie zodpovednosti za udržiavanie primeranej miery ochrany jednotlivých aktív,
- riadenie prístupu - obsahuje pravidlá prideľovania prístupu ku všetkým prostriedkom informačných a komunikačných systémov vrátane sledovania spôsobu využívania dostupných prostriedkov,
- organizovanie bezpečnosti informácií - upresňuje štruktúry pre riadenie informácií vo vnútri organizácie a riadenie bezpečnosti vo vzťahu k externým subjektom (zákazníkom, dodávateľom),
- bezpečnosť z hľadiska ľudských zdrojov - vymedzuje povinnosti na ochranu informácií pre všetkých pracovníkov a zabezpečenie potrebného bezpečnostného povedomia,
- fyzická bezpečnosť a bezpečnostné prostredie - definuje pravidlá pre prístup osôb do kľúčových priestorov organizácie a ochranu zariadenia, vrátane zariadenia informačnej technológie,
- riadenie komunikácie a riadenie prevádzky - zabezpečuje spoľahlivý a bezpečný chod produkčných informačných a komunikačných systémov organizácie,
- akvizícia, vývoj a údržba informačných systémov - presadzuje princípy bezpečnosti informácií do projektov rozvoja informačných technológií a ďalších podporných aktivít,

- riadenie kontinuity činností organizácie - zahŕňa postupy prevencie a minimalizácie škôd plynúcich z havárií, živelných pohrôm či iných mimoriadnych udalostí,
- zvládanie bezpečnostných incidentov - obsahuje pravidlá a postupy určené pre riešenie bezpečnostných incidentov vrátane zhromažďovania potrebných dôkazov,
- súlad s požiadavkami organizácie - dokladuje naplnenie požiadaviek vyplývajúcich z právnych, zmluvných a iných záväzkov.[13]

2.2 Vymedzenie pojmov v oblasti kybernetickej bezpečnosti

Kybernetická bezpečnosť pokrýva veľmi veľkú oblasť spoločenského života. Je preto dôležité zoznámiť sa so základnými pojmami, ktoré s oblasťou kybernetickej bezpečnosti súvisia a popisujú ju.

2.2.1 Kybernetická bezpečnosť

Na výklad a definíciu kybernetickej bezpečnosti existuje niekoľko pohľadov. Kybernetická bezpečnosť je termín, ktorým sa všeobecne označujú technológie slúžiace k ochrane počítačových systémov a užívateľských dát pred nedovolenou manipuláciou.[14] Výkladový slovník kybernetickej bezpečnosti zasa interpretuje kybernetickú bezpečnosť ako súhrn právnych, organizačných, technických a vzdelávacích prostriedkov smerujúcich k zaisteniu bezpečnosti kybernetického priestoru.[16] Pre úplnosť musíme do kybernetickej bezpečnosti zahrnúť aj ľudí, ktorí na informačných prostriedkoch pracujú a obsluhujú. Kybernetická bezpečnosť patrí do informačnej bezpečnosti, ale zameriava sa na ochranu informácií v elektronickej, digitálnej podobe. Účelom kybernetickej bezpečnosti je zabezpečiť ochranu pred pôsobením kybernetických útokov. Jej dôležitosť v dnešnej „digitálnej“ dobe snáď ani netreba pripomínať.

2.2.2 Kybernetický priestor

Kybernetický priestor, alebo skrátene kyberpriestor, nemá úplne jasnú definíciu, ale v dnešnej podobe sa s ním stretávame ako s virtuálnym počítačovým svetom v internete tvorenom dátami a informáciami.[14] Definícií tohto termínu je však dostupných viac, v odbornej literatúre aj v strategických a legislatívnych dokumentoch. Zákon o kybernetickej bezpečnosti č. 69/2018 Z. z. prijatý v Slovenskej republike definuje kybernetický priestor ako globálny otvorený systém sietí a informačných systémov, ktorý tvoria aktivované prvky

kybernetického priestoru, osoby vykonávajúce aktivity v tomto systéme a vzťahy a interakcie medzi nimi.[17]

2.2.3 Kybernetická kriminalita

Kybernetická kriminalita veľmi úzko súvisí s problematikou kybernetickej bezpečnosti. Obe tieto oblasti sú len ťažko oddeliteľné v prepojenom prostredí kybernetického priestoru. Kybernetická kriminalita predstavuje trestnú činnosť, ktorá zahrňuje počítač, alebo sieťové zariadenie[14] Tieto dve oblasti sa však v žiadnom prípade úplne nekryjú. Kybernetická bezpečnosť je totiž problematika administratívna, zatiaľ čo počítačová kriminalita trestnoprávna. Pojmov označujúcich to, čo chápeme ako počítačovú kriminalitu, je skutočne mnoho, a ako príklad uvádzam iba niektoré: počítačová kriminalita, internetová kriminalita či e-kriminalita.

2.2.4 Kybernetická hrozba

Pojmom kybernetická hrozba môžeme označiť negatívnu udalosť kybernetického charakteru, ktorá môže ohroziť určitý druh aktíva. Kybernetickým charakterom je myslená podstata hrozby, ktorá vychádza z kybernetického priestoru a je realizovaná prostredníctvom nástrojov informačných a komunikačných technológií.[18] Vo všeobecnosti je hrozba chápaná ako niečo nežiadúce, negatívne. Výsledkom pôsobenia hrozby na akýkoľvek objekt je ujma, alebo všeobecnejšie negatívny dopad. Takýto dopad, alebo ujma má nemateriálnu – informačnú, logickú, alebo materiálnu – fyzikálnu, chemickú povahu.[11] V dnešnej dobe sú hrozby v kybernetickom priestore vážnym ohrozením bezpečnosti organizácií, alebo celých štátov. Spolu s vývojom informačných technológií dochádza aj k vývoju hrozieb, ktoré sa stávajú sofistikovanejšími a predstavujú veľké riziko pre aktíva organizácií a štátov.

2.2.5 Riziko

Riziko je obvykle definované ako parameter, zahrňujúci pravdepodobnosť expozície hrozby a veľkosť jej negatívneho dopadu na referenčný objekt. Veľkosť rizika sa vyjadruje kvantitatívne a kvalitatívne.[11] Analýzou rizík vieme dopady na aktíva organizácií rozdeliť podľa ich nebezpečnosti a závažnosti.

2.2.6 Odolnosť

Každá organizácia má určitú schopnosť odolávať pôsobeniu hrozieb. Túto vlastnosť definujeme ako odolnosť. Odolnosť je chápaná ako schopnosť referenčného objektu zaistiť svoju funkciu, alebo ochranu záujmov v podmienkach pôsobenia vonkajších a vnútorných činiteľov.[11] V oblasti kybernetickej bezpečnosti hovoríme predovšetkým o sieťových zariadeniach a ich vlastnostiach, ako sú routre, firewaly, demilitarizovaná zóna (DMZ) a ich programovom vybavení, ktoré práve takúto odolnosť voči kybernetickým hrozbám zaisťujú.

2.2.7 Zraniteľnosť

Aj pri najlepšom plánovaní bezpečnosti v organizáciách nikdy nevieme zabezpečiť ich 100% bezpečnosť. To aké slabiny organizácia má a do akej miery je na vznik ujmy citlivá nazývame zraniteľnosť. Zraniteľnosť vyjadruje citlivosť referenčného objektu na vznik ujmy. Jedná sa o slabé miesta, ktoré môžu byť v referenčnom objekte ľahko prekonané a môže dôjsť k narušeniu bezpečnosti.[11] S pohľadu kybernetickej bezpečnosti sa môže jednať napríklad o VPN pripojenia, ktoré sú slabo zabezpečené, zlý návrh a implementácia informačného systému organizácie alebo krádež identity.

2.3 Kybernetické hrozby

S rozvojom stále nových a nových technológií, ktoré prinášajú človeku obrovské množstvo výhod, prichádza aj obrovské množstvo nevýhod a rizika. Počítače a zariadenia sú spolu prepojené do zložitej sieťovej štruktúry, ktorá nám umožňuje pohodlne ich na diaľku ovládať a prináša nám užívateľský komfort. A každé z týchto zariadení je potencionálny zdroj citlivých informácií, cenných pre útočníkov - hackerov. Vo väčšine prípadov stačí iba jedno jediné zariadenie, ktoré je nedostatočné zabezpečené, resp. je nezabezpečené, a umožní útočníkovi, alebo útočníkom prístup do celej siete. Počítačové hrozby sa stali viacej prepracovanejšie, čo má za následok väčšie škody a tým aj finančné straty podnikov, alebo ohrozenie bezpečnosti štátu v prípade kybernetickej špionáže. Kybernetické hrozby útočia na dôvernosť, dostupnosť a integritu dát. Dokážu znefunkčniť celú sieť, poškodiť samotné dáta, alebo zablokovaním prístupu k dátam pomocou ransomware vydierať poškodený podnik, alebo jednotlivca. Útoky v kybernetickom priestore predstavujú vážne nebezpečenstvo pre všetky organizácie v súkromnej aj verejnej sfére a ochrana pred nimi by nemala byť podceňovaná.

2.3.1 Malware – škodlivý softvér

Malware je škodlivý softvér, ktorý po infiltrácií do zariadenia poškodzuje dôvernosť, integritu a prístup k dátam, alebo umožňuje diaľkové ovládanie napadnutého systému. Ochranu pred ním poskytuje antivírový program.[14]

- **ransomware** – je škodlivý program, ktorý po infiltrácií systému zašifruje dáta v ňom uložené a vydieraním sa snažia autori kódu vylákať od obete peňažné prostriedky výmenou za odblokovanie dát. Ako ochrana sa odporúča používať programové vybavenie, ktoré je stále aktuálne a pravidelne zálohovanie dát.[14]
- **spyware** – je škodlivý počítačový program, ktorého úlohou je bez vedomia používateľa monitorovať a odosielať informácie z napadnutého systému, vrátane stlačenia kláves. Je to veľmi nebezpečný malware, pretože je veľmi obťažne identifikovateľný aj antivírovými programami.[14]
- **adware** – tento škodlivý kód, ktorý monitoruje činnosť používateľa na internete. Znakom infikovania systému adware je zobrazovanie rôznych nežiadúcich reklám, alebo presmerovanie stránok v prehliadači tak, aby ste navštívili určité internetové stránky.[14]
- **vírus** – počítačový vírus je program, ktorý sa rozširuje svojím kopírovaním do ďalšieho programu bez vedomia používateľa. Rozširujú sa väčšinou ako prílohy emailov, alebo ako voľne stiahnuteľné programy a bez zásahu používateľa sa sám nespustí. Ako ochrana proti počítačovým vírusom sa odporúča vôbec neotvárať prílohy mailov poslaných z neznámych adries a používať antivírový program.[14]
- **počítačový červ** – je podobne ako počítačový vírus škodlivý program, ktorý sa ale na rozdiel od vírusu šíri sám bez vedomia používateľa. Jeho súčasťou je program, ktorý na infikovanom systéme automaticky vyhľadáva ďalšie možnosti svojho prenosu na nový systém väčšinou cez emailové adresy uložené v infikovanom systéme. Spôsobujú problémy s výkonom a stabilitou počítačových sietí a systémov.[14]
- **trojský kôň** – je škodlivý program, ktorý si do počítača nainštaluje sám používateľ v domnení, že sa jedná o neškodnú aplikáciu, napríklad ako nový, lepší antivírový program. Trojan následne na pozadí kontroluje činnosť počítača, posiela informácie útočníkom, alebo úplne ovládne napadnutý počítač. Ako ochrana sa odporúča

kombinácia antivírového programu, nespúšťania neznámych súborov a neotvárania elektronickej pošty.[14]

2.3.2 Denial of Service (DoS)

Denial of Service - DoS, alebo odmietnutie služby je typ kybernetického útoku zameraného na systémy poskytujúce určitú službu, napríklad servery rôznych organizácií a inštitúcií. Podstatou útoku je zahltenie servera veľkým množstvom požiadaviek, ktoré zahltia napádaný server a ten prestane poskytovať svoje služby, alebo v horšom prípade nedôjde k jeho návratu do normálnej prevádzky. Za dôvody takéhoto útoku sa považujú konkurenčný boj, kybernetický terorizmus, odplata, forma demonštrácie, alebo odpútanie pozornosti od niečoho iného. V prípade, že takýto útok prichádza z viacerých zdrojov hovoríme o Distributed Denial of Service – DDoS.[14]

2.3.3 Sociálne inžinierstvo

Sociálne inžinierstvo patrí medzi najefektívnejšie netechnické spôsoby prelomenia kybernetickej bezpečnosti. Nevyžaduje žiadne zložité programové vybavenie a hlboké znalosti z počítačových systémov. Tento typ kybernetických útok sa spolieha na ľudskú hlúposť, naivitu, nevedomosť a neopatrnosť a s využitím rôznych manipulačných techník k získaniu citlivých údajov, alebo prístupu k informačným systémom. Ako ochrana sa odporúča používať zdravý rozum, zvyšovanie povedomia o informačných technológiách a technikách sociálneho inžinierstva a nezverejňovanie citlivých údajov o sebe samom.

- **phishing** – je typ kybernetického útoku, najčastejšie vykonávaný prostredníctvom zasielania podvodných emailov, kde útočník získava informácie od obete vydávaním sa za dôveryhodnú inštitúciu. Asi najznámejšie sú emailové správy týkajúce sa internetového bankovníctva, ktoré sú navrhované tak, aby vzbudili u obete dôveru, že odosielateľom je banka. Po kliknutí na odkaz je užívateľ presmerovaný na falošnú internetovú stránku, ktorá je veľmi podobná originálnej.[14]
- **pharming** – princíp pharmingu spočíva v tom, že škodlivý kód, ktorý sa v infikovanom počítači nachádza, bez vedomia používateľa zmení nastavenia Domain Name System (DNS) a presmeruje užívateľa na falošné internetové stránky, ktoré sú vo väčšine prípadov na nerozoznanie od originálnych internetových stránok. Používateľ veľakrát ani nezistí, že je na falošnej internetovej stránke.[27]

- **baiting** – pri tomto type kybernetického útoku ide o podvrhnutie fyzického média obeti, na ktorom je uložený infikovaný program, a keďže je používateľ zvedavý, pripojí si toto médium k počítači a škodlivý kód sa nainštaluje. Od tohto momentu získava útočník prístup a kontrolu nad počítačom obete resp. do vnútornej siete organizácie v ktorej obeť pracuje.[27]
- **reverzné sociálne inžinierstvo** – je veľmi nebezpečný typ kybernetického útoku, pretože podstata spočíva v tom, že obeť sama vyhľadá útočníka, aby jej pomohol s riešením problému, ktorý útočník sám vyrobil. Pri takomto konaní už zo samotnej podstaty vyplýva, že obeť bude útočníkovi dôverovať. Tento typ útoku napácha obrovské škody, pretože obeť ľahšie poskytne útočníkovi dôverné informácie. Na záver iba dodám, že je to veľmi náročný typ kybernetického útoku a vyžaduje okrem náročnej prípravy aj kus povestného šťastia.[27]

2.4 Scenáre priebehu bezpečnostnej situácie a dopady na organizáciu

Organizácie využívajú na svoje fungovanie informačné systémy podľa toho akú činnosť vykonávajú. Výrobná spoločnosť používa informačný systém, ktorý jej pomáha riadiť výrobu konkrétneho výrobku, analyzuje a pomáha odstraňovať nežiadúce javy vo výrobnom procese a v neposlednom rade vyhodnocuje aktivity operátorov. Obchodná spoločnosť zase používa informačný systém, pomocou ktorého eviduje tovar na sklade a jeho pohyb, má pod kontrolou systém objednávok, evidenciu faktúr a platieb. Organizácia poskytujúca ubytovanie zasa používa informačný systém na rezerváciu izieb, umožňuje vytváranie prehľadov o obsadenosti izieb, riadi aktivity hostí a napríklad aj skladovanie potravín. Na druhej strane existujú informačné systémy, ktoré používajú organizácie bez ohľadu na predmet činnosti. Jedná sa väčšinou o dochádzkové a mzdové systémy. Nato, aby sme vedeli stanoviť výšku dopadov kybernetických útokov na organizácie si musíme popísať a charakterizovať jednotlivé kybernetické hrozby, na aké prvky informačného systému organizácie sú zamerané a aké dopady na organizáciu majú. V podkapitole 2.3 sú popísané najviac rozšírené kybernetické hrozby a preto sa viacej zameriame na to aké prvky sú takýmito hrozbami ohrozené, spolu z ich dopadmi na organizácie a rozdelíme hrozby podľa nebezpečnosti.

2.4.1 Útok prostredníctvom ransomware

- **popis** - útok je uskutočnený pomocou škodlivého softvéru, ktorý uzamkne, alebo zablokuje celý informačný systém, alebo zašifruje užívateľské dáta na pevnom disku. Pod hrozbou zmazania, alebo znefunkčnenia informačného systému požadujú útočníci zaplatenie výkupného,
- **ohrozené časti informačného systému** - útokom prostredníctvom ransomware sú najviac ohrozené samotné servery informačného systému, dáta uložené na pevných diskoch organizácie, programy používané organizáciou, segmenty siete,
- **dopady útoku** - dopady takéhoto kybernetického útoku na výrobnú, alebo nevýrobnú organizáciu sú vždy závažné. Nedostupnosť kľúčových dát priamo ohrozuje chod organizácie zastavením výroby, poškodením dodávateľsko-odberateľských vzťahov z dôvodu neplnenia svojich záväzkov. Z toho vyplýva aj poškodenie dobrého mena organizácie a rátať musíme aj s pokutami pre niektoré organizácie za nezverejňovanie povinných údajoch a pokutách vyplývajúcich zo zmluvných vzťahov. V prípade útoku na informačný systém nevýrobnej organizácie vznikajú náklady na mzdy pracovníkov, ktorý nemôžu na napadnutom informačnom systéme vykonávať svoju prácu,
- **scenár vývoja bezpečnostnej situácie** - organizácia zisťuje, že sa stala terčom kybernetického útoku. Okamžite začína podnikať kroky a prijímať protiopatrenia na zmiernenie dopadov kybernetického útoku. Snaží sa zamedziť pokračovaniu útoku napríklad odpojením od verejnej internetovej siete, alebo vypínaním zariadení, ktoré sú kybernetickým útokom zasiahnuté. Po zistení, že nie je možné sa dostať k dátam uloženým na diskoch, začína organizácia pracovať na postupnej obnove dát zo zálohy, ktorú si pravidelne robila. Obnoveniu predchádza preinštalovanie zariadení používaných v organizácii. Základné činnosti sú obmedzené na najnutnejšiu možnú mieru a tie sú spracovávané papierovou formou. Po postupnom obnovovaní systému začína organizácia obnovovať aj svoje základné činnosti, až do doby, kedy organizácia funguje v normálnom režime.

2.4.2 Únik dát z dôvodu nedbanlivosti, alebo ako úmyselná činnosť

- **popis** - jedná sa o jeden z najčastejších dôvodov, kedy sa dáta organizácie dostanú mimo informačný systém. Je dôsledkom neúmyselného, alebo úmyselného konania a je spôsobený zanedbaním povinnosti pri manipulácií s internými informáciami,
- **ohrozené časti informačného systému** - takýmto únikom dôverných interných informácií je najčastejšie ohrozená tá časť informačného systému, kde sú informácie uložené, spracovávané, alebo prezentované,
- **dopady úniku** - ak sa takéto interné dáta dostanú k nepovolaným osobám, tak ich následným zneužitím môže dôjsť k škodám veľkého rozsahu. V prípade odcudzenia dát vzniknú ďalšie náklady na odstránenie dôsledkov takéhoto úniku, resp. odstránenie problému, ktorý takýmto vyzradením interných informácií vznikol a znovuzískanie konkrétnej výhody. Ak sa takýto incident medializuje, je pravdepodobné, že dôjde aj k poškodeniu dobrého mena organizácie a zničenie reputácie obchodnej značky a nesmieme zabudnúť ani na pokuty od kontrolných orgánov,
- **scenár vývoja bezpečnostnej situácie -** prepustený zamestnanec, ktorému neboli vyplatené odchodné náležitosti si urobí zálohu firemnej databázy a potom ju vymaže. Následne oznámi, že ak mu náležitosti nebudú do určitého času vyplatené, nevráti zálohované dáta organizácii. Činnosti organizácie sú obmedzené na minimum. Prestáva si plniť svoje záväzky voči svojím zákazníkom a dodávateľom a hrozia pokuty podľa uzatvorených zmlúv. Firma je nútená záväzky voči bývalému zamestnancovi uhradiť a získava svoje dáta naspäť. Obnovuje sa činnosť organizácie.

2.4.3 Útok typu Denial of Service (DoS)

- **popis** - dohodnutý útok na informačný systém prevádzkovateľa, ktorý pod nadmerným množstvom požiadaviek na zobrazenie napríklad internetovej stránky odmietne túto stránku zobrazovať. Neslúži na ukradnutie dát, alebo ovládnutie informačného systému, ale v prípade nevhodnej konfigurácie servera, môže dôjsť aj k úplnému znefunkčneniu informačného systému,
- **ohrozené časti organizácie a informačného systému** - v prípade útoku DDoS sú najviac ohrozené servery organizácie, určité segmenty siete, softvér a dáta,

- **dopady útoku** - okrem priamych škôd, ktoré závisia od intenzity a dĺžky útoku, a ktoré sa dajú ľahko vyčísliť, môže dôjsť aj k poškodeniu dobrého mena organizácie ako dôsledok neuskutočnenia online obchodov práve v čase trvania útoku. Zákazníci často v prípade nedostupnosti takejto služby rýchlo prechádzajú ku konkurencii,
- **scenár vývoja bezpečnostnej situácie -** na server organizácie prichádza obrovské množstvo požiadaviek na službu. Server organizácie je zahltený a nedokáže všetky požiadavky obslúžiť. Organizácia nedokáže odfiltrovať všetky požiadavky a vypína server. Prestáva poskytovať svoje služby verejnosti a prichádza o zisk a je poškodené dobré meno organizácie. Po odrazení útoku organizácia obnovuje svoju činnosť znova začína poskytovať svoje služby.

2.4.4 Útok formou úmyselnej trestnej činnosti – hacker

- **popis** - hacking znamená prienik do systému inou ako štandardnou cestou, teda obídenie, alebo prelomenie jeho bezpečnostnej ochrany.[18] Hackeri sú veľmi šikovní programátori, alebo počítačový odborníci, ktorí zasahujú priamo do štruktúry programov a modifikujú ich za účelom získania, alebo modifikácie dát,
- **ohrozené časti informačného systému** - hackeri najčastejšie útočia na servery organizácie, dáta uložené v dátových úložiskách, segmenty siete a hardware,
- **dopady útoku** - dopady útoku spôsobený hackerom bývajú vo väčšine prípadov rozsiahle. Zámerom hackera je, aby nebol hneď odhalený a dostal sa k citlivým dátam, ktoré nie sú bežne prístupné a preto sa takýto útok detekuje až keď sú škody obrovské. V prípade odcudzenia citlivých dát ako sú údaje o zákazníkoch a zamestnancoch a straty dôvery môže prispieť aj k prerušeniu činnosti organizácie. Náklady na obnovu dát bývajú častokrát veľké a niekedy nie je ani možné takto zmazané dáta obnoviť. V prípade odcudzenia osobných údajov vznikajú náklady na oznámenie úniku príslušným úradom a na právne služby. Útokom môže byť poškodený aj samotný informačný systém, ktorý treba opraviť. V neposlednom rade je poškodené aj dobré meno organizácie a obnova dôvery zákazníkov v organizáciu a jej schopnosť v budúcnosti odolávať kybernetickým útokom,
- **scenár vývoja bezpečnostnej situácie** - hacker prelomením zabezpečenia sa dostal do počítačovej siete organizácie. Organizácia zatiaľ nemá vedomie o prebiehajúcom útoku. Hacker sa dostal k citlivým osobným a technologickým informáciám

uložených na dátovom úložisku organizácie, ktoré ukradne. Organizácia zisťuje, že sa stala terčom útoku hackera. Oznam o rozsahu útoku sa dostáva na verejnosť, čo poškodí dobré meno organizácie. Niektoré dáta sa podarí obnoviť zo zálohy, ale niektoré sú nenávratne stratené. Organizácia dostáva pokutu od úradu za únik citlivých osobných údajov.

2.4.5 Útok s využitím metód sociálneho inžinierstva

- **popis** - je to jeden z najjednoduchších kybernetických útokov. Paradoxne nevyžaduje podrobnú znalosť informačného systému, pretože sa zameriava na najslabšie miesto celého systému a to je človek. Vychádza zo zlyhania ľudského faktora, ktorý je neodmysliteľnou súčasťou informačnej bezpečnosti a je založený na netechnickej manipulácii a ovplyvňovaní človeka s cieľom získania prístupu k informačnému systému, alebo citlivým dátam organizácie,
- **ohrozené časti informačného systému** - cieľom útoku je získať prístupy k informačnému systému organizácie, dátam uloženým na pevných diskoch, hardware a software organizácie,
- **dopady útoku** - dopady útoku s využitím sociálneho inžinierstva môžu byť tak isto ako v prípade predchádzajúcej hrozby veľmi rozsiahle. V prípade krádeže citlivých dát a následnej straty dôvery môže dôjsť až k znefunkčneniu organizácie. V prípade získania prístupu k informačnému systému môže dôjsť k narušeniu vnútorného prostredia organizácie a poškodeniu informačného systému spolu s jeho vyradením z prevádzky. Strata osobných údajov a jej oznámenie kontrolným úradom spolu s právnymi službami generujú ďalšie náklady. Ako aj v predchádzajúcich kybernetických útokoch aj v tomto prípade dochádza k poškodeniu dobrého mena organizácie a dodávateľsko-odberateľských vzťahov,
- **scenár vývoja bezpečnostnej situácie -** útočník telefonický kontaktuje zamestnancov organizácie s cieľom prinútiť kliknúť zamestnancov na podvrhnutý odkaz, alebo s cieľom získať prístupové údaje k mailom, alebo priamo k informačnému systému organizácie. Organizácia nemá vedomosť o prebiehajúcom útoku. Útočníkovi sa podarí takýmto spôsobom získať potrebné údaje a následne prenikne do informačného systému organizácie. Dáta o klientoch a dáta organizácie sú ukradnuté a následne zneužité k páchaniu inej trestnej činnosti. Útočníkovi sa

podarí previezť značnú hotovosť z účtov organizácie, čím jej spôsobí škodu. Je poškodené dobré meno firmy a organizácia stráca zákazníkov.

Kybernetickú bezpečnosť je treba chápať ako jednu z veľmi dôležitých častí bezpečnosti. Kybernetická bezpečnosť nie je len o zabránení posielania nevyžiadaných mailov, detekcii vírusov, alebo zabránení neoprávneného prístupu do informačného systému. Musí byť založená na komplexnom prístupe a musí zahrňovať prácu so zamestnancami a vedením organizácií, aby boli oboznámení s najnovšími hrozbami, a aby vedeli ako chrániť informačné systémy používané v organizácii.

3 OCEŇOVANIE HMOTNÝCH A NEHMOTNÝCH AKTÍV

Dosahovanie zisku je hlavným cieľom organizácií v podnikateľskom prostredí. Ten naplňujú získavaním finančných prostriedkov predajom hmotného tovaru, alebo služieb. Prudký rozvoj informačných technológií, veľká hospodárska súťaž a z toho vyplývajúci tlak na konkurencieschopnosť podnikov, mali za následok, že organizácie začali čoraz viacej disponovať aj nehmotnými aktívami. Tým, že sa v niektorých prípadoch stali súčasťou aj hmotných aktív, alebo boli priamo súčasťou kúpno-predajných vzťahov. Vystala potreba takéto nehmotné aktíva zahrňovať do majetku podniku a stanovovať ich cenu. Pri organizáciách vo verejnom sektore zasa vystala požiadavka oceňovania nehmotných aktív z iného dôvodu. Inštitúcie začali svoje služby ponúkať prostredníctvom informačných technológií, čo viedlo k vytváraniu databáz z citlivými údajmi, ktoré odrazu boli prístupné online. Ako vieme, s rozvojom informačných technológií prišlo aj k rozmachu kybernetickej kriminality, ktorá neobišla ani tieto verejné inštitúcie a organizácie, kde došlo následkom kybernetických útokov k škodám, ktoré bolo treba vyčísliť.

V tejto kapitole si objasníme základné pojmy z oblasti oceňovania nehmotného majetku, nehmotných aktív a práv k ním, a metód vyčíslenia hodnoty nehmotného aktíva. Popíšeme ako bude organizácia fungovať a aká bude jej ujma v prípade výpadku informačného systému ako následku kybernetického útoku, so zameraním na ocenenie takejto ujmy.

3.1 Základné pojmy

Na to, aby sme sa zorientovali v problematike oceňovania hmotného a nehmotného majetku, musíme si ozrejmiť základne pojmy v tejto oblasti.

3.1.1 Hmotné aktívum

Ak sa na aktíva podniku, alebo organizácie pozrieme pohľadom ekonómov prípadne účtovníkov, tak hmotné aktívum môžeme charakterizovať ako majetok organizácie, ktorý ma hmotnú povahu, tzn. fyzický existuje v priestore a vieme ho vnímať našimi zmyslami. Existuje niekoľko kategórií, na ktoré môžeme hmotný majetok rozdeľovať – na základe časového hľadiska, z hľadiska prevádzkového cyklu, z hľadiska podstaty a podobne.

Delenie z hľadiska podstaty

- hnuteľný majetok – nie je pevne pripevnený a ktorým vieme hýbať,
- nehnuteľný majetok – je pevne spojený so zemou, resp. pôdou pevným základom.

Delenie z časového hľadiska

- krátkodobý majetok – slúži na činnosť kratšie ako jeden rok,
- dlhodobý majetok – slúži na činnosť dlhšie ako jeden rok.

Delenie z hľadiska prevádzkového cyklu

- obežný majetok – krátkodobé zložky majetku v podniku,
- neobežný majetok – používa sa dlhodobo, niekoľko cyklov.

Delenie z hľadiska likvidity

- likvidný majetok – prostriedky, ktorými podnik rýchlo uhrádza svoje pohľadávky,
- s nižším stupňom likvidity – prostriedky, väčšinou časovo viazané,
- nelikvidný majetok – podnik musí tento majetok najprv premeniť na prostriedky.

3.1.2 Nehmotné aktívum

Nehmotné aktívum ako pojem v sebe zahrňuje širokú oblasť majetku vzťahujúcu sa napríklad k výskumu, autorstvu, vývoju a uvádzaniu inovatívnych postupov do praxe, umeniu, marketingu, zákazníkom, majetku uloženom na nosičoch dát a pod. Nehmotné aktívum je svojou povahou nehmotné, tzn. nemá finančnú a ani fyzickú povahu. Občiansky zákonník v § 118 vymedzuje, že predmetom občianskoprávnych vzťahov sú veci a pokiaľ to ich povaha pripúšťa, práva, alebo iné majetkové hodnoty. Pretože aktuálny občiansky zákonník v § 119 definuje veci iba ako predmety hnuteľné a nehnuteľné, na nehmotné predmety je treba pozerať z pohľadu právneho buď ako na „práva“ alebo „iné majetkové hodnoty“.[19] Medzinárodný účtovný štandard definuje nehmotné aktívum ako identifikovateľný nepeňažný majetok bez fyzickej podstaty.

Identifikovateľnosť nehmotného aktíva znamená, že:

- nehmotný majetok je oddeliteľný od iných aktív,
- vyplýva zo zmluvných, alebo iných práv,
- je kontrolovateľné,
- je výsledkom minulej činnosti,
- bude mať budúci prínos ekonomických úžitkov,
- existuje možnosť spoľahlivého ocenenia.[20]

Neoddeliteľnou súčasťou nehmotných aktív je duševné vlastníctvo, ktoré okrem práv k nehnuteľnému aktívu upravuje aj vzťahy, ktoré pri uplatňovaní takýchto práv v spoločnosti vznikajú. Oblasť duševného vlastníctva poskytuje ochranu zvlášť pre systém autorského práva a zvlášť pre systém priemyselného práva.

Rozdelenie nehmotných aktív

- *autorské práva (Copyright)*
  - autorské diela,
  - súvisiace diela,
  - software.
- *priemyselné práva (Industrial Property)*
  - technické riešenia
    - vynálezy,
    - úžitkový vzor,
    - topografia.
  - označenie
    - ochranná známka,
    - obchodná firma,
    - označenie pôvodu,
    - zemepisné označenie,

- domény.

- ostatné
  - know-how,
  - objavy,
  - priemyselný vzor,
  - goodwill,
  - odrody rastlín.[19]

3.2 Prístupy k oceňovaniu hmotného majetku

Definovanie a charakteristika jednotlivých súčastí majetku a záväzkov hrá dôležitú úlohu pri oceňovaní o jednotlivých zmenách majetku a záväzkov počas účtovného obdobia, ako aj pri vykazovaní stavu majetku, záväzkov a vlastného imania účtovnej jednotky. Podstata oceňovania hmotného majetku subjektu je priraďovanie finančnej čiastky jednotlivým zložkám majetku podniku.

3.2.1 Oceňovanie hmotného majetku v SR

Na Slovensku základnou právnou normou v oblasti vedenia účtovníctva je Zákon o účtovníctve č. 431/2002 Z. z. Tento zákon venuje značnú pozornosť aj oceňovanie majetku a záväzkov účtovných jednotiek. Slovenská legislatíva presne ustanovuje povinnosť oceňovať majetok a záväzky ku dňu ocenenia, pričom deň ocenenia sa v legislatíve definuje nasledovne:

- deň uskutočnenia účtovného prípadu (oceňuje sa spôsobmi podľa §25),
- deň ku ktorému sa zostavuje účtovná závierka (oceňuje sa spôsobom podľa 27),
- iný deň v priebehu účtovného obdobia, ak to vyžaduje osobitný predpis oceňuje sa spôsobom podľa §27).[23]

Spôsoby oceňovania hmotného majetku podľa Zákona o účtovníctve č. 431/2002 Z. z.:

obstarávacou cenou

- hmotný majetok, s výnimkou toho, ktorý bol vytvorený vlastnou činnosťou,
- zásoby, s výnimkou tých vytvorených vlastnou činnosťou,

- podiely na vlastnom imaní obchodných spoločností, cenné papiere a deriváty,
- nehmotný majetok s výnimkou toho, ktorý bol vytvorený vlastnou činnosťou,
- záväzky pri ich prevzatí.

vlastnými nákladmi

- zásoby vytvorené vlastnou činnosťou,
- hmotný majetok vytvorený vlastnou činnosťou,
- nehmotný majetok vytvorený vlastnou činnosťou.

menovitou hodnotou

- peňažné prostriedky a ceniny,
- pohľadávky pri ich vzniku,
- záväzky pri ich vzniku.

reprodukčnou obstarávacou cenou

- majetok v prípade bezodplatného nadobudnutia,
- nehmotný majetok vytvorený vlastnou činnosťou, ak sú vlastné náklady

vyššie ako reprodukčná obstarávacia cena

- majetok preradený z osobného vlastníctva do podnikania,
- nehmotný a hmotný majetok doteraz nezachytený v účtovníctve.[23]

Oceňovanie zásob podniku vedených na sklade, alebo cenných papieroch, pokiaľ ide o rovnaký druh, zákon umožňuje ocenenie ich úbytku aj cenou zistenou váženým aritmetický priemerom alebo spôsobom FIFO, nie však LIFO.

Zákon o účtovníctve číslo 431/2002 Z. z. upravuje jednotlivé spôsoby v oblasti oceňovania hmotného majetku nasledovne:

- **obstarávacou cenou** je cena, za ktorú sa majetok obstaral a náklady súvisiace s jeho obstaraním,
- **reprodukčnou obstarávacou cenou** je cena, za ktorú by sa majetok obstaral v čase keď sa o ňom účtuje,

- **vlastnými nákladmi**, pri zásobách vytvorených vlastnou činnosťou sú to priame náklady vynaložené na výrobu alebo inú činnosť. Pri hmotnom majetku okrem zásob a pri nehmotnom okrem pohľadávok sú to priame náklady vynaložené na výrobu alebo inú činnosť, menovitou hodnotou je cena, ktorá je uvedená na peňažných prostriedkoch a ceninách alebo suma, na ktorú pohľadávka alebo záväzok znie.[23]

Pri oceňovaní hmotného majetku je veľmi podstatná zásada opatrnosti. Táto zásada opatrnosti vyžaduje aby účtovná jednotka ku dňu, ku ktorému sa zostavuje účtovná závierka, zohľadnila predpokladané riziká a straty, ktoré sa týkajú majetku a záväzkov. Zníženie hodnoty sa musí zohľadniť vždy, bez ohľadu na to, či výsledkom hospodárenia je zisk alebo strata.

Predpokladané riziká, straty, a zníženia hodnoty, ktoré sa týkajú majetku a záväzkov, sa vyjadrujú prostredníctvom rezerv, opravných položiek a odpisov, pričom v zákone sú presne vymedzené:

- rezervy sú záväzky s neurčitým časovým vymedzením alebo výškou,
- opravné položky sa vytvárajú pri prechodnom znížení hodnoty majetku,
- odpisy predstavujú trvalé zníženie hodnoty majetku.

Pri finančnom majetku a záväzkoch, ktoré sa podľa zákona o účtovníctve neoceňujú reálnou hodnotou, sa postupuje takto:

- pri cenných papieroch držaných do splatnosti a cenných papieroch obstaraných v primárnych emisiách neurčených na obchodovanie sa ich ocenenie odo dňa vyrovnania nákupu do dňa ich splatnosti postupne zvyšuje o úrokové výnosy,
- podiel na vlastnom imaní v obchodných spoločnostiach sa môže oceniť metódou vlastného imania. Ak ju účtovná jednotka použije, je povinná použiť ju na ocenenie všetkých takýchto podielov,
- pri cenných papieroch emitovaných účtovnou jednotkou sa ich ocenenie odo dňa vyrovnania emisie do dňa splatnosti postupne zvyšuje o úrokové náklady na emitované cenné papiere.

Opatrenia Ministerstva financií SR o postupoch účtovania upravujú oceňovanie v oblasti vedenia účtovníctva v systéme podvojného účtovníctva, banky, poisťovne a zaisťovne. Bližšie sa pozrieme na úpravy pre podnikateľov.

3.2.2 Oceňovanie hmotného majetku podľa IFRS a US GAAP

Podľa medzinárodných štandardov je základným pravidlom ako klasifikovať položku ako dlhodobý hmotný majetok je skutočnosť, že podnik pravdepodobne v budúcnosti prinesie ekonomický prospech, a je možné spoľahlivo zistiť jeho nadobúdaciu hodnotu. Vo všeobecnosti podľa medzinárodných štandardov je nadobúdacou hodnotou majetku jeho obstarávacia cena. Obstarávacia cena pozostáva z nákupnej ceny, ceny dopravy, ceny za inštaláciu a podobne. Do ceny majetku je možné zahrnúť tiež položky ako očakávané náklady na vyradenie, úroky a technické zhodnotenie.[24]

Špeciálnou triedou hmotného majetku podľa medzinárodných štandardov sú pozemky, ktoré na rozdiel od ostatného majú neurčitú dobu životnosti. Účtovníctvo pre pozemky sa odvíja od účelu ktorému slúžia. V hospodárskej praxi existujú zvyčajne:

- nezastavané pozemky - pozemok sa zaúčtuje v obstarávacej hodnote a neodpisuje sa,
- zastavané pozemky - pozemok aj stavba sa zaúčtujú v obstarávacej hodnote a ďalej sa vedú v účtovníctve oddelene,
- pozemok držaný za účelom zástavby – pod týmto pojmom sa rozumie pozemok na ktorom zatiaľ žiadna stavba nestojí, ale na ktorom má subjekt úmysel ju postaviť, alebo pozemok, na ktorom stavba síce je, ale sa bude nahradzovať inou. Pokiaľ na pozemku žiadna stavba nestojí, náklady sa musia rozdeliť podľa toho či súvisia s pozemkom úprava terénu, výrub stromov, alebo súvisia so samotnou stavbou (kanalizácia, príjazdové cesty),
- pozemok držaný za investičnými účelmi.[24]

3.3 Prístupy k oceňovaniu nehmotného majetku

Všeobecne oceňovanie akéhokoľvek majetku je dôležitým prvkom pri spravovaní a riadení organizácií. Oceňovaním priraďujeme peňažnú hodnotu majetku, či už hmotnému, alebo nehmotnému. Správne stanovenie hodnoty majetku nám podáva ucelený obraz o skladbe majetku spoločnosti a výsledkoch podnikateľskej činnosti organizácie. Oceňovanie z pohľadu účtovníctva patrí medzi najnáročnejšie problémy a správne prevedenie oceňovania má dôležitý vplyv na celkový stav organizácie a jej fungovanie.

Nehmotné statky produkujú hodnoty zvláštnym spôsobom. Nielenže ich možno súčasne používať na mnohých miestach, ale používanie môže realizovať tak majiteľ, ako aj v rámci

transferu licenčný nadobúdateľ, v rámci novo vytvoreného podniku, ale tiež tým, že takéto právo zabraňuje konkurencii používať chránené riešenia a vytvára tak predpoklady pre intenzívnejšie používanie či uplatnenie iných riešení, a to všetko často bez úbytku ich hodnoty.[21] K stanoveniu hodnoty nehmotného aktíva sa používajú prístupy výnosový, nákladový a trhový, ktorých úlohou je zachytiť charakteristiky nehmotného majetku z pohľadu ekonomického, fyzického a porovnávacieho.

3.3.1 Prístupy oceňovania nehmotného majetku

- **trhový (porovnávací) prístup** – jeho podstata spočíva v porovnávaní hodnôt nehmotných aktív prítomných na trhu a využíva princípu akejsi rovnováhy, ktorú trh vytvára,
- **výnosový prístup** – je založený na princípe ekonomického očakávania, teda myšlienke, že záujemca nie je ochotný za nehmotné aktívum zaplatiť viac, ako je súčasná hodnota očakávaných príjmov z využitia aktíva pri miere rizika na úrovni porovnateľnej investície,[19]
- **nákladový prístup** – podstata spočíva v tom, že záujemca by nezaplatil za nehmotné aktívum viac, ako by zaplatil za vytvorenie iného nehmotného aktíva s porovnateľnou úžitkovosťou.

3.4 Metódy oceňovania nehmotného majetku

Z troch základných princípov oceňovania nehmotného majetku vychádzajú metódy oceňovania, ktoré používajú reálne tržné ceny používanie pri skutočných obchodných transakciách, pre čo najpresnejšie stanovenie trhovej hodnoty oceňovaného nehmotného aktíva.

3.4.1 Metóda násobiteľov

Metóda násobiteľov vychádza z porovnávacieho prístupu a používa sa na rovnakých, alebo veľmi podobných nehmotných aktívach a umožňuje porovnať vybrané ekonomické parametre. Používa sa najmä pri nehmotných aktívach obchodovaných na aukciách za absolútne ceny. V prípadoch kde je menšie množstvo transakcií dostupných na porovnanie sa táto metóda odporúča použiť ako podporná. Matematické vyjadrenie priameho porovnávacieho prístupu s použitím násobiteľov určuje tento vzorec (1):

$$HNA = \frac{C_S}{X_S} * XNA \quad (1)$$

kde H_{NA} je hodnota nehmotného aktíva pri porovnaní s jedným porovnateľným nehmotným aktívom,

C_S je cena porovnateľného aktíva,

X_S je kľúčová ekonomická charakteristika porovnateľného nehmotného aktíva,

X_{NA} je podobná ekonomická charakteristika hospodárenia oceňovaného nehmotného aktíva.[19]

3.4.2 Metóda nákladov reprodukcie

Táto metóda sa odvíja od nákladového prístupu a jej podstata vychádza z vytvorenia rovnakého nehmotného aktíva ako toho, ktoré oceňujeme. Zahrňuje v sebe aj mieru opotrebovania, ktorá má za následok aj určitý pokles využitia takto vytvoreného aktíva. K vytvoreniu rovnakého aktíva používa pôvodne postupy a vstupy v cenách ku dňu ocenenia. Použitie tejto metódy sa odporúča pri oceňovaní nehmotného aktíva, pri vytvorení ktorého nie sú veľké náklady obetovanej príležitosti a súčasne s veľkou pravdepodobnosťou dokončenej substitúcie zo strany kupujúceho. V našom prípade by sa jednalo o napríklad softvérové riešenia bez vzťahu ku konkurenčnej výhode, pri ISO certifikácii, kvalifikovanom personáli, alebo na vzťahy so zákazníkmi. K vyjadreniu metódy nákladov reprodukcie sa používa nasledujúci matematický vzorec (2):

$$H_{NA} = \sum_{i=1}^{n} \sum_{t=O}^{T} [N_i * (1 + I_{CPI})^t * (1 + i)^t] * (1 - A) + TAB \quad (2)$$

kde H_{NA} je hodnota nehmotného aktíva pri porovnaní s jedným porovnateľným nehmotným aktívom,

Ni je hodnota nákladovej položky vynaloženej na vytvorenie pôvodného nehmotného aktíva (v počte i = 1 až n nákladových položiek),

I_{CPI} je miera zmeny cien nákladových položiek medzi obdobím vynaloženia (t) a dátumom ocenenia (T), merané vhodným cenovým indexom (CPI, alebo PPI), alebo inou veličinou,

i sú náklady ušlej príležitosti,

A je miera zníženia užitočnosti vynaložených nákladov k dátumu ocenenia, pokiaľ k zastaraniu prišlo,

TAB je prínos z daňovo odpisovaného aktíva.[19]

3.4.3 Metóda nákladov nahradenia

Metóda vychádza z nákladového prístupu oceňovania nehmotného aktíva a spočíva vo vytvorení nehmotného aktíva s porovnateľnou užitočnosťou, ale pri použití súčasnej, resp. k dátumu ocenenia nehmotného aktíva, úrovne znalostí a stavu techniky potrebných na znovu vymyslenie takéhoto riešenia.[22] Matematické vyjadrenie metódy udáva tento vzorec (4):

$$H_{NA} = \sum_{i=1}^{n} N_i * (1+i)^t + TAB \tag{3}$$

kde N_i je hodnota nákladovej položky vynaloženej na vytvorenie nehmotného aktíva s porovnateľnou úžitkovosťou (v počte $i = 1$ až n nákladových položiek).[19]

3.4.4 Metóda licenčnej analógie

Táto metóda je najviac používanou metódou na určovanie ceny nehmotného aktíva. Vychádza z výnosového prístupu a je založená na princípe, že výrobca musí zaplatiť určitú cenu tretej osobe za súhlas s využitím chráneného riešenia. Takýto súhlas na využívanie chráneného riešenia sa poskytuje formou licenčnej zmluvy a za jej udelenie sa platia licenčné poplatky. Metóda licenčnej analógie priamo oceňuje práva duševného vlastníctva, ktoré je obchodované formou licenčných zmlúv, ale nie je vhodná, a ani sa neodporúča použiť ju pri oceňovaní nehmotných aktív ako sú výhodne zmluvy, alebo vzťahy so zákazníkmi. Najlepšie využitie je najmä pri oceňovaní nehmotných aktív s globálnym trhovým vplyvom, pretože je dostupných viac transakčných údajov. Metódu licenčnej analógie môžeme použiť nasledujúcim spôsobom:

- **analógia nadobudnutia licencie** – hodnota je daná súčtom príjmov z úspor na licenčných poplatkoch, tým že nehmotné aktívum vlastníme,
- **analógia poskytnutia licencie** – hodnota je daná súčtom príjmov z poskytnutia licencie tretej osobe,
- **kombinovaná analógia** – hodnota je daná použitím oboch spôsobov a to príjmom z vlastnej výroby a z príjmov z licenčnej výroby treťou stranou.[19]

Nasledujúci vzorec (4) matematický vyjadruje výpočet hodnoty podľa metódy licenčnej analógie:

$$H_{NA} = \sum_{t=1}^{n} \frac{T_t * PM * LP * K_t * (1-d)}{(1+i)^t} + TAB \quad (4)$$

kde T_t je plán objemu predaja výrobku obsahujúceho oceňované nehmotné aktívum (čisté tržby),

PM je podiel nehmotného aktíva na objemu predaja výrobku obsahujúceho oceňované nehmotné aktívum,

LP je sadzba licenčného poplatku v %,

K_t je index zastarania (pri technických riešeniach),

i sú náklady ušlej príležitosti v % p.a.,

t je zostávajúca doba životnosti nehmotného aktíva,

d je sadzba dane z príjmu právnických osôb,

TAB je prínos z daňovo odpisovaného aktíva.[19]

3.4.5 Metóda podielu na zisku

Metóda podielu na zisku má za úlohu oceniť hodnotu nehmotného aktíva ako súčasnú hodnotu podielov na zisku plynúcich z používania takéhoto nehmotného aktíva.[19] Vychádza z výnosového prístupu oceňovania nehmotného aktíva. Využíva sa v prípadoch, kedy výrobky vyrobené na základe nehmotného aktíva majú vo svojej cene započítaný väčší zisk ako rovnaký, alebo podobný konkurenčný výrobok. Matematicky sa hodnota nehmotného aktíva metódou podielu na zisku vypočíta podľa vzorca (5):

$$HNA = \sum_{t=1}^{n} \frac{T_t * ZM * PM * LP^{ZM} * K_t * (1-d)}{(1+i)^t} + TAB \quad (5)$$

kde T_t je plán objemu predaja výrobku obsahujúceho oceňované nehmotné aktívum (čisté tržby),

ZM je zisková marža z predaja výrobku obsahujúceho využitie nehmotného aktíva,

PM je podiel nehmotného aktíva na objemu predaja výrobku obsahujúceho oceňované nehmotné aktívum,

LP^{ZM} je sadzba licenčného poplatku vyjadrená zo zisku v %,

K_t je index zastarania (pri technických riešeniach),

i sú náklady ušlej príležitosti v % p.a.,

t je zostávajúca doba životnosti nehmotného aktíva,

d je sadzba dane z príjmu právnických osôb,

TAB je prínos z daňovo odpisovaného aktíva.[19]

3.4.6 Metódy prémií

Princípom metódy prémie je odhadnúť hodnotu nehmotného aktíva ako súčasnú hodnotu určitým spôsobom vyjadrenej hodnotovej prémie, ktorú môžeme prisúdiť vplyvu oceňovaného nehmotného aktíva.[19] Metódy prémií sa odvíjajú od výnosového prístupu oceňovania nehmotných aktív. Rozoznávame tieto prémie:

- **cenová prémia** – vychádza z predpokladu, že výrobok v ktorom sa oceňované aktívum nachádza sa predáva za vyššiu cenu ako výrobok rovnakej funkcie, v ktorom sa oceňované aktívum nenachádza. Matematický vzorec (6) na výpočet hodnoty pomocou metódy cenovej prémie:

$$HNA = \sum_{t=1}^{n} \frac{Q_t * (P_{ts} - P_{tBEZ}) * K_t * (1-d)}{(1+i)^t} + TAB \quad (6)$$

kde Q_t je objem predanej produkcie v MJ,

P_{ts} je cena výrobku, ktorý obsahuje oceňované nehmotné aktívum,

P_{tBEZ} je cena výrobku bez oceňovaného nehmotné aktívum,

K_t je index zastarania (pri technických riešeniach),

TAB je prínos z daňovo odpisovaného aktíva,

n je životnosť nehmotného aktíva.[19]

- **zisková prémia** – podobne ako cenová prémia rozlišuje výrobok s a bez obsahu nehmotného aktíva, ale hodnota týchto výrobkov je meraná výškou zisku, resp. marže. Matematický vzorec (7) na vyjadrenie hodnoty pomocou metódy ziskovej prémie je:

$$HNA = \sum_{t=1}^{n} \frac{T_t * (ZM_{ts} - ZM_{tBEZ}) * K_t * (1-d)}{(1+i)^t} + TAB \quad (7)$$

kde ZM_{ts} je zisková marža výrobku, ktorý obsahuje oceňované nehmotné aktívum,

ZM_{tBEZ} je zisková marža výrobku bez oceňovaného nehmotné aktívum,

T_t sú tržby za výrobky obsahujúce oceňované aktívum.[19]

- **nákladová prémia** – predpokladá, že výrobok s oceňovaným nehmotným aktívom vytvára nákladovú úsporu oproti výrobku bez oceňovaného aktíva pri porovnateľných cenách a vyrobených množstvách výrobkov. Matematický sa hodnota oceňovaného aktíva podľa metódy nákladovej prémie vypočíta zo vzorca (8):

$$HNA = \sum_{t=1}^{n} \frac{Q_t * (N_{tBEZ} - N_t) * K_t * (1-d)}{(1+i)^t} + TAB \quad (8)$$

kde N_{ts} sú priemerné prevádzkové náklady výrobku, ktorý obsahuje oceňované nehmotné aktívum,

N_{tBEZ} sú priemerné prevádzkové náklady výrobku bez oceňovaného nehmotné aktívum.[19]

- **prémia z výnosnosti kapitálu** – táto metóda porovnáva rentability kapitálov podniku s výrobkom používajúcim oceňované aktívum a porovnateľných podnikov s výrobkom bez oceňovaného aktíva. Hodnotu nehmotného aktíva podľa metódy prémie z výnosnosti kapitálu vypočíta podľa vzorca (9):

$$HNA = \sum_{t=1}^{n} \frac{A_t * (ROA_{ts} - ROA_{tBEZ}) * K_t * (1-d)}{(1+i)^t} + TAB \quad (9)$$

kde A_t sú prevádzkovo potrebné aktíva podniku používajúceho nehmotné aktívum,

ROA_{ts} je rentabilita aktív podniku obsahujúce oceňovaného nehmotné aktívum,

ROA_{tBEZ} je rentabilita aktív podniku bez oceňovaného nehmotného aktíva,

K_t je index zastarania (pri technických riešeniach),

TAB je prínos z daňovo odpisovaného aktíva,

n je životnosť nehmotného aktíva.[19]

3.5 Komparácia pozitív a negatív rôznych prístupov oceňovania

V predchádzajúcich častiach diplomovej práce sú podrobne popísané prístupy a metódy oceňovania hmotných a nehmotných aktív. Každý z týchto prístupov má svoje pozitíva a negatíva, ktoré ho charakterizujú. Každá metóda môže mať svoje potenciálne uplatnenie v hospodárskej praxi vrátane obdobia kybernetických útokov.

- **nákladový prístup** predpokladá, že hmotné a nehmotné aktíva môžu byť ocenené na základe minulých nákladov, ktoré boli vynaložené pri jeho vzniku. Náklady sú prepočítané na súčasnú hodnotu, alebo ako súčet nákladov, ktoré by museli byť vynaložené na rovnaký alebo veľmi podobný majetok v prípade, že by sme ho chceli vytvoriť znova. Problémom pri tejto metóde môže byť slabá väzba medzi vynaloženými nákladmi, čiže hodnotou a jej budúcimi prínosmi (či už v podobe zisku, alebo výnosov). Druhým problémom môže byť fakt, že hodnota pre majiteľa hmotného resp. nehmotného aktíva môže byť o mnoho vyššia než hodnota, ktorú vyčíslime pomocou minulých nákladov.
- **výnosový prístup** má veľké množstvo pozitív a negatív podobne ako ostatné prístupy oceňovania. V hospodárskej praxi je však aplikovaný častejšie ako nákladový prístup, a to najmä v prípade nehmotných aktív podniku, no dá sa aplikovať aj pre hmotné aktíva. Vychádza sa z predpokladu budúceho výnosu, ktorý nám daný hmotný resp. nehmotný majetok prinesie. Výnosové prístupy sú preferované najmä u aktív, pre ktoré sú budúce výnosy pomerne isté a hrozí len pomerne nízka miera rizík. Výnosový prístup je tak do značnej miery determinovaný stabilitou podnikateľského prostredia.
- **porovnávací prístup** stanovuje hodnotu hmotného resp. nehmotného aktíva na základe porovnania cien rovnakých alebo veľmi podobných aktív na relevantnom

trhu. Problémom porovnávacieho prístupu je skutočnosť, že v hospodárskej praxi sa len veľmi ťažko získavajú potrebné informácie o cenách, dodacích podmienkach a ďalších parametroch obchodov. Problémom môže byť aj identifikovanie porovnateľného aktíva. Značná časť hmotného aj nehmotného majetku je veľmi špecifická a nájsť na trhu rovnaký, alebo aspoň veľmi podobný majetok je priam nemožné.

Nasledujúca tabuľka prehľadne porovnáva najdôležitejšie pozitíva a negatíva jednotlivých oceňovacích prístupov.

Tabuľka 1 Komparácia pozitív a negatív oceňovacích prístupov

Prístupy	Pozitíva	Negatíva
Nákladový	• Podstatou je založený na jednoduchom princípe ekonomickej substitúcie. • Identifikácia a celková výška nákladov je jednoducho dostupná. • Pomerne jednoduchý a rýchly spôsob výpočtu ceny aktíva. • Prínosný najmä v situáciách, keď budúci prínos aktíva nie je jednoznačný. • Hodnota oceňovaného aktíva sa hneď po vzniku odzrkadlí v účtovníctve	• Výsledok ocenenia aktíva nereprezentuje potenciálny úžitok z daného aktíva. • Pri kvantifikácii ceny tento prístup neberie do úvahy budúce výnosy, ktoré môže v budúcnosti aktívum prinášať. • Náklady nie sú konštantné a v čase sa menia. • Neexistuje priama interakcia medzi nákladmi na aktívum a trhovou hodnotou aktíva.
Výnosový	• Vychádza z predpokladu budúceho ekonomického výnosu. • Kvantifikácia ceny nie je matematicky ani časovo náročná. • Potrebné informácie a údaje sú vo väčšine prípadov dostupné z evidencie podniku. • Výnosové prístupy sú všeobecne použiteľné pre väčšinu aktív.	• Nevýhodou prístupu je, že vychádza z neistých predpokladov budúceho vývoja, ktorý je vždy spojený s určitým rizikom. • Nevýhodou sú aj možné zmeny v ekonomickom prostredí, napríklad zmena úrokových mier. • Neexistuje priama interakcia medzi budúcimi výnosmi aktíva a trhovou hodnotou aktíva.
Porovnávací	• Podstatou je založený na jednoduchom princípe porovnávania cien.	• Potrebné informácie a údaje pre ocenenie nie sú vždy verejne dostupné, alebo nie sú úplné.

	• Ide o relatívne jednoduchý a rýchly prístup určenia ceny aktíva. • Berie do úvahy trhovú cenu porovnávaných aktív. • Porovnávacie prístupy sú všeobecne použiteľné pre väčšinu aktív.	• Nevyhnutným predpokladom je pomerne vysoká úroveň informatizácie ekonomiky. • Vysoko špecifické a jedinečné hmotné a nehmotné aktíva sa len veľmi ťažko porovnávajú.

II. PRAKTICKÁ ČASŤ

4 KYBERNETICKÁ BEZPEČNOSŤ VO VYBRANÝCH ORGANIZÁCIÁCH

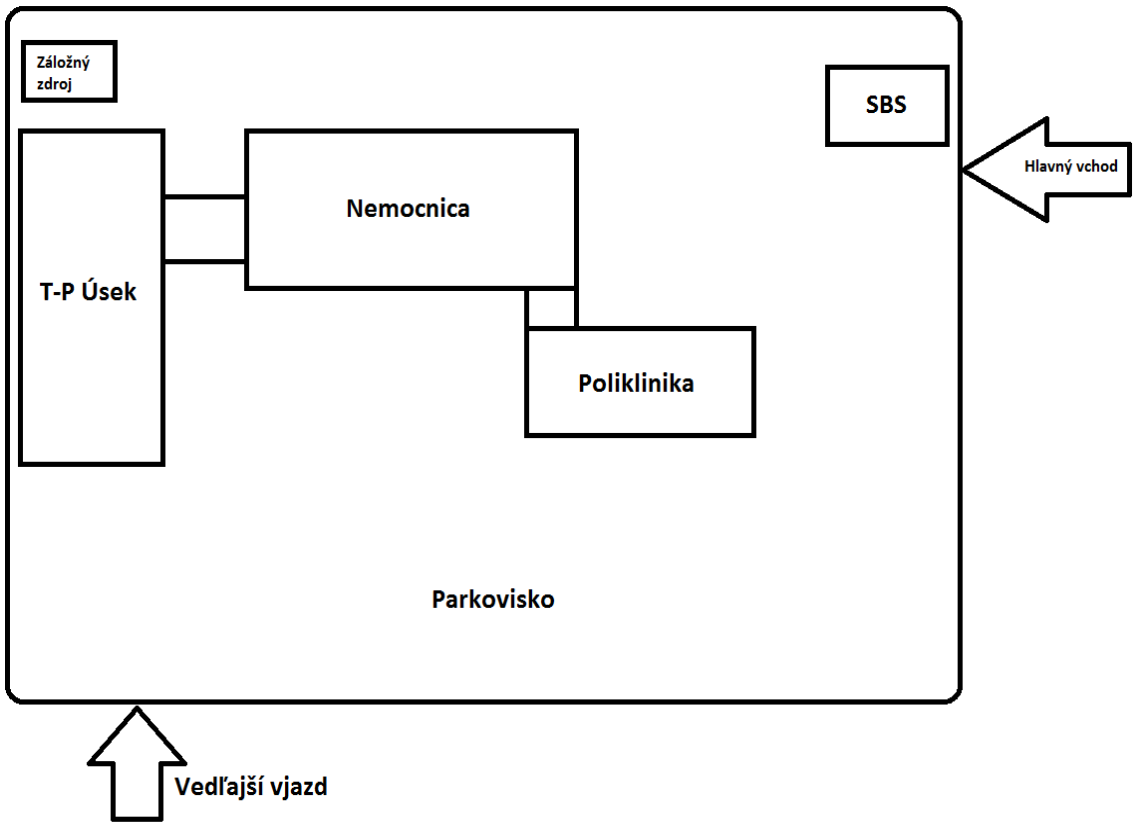
Pre stanovenie dopadov kybernetických hrozieb na organizácie si vymodelujeme hypotetické organizácie pôsobiace v súkromnom a verejnom sektore. Charakterizujeme si ich účel a predmet činnosti, organizačnú štruktúru, ich aktíva a technické vybavenie. Z hľadiska kybernetickej bezpečnosti si definujeme kybernetické hrozby, ktoré organizácie ohrozujú, na základe analýzy rizík určíme poradie troch najnebezpečnejších kybernetických hrozieb, pre ktoré spracujeme scenár vývoja bezpečnostnej situácie a dopadov na tieto hypotetické organizácie. Údaje potrebné k modelovaniu hypotetických organizácií budeme čerpať z verejne dostupných zdrojov, ako sú napríklad výročné správy a účtovné uzávierky podobne veľkých a v rovnakom odvetví pôsobiacich organizácií v Slovenskej republike. Prvou organizáciou je zdravotnícke zariadenie A poskytujúce ambulantnú a ústavnú zdravotnú starostlivosť a druhou je súkromná strojárska organizácia B pôsobiaca vo výrobnej sfére. V týchto organizáciách namodelujeme všetky údaje potrebné k stanoveniu dopadov kybernetických hrozieb.

4.1 Charakteristika zdravotníckeho zariadenia A

Zdravotnícke zariadenie A je nemocnica s poliklinikou s okresnou pôsobnosťou. Je to neštátne zdravotnícke zariadenie, ktoré poskytuje ucelenú zdravotnú a sociálnu starostlivosť pre spádovú oblasť cca 60000 obyvateľov. Zakladateľmi sú samosprávny kraj XY a nezisková organizácia XY, n.o.. Poskytovaná je primárna odborná starostlivosť, špecializovaná ambulantná a ústavná zdravotná starostlivosť na lôžkovej časti. Zdravotnícke zariadenie vykonáva aj hospodársko-technické činnosti v stanovenom rozsahu. Organizačná štruktúra nemocnice je líniovo – štábna. Na čele nemocnice s poliklinikou stojí generálny riaditeľ, ktorého volí správna rada. Riaditeľ má troch námestníkov, jedného pre ekonomický úsek, ďalšieho pre úsek liečebno-preventívnej starostlivosti a ošetrovateľstvo a posledného pre technicko-prevádzkový úsek. Nemocnica s poliklinikou má vlastný oplotený areál s jednou hlavnou vstupnou bránou a jednou vedľajšou, zásobovacou bránou a vstup osôb ako aj vjazd automobilov do areálu nemocnice je kontrolovaný vlastnou strážnou službou. Nemocnica s poliklinikou je umiestnená v zastavanom území okresného mesta a situovaná je na jeho okraji. So zdravotníckym zariadením susedí niekoľko priľahlých budov a verejných priestranstiev. Samotná nemocnica s poliklinikou je zložená z troch budov:

- štvorpodlažnej, v ktorej sídli poliklinika a dve operačné sály jednodňovej chirurgie,
- osempodlažnej, ktorá je sídlom lôžkových oddelení nemocnice a operačných sál,
- dvojpodlažnej, v ktorej je umiestnený ekonomický úsek spolu s technicko-hospodárskym úsekom.

Poliklinika disponuje 34 odbornými ambulanciami vrátane biochemického laboratória a pracoviska RTG, USG a CT. Ďalej sa v zdravotníckom zariadení nachádza päť operačných sál a dve operačné sály pre jednodňovú chirurgiu. V nemocničnej časti je na 12. lôžkových oddeleniach spolu 350 lôžok. Celkový počet zamestnancov v nemocnici s poliklinikou je 700.



Obrázok 6 Situačný plán areálu zdravotníckeho zriadenia [Vlastné spracovanie]

4.1.1 Informačné technológie

Hardvér

V zdravotníckom zariadení je vybudovaná počítačová sieť typu klient-server, ktorá prepája jednotlivé pracovné stanice, medicínske a diagnostické prístroje, tlačiarne, sieťové prvky

a serveri. Fyzicky ju tvorí štruktúrovaná kabeláž, ktorá je z jednotlivých kancelárií, ambulancií, vyšetrovní, laboratórií a ostatných miestností zdravotníckeho zariadenia inštalačnými tunelmi, alebo žľabmi privedená do jednotlivých dátových rozvádzačov umiestnených v rozvodných miestnostiach. Tie sa nachádzajú na každom poschodí vo všetkých troch budovách zdravotníckeho zariadenia. V dátových rozvádzačoch sú umiestnené prístupové switche, cez ktoré je užívateľ pripojený pomocou prepojovacích káblov do počítačovej siete zdravotníckeho zariadenia a záložné zdroje UPS. V jednotlivých kanceláriách nemedicínskych pracovísk, ambulanciách, vyšetrovniach na lôžkových oddeleniach a ostatných medicínskych pracoviskách sa nachádza spolu 241 osobných počítačov, diagnostických a laboratórnych prístrojov, ktoré sú takýmto spôsobom pripojené do siete.

Tabuľka 2 Prehľad zariadení pripojených do počítačovej siete na budove T-P úseku

Oddelenie	**PC, tlačiarne, prístroje**
Generálny riaditeľ, sekretariát	2
Námestníci, sekretariát	6
Ekonomický úsek	25
Úsek LPS a O	15
T-P úsek	23
Spolu	**71**

Tabuľka 3 Prehľad zariadení pripojených do počítačovej siete na budove polikliniky

Oddelenie	**PC, tlačiarne, prístroje**
Ambulancia audiometrie a fonometrie	3
Ambulancia cievnej chirurgie	4
Ambulancia dermatovenerologická	2
Ambulancia diabetologická	3
Ambulancia endokrinologická	3
Ambulancia gastroenterologická	4
Ambulancia geriatrická	2
Ambulancia gynekologicko-pôrodnícka	3
Ambulancia chemoterapeutická	3
Ambulancia chirurgická	3

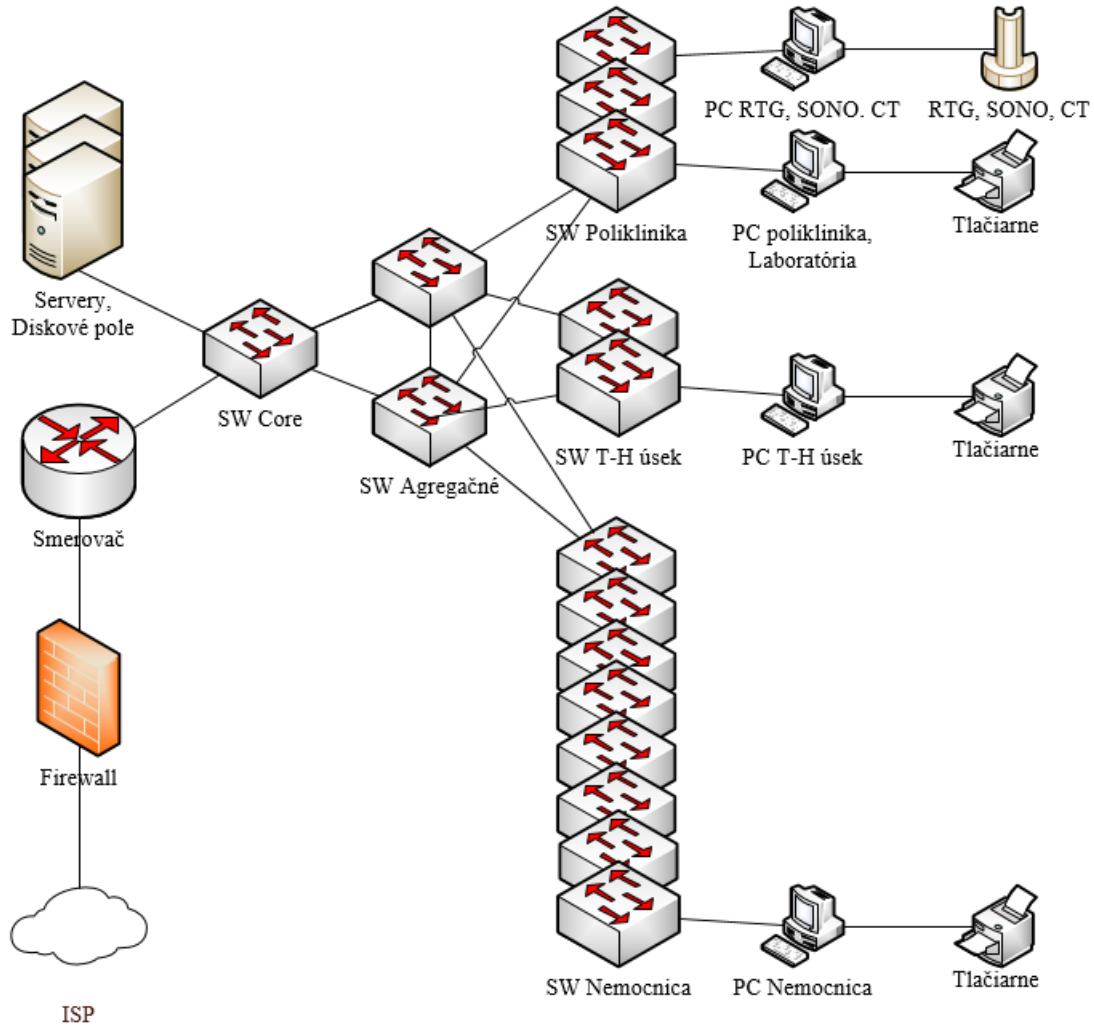
Ambulancia infektologická	2
Ambulancia kardiologická	3
Ambulancia klinickej hemat. a transf.	2
Ambulancia klinickej onkológie	2
Ambulancia klinickej psychológie	2
Ambulancia neonatológie	2
Ambulancia neurologická	2
Ambulancia oftalmologická	5
Ambulancia ortopedická	2
Ambulancia otorinolaringologická	4
Ambulancia pediatrická	2
Ambulancia pneumologická	3
Ambulancia radiačnej onkológie	4
Ambulancia reumatologická	3
Ambulancia urologická	2
Klinické laboratória	20
Ambulancia vnútorného lekárstva	3
CT pracovisko	4
USG pracovisko	6
RTG pracovisko	4
Spolu	**107**

Tabuľka 4 Prehľad zariadení pripojených do počítačovej siete na budove nemocnice

Oddelenie	**PC, tlačiarne, prístroje**
Operačné sály	28
Oddelenie AIM	10
Oddelenie dlhodobo chorých	2
Geriatrické oddelenie	2
Oddelenie gynekológie a pôrodníctva	2
Chirurgické oddelenie	2
Oddelenie onkológie a rádioterapie	5
Neurologické oddelenie	2
Ortopedické oddelenie	2
Pediatrické oddelenie	2
Urologické oddelenie	2
Oddelenie úrazovej chirurgie	2
Oddelenie vnútorného lekárstva	2
Spolu	**63**

Prístupové switche, umiestnené v dátových rozvádzačoch na jednotlivých poschodiach v budovách zdravotníckeho zariadenia, sú priamym up-linkom pripojené k dvom distribučným switchom, umiestneným v dátovom rozvádzači v hlavnej serverovej miestnosti, ktorá sa nachádza v suteréne budovy technicko-prevádzkového a ekonomického úseku. Počítačová sieť v takomto stromovom zapojení je rozdelená do segmentov, ktoré umožňujú jej fyzickú škálovateľnosť. Logický je počítačová sieť rozdelená prostredníctvom VLAN na segmenty určené pre medicínskych zamestnancov, pre ekonomické oddelenie, personálne oddelenie, management siete apod. V hlavnej serverovej miestnosti sú umiestnené serveri s diskovými poľami kam sú ukladané všetky dáta. Ďalej v hlavnom dátovom rozvádzači je umiestnený router určený pre pripojenie zdravotníckeho zariadenia k internetu, hardvérový firewall, dva core switch pre prepojenie serverov, routra a distribučných switchov, záložný zdroj UPS spolu s batériami. Ďalej je tu umiestnený aj hlavný elektrický rozvádzač spolu s ovládacími, meracími a regulačnými prvkami pre motor generátor, ktorý slúži ako záložný zdroj napájania celého zdravotníckeho zariadenia. Vo vybraných miestnostiach, hlavne na operačných sálach, ale aj niektorých kanceláriách a ambulanciách je nainštalovaná vzduchotechnika, ktorá spolu so záložným zdrojom je

kontrolovaná prostredníctvom priemyselného počítača. Bezdrôtové pripojenie k internetu prostredníctvom Wi-Fi nie je realizované.



Obrázok 7 Schéma počítačovej siete zdravotníckeho zariadenia [Vlastné spracovanie]

Softvér

Na serveroch sú nainštalované serverové operačné programy systému LINUX a Windows Server 2019. Databáza je postavená na platforme Microsoft SQL. Správa serveru je možná len pomocou vzdialenej plochy. Na aktívnych prvkoch siete sú spustené sieťové operačné programy Cisco IOS od verzie 15.0 a vyššie, ktoré smeruje prevádzku do a z internetu a prepínajú prevádzku v samotnej sieti. Na firewalle Cisco ASA je spustený operačný systém na kontrolu dátovej prevádzky vrátane inšpekcie paketov, ktorá smeruje do a z vnútornej počítačovej siete zdravotníckeho zariadenia. V zdravotníckom zariadení je

nainštalovaný Komplexný nemocničný informačný systém (KNIS), ktorý je určený na zber, spracovávanie, uchovávanie, distribúciu, interpretáciu a adresné sprístupňovanie informácií o pacientoch, evidencií materiálu, personálnu a ekonomickú agendu priamo pre nemocnicu, jej ambulantné zariadenia a obslužné útvary v pôsobnosti zdravotníckeho zariadenia. Zohľadňuje vnútornú organizačnú štruktúru zdravotníckeho zariadenia, nazerá na neho ako na celok a súčasne spracováva požiadavky pre zmluvných dodávateľov zdravotníckeho zariadenia ako sú napríklad zdravotné poisťovne, alebo rôzne dodávateľské firmy.

Zdravotnícke zariadenie používa aj informačný systém PACS na bez filmovú správu, distribúciu a archiváciu všetkých rádiologických vyšetrení, personálny a dochádzkový systém VEMA, ekonomický informačný systém HELIOS a informačný systém CGM S4M pre pracovisko klinickej mikrobiológie. Prehľad systémov, ich účelov a funkcií uvádzame v nasledujúcej tabuľke.

Tabuľka 5 Prehľad softvérov používaných v zdravotníckom zariadení

Informačný systém	Účel	Funkcie	Oddelenie
HELIOS	ekonomický softvér	platby pre dodávateľov, platby za služby, mzdy zamestnancov, účtovanie platieb pre poisťovne	ekonomické oddelenie, ambulancie, nemocnica
VEMA	personálny a dochádzkový softvér	evidencia prítomnosti na pracovisku, evidencia obsadenosti pracovných pozícií	personálne oddelenie, ambulancie, nemocnica
KNIS	Komplexný nemocničný informačný systém	evidencia pacientov, manažment pacientov, správa zdravotníckeho materiálu a liekov,	ambulancie, nemocnica, oddelenia služieb
CGM S4M	softvér pre laboratória	správa a evidencia žiadaniek na vyšetrenie, výsledky laboratórnych vyšetrení	laboratória, ambulancie, nemocnica
PACS	bez filmový softvér pre správu rádiologických vyšetrení	správa a evidencia žiadaniek na vyšetrenie, výsledky rádiologických vyšetrení	RTG, CT, USG pracoviská

Počítače sú chránené prístupovými heslami k jednotlivým účtom. Na počítačoch sú nainštalované operačné systémy Windows 7 Pro a 10. Na vybraných počítačoch je nainštalovaný program na obsluhu a ovládanie medicínskych prístrojoch, ako sú napríklad počítačový tomograf, prístroj na ultrazvukové vyšetrovanie, röntgen, prístroje na diagnostiku a rozbor telesných tekutín a pod. Na počítačoch je nainštalované komerčné riešenie antivírového programu ESET End point Antivírus. Systémy nepodliehajú žiadnemu

obmedzeniu z pohľadu manipulácie s dátami či dátovými nosičmi vrátane USB pamäťových diskov. Prístup k intranetu a internetu, ako aj možnosť sťahovať akékoľvek dáta, je po prihlásení sa svojím účtom možné na všetkých počítačoch.

V ordinácii je využívaný Komplexný nemocničný informačný systém na vedenie elektronickej zdravotnej dokumentácie pacientov, ktorý umožňuje tlačenie receptov, žiadaniek či ďalších formulárov. Fyzická karta pacienta je uložená v kartotéke príslušnej ambulancie. Chorobopis pacienta je po celú dobu hospitalizácie umiestnený na lôžkovom oddelení. Pri ukončení tejto hospitalizácie je staničnou sestrou skompletizovaný a odovzdaný dokumentačnej pracovníčke daného oddelenia k vyúčtovaniu poskytnutej zdravotnej starostlivosti. Tá po zaúčtovaní všetkých vykonaných výkonov a poskytnutých liekov odovzdáva chorobopis k ďalšej kontrole, a to na oddelenie zdravotných poisťovní. Vopred určený pracovník, podľa prideleného oddelenia, vykonáva záverečnú kontrolu správnosti vykázanej starostlivosti. Následne je chorobopis vrátený späť na oddelenie dokumentačnej sestre, ktorá vedie archív zdravotnej dokumentácie daného oddelenia.

Komplexný nemocničný informačný systém obsahuje modul, ktorý manažuje pacientov a upozorňuje sestry a lekárov na kontrolné alebo preventívne vyšetrenia pacientov. Ďalej sa tu nachádza databáza liečiv a rôzne štatistické nástroje, ktoré využívajú hlavne lekári. Priamo zo systému je potom možné tlačiť zostavy pre zdravotné poisťovne. Komplexný nemocničný informačný systém obsahuje rozhranie, pomocou ktorého odosiela laboratóriá výsledky laboratórnych testov priamo lekárom, ktorí predmetné vyšetrenie žiadali. Na komunikáciu s pacientami, ale aj so zmluvnými dodávateľmi zamestnanci a lekári využívajú z veľkej časti e-mail. Do počítačov sa zamestnanci prihlasujú svojím jedinečným heslom do vytvoreného účtu. Práva na prístup do informačného systému zdravotníckeho zariadenia prideľuje oddelenie informačných technológií na základe žiadostí vedúceho, alebo nadriadeného zamestnanca. Vstupy do jednotlivých kancelárií a ambulancií má na starosti každý pracovník, ktorému je kancelária, alebo ambulancia pridelená. Na lôžkových oddeleniach je personál prítomný nepretržite. V prípade mimoriadnej udalosti sú pre každú miestnosť náhradné kľúče uložené v miestnosti strážnej služby.

4.1.2 Ohrozené prvky zdravotníckeho zariadenia z pohľadu kybernetickej bezpečnosti a ich hodnota

Na to, aby sme mohli stanoviť najdôležitejšie prvky organizácie, potrebujeme ich ohodnotiť podľa dôležitosti, ktorú predstavujú pre organizáciu. Použijeme na to škálu čísel od 1 po 5, kde číslo 1 je najmenej dôležitý a číslo 5 je najviac dôležitý prvok pre organizáciu z pohľadu kybernetickej bezpečnosti.

Tabuľka 6 Ohrozené prvky zdravotníckeho zariadenia

Ohrozený prvok	Dôležitosť ohrozeného prvku
servery	**5**
diskové polia	**5**
router	**5**
switche	**5**
počítače	**3**
diagnostické prístroje	**5**
záložný zdroj elektrickej energie	**5**
tlačiarne	**1**
operačné systémy	**4**
KNIS	**5**
databázový systém	**5**
medicínsky a laboratórny softvér	**5**
náklady na rekonštrukciu dát	**5**
náklady na obnovu dát	**5**
ušlý zisk	**5**
pokuta od kontrolných orgánov	**5**
poškodenie vzťahov s pacientami	**5**
poškodenie vzťahov s dodávateľmi	**5**

4.1.3 Hodnotenie aktív

Aktíva sú ohodnotené z pohľadu posúdenia požiadaviek na dostupnosť, integritu a dôvernosť dát. Škála je stanovená na základe hodnotiacich kritérií 1 až 5, pričom 1 sú

najmenej dôležité aktíva a 5 sú najdôležitejšie aktíva. Výsledná hodnota je vypočítaná ako aritmetický priemer všetkých troch hodnôt a zaokrúhlená na celé číslo.

Tabuľka 7 Prehľad aktív zdravotníckeho zariadenia

Aktíva zdravotníckeho zariadenia	Dostupnosť	Dôvernosť	Integrita	Hodnota
elektronická zdravotná dokumentácia	5	5	5	**5**
papierová zdravotná dokumentácia	2	5	4	**4**
archivovaná (papierová) zdravotná dokumentácia	2	5	4	**4**
personálne a účtovné dáta	2	5	3	**3**
zálohy na serveri	4	5	4	**4**
dodávateľské zmluvy	3	5	5	**4**
KNIS	5	5	5	**5**
operačný systém Windows Server 2019, Linux	5	5	5	**5**
počítače	3	5	4	**4**
periférne zariadenie (UPS, tlačiarne)	2	2	3	**2**
servery	5	5	5	**5**
aktívne sieťové prvky	4	5	5	**5**

Na základe hodnotenia vyplýva, že najvyššie nároky na dôvernosť, integritu a dostupnosť dát majú tieto aktíva zdravotníckeho zariadenia:

- elektronická zdravotná dokumentácia,
- Komplexný nemocničný informačný systém,
- operačné systémy serverov, počítačov a diagnostických prístrojov,
- servery,
- aktívne sieťové prvky.

4.1.4 Identifikácia hrozieb a analýza rizík zdravotníckeho zariadenia

Ďalším predpokladom pre úspešnú analýzu rizík je identifikácia, ohodnotenie a pravdepodobnosť dopadu hrozieb, ktoré pôsobia, alebo môžu pôsobiť na zdravotnícke

zariadenie. Je dôležité stanoviť stupnicu závažnosti negatívneho dopadu hrozby na aktíva organizácie a stupnicu pravdepodobnosti výskytu hrozby. Hodnotiaca škála pre závažnosť dopadu hrozby je stanovená opäť od hodnoty 1 pre veľmi malú závažnosť negatívneho dopadu hrozby, až do hodnoty 5 pre katastrofickú závažnosť dopadu hrozby.

Tabuľka 8 Úrovne závažnosti dopadu hrozby

Závažnosť dopadu hrozby	**Označenie**	**Popis**
Veľmi nízka	1	Veľmi malý negatívny dopad na činnosť organizácie
Nízka	2	Malý negatívny dopad na činnosť organizácie
Stredne vysoká	3	Závažný negatívny dopad na činnosť organizácie
Vysoká	4	Veľmi závažný negatívny dopad na činnosť organizácie
Veľmi vysoká	5	Katastrofický dopad na činnosť organizácie

Nasledujúca tabuľka zobrazuje možné hrozby pôsobiace na zdravotnícke zariadenie a vyjadrenie úrovne závažnosti dopadu takejto hrozby.

Tabuľka 9 Dopady kybernetických hrozieb na aktíva zdravotníckeho zariadenia

Hrozba	**Úroveň závažnosti dopadu hrozby**
poškodenie výpadkom elektrickej energie	**2**
ransomware	**5**
počítačový vírus	**4**
zlyhanie softvéru	**4**
zlyhanie pripojenia	**2**
zlyhanie hardvéru	**3**
odpočúvanie komunikácie	**4**
neoprávnený prístup	**5**
falšovanie identity	**3**

chyba užívateľa	**3**
krádež dát	**4**
úmyselné poškodenie	**2**
prezradenie tajných informácií	**3**

Stupnica pravdepodobnosti existencie hrozby na zdravotnícke zariadenie je tak isto stanovená od najmenšej hodnoty 1 pre nepatrnú pravdepodobnosť existencie až po najvyššiu hodnotu 5 pre pravdepodobnú pravdepodobnosť výskytu hrozby na zdravotnícke zariadenie.

Tabuľka 10 Úrovne pravdepodobnosti existencie hrozby

Pravdepodobnosť výskytu hrozby	**Označenie**	**Popis**
Nepatrná	1	K narušeniu bezpečnosti takmer nedochádza
Málo možná	2	K nar. bezpeč. dochádza veľmi málo, ale netreba ju zanedbať
Niekedy	3	Narušenie bezpečnosti sa v okolí vyskytuje občas
Niekoľkokrát	4	Narušenie bezpečnosti sa v okolí vyskytuje často
Vzniká veľmi často	5	Narušenie bezpečnosti je pravdepodobné

Pravdepodobnosť existencie konkrétnej kybernetickej hrozby na zdravotnícke zariadenie sme zobrazili v nasledujúcej prehľadnej tabuľke.

Tabuľka 11 Pravdepodobnosť existencie kybernetickej hrozby

Hrozba	**Pravdepodobnosť existencie hrozby**
poškodenie výpadkom elektrickej energie	**3**
ransomware	**5**
počítačový vírus	**4**
zlyhanie softvéru	**5**
zlyhanie pripojenia	**3**
zlyhanie hardvéru	**4**
odpočúvanie komunikácie	**4**
neoprávnený prístup	**5**
falšovanie identity	**3**
chyba užívateľa	**4**
krádež dát	**4**
úmyselné poškodenie	**2**
prezradenie tajných informácií	**3**

Na základe predchádzajúcich ohodnotenia aktív a hodnotenia pravdepodobnosti existencie hrozieb sme zostavili maticu zraniteľnosti, ktorá vyjadruje zraniteľnosť aktíva zdravotníckeho zariadenia konkrétnou kybernetickou hrozbou. V matici figurujú aktíva zdravotníckeho zariadenia a pravdepodobnosť existencie kybernetických hrozieb, ktoré môžu na tieto aktíva pôsobiť.

Tabuľka 12 Matica zraniteľnosti aktíva zdravotníckeho zariadenia hrozbou

Zraniteľnosť V	**A** ↓	**Výpadok el. energie**	**Ransomware**	**Počítačový vírus**	**Zlyhanie softvéru**	**Zlyhanie pripojenia**	**Zlyhanie hardvéru**	**Odpočúvanie komunikácie**	**Neoprávn. prístup**	**Falšovanie identity**	**Chyba užívateľa**	**Krádež dát**	**Úmyselné poškodenie**	**Prezradenie utaj. inf.**
T →		**3**	**5**	**4**	**5**	**3**	**4**	**4**	**5**	**3**	**4**	**4**	**2**	**3**
El. zdravotná dokumentácia	**5**	3	4	5	5	4	4	4	5	4	5	5	4	5
Papierová zdrav. dokumentácia	**4**								5	5	3	5	4	5
Archivovaná zdrav. dok.	**4**								3	3	3	5	5	3
Personálne a účtov. dáta	**3**	2	4	4	2	1	1	2	4	3	3	5	4	5
Zálohy na serveri	**4**	5	5	5	4	4	5	4	5	3	4	5	4	5
Dodávateľské zmluvy	**4**									3	2	3	2	3
KNIS	**5**	4	4	4	5	3	4	5	5	4	4	5	3	3
Operačný systém	**5**	4	4	5	4	4	3	3	4	2	4	2	3	1
Počítače	**4**	5	4	4	1	1	4	2	4	4	4	1	3	1
Periférne zar.	**2**	3	2	2			3			1	2		1	
Servery	**5**	5	5	5	4	5	5	5	5	5	2	5	4	3
Aktívne sieťové prvky	**5**	4	3	5	3	3	3	4	4	4	2		2	2

4.1.5 Výpočet miery rizika

Nasledujúcim krokom pri analýze rizík je vypočítanie miery rizika podľa vzorca (10):

$$R = T * A * V \tag{10}$$

kde: R je miera rizika,

T je pravdepodobnosť vzniku hrozby,

A je hodnota aktíva pre organizáciu,

V je zraniteľnosť aktíva.[18]

Pri najvyššej pravdepodobnosti výskytu hrozby (5), najvyššej hodnote aktíva (5) a najväčšej zraniteľnosti (5) je dosiahnutá maximálna výsledná hodnota rizika, ktorá dosahuje úroveň 125. V nasledujúcej tabuľke predstavujeme maticu rizík R, ktorá vychádza z predchádzajúcich získaných hodnôt.

Tabuľka 13 Farebná úroveň hodnotenia rizík

Hodnota	Miera rizika
0 – 10	bezvýznamné riziko
11 – 30	akceptovateľné riziko
31 – 50	mierne riziko
51 – 70	nežiadúce riziko
71 – a viac	neprijateľné riziko

Tabuľka 14 Matica rizík zdravotníckeho zariadenia

Riziko **R**	**A** ↓	**Výpadok el. energie**	**Ransomware**	**Počítačový vírus**	**Zlyhanie softvéru**	**Zlyhanie pripojenia**	**Zlyhanie hardvéru**	**Odpočúvanie komunikácie**	**Neoprávn. prístup**	**Falšovanie identity**	**Chyba užívateľa**	**Krádež dát**	**Úmyselné poškodenie**	**Prezradenie utaj. inf.**
T →		**3**	**5**	**4**	**5**	**3**	**4**	**4**	**5**	**3**	**4**	**4**	**2**	**3**
El. zdravotná dokumentácia	**5**	**45**	**100**	**100**	**125**	**60**	**80**	**80**	**125**	**60**	**100**	**100**	**40**	**75**
Papierová zdrav. dok.	**4**								**100**	**60**	**48**	**80**	**32**	**60**
Archivovaná zdrav. dok.	**4**								**60**	**36**	**48**	**80**	**40**	**36**
Personálne a účtov. dáta	**3**	**18**	**60**	**48**	**30**	**9**	**12**	**24**	**60**	**27**	**36**	**60**	**24**	**45**
Zálohy na serveri	**4**	**60**	**100**	**80**	**80**	**48**	**80**	**64**	**100**	**36**	**64**	**80**	**32**	**60**
Dodávateľské zmluvy	**4**									**36**	**32**	**48**	**16**	**36**
KNIS	**5**	**60**	**100**	**80**	**125**	**45**	**80**	**100**	**125**	**60**	**80**	**100**	**30**	**45**
Operačný systém	**5**	**60**	**100**	**100**	**100**	**60**	**45**	**60**	**100**	**30**	**80**	**40**	**30**	**15**
Počítače	**4**	**60**	**80**	**64**	**20**	**12**	**64**	**32**	**80**	**48**	**64**	**16**	**24**	**12**
Periférne zariadenia	**2**	**18**	**20**	**16**			**24**			**6**	**16**		**4**	
Servery	**5**	**75**	**125**	**100**	**100**	**75**	**100**	**100**	**125**	**75**	**40**	**100**	**40**	**45**
Aktívne sieťové prvky	**5**	**60**	**75**	**100**	**45**	**45**	**45**	**80**	**100**	**60**	**40**		**20**	**30**

Z analýzy rizík nám vychádza, že najväčšie riziká vznikajú pri pôsobení hrozieb na zdravotnú dokumentáciu v elektronickej podobe uloženú v nemocničnej databáze vrátane ich záloh, na Komplexný nemocničný informačný systém, operačné systémy serverov a aktívne sieťové prvky. Ako možné hrozby podľa analýzy rizík sú počítačový vírus, ransomware a neoprávnený prístup.

4.1.6 Vývoj kybernetickej situácie a dopady na zdravotnícke zariadenie

V nasledujúcich tabuľkách je prehľadne popísaný časový prehľad prebiehajúcich útokov, ktorých prvkov sa útok týka, aké sú dopady jednotlivých útokov a aký mal útok dopad na funkčnosť zdravotníckeho zariadenia.

Útok prostredníctvom počítačového vírusu

Tabuľka 15 Prehľad útoku počítačovým vírusom

Čas	Činnosť	Poškodené prvky/aktíva firmy	Dopady na zdravotnícke zariadenie	Funkčnosť zariadenia
0	prijatý email s infikovanou prílohou			100%
0 - 15 min	otvorenie infikovanej prílohy a aktivovanie škodlivého kódu			100%
15 - 25 min	škodlivý kód poškodzuje programy v PC	počítače zdravotníckeho zariadenia	zavírované počítače sa nedajú použiť na prácu a vyšetrovanie pacientov, nemožnosť prístupu k dátam na diskoch, ušlý zisk	75%
25 - 60 min	vypnutie napadnutých počítačov	počítače zdravotníckeho zariadenia	zavírované počítače sa nedajú použiť na prácu a vyšetrovanie pacientov, nemožnosť prístupu k dátam na diskoch, ušlý zisk	75%
1 - 96 hod	prebieha preinštalovanie počítačov	napadnuté počítače zdravotníckeho zariadenia	neposkytuje všetky svoje služby, niektorých pacientov presúva do iných zariadení, ušlý zisk	75%
4 - 14 dní	čiastočné obnovenie	napadnuté počítače zdravotníckeho zariadenia	postupne obnovuje svoje činnosti, výpadok ušlého zisku sa zmenšuje	95%
po 14 dňoch	po preinštalovaní počítačov		náklady na obnovu, poskytuje všetky svoje služby	100%

Útok prostredníctvom škodlivého programu ransomeware

Tabuľka 16 Prehľad útoku škodlivým programom ransomware

Čas	Činnosť	Poškodené prvky/aktíva firmy	Dopady na zdravotnícke zariadenie	Funkčnosť zariadenia
0	prijatý email s infikovanou prílohou			100%
0 - 10 min	otvorenie infikovanej prílohy a aktivovanie škodlivého kódu, škodlivý program kontaktuje riadiaci server			100%
10 - 90 min	zašifrovanie dát na pevných diskoch, požadovanie výkupného	dáta o pacientoch uložené na serveroch	nedá sa pristupovať k dátam, zariadenie nevyšetruje, ušlý zisk	25%
1,5 - 120 hod	prebieha preinštalovanie serverov zo zálohy	servery, dáta	neposkytuje všetky svoje služby, niektorých pacientov presúva do iných zariadení ušlý zisk	25%
5 - 20 dní	čiastočné obnovenie	servery, dáta	obnovenie svojej činnosti, výpadok ušlého zisku sa zmenšuje	65%
po 20 dňoch	po preinštalovaní serverov		náklady na obnovu, poskytuje všetky svoje služby	100%

Útok prostredníctvom neoprávneného prístupu

Tabuľka 17 Prehľad útoku ako neoprávnený prístup

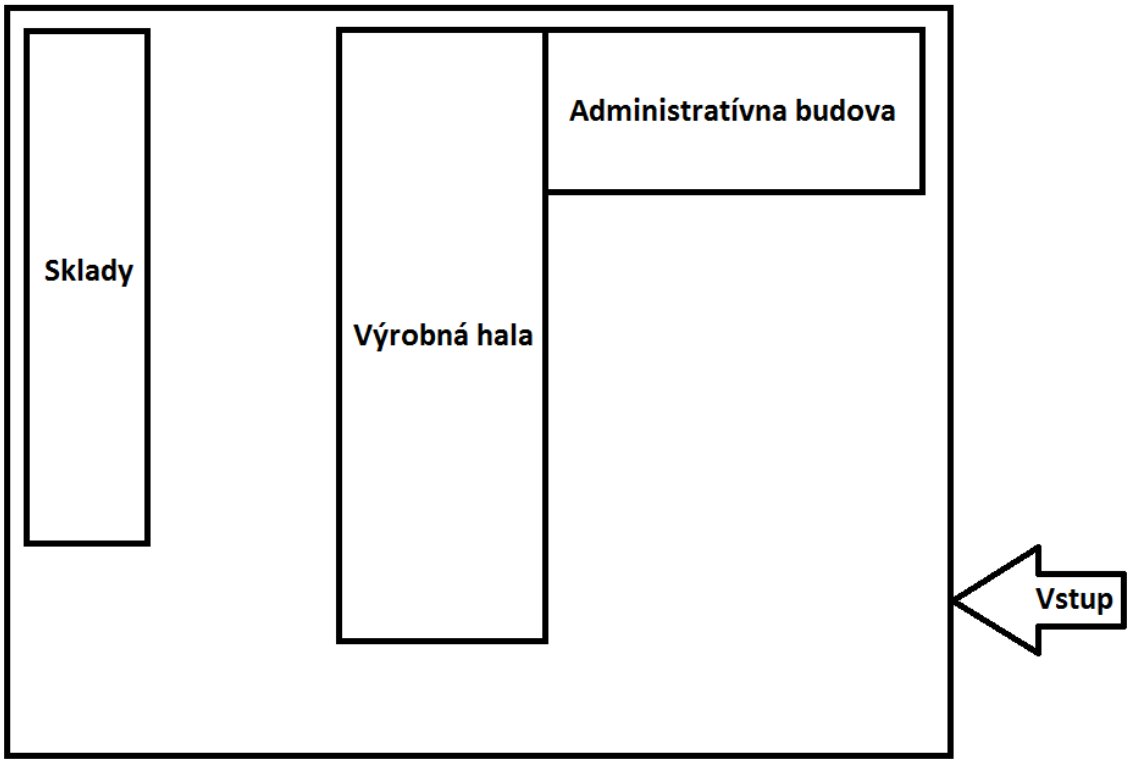
Čas	Činnosť	Poškodené prvky/aktíva firmy	Dopady na zdravotnícke zariadenie	Funkčnosť zariadenia
0	prelomenie hesla	informačný systém		100%
0 - 120 min	získanie ďalších prístupov	servery, dáta		100%
120 - 180 min	ukradnutie dát uložených na pevných diskoch,	dáta o pacientoch, zamestnancoch a dodávateľoch uložené na serveroch	nedá sa pristupovať k dátam, zariadenie nevyšetruje, nemedicínsky zamestnanci nepracujú, ušlý zisk	5%
3 - 144 hod	prebieha, preinštalovanie serverov, obnovovanie a rekonštrukcia dát zo zálohy	servery, dáta	neposkytuje všetky svoje služby, niektorých pacientov presúva do iných zariadení, ušlý zisk	5%
6 - 25 dní	čiastočné obnovenie	servery, dáta	obnovenie svojej činnosti, výpadok ušlého zisku sa zmenšuje	55%
po 25 dňoch	po preinštalovaní serverov		náklady na obnovu, poskytuje všetky svoje služby	100%

Podľa celosvetových výskumov je oblasť zdravotníctva jedným z najviac postihnutých odvetví v oblasti kybernetických útokov. Aj napriek narastajúcej hrozbe veľká väčšina nemocníc a zdravotníckych zariadení nie je pripravená kybernetickým hrozbám čeliť. Ako najčastejšie kybernetické útoky sa spomínajú ransomware, únik citlivých údajov o pacientoch a phisingové maily nabádajúce zamestnancov, aby klikli na nebezpečný internetový odkaz. Analýza kybernetických hrozieb na hypotetické zdravotnícke zariadenie potvrdila, že takéto útoky sú reálne a zdravotnícke zariadenia by sa mali obranou pred kybernetickými hrozbami vážne zaoberať.

4.2 Charakteristika strojárskej firmy B

Strojárska firma B je súkromná spoločnosť s právnym štatútom spoločnosti s ručením obmedzeným (s.r.o.). Pôsobí v strojárenskej oblasti a hlavným výrobným programom spoločnosti je výroba oceľových komponentov do prevodoviek automobilov niekoľkých

značiek. Okrem toho sa spoločnosť venuje aj malosériovej strojárskej výrobe priemyselných strojov, strojárskeho náradia a nástrojov. Strojárska firma bola založená dvomi spoločníkmi a v mene spoločnosti vystupuje jeden konateľ. Organizačná štruktúra strojárskej firmy je líniovo - štábna. Konateľ spoločnosti je súčasne aj riaditeľ, ktorý má v podriadenosti výrobného riaditeľa, technického riaditeľa a riaditeľa pre výskum a inovácie. Do podriadenosti výrobného riaditeľa spadajú všetci výrobní zamestnanci vrátane dielenských majstrov. Technický riaditeľ má na starosti personálne a ekonomické oddelenie a riaditeľ pre výskum a inovácie má v podriadenosti vývojove oddelenie. Strojárska spoločnosť sídli vo vlastnom oplotenom areáli v priemyselnej časti krajského mesta. Do areálu je možné sa dostať iba jednou hlavnou bránou, ktorá slúži zároveň pre vjazd automobilov a pre vstup zamestnancov a návštev. Areál a vstup do areálu je strážený súkromnou strážnou službou, ktorú si strojárska spoločnosť platí ako službu. Strojárska spoločnosť zamestnáva 74 zamestnancov, ktorí pracujú vo výrobnej hale a priľahlej dvoj podlažnej administratívnej budove. Súčasťou areálu sú aj kryté skladové priestory.



Obrázok 8 Situačný plán areálu strojárskej firmy [Vlastné spracovanie]

4.2.1 Informačné technológie

Hardvér

V strojárskej firme je počítačová sieť typu klient-server rozdelená na administratívnu a priemyselnú časť. Administratívna časť počítačovej siete je vybudovaná v administratívnej budove a prepája jednotlivé pracovné stanice, tlačiarne, sieťové prvky a serveri a je primárne určená pre administratívne aplikácie. Fyzicky je tvorená štruktúrovanou kabelážou, ktorá je z jednotlivých kancelárií a ostatných miestností strojárskej firmy inštalačnými tunelmi, alebo žľabmi privedená do jednotlivých dátových rozvádzačov umiestnených v rozvodných miestnostiach na prízemí, prvom a druhom poschodí administratívnej budovy. V dátových rozvádzačoch sú umiestnené prístupové switche, cez ktoré je užívateľ pripojený pomocou prepojovacích káblov do počítačovej siete strojárskej firmy a záložné zdroje UPS. V jednotlivých kancelárskych pracoviskách sa nachádza spolu 25 osobných počítačov a tlačiarní, ktoré sú takýmto spôsobom pripojené do siete.

Tabuľka 18 Prehľad zariadení pripojených do počítačovej siete v administratívnej budove

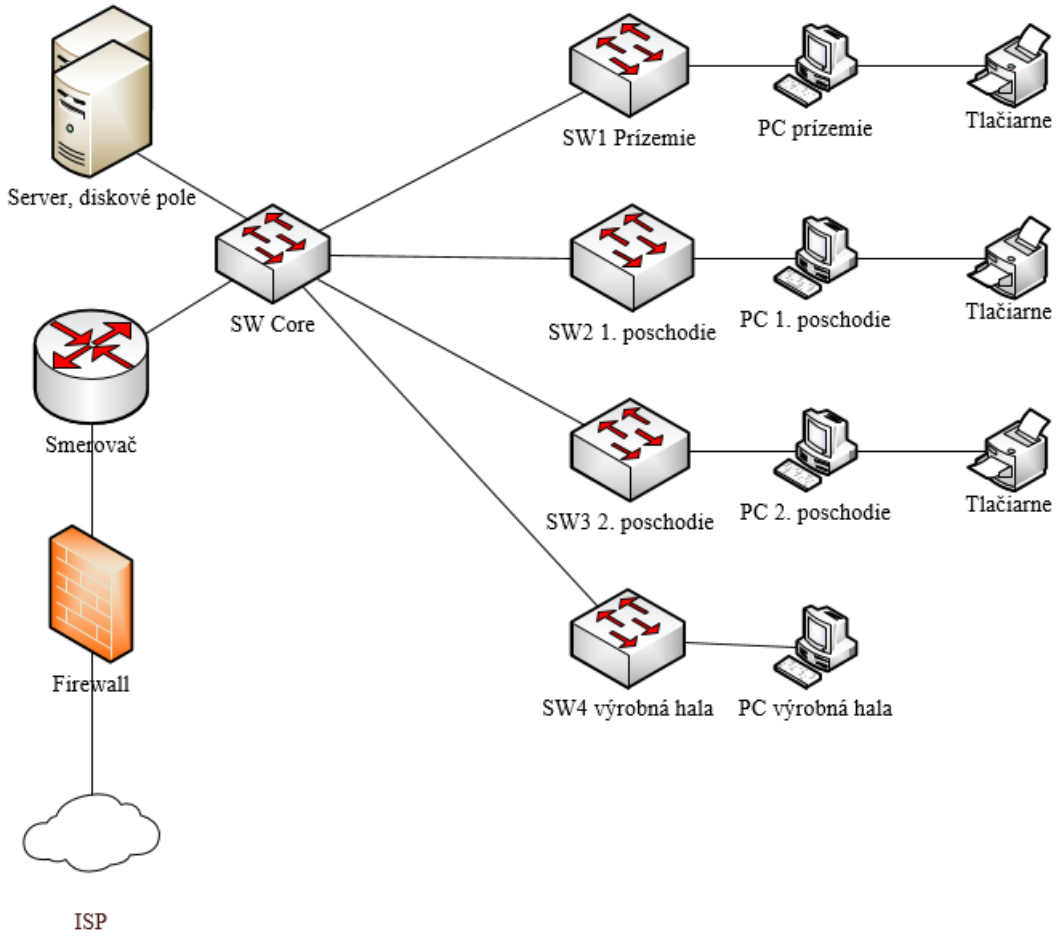
Oddelenie	PC, tlačiarne
Riaditeľ - konateľ, sekretariát	3
Technický riaditeľ	2
Výrobný riaditeľ	2
Riaditeľ pre výskum a inovácie	3
Personálne oddelenie	2
Ekonomické oddelenie	4
Vývojové oddelenie	6
Dielenskí majstri	3
Spolu	**25**

Vo výrobnej hale je priemyselná časť počítačovej siete fyzický takisto tvorená štruktúrovanou kabelážou, ktorá je vedená z prístupového switchu umiestneného v dátovom rozvádzači vo výrobnej hale, podľa potrieb strojárskej výroby k jednotlivým riadiacim počítačom, ktoré slúžia na ovládanie výrobnej linky a niekoľkých obrábacích strojov. Prístupový switch z výrobnej haly je pripojený k switchu v hlavnom dátovom rozvádzači, cez ktorý má prístup k serveru.

Tabuľka 19 Prehľad zariadení pripojených do počítačovej siete vo výrobnej hale

Výrobná hala	**Riadiace PC**
PC výrobná linka	3
PC fréza	1
PC sústruh	1
PC zváranie, rezanie	1
Spolu	**6**

Prístupové switche v administratívnej budove sú priamym up-linkom pripojené k hlavnému switchu, ktorý sa nachádza v hlavnom dátovom rozvádzači v serverovej miestnosti, umiestnenej na najvyššom, druhom, poschodí administratívnej budovy strojárskej firmy. Počítačová sieť v takomto stromovom zapojení je rozdelená do segmentov, ktoré umožňujú jej fyzickú a logickú škálovateľnosť. V hlavnej serverovej miestnosti sú umiestnené serveri s diskový poľom kam sú ukladané všetky dáta. Ďalej v hlavnom dátovom rozvádzači je umiestnený router určený pre pripojenie strojárskej spoločnosti k internetu, hardvérový firewall, jeden core switch pre prepojenie serverov, routra a prístupových switchov, záložný zdroj UPS spolu s batériami.



Obrázok 9 Schéma počítačovej siete v strojárskej firme [Vlastné spracovanie]

Softvér

Na serveri je nainštalovaný štandardný serverový operačný systém Windows Server 2019. Databáza je postavená na platforme Microsoft SQL. Na aktívnych prvkoch siete sú spustené sieťové operačné programy Cisco IOS od verzie 15.0 a vyššie, ktoré smerujú prevádzku do a z internetu a prepínajú prevádzku v samotnej sieti. Na firewalle Cisco ASA je spustený operačný systém na kontrolu dátovej prevádzky vrátane inšpekcie paketov, ktorá smeruje do a z vnútornej počítačovej siete strojárskej spoločnosti.

V administratívnej časti počítačovej siete strojárskej firmy je nainštalovaných niekoľko softvérov. Prehľad softvérov je uvedený v nasledujúcej tabuľke:

Tabuľka 20 Prehľad softvérov používaných v strojárskej firme

Informačný systém	Účel	Funkcie	Oddelenie
HELIOS	ekonomický softvér	platby pre dodávateľov a odberateľov, platby za služby, mzdy zamestnancov,	ekonomické oddelenie
OBERON	personálny a dochádzkový softvér	evidencia prítomnosti na pracovisku, evidencia obsadenosti pracovných pozícií	personálne oddelenie
T-Flex CAD	grafický a konštrukčný softvér	nástroj na tvorbu 3D modelov a príslušnej výrobnej dokumentácie	vývojové oddelenie, majstri, výroba

V priemyselnej časti siete je na serveri a na priemyselných počítačoch vo výrobnej hale nainštalovaný operačný program LINUX, na ktorom je spustený riadiaci informačný systém typu SCADA/HMI, a ktorý pomocou príslušného hardvéru slúži na vizualizáciu technologického procesu, zber dát v reálnom čase, riadenie a kontrolu výrobného procesu a samostatných strojných zariadení v strojárskej firme.

Počítače v strojárskej firme sú chránené prístupovými heslami k jednotlivým účtom a po upgrade je na nich nainštalovaný operačný systém Windows 10. Na počítačoch v administratívnej časti siete je nainštalované komerčné riešenie antivírového programu ESET End point Antivírus, ktorý sa sám aktualizuje. Systémy nepodliehajú žiadnemu obmedzeniu z pohľadu manipulácie s dátami či dátovými nosičmi vrátane USB pamäťových diskov. Prístup k intranetu a internetu, ako aj možnosť sťahovať akékoľvek dáta, je po prihlásení sa svojím účtom možné na všetkých počítačoch. Na komunikáciu s dodávateľmi a odberateľmi zamestnanci využívajú firemný e-mail. Do počítačov sa zamestnanci prihlasujú svojím jedinečným heslom do vytvoreného účtu. Správa a údržba informačného systému v strojárskej spoločnosti je riešená outsourcingom externou firmou.

4.2.2 Ohrozené prvky strojárskej firmy z pohľadu kybernetickej bezpečnosti a ich hodnota

Na stanovenie najdôležitejších prvkov strojárskej firmy, ktoré sú pre organizáciu dôležité, použijeme stupnicu čísel od 1 po 5, kde číslo 1 je najmenej dôležitý a číslo 5 je najviac dôležitý prvok pre strojársku firmu z pohľadu kybernetickej bezpečnosti.

Tabuľka 21 Ohrozené prvky strojárskej firmy

Ohrozený prvok	Hodnota ohrozeného prvku
server	**5**
diskové pole	**5**
router	**5**
switche	**4**
administratívne počítače	**3**
priemyselné počítače	**5**
operačné systémy	**4**
databázový systém	**5**
priemyselný softvér	**3**
náklady na rekonštrukciu dát	**4**
náklady na obnovu dát	**4**
ušlý zisk	**5**
pokuta od kontrolných orgánov	**4**
poškodenie vzťahov s odberateľmi	**5**
poškodenie vzťahov s dodávateľmi	**5**

4.2.3 Hodnotenie aktív

Aktíva sú znova ohodnotené na základe posúdenia požiadaviek na dostupnosť, integritu a dôvernosť dát. Stupnica je štandardne stanovená na základe hodnotiacich kritérií 1 až 5, pričom číslom 1 sú označené najmenej dôležité aktíva a číslom 5 sú označené najdôležitejšie aktíva. Výsledná hodnota je vypočítaná ako aritmetický priemer všetkých troch hodnôt a zaokrúhlená na celé číslo.

Tabuľka 22 Prehľad strojárskej firmy

Skupina	Dostupnosť	Dôvernosť	Integrita	Hodnota
popisné dáta systému	1	2	2	**2**
historické prevádzkové dáta	2	2	3	**2**
manipulačné dáta reálneho času	4	5	5	**5**
personálne a účtovné dáta	2	5	4	**4**
zálohy na serveri	4	5	5	**4**
operačné systémy	4	3	4	**4**
aplikačné SW systému SCADA	5	5	4	**5**
server	5	5	5	**5**
počítače	3	4	4	**4**
aktívne sieťové prvky	4	5	5	**5**
periférne zariadenia (UPS, tlačiarne)	2	2	3	**2**
kontrolné a riadiace zariadenia systému SCADA	5	5	5	**5**
dodávateľské zmluvy	3	5	5	**4**
odberateľské zmluvy	3	5	5	**4**

Na základe hodnotenia vyplýva, že najvyššie nároky na dôvernosť, integritu a dostupnosť dát majú tieto aktíva strojárskej firmy:

- manipulačné dáta reálneho času,
- aplikačné SW systému SCADA/HMI,
- server,
- aktívne sieťové prvky,
- kontrolné a riadiace zariadenia systému SCADA/HMI.

4.2.4 Identifikácia hrozieb a analýza rizík strojárskej firmy

Pre úspešnú analýzu rizík je potrebné identifikovať a ohodnotiť hrozby, ktoré môžu pôsobiť na strojársku firmu. Hodnotiaca škála závažnosti dopadu kybernetickej hrozby je stanovená

opäť od hodnoty 1 pre veľmi malú závažnosť dopadu hrozby, do hodnoty 5 pre katastrofickú závažnosť dopadu hrozby.

Tabuľka 23 Dopady kybernetických hrozieb na aktíva strojárskej firmy

Hrozba	**Úroveň závažnosti dopadu hrozby**
poškodenie výpadkom elektrickej energie	**4**
ransomware	**4**
počítačový vírus	**4**
zlyhanie softvéru	**5**
zlyhanie pripojenia	**2**
zlyhanie hardvéru	**5**
odpočúvanie komunikácie	**3**
neoprávnený prístup	**4**
zlyhanie údržby IT	**2**
chyba užívateľa	**2**
krádež dát	**3**
úmyselné poškodenie	**5**
prezradenie tajných informácií	**2**

Stupnica pravdepodobnosti existencie hrozby na strojársku firmu je tak isto stanovená od najmenšej hodnoty 1 pre nepatrnú pravdepodobnosť výskytu až po najvyššiu hodnotu 5 pre pravdepodobnú pravdepodobnosť existencie hrozby na strojársku firmu.

Tabuľka 24 Pravdepodobnosť existencie kybernetickej hrozby

Hrozba	Pravdepodobnosť existencie hrozby
poškodenie výpadkom elektrickej energie	**3**
ransomware	**4**
počítačový vírus	**4**
zlyhanie softvéru	**5**
zlyhanie pripojenia	**2**
zlyhanie hardvéru	**5**
odpočúvanie komunikácie	**4**
neoprávnený prístup	**4**
zlyhanie údržby IT	**3**
chyba užívateľa	**3**
krádež dát	**3**
úmyselné poškodenie	**5**
prezradenie tajných informácií	**3**

Na základe predchádzajúcich ohodnotenia aktív a hodnotenia pravdepodobnosti existencie hrozieb sme zostavili maticu zraniteľnosti, ktorá vyjadruje zraniteľnosť aktíva strojárskej firmy konkrétnou kybernetickou hrozbou. V matici figurujú aktíva strojárskej firmy a pravdepodobnosť existencie kybernetických hrozieb, ktoré môžu na tieto aktíva pôsobiť.

Tabuľka 25 Matica zraniteľnosti aktíva strojárskej firmy hrozbou

Zraniteľnosť V	**A** ↓	**Výpadok el. energie**	**Ransomware**	**Počítačový vírus**	**Zlyhanie softvéru**	**Zlyhanie pripojenia**	**Zlyhanie hardvéru**	**Odpočúvanie komunikácie**	**Neoprávn. prístup**	**Zlyhanie údržby IT**	**Chyba užívateľa**	**Krádež dát**	**Úmyselné poškodenie**	**Prezradenie utaj. inf.**
T →		**3**	**4**	**4**	**5**	**2**	**5**	**4**	**4**	**3**	**3**	**3**	**5**	**3**
Popisné dáta systému	**2**	1	2	2	2	1	2	1	1	1	2	3	3	2
Historické prev. dáta	**2**	1	3	3	2	1	3	2	2	2	2	3	3	2
Manip. dáta reálneho času	**5**	4	5	5	5	1	5	4	3	3	4	3	5	3
Personálne a účtov. dáta	**4**	2	4	4	2	2	5	4	5	2	2	4	4	3
Zálohy na serveri	**4**	2	5	5	3	1	5	2	4	4	4	5	4	2
Operačné systémy	**4**	2	4	4	4	1	5	2	2	4	2	2	4	2
Aplik. SW systému SCADA/HMI	**5**	3	5	5	5	1	5	2	5	4	4	1	4	2
Server	**5**	4	5	5	4	2	5	3	4	3	3	5	3	2
Počítače	**4**	2	4	4	5	4	5	3	3	3	3	4	3	2
Aktívne sieťové prvky	**5**	3	5	5	5	3	5	5	5	3	2	3	3	2
Periférne zariadenia	**2**	1	2	2	1	1	1	1	1	1	1	1	1	1
Kontrol. a riadiace zariadenia systému SCADA/HMI	**5**	3	5	5	5	1	5	2	4	4	2	3	4	2
Odberateľské zmluvy	**4**	1	4	4	2	1	1	1	3	1	1	4	1	3
Dodávateľské zmluvy	**4**	1	4	4	2	1	1	1	3	1	1	4	1	3

4.2.5 Výpočet miery rizika

Nasledujúcim krokom pri analýze rizík je vypočítanie miery rizika podľa vzorca (11):

$$R = T * A * V \tag{11}$$

kde: R je miera rizika,

T je pravdepodobnosť vzniku hrozby,

A je hodnota aktíva pre organizáciu,

V je zraniteľnosť aktíva.[18]

Pri najvyššej pravdepodobnosti výskytu hrozby (5), najvyššej hodnote aktíva (5) a najväčšej zraniteľnosti (5) je dosiahnutá maximálna výsledná hodnota rizika, ktorá dosahuje úroveň 125. V ďalšom kroku predstavujeme maticu rizík R, ktorá vychádza z predchádzajúcich získaných hodnôt.

Tabuľka 26 Matica rizík strojárskej firmy

Riziko R	**A** ↓	**Výpadok el. energie**	**Ransomware**	**Počítačový vírus**	**Zlyhanie softvéru**	**Zlyhanie pripojenia**	**Zlyhanie hardvéru**	**Odpočúvanie komunikácie**	**Neoprávnený prístup**	**Zlyhanie údržby IT**	**Chyba užívateľa**	**Krádež dát**	**Úmyselné poškodenie**	**Prezradenie utaj. inf.**
T →		**3**	**4**	**4**	**5**	**2**	**5**	**4**	**4**	**3**	**3**	**3**	**5**	**3**
Popisné dáta systému	**2**	6	16	16	20	4	20	8	8	6	12	18	30	12
Historické prev. dáta	**2**	6	24	24	20	4	30	16	16	12	12	18	30	12
Manip. dáta reálneho času	**5**	60	100	100	125	10	125	100	60	45	60	45	125	45
Personálne a účtov. dáta	**4**	24	64	64	40	40	100	64	100	24	24	36	80	36
Zálohy na serveri	**4**	24	80	80	60	8	100	40	64	48	36	60	80	36
Operačné systémy	**4**	24	64	64	80	8	100	24	24	48	24	24	80	24
Aplik. SW systému SCADA/HMI	**5**	45	100	100	125	10	125	40	100	60	60	15	100	30
Server	**5**	60	100	100	100	20	125	60	80	45	45	75	75	30
Počítače	**4**	24	64	64	100	32	100	48	48	36	36	36	60	24
Aktívne sieťové prvky	**5**	45	100	100	125	30	125	100	100	45	30	45	60	30
Periférne zariadenia	**2**	6	16	16	10	4	10	8	8	6	6	6	10	6
Kontrol. a riadiace zariadenia systému SCADA/HMI	**5**	45	100	100	125	10	125	40	80	60	30	45	100	30
Odberateľské zmluvy	**4**	12	64	64	40	8	20	16	48	12	12	36	20	36
Dodávateľské zmluvy	**4**	12	64	64	40	8	20	16	48	12	12	36	20	36

Z analýzy rizík nám vychádza, že najväčšie riziká pre strojársku firmu vznikajú pri pôsobení hrozieb na kontrolné a riadiace zariadenia systému SCADA/HMI, aplikačné softvéry systému SCADA/HMI, operačné systémy serverov, manipulačné dáta v reálnom čase, zálohy dát na serveri a aktívne sieťové prvky. Ako možné hrozby podľa analýzy rizík sú ransomware, zlyhanie softvéru a zlyhanie hardvéru.

4.2.6 Vývoj kybernetickej situácie a dopady na strojársku firmu

V nasledujúcich tabuľkách je prehľadne popísaný časový prehľad prebiehajúcich útokov, ktorých prvkov sa útok týka a aké sú dopady jednotlivých útokov na strojársku firmu.

Útok prostredníctvom škodlivého programu ransomware

Tabuľka 27 Prehľad útoku škodlivým programom ransomware

Čas	Činnosť	Poškodené prvky/aktíva firmy	Dopady na zdravotnícke zariadenie	Funkčnosť zariadenia
0	prijatý email s infikovanou prílohou			100%
0 - 10 min	otvorenie infikovanej prílohy a aktivovanie škodlivého kódu			100%
10 - 14 min	škodlivý kód kontaktuje riadiaci server, zašifruje dáta na diskoch	dáta firmy uložené na diskovom poli	účtovné a personálne dáta nie sú prístupne pre PC v administratívnej časti siete, útok nemá dopad na strojársku výrobu	60%
14 - 20 min	požadovanie výkupného		v prípade zaplatenia je dopad na financie firmy	60%
20 - 60 min	vypnutie serverov, PC	servery, diskové pole	firma nemá prístup k účtovným a personálnym dátam	60%
1 - 48 hod	obnovenie a rekonštrukcia dát	servery, počítače, dáta, dobré meno firmy, vzťahy s odberateľmi	firma neuhrádza záväzky, čiastočne prijíma tovar a objednávky, čiastočne dodáva výrobky, evidencia v papierovej forme	80%
2 - 5 dní	čiastočné obnovenie systému	servery, PC, dáta, dobré meno firmy, vzťahy s odberateľmi	firma neuhrádza záväzky, čiastočne prijíma tovar a objednávky, čiastočne dodáva výrobky, evidencia v papierovej forme	80%
po 5 dňoch	obnovenie systému	dobré meno, vzťahy s odberateľmi	zmluvné pokuty, náklady na obnovu, ušlý zisk	100%

Zlyhanie softvéru ako následok útoku

Tabuľka 28 Prehľad zlyhania softvéru ako následok útoku

Čas	Činnosť	Poškodené prvky / aktíva firmy	Dopady na firmu	Funkčnosť firmy
0	stiahnutý inštalačný SW s infikovaným škodlivým kódom			100%
0 - 30 min	aktivovanie škodlivého kódu, aktualizáciou FW	systémy SCADA/HMI		100%
30 - 60 min	škodlivý kód prevezme kontrolu nad PC ovládajúcim výrobnú linku	systémy SCADA/HMI	manipuláciou SW je vypnutá výrobná linka, útok nemá dopad na administratívnu časť siete	30%
1 - 48 hod	obnovovanie systému	servery, počítače, dáta, dobré meno firmy, vzťahy s odberateľmi,	firma neuhrádza záväzky, neprijíma objednávky, tovar, nedodáva výrobky,	40%
2 - 3 dňoch	čiastočné obnovenie systému	servery, počítače, dáta, dobré meno firmy, vzťahy s odberateľmi	firma neuhrádza záväzky, čiastočne prijíma tovar a objednávky, čiastočne dodáva výrobky, evidencia v papierovej forme	60%
po 3 dňoch	obnovenie systému	dobré meno firmy, vzťahy s odberateľmi	zmluvné pokuty, náklady na obnovu, ušlý zisk	100%

Zlyhanie hardvéru ako následok útoku

Tabuľka 29 Prehľad zlyhania hardvéru ako následok útoku

Čas	Činnosť	Poškodené prvky / aktíva firmy	Dopady na firmu	Funkčnosť firmy
0	stiahnutý inštalačný SW s infikovaným škodlivým kódom			100%
0 + 45 min	aktivovanie škodlivého kódu, aktualizáciou FW	systémy SCADA/HMI		100%
30 + 90 min	škodlivý kód prevezme kontrolu nad servermi strojárskej firmy	servery, systémy SCADA/HMI	manipuláciou SW sú vypnuté servery pre administratívnu aj priemyselnú časť siete, neuhrádza záväzky, neprijíma objednávky, nevyrába, nedodáva výrobky	5%
1 + 24 hod	vypnutie serverov, PC	všetky servery, diskové pole,	firma nemá prístup k žiadnym dátam, neuhrádza záväzky, neprijíma objednávky, nevyrába, nedodáva výrobky	5%
1 + 5 dní	obnovovanie a preinštalovanie systému	servery, počítače, dáta, dobré meno firmy, vzťahy s odberateľmi,	firma neuhrádza záväzky, neprijíma objednávky, nevyrába, nedodáva výrobky	5%
5 - 7 dní	čiastočné obnovenie systému	servery, počítače, dáta, dobré meno firmy, vzťahy s odberateľmi	firma neuhrádza záväzky, čiastočne prijíma tovar a objednávky, čiastočne dodáva výrobky, evidencia v papierovej forme	75%
po 7 dňoch	obnovenie systému	dobré meno firmy, vzťahy s odberateľmi	zmluvné pokuty, náklady na obnovu, ušlý zisk	100%

Počet kybernetických útokov na organizácie každý rok stúpa. Nevyhýbajú sa ani priemyselným podnikom. Napriek tomu veľká časť podnikov žije v domnení, že „nám sa to nemôže stať“. Firmy fungujú na zastaraných sieťových architektúrach, ktoré sú ľahko

ochromiteľné. Veľká časť výrobných systémov je z nevedomosti, alebo z pohodlnosti napojená priamo na internet, čo zvyšuje riziko bezpečnostných incidentov. Kybernetická bezpečnosť je nikdy nekončiaci proces, a ako sme aj v tejto kapitole analýzou zistili, firmy by nemali túto oblasť bezpečnosti podceňovať.

5 OCEŇOVANIE DOPADOV KYBERNETICKÝCH HROZIEB

Pri oceňovaní dopadov kybernetických hrozieb budeme oceňovať škody, ktoré spôsobia kybernetické hrozby na hypotetické organizácie. Na základe analýz, ktoré sme vykonali sme definovali tri najnebezpečnejšie kybernetické hrozby pre každú organizáciu. Každá hrozba ohrozuje aktíva organizácií inak. Výsledkom ich pôsobenia je však čiastočné, alebo celkové znefunkčnenie organizácií. Pri oceňovaní dopadov kybernetických hrozieb budeme používať nákladový spôsob, z ktorého budeme vychádzať, aby sme čo najpresnejšie stanovili výšku dopadu na hypotetické organizácie. Vyčíslime si náklady, ktoré organizácie vynaložili na obstaranie hardvéru, softvéru, vypočítame si náklady na obnovu dát, ušlý zisk a odhadneme výšku pokuty za úniky citlivých údajov od kompetentných úradov.

5.1 Postup oceňovania dopadov kybernetických hrozieb

Na účely oceňovania dopadov kybernetických hrozieb na naše vymodelované organizácie použijeme postup, ktorý popísal v roku 2019 Pavlík vo svojej dizertačnej práci *„Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti“*. Jeho podstatou je, že hodnotu, ktorú sme vypočítali v matici rizík pre vybranú kybernetickú hrozbu vydelíme počtom interakcií tejto kybernetickej hrozby na vybrané ohrozené aktíva. Hodnotu, ktorú takto dostaneme prevedieme podľa tabuľky klasifikácie závažnosti kybernetickej hrozby na výšku škody v percentách, ktorú môže vybraná kybernetická hrozba organizácii spôsobiť. Tabuľka klasifikácie hrozby udáva stupne závažnosti hrozby, ktorá môže byť pre najzávažnejšiu kybernetickú hrozbu pridelená a vychádza z matice rizík. V našom prípade je pre najnebezpečnejšiu kybernetickú hrozbu najnižšia dosiahnutá hodnota 71 a najvyššia hodnota, ktorá môže byť dosiahnutá je 125.

Tabuľka 30 Vyjadrenie závažnosti dopadu hrozby v %

Stupeň závažnosti hrozby	Percentuálny podiel z celkovej čiastky
71 – 76	10 %
77 – 82	20 %
83 – 88	30 %
89 – 94	40 %
95 - 100	50 %
101 – 106	60 %
107– 112	70 %
113– 117	80 %
118– 121	90 %
122 - 125	100 %

Na to aby sme mohli uvedený postup aplikovať a pomocou neho určiť výšku spôsobenej škody na vybrané organizácie, musíme najprv stanoviť celkovú finančnú hodnotu všetkých ohrozených prvkov zdravotníckej organizácie. Túto výslednú hodnotu ohrozených prvkov organizácie nakoniec vynásobíme percentuálnou hodnotou výšky škody pre konkrétnu kybernetickú hrozbu.[18]

5.2 Oceňovanie dopadov kybernetických hrozieb na zdravotnícke zariadenie A

Pri oceňovaní dopadov kybernetických hrozieb na zdravotnícke zariadenie použijeme nákladový prístup oceňovania. Vyčíslime si náklady na obstaranie hardvéru a softvéru zdravotníckeho zariadenia, podľa vzorcov si vypočítame úšlý zisk zdravotníckeho zariadenia, náklady na rekonštrukciu dát a ďalšie vynaložené náklady spojené s dopadom kybernetickej hrozby.

5.2.1 Stanovenie finančnej hodnoty ohrozených prvkov zdravotníckej organizácie

Hardvér

- servery - **35 000,-** EUR, zdravotnícke zariadenie používa 14 serverov v cene cca 2500,- EUR za kus,

- diskové polia - **24 000,-** EUR, zdravotnícke zariadenie používa 4 diskové polia v cene cca 6000,- EUR za kus,
- hardvérový firewall - **10 000,-** EUR,
- router - **7000,-** EUR,
- switche - **24 000,-** EUR, zdravotnícke zariadenie používa 16 switchov v cene cca 1500,- EUR za kus,
- počítačové zostavy - **96 400,-** EUR, zdravotnícke zariadenie používa 241 počítačových zostáv s monitorom v cene cca 400,- EUR za kus,
- počítače pre obsluhu CT, USG, RTG a laboratórne prístroje - cca **55 000,-** EUR, zdravotnícke zariadenie disponuje niekoľkými druhmi a tipmi medicínskych prístrojov, cena je uvedená ako približný odhad počítačov pre všetky zariadenia.

Celkom za hardvér - **251 400,-** EUR

Softvér

Pri cene softvéru uvažujeme iba cenu vynaloženú na jeho reinštaláciu a to vo výške cca **2 700,-** EUR.

Náklady na rekonštrukciu a obnovu dát

Podľa Ponemon Study, ktorú vydáva Ponemon Institute spolu so spoločnosťou IBM Security je možné stanoviť priemernú cenu za ukradnuté, alebo stratené dáta na osobu. Za rok 2019 je jej priemerná hodnota na osobu vo výške 150,- USD a po prepočte na euro je to cca 132,- EUR.[28] Na výpočet nákladov na rekonštrukciu a obnovu dát použijeme vzorec (12):

$$NR = CD * \sum_{i=1}^{n} P_D \tag{12}$$

kde N_R sú náklady na obnovu a rekonštrukciu dát,

C_D je cena za stratené, alebo ukradnuté dáta na osobu,

P_D je počet dátových položiek, ktoré môžu byť stratené, v tomto prípade použijeme počet počítačov v zdravotníckom zariadení.[18]

N_R = 132 * 241 = **31 812,-** EUR

Dobré meno organizácie

Vzhľadom k faktu, že zdravotnícke zariadenie nie je podnikateľská organizácia generujúca zisk, a že ľudia zo spádovej oblasti pri svojich chorobách a úrazoch prídu vždy na ošetrenie do tohoto zdravotníckeho zariadenia, nemá stanovenie finančnej hodnoty dobrého mena zdravotníckeho zariadenia pre náš výpočet dopadov zásadný význam. Zdravotnícke zariadenie neutrpí na poškodení dobrého mena žiadnu významnú stratu tak na strane dodávateľov ako aj pacientov. Dôležitá je kvalita poskytovanej zdravotnej starostlivosti, ktorá sa síce počas kybernetického útoku na nejaký čas zastaví, ale po obnovení činnosti informačných systémov je znova k dispozícii na vysokej úrovni. Zdravotnícke zariadenie ale investuje finančné prostriedky vo výške 2500,-EUR ročne do reklamy, ktoré môžeme zarátať do vybraných ohrozených prvkov zdravotníckeho zariadenia.

Ušlý obrat

Na vypočítanie ušlého obratu pri kybernetickom útoku si musíme najprv vypočítať koľko eur obratu zdravotnícke zariadenie generuje za jeden deň. Ten zistíme tak, že celkový obrat za jeden rok zdravotníckeho zariadenia vydelíme počtom dní v roku. Tento denný obrat potom vynásobíme počtom dní, ktoré zdravotnícke zariadenie nemohlo generovať obrat z dôvodu napadnutia kybernetickou hrozbou. Pre výpočet ušlého obratu napríklad na dobu piatich dní použijeme vzorec (13):

$$U_Z = \frac{O_f}{M_r} * M_t \qquad (13)$$

kde U_Z je ušlý obrat,

O_f je obrat organizácie za rok,

M_r je počet dní v roku,

M_t je počet dní kedy organizácia negeneruje obrat.[18]

$U_Z = \frac{22\,553\,410}{365} * 1 =$ **61 790,-** EUR.

Náklady na oznámenie straty, alebo úniku údajov

Náklady na oznámenie straty, alebo úniku údajov si vypočítame podľa vzorca (14):

$$N_u = M_z * H_z * T_z \quad (14)$$

kde N_u sú náklady na oznámenie úniku, alebo straty údajov úradu,

M_z je počet zamestnancov, ktorí takýto únik úradu ohlasujú,

H_z je hodinový plat zamestnanca, ktorý ohlasujú únik údajov úradu,

T_z je počet hodín vynaložených na kontaktovanie úradu.[18]

Nu = 2 * 15 * 30 = **900,-** EUR

Pokuty

Podľa zákona o ochrane osobných údajov č. 18/2018 Z.z. môže organizácia dostať pokutu za stratu alebo únik osobných údajov až do výšky 20 000 000,- EUR. Výška pokuty závisí od viacerých faktorov a rozhoduje o nej Úrad na ochranu osobných údajov SR. Doposiaľ najviac udelená pokuta v SR bola vo výške 50 000,- EUR verejnoprávnej inštitúcii. Výšku pokuty pre zdravotnícke zariadenie sme stanovili na 50 000,- EUR.

Sumár hodnoty ohrozených prvkov zdravotníckeho zariadenia

Tabuľka 31 Hodnoty ohrozených prvkov zdravotníckeho zariadenia

Hardvér	251 400,- EUR
Softvér	2 700,- EUR
Náklady na rekonštrukciu a obnovu dát	31 812,- EUR
Dobré meno organizácie	2 500,- EUR
Ušlý obrat na dobu jedného dňa	61 790,- EUR
Náklady na oznámenie straty, alebo úniku dát	900,- EUR
Pokuta	50 000,- EUR
Spolu	**398 602,- EUR**

5.2.2 Výpočet hodnoty dopadov kybernetických hrozieb po jednotlivých fázach vývoja

Dopady kybernetického útoku prostredníctvom počítačového vírusu

Súčet hodnôt v tabuľke rizík pre kybernetickú hrozbu útoku počítačovým vírusom je 560. Počet interakcií s ohrozenými prvkami je 6. Priemerná hodnota závažnosti hrozby je 560 / 6 = **93,33**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške **40%** z hodnoty ohrozených prvkov zdravotníckeho zriadenia. Vo finančnom vyjadrení sa jedná o sumu 398 602 x 0,4 = **159 441,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na zdravotnícke zariadenie v prípade poškodenia všetkých hmotných aj nehmotných aktív zdravotníckeho zariadenia prostredníctvom počítačového vírusu za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém nebol funkčný sú 4 z celkového počtu 14 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby v zdravotníckom zariadení vôbec nefungovalo 61 počítačov napadnutých počítačovým vírusom čo tvorí približne 25% zo všetkých počítačov, a ktoré nemohli byť použité na vyšetrovanie pacientov, alebo administratívnu prácu. K úniku dát nedošlo a ani hardvér nebol fyzický poškodený. V tejto fáze je dopad kybernetickej hrozby najväčší. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **2 700,-** EUR, náklady na rekonštrukciu dát v zavírovaných 61 počítačoch 31 812 / 241 x 61 = **8 052,-** EUR a ušlý obrat zdravotníckeho zariadenia za 4 dni pri nefunkčnosti 25% počítačov. Ušlý obrat predstavuje sumu 61 790 x 4 x 0,25 = **61 790,-** EUR. Výška dopadu kybernetického útoku počítačovým vírusom na zdravotnícke zariadenie bude v prvých 4 dňoch vo výške **72 542,-** EUR

Fáza po čiastočnej obnove systému

Počet dní kedy boli zavírované počítače čiastočne obnovované až do plnej funkčnosti je 10 z celkového počtu 14 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby zdravotnícke zariadenie fungovalo v obmedzenom režime, nefungovalo ešte 12 počítačov. To tvorilo 5% zo všetkých počítačov v zdravotníckom zariadení. Dopad kybernetickej hrozby sa zmenšoval. Finančne tento dopad vypočítame z nákladov na preinštalovanie softvéru **2 700,-**EUR, náklady na rekonštrukciu dát v zavírovaných 12 počítačoch 31 812 / 241 x 12 = **1 584,-** EUR a ušlý obrat zdravotníckeho zariadenia za 10 dní pri nefunkčnosti 5% počítačov. Ušlý obrat predstavuje sumu

61 790 x 10 x 0,05 = **30 895,-** EUR. Výška dopadu kybernetického útoku počítačovým vírusom na zdravotnícke zariadenie bude v ďalších 10 dňoch po čiastočnom obnovovaní počítačov vo výške **35 179,-** EUR

Celkový dopad kybernetického útoku na zdravotnícke zariadenie prostredníctvom počítačového vírusu predstavuje za 14 dní čiastku 72 542 + 35 179 = **107 721,-** EUR.

Dopady kybernetického útoku prostredníctvom ransomware

Súčet hodnôt v tabuľke rizík pre kybernetickú hrozbu útoku prostredníctvom ransomwaru je 680. Počet interakcií s ohrozenými prvkami je 7. Priemerná hodnota závažnosti hrozby je 680 / 7 = **97,14**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške **50%** z hodnoty ohrozených prvkov zdravotníckeho zriadenia. Vo finančnom vyjadrení sa jedná o sumu 398 602 x 0,5 = **199 301,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na zdravotnícke zariadenie v prípade poškodenia všetkých hmotných aj nehmotných aktív zdravotníckeho zariadenia prostredníctvom ransomware za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém nebol funkčný je 5 z celkového počtu 20 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby nemohlo k dátam o pacientoch pristupovať 180 počítačov v zdravotníckej časti zariadenia, čo tvorí približne 75% všetkých počítačov v zdravotníckom zariadení. Zdravotnícke zariadenie neprijímalo ani nevyšetrovalo žiadnych pacientov a vtedy bol dopad kybernetickej hrozby najväčší. Počítače v administratívnej časti zdravotníckeho zariadenia mohli pristupovať k nemedicínskym dátam a nemedicínsky zamestnanci pracovali bez obmedzení. K fyzickému poškodeniu hardvéru nedošlo a ani únik dát nebol zaznamenaný. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **2 700,-** EUR, náklady na rekonštrukciu dát pre 180 počítačov 31 812 / 241 x 180 = **23 760,-** EUR a ušlý obrat zdravotníckeho zariadenia za 5 dni pri nefunkčnosti 75% počítačov. Ušlý obrat predstavuje sumu 61 790 x 5 x 0,75 = **231 713,-** EUR. Výška dopadu kybernetického útoku ransomware na zdravotnícke zariadenie bude v prvých 5 dňoch vo výške **258 173,-** EUR

Fáza po čiastočnej obnove systému

Počet dní kedy bol systém čiastočne funkčný po obnovení dát je 15 z celkového počtu 20 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby zdravotnícke zariadenie fungovalo v obmedzenom režime. Počet počítačov, ktoré ešte nemohli pristupovať k dátam pacientov bol 85 čo tvorí 35% všetkých počítačov

v zdravotníckom zariadení. Dopad kybernetickej hrozby sa zmenšoval. Finančne tento dopad vypočítame z nákladov na preinštalovanie softvéru **2 700,-**EUR, náklady na rekonštrukciu dát pre 85 počítačov 31 812 / 241 x 85 = **11 220,-** EUR a ušlý obrat zdravotníckeho zariadenia za 15 dní pri nefunkčnosti 35% počítačov. Ušlý obrat predstavuje sumu 61 790 x 15 x 0,35 = **324 398,-** EUR. Výška dopadu kybernetického útoku počítačovým vírusom na zdravotnícke zariadenie bude v ďalších 15 dňoch po čiastočnej rekonštrukcii dát vo výške **338 318,-** EUR

Celkový dopad kybernetického útoku na zdravotnícke zariadenie prostredníctvom ransomware predstavuje za 20 dní čiastku 258 173 + 338 318 = **596 491,-** EUR.

Dopady neoprávneného prístupu ako kybernetického útoku

Súčet hodnôt v tabuľke rizík pre kybernetickú hrozbu útoku prostredníctvom neoprávneného prístupu je 855. Počet interakcií s ohrozenými prvkami je 8. Priemerná hodnota závažnosti hrozby je 855 / 8 = **106,88**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške **70%** z hodnoty ohrozených prvkov zdravotníckeho zriadenia. Vo finančnom vyjadrení sa teda, rovnako ako pri kybernetickom útoku počítačovým vírusom, jedná o sumu 398 602 x 0,7 = **279 021,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na zdravotnícke zariadenie v prípade poškodenia všetkých hmotných aj nehmotných aktív zdravotníckeho zariadenia prostredníctvom neoprávneného prístupu za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém nebol funkčný je 6 z celkového počtu 25 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby nemohlo k nemedicínskym dátam a dátam o pacientoch pristupovať 229 počítačov v zdravotníckom zariadení, čo tvorí približne 95% všetkých počítačov v zdravotníckom zariadení. Zdravotnícke zariadenie neprijímalo ani nevyšetrovalo žiadnych pacientov, neuhrádzalo platby svojím dodávateľom, nefakturovalo platby zdravotným poisťovniam a vtedy bol dopad kybernetickej hrozby najväčší. K fyzickému poškodeniu hardvéru nedošlo a bol zaznamenaný únik citlivých údajov. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **2 700,-** EUR, náklady na rekonštrukciu dát pre 229 počítačov 31 812 / 241 x 229 = **30 228,-** EUR a ušlý obrat zdravotníckeho zariadenia za 6 dni pri nefunkčnosti 95% počítačov. Ušlý obrat predstavuje sumu 61 790 x 6 x 0,95 = **352 203,-** EUR. Náklady na oznámenie úniku citlivých údajov budú vo výške **900.-** EUR a pokuta od kontrolných orgánov bola stanovená vo výške **50 000,-** EUR. Výška dopadu kybernetického útoku

prostredníctvom neoprávneného prístupu na zdravotnícke zariadenie bude v prvých 6 dňoch vo výške **436 031,-** EUR.

Fáza po čiastočnej obnove systému

Počet dní kedy bol systém čiastočne funkčný po obnovení dát je 19 z celkového počtu 25 dní kedy začalo zdravotnícke zariadenie fungovať v normálnom režime. Počas tejto doby zdravotnícke zariadenie fungovalo v obmedzenom režime. Počet počítačov, ktoré ešte nemohli pristupovať k dátam pacientov bol 133 čo tvorí 45% všetkých počítačov v zdravotníckom zariadení. Dopad kybernetickej hrozby sa zmenšoval. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **2 700,-** EUR, náklady na rekonštrukciu dát pre 133 počítačov 31 812 / 241 x 133 = **17 556,-** EUR a ušlý obrat zdravotníckeho zariadenia za 19 dni pri nefunkčnosti 45% počítačov. Ušlý obrat predstavuje sumu 61 790 x 19 x 0,45 = **528 305,-** EUR. Náklady na oznámenie úniku citlivých údajov a pokuta od kontrolných orgánov už boli zarátané vo výpočte pri celkovom poškodení informačného systému zdravotníckeho zariadenia. Výška dopadu kybernetického útoku prostredníctvom neoprávneného prístupu na zdravotnícke zariadenie bude v ďalších 19 dňoch vo výške **548 561,-** EUR.

Celkový dopad kybernetického útoku na zdravotnícke zariadenie prostredníctvom neoprávneného prístupu predstavuje za 25 dní čiastku 436 031 + 548 561 = **984 592,-** EUR.

Tabuľka 32 Vyčíslenie dopadov kybernetických hrozieb na zdravotnícke zariadenie

Kybernetická hrozba	**Celková výška dopadu**	**Najvážnejšie/čiastočné poškodenie**	**Počet dní trvania poškodenia**
Počítačový vírus	107 721,- EUR	72 542,- EUR	4 dní
		35 179,- EUR	10 dní
Ransomware	596 491,- EUR	258 173,- EUR	5 dní
		338 318,- EUR	15 dní
Neopráv. prístup	984 592,- EUR	436 031,- EUR	6 dní
		548 561,- EUR	19 dní

5.3 Oceňovanie dopadov kybernetických hrozieb na strojársku firmu B

Podobne budeme postupovať aj pri oceňovaní dopadov kybernetických hrozieb na strojársku firmu. Aj v tomto prípade použijeme rovnaký, nákladový prístup oceňovania dopadov kybernetických hrozieb na strojársku firmu.

5.3.1 Stanovenie finančnej hodnoty ohrozených prvkov strojárskej firmy

Hardvér

- servery - **7 000,-** EUR, strojárska firma používa 2 serveri v cene cca 3500,- EUR za kus,
- diskové polia - **6 000,-** EUR, strojárska firma používa 1 diskové pole v cene cca 6000,- EUR za kus,
- hardvérový firewall - **5 000,-** EUR,
- router - **3 000,-** EUR,
- switche - **5 000,-** EUR, zdravotnícke zariadenie používa 5 switchov v cene cca 1000,- EUR za kus,
- počítačové zostavy - **13 750,-** EUR, zdravotnícke zariadenie používa 25 počítačových zostáv s monitorom v cene cca 550,- EUR za kus,
- počítače pre obsluhu zariadení systému SCADA/HMI a počítače na obsluhu samostatných strojárskych strojov (CNC fréza, zváračka, laserová rezačka) - cca **15 000,-** EUR.

Celkom za hardvér - **54 750,-** EUR

Softvér

Pri cene softvéru uvažujeme iba cenu vynaloženú na jeho reinštaláciu a to vo výške cca **5 000,-** EUR.

Náklady na rekonštrukciu a obnovu dát

$$N_R = 132 * 31 = \textbf{4 092,-}\ \text{EUR}$$

Dobré meno organizácie

Strojárska firma utrpí pri kybernetickom útoku aj poškodenie dobrého mena. Počas výpadku informačných systémov a systémov SCADA/HMI, ktoré ovládajú technologickú linku

nebude schopná plniť svoje záväzky, čo sa môže v budúcnosti odraziť na strate aktuálnych odberateľov, alebo nezískaní nových. Aby sme vyrátali finančný dopad poškodenia dobrého mena strojárskej firmy potrebujeme zmerať priemerný zisk, priemerné úbytky a prírastky zákazníkov, od ktorých odpočítame priemerné náklady na reklamu a image vynaložené na budovanie dobrého mena strojárskej firmy. Hodnoty dosadíme do nasledujúceho vzorca (15) a vypočítame:

$$RI = (PPK * \frac{\sum_{t=1}^{n} N_{ki}}{n} - PPK * \frac{\sum_{t=1}^{n} Z_{ki}}{n}) - \frac{\sum_{t=1}^{n} N_{ir}}{n} \quad (15)$$

kde RI sú náklady na reklamu a image,

PPK je priemerný príjem na klienta,

N_{ki} sú noví klienti za rok,

Z_{ki} sú stratení klienti za rok,

N_{ir} sú náklady na reklamu a image za rok,

n je hodnota sledovaného obdobia.[18]

Vzorec (16) pre diskontovanie na ďalší rok zohľadňuje faktor času, ktorý je pre úplnosť potrebné k výpočtu poškodenia dobrého mena pridať:

$$PPK = \frac{\sum_{i=1}^{n} Xi}{\sum_{i=1}^{n} Nki} \quad (16)$$

kde PPK je priemerný príjem na klienta,

N_{ki} sú noví klienti za rok,

X_i je ročný príjem z obchodov.[18]

Tabuľka 33 Údaje potrebné k vyčísleniu dobrého mena strojárskej firmy

Rok	Príjem z činnosti	Počet nových zákazníkov	Počet stratených zákazníkov	Náklady na reklamu
2015	104 865,-	28	4	5 750,-
2016	96 759,-	25	5	5 500,-
2017	117 852,-	31	3	6 200,-
2018	95 634,-	38	2	5 500,-
2019	124 103,-	29	4	6 900,-

$PPK = \frac{539\,213}{151} =$ **3 571,-** EUR na klienta,

$RI = (3\,571 * \frac{151}{5} - 3\,571 * \frac{18}{5}) - \frac{29850}{5} =$ **94 455,-** EUR

Ušlý obrat

$U_Z = \frac{4\,953\,669}{365} * 1 =$ **13 572,-** EUR.

Náklady na oznámenie straty, alebo úniku údajov

$N_u = 2 * 12 * 20 =$ **480,-** EUR

Pokuty

Výška pokuty za stratu, alebo únik dát pre strojársku firmu bola stanovená na **10 000,-** EUR.

Sumár hodnoty ohrozených prvkov strojárskej firmy

Tabuľka 34 Hodnoty ohrozených prvkov strojárskej firmy

Hardvér	54 750,- EUR
Softvér	5000,- EUR
Náklady na rekonštrukciu a obnovu dát	4 092,- EUR
Dobré meno organizácie	94 455,- EUR
Ušlý obrat na dobu jedného dňa	13 572,- EUR
Náklady na oznámenie straty, alebo úniku dát	480,- EUR
Pokuta	10 000,- EUR
Spolu	**182 349,- EUR**

5.3.2 Výpočet hodnoty dopadov kybernetických hrozieb po jednotlivých fázach vývoja

Dopady kybernetického útoku prostredníctvom ransomware

Súčet hodnôt v tabuľke rizík pre kybernetickú hrozbu útoku prostredníctvom ransomwaru je 580. Počet interakcií s ohrozenými prvkami je 6. Priemerná hodnota závažnosti hrozby je 580 / 6 = **96,67**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške **50%** z hodnoty ohrozených prvkov strojárskej firmy. Vo finančnom vyjadrení sa jedná o sumu 182 349 x 0,5 = **91 175,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na strojársku firmu v prípade poškodenia všetkých hmotných aj nehmotných aktív strojárskej firmy prostredníctvom ransomware za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém nebol funkčný je 2 z celkového počtu 5 dní kedy začala strojárska firma fungovať v normálnom režime. Počas tejto doby nemohlo k účtovným a personálnym dátam pristupovať 13 počítačov v administratívnej časti strojárskej firmy. To tvorí približne 40% všetkých počítačov v strojárskej firme. Tento útok neovplyvnil výrobný proces v strojárskej firme, ale firma nemohla vykonávať administratívnu agendu, uhrádzať svoje záväzky a nedodávala vyrobený tovar svojím odberateľom. K fyzickému poškodeniu

hardvéru nedošlo a ani únik dát nebol zaznamenaný. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **5 000,-** EUR, náklady na rekonštrukciu dát pre 13 počítačov 4 092 / 31 x 13 = **1 716,-** EUR, ušlý obrat strojárskej firmy za 2 dni pri nefunkčnosti 40% počítačov. Ušlý obrat predstavuje sumu 13 572 x 2 x 0,4 = **10 858,-** EUR. Vzhľadom k tomu, že strojárska firma nemohla plniť svoje záväzky po dobu 2 dní, bolo poškodené aj jej dobré meno. Vyčíslenie výšky poškodenia dobrého mená vypočítame ako 40% z dvoch tretín maximálnej hodnoty poškodenia dobrého mena strojárskej firmy, 94 455 / 3 x 2 x 0,4 = **25 188,-** EUR. Výška dopadu kybernetického útoku ransomware na strojársku firmu bude v prvých 2 dňoch vo výške **42 489,-** EUR

Fáza po čiastočnej obnove systému

Počet dní kedy bol systém čiastočne funkčný po obnovení dát je 1 z celkového počtu 3 dní kedy začala strojárska firma fungovať v normálnom režime. Počas tejto doby fungovala strojárska firma v obmedzenom režime. Počet počítačov, ktoré ešte nemohli pristupovať k dátam firmy bol 5 čo tvorí 20% všetkých počítačov v strojárskej firme. Dopad kybernetickej hrozby sa zmenšoval. Finančne tento dopad vypočítame z nákladov na preinštalovanie softvéru **5 000,-**EUR, náklady na rekonštrukciu dát pre 5 počítačov 4 092 / 31 x 5 = **660,-** EUR a ušlý obrat strojárskej firmy za 1 deň pri nefunkčnosti 20% počítačov. Ušlý obrat predstavuje sumu 13 572 x 0,2 = **2 714,-** EUR. Výška dopadu kybernetického útoku ransomware na strojársku firmu bude v ďalšom 1 dni po čiastočnej rekonštrukcii dát vo výške **8 374,-** EUR

Celkový dopad kybernetického útoku na strojársku firmu prostredníctvom ransomware predstavuje za 5 dní čiastku 42 489 + 8 374 = **50 863,-** EUR.

Dopady zlyhania softvéru ako následok kybernetického útoku

Súčet hodnôt v tabuľke rizík je 780. Počet interakcií s ohrozenými prvkami je 7. Priemerná hodnota závažnosti hrozby je 780 / 7 = **111,43**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške **70%** z hodnoty ohrozených prvkov strojárskej firmy. Vo finančnom vyjadrení sa jedná o sumu 182 349 x 0,7 = **127 644,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na strojársku firmu v prípade poškodenia všetkých hmotných aj nehmotných aktív strojárskej firmy prostredníctvom zlyhania softvéru ako kybernetického útoku za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém SCADA/HMI v priemyselnej časti počítačovej siete strojárskej firmy nebol úplne funkčný je 1 z celkového počtu 3 dní kedy začala strojárska firma znova vyrábať. K úniku dát a poškodeniu hardvéru nedošlo. Následkom útoku prišlo k vypnutiu výrobnej linky strojárskej firmy a nefungovali ani ostatné zariadenia na výrobu a obrábanie súčiastok. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **5 000,-** EUR, ušlý obrat strojárskej firmy za 1 deň pri nefunkčnosti 60% počítačov a zariadení. Ušlý obrat predstavuje sumu 13 572 x 0,6 = **8 143,-** EUR. Vzhľadom k tomu, že strojárska firma nemohla plniť svoje záväzky po dobu 1 dňa, bolo poškodené aj jej dobré meno. Vyčíslenie výšky poškodenia dobrého mená za 1 deň nefunkčnosti výrobných zariadení vypočítame ako 60% jednej tretiny maximálnej hodnoty poškodenia dobrého mena strojárskej firmy. Hodnota poškodenia dobrého mena strojárskej firmy je 94 455 / 3 x 0,6 = **18 891,-** EUR. Výška dopadu zlyhania softvéru ako následok kybernetického útoku pre strojársku firmu bude v prvý deň vo výške **32 034,-** EUR.

Fáza po čiastočnej obnove systému

Počet dní kedy bol systém už čiastočne funkčný je 2 z celkového počtu 3 dní kedy začala strojárska firma obnovovať svoju výrobu. Počas tejto doby fungovala strojárska firma ešte v obmedzenom režime. Výrobná linka a zariadenia na obrábanie súčiastok v priemyselnej časti počítačovej siete strojárskej firmy fungujú na 60%. Dopad kybernetickej hrozby sa zmenšoval. Finančne tento dopad vypočítame z nákladov na preinštalovanie softvéru 5 000,- EUR, ušlý obrat strojárskej firmy za 2 dni pri nefunkčnosti 40% zariadení v priemyselnej časti počítačovej siete strojárskej firmy. Ušlý obrat predstavuje sumu 13 572 x 2 x 0,4 = **10 858,-** EUR. Vzhľadom k tomu, že strojárska firma nemohla plniť svoje záväzky po dobu ďalších 2 dní, bolo poškodené aj jej dobré meno. Vyčíslenie výšky poškodenia dobrého mená za 2 dni po čiastočnej obnove systému vypočítame ako 40% dvoch tretín maximálnej hodnoty poškodenia dobrého mena strojárskej firmy. Hodnota poškodenia dobrého mena strojárskej firmy je 94 455 / 3 x 2 x 0,4 = **25 188,-** EUR. Výška dopadu zlyhania softvéru ako následok kybernetického útoku na strojársku firmu bude po ďalších 2 dňoch a po čiastočnej obnove zariadení vo výške **41 046,-** EUR

Celkový dopad zlyhania softvéru ako následok kybernetického útoku na strojársku firmu za 3 dní je vo výške 32 034 + 41 046 = **73 080,-** EUR.

Dopady zlyhania hardvéru ako následok kybernetického útoku

Súčet hodnôt v tabuľke rizík je 1 025. Počet interakcií s ohrozenými prvkami je 9. Priemerná hodnota závažnosti hrozby je 1 025 / 9 = **113,89**. V percentuálnom vyjadrení je dopad kybernetického útoku vo výške 80%. Vo finančnom vyjadrení sa jedná o sumu 198 057 x 0,8 = **158 446,-** EUR. Táto finančná hodnota nám udáva maximálnu sumu dopadu na strojársku firmu v prípade poškodenia všetkých hmotných aj nehmotných aktív strojárskej firmy prostredníctvom zlyhania hardvéru ako kybernetického útoku za jeden deň.

Fáza najzávažnejšieho poškodenia systému

Počet dní kedy systém nebol funkčný je 5 z celkového počtu 7 dní kedy začala strojárska firma fungovať v normálnom režime. Počas tejto doby nemohlo k účtovným a personálnym dátam pristupovať 29 počítačov v celej počítačovej sieti strojárskej firmy. To tvorí približne 95% všetkých počítačov v strojárskej firme. Tento útok ovplyvnil aj výrobný proces v strojárskej firme. Strojárska firma nemohla vykonávať administratívnu agendu, uhrádzať svoje záväzky a nedodávala vyrobený tovar svojím odberateľom. K fyzickému poškodeniu hardvéru a dát nedošlo. Vyčíslenie výšky dopadu budeme počítať z nákladov na preinštalovanie softvéru **5 000,-** EUR, náklady na rekonštrukciu dát pre 29 počítačov 4 092 / 31 x 29 = **3 828,-** EUR, ušlý obrat strojárskej firmy za 5 dni pri nefunkčnosti 95% počítačov a zariadení. Ušlý obrat predstavuje sumu 13 572 x 5 x 0,95 = **64 467,-** EUR. Vzhľadom k tomu, že strojárska firma nemohla plniť svoje záväzky po dobu 5 dní, bolo poškodené aj jej dobré meno. Vyčíslenie výšky poškodenia dobrého mená vypočítame ako 95% z piatich sedmín maximálnej hodnoty poškodenia dobrého mena strojárskej firmy, 94 455 / 7 x 5 x 0,95 = **64 094,-** EUR. Výška dopadu zlyhania hardvéru ako kybernetického útoku na strojársku firmu bude v prvých 5 dňoch vo výške **137 389,-** EUR.

Fáza po čiastočnej obnove systému

Počet dní kedy bol systém už čiastočne funkčný sú 2 z celkového počtu 7 dní kedy začala strojárska firma fungovať v normálnom režime. Počas tejto doby fungovala strojárska firma v obmedzenom režime. Počet počítačov, ktoré ešte nemohli pristupovať k dátam firmy bol 8 čo tvorí 25% všetkých počítačov a zariadení v strojárskej firme. Dopad kybernetickej hrozby sa zmenšoval. Finančne tento dopad vypočítame z nákladov na preinštalovanie softvéru **5 000,-**EUR, náklady na rekonštrukciu dát pre 8 počítačov 4 092 / 31 x 8 = **1 056,-** EUR a ušlý obrat strojárskej firmy za 2 dni pri nefunkčnosti 25% počítačov. Ušlý obrat predstavuje sumu 13 572 x 2 x 0,25 = **6 786,-** EUR. Vzhľadom k tomu,

že strojárska firma nemohla plniť svoje záväzky ešte po dobu 2 dní, bolo poškodené aj jej dobré meno. Vyčíslenie výšky poškodenia dobrého mená vypočítame ako 25% z dvoch sedmín maximálnej hodnoty poškodenia dobrého mena strojárskej firmy, 94 455 / 7 x 2 x 0,25 = **6 747,-** EUR. Výška dopadu kybernetického útoku ransomware na strojársku firmu bude v ďalších 2 dňoch po čiastočnej obnove činnosti vo výške **19 589,-** EUR.

Celkový dopad zlyhania hardvéru ako následok kybernetického útoku na strojársku firmu za 7 dní je vo výške 137 389 + 19 589 = **156 978,-** EUR.

Tabuľka 35 Vyčíslenie dopadov kybernetických hrozieb na strojársku firmu

Kybernetická hrozba	Celková výška dopadu	Najvážnejšie/čiastočné poškodenie	Počet dní trvania poškodenia
Ransomware	50 863,- EUR	42 489,- EUR	2 dní
		8 374,- EUR	1 deň
Zlyhanie softvéru	73 080,- EUR	32 034,- EUR	1 deň
		41 046,- EUR	2 dní
Zlyhanie hardvéru	156 978,- EUR	137 389,- EUR	5 dní
		19 589,- EUR	2 dní

ZÁVER

V súčasnej dobe, kedy sú informačné a komunikačné technológie jednoznačne potrebné pre fungovanie takmer každej modernej spoločnosti, stúpa riziko zneužitia týchto systémov. Organizácie tieto systémy využívajú ako konkurenčnú výhodu oproti ostatným. Prvou výhodou môže byť to, že daný systém vôbec vlastnia a vedia si s ním zjednodušiť a zefektívniť pracovné činnosti. Druhá rovina konkurenčnej výhody môže byť chápaná ako schopnosť s týmito systémami správne zaobchádzať. To už ale nestačí len štandardne obsluhovať IT zariadenia, ale aj uvažovať nad ich bezpečným používaním.

V tejto diplomovej práci, v jej teoretickej časti, sme sa najprv zaoberali rozdelením spoločností a organizácií, ktoré môžu na základe zákona v Slovenskej republike existovať, ich právnu formu a organizačnú štruktúru a venovali sme sa aktívam, ktoré spoločnosti vlastnia. Okrajovo sme pokračovali informačnou bezpečnosťou, aby sme čitateľa viac a hlbšie oboznámili s kybernetickou bezpečnosťou organizácií, kde sme analyzovali možné riziká pôsobiace na organizácie a vyhodnocovali kybernetické hrozby a ich dopady pre organizácie. Záver teoretickej časti sa venuje oblasti oceňovania majetku organizácií so zameraním na oceňovanie nehmotných aktív, definovaním prístupov a metódami oceňovania nehmotného majetku.

V úvode praktickej časti sme ako prvé definovali hypotetické verejné zdravotnícke zariadenie, nemocnicu s poliklinikou s okresnou pôsobnosťou. Zamerali sme sa na jej aktíva, ktorými disponuje, a ktoré sú z pohľadu kybernetickej bezpečnosti potencionálnou kybernetickou hrozbou najviac ohrozené. Na základe vykonanej analýzy kybernetických hrozieb, ktoré na zdravotnícke zariadenie môžu pôsobiť sme vybrali tri najzávažnejšie hrozby. U týchto troch kybernetických hrozieb sme spracovali scenár vývoja bezpečnostnej situácie a pomocou vhodného postupu sme po jednotlivých fázach vývoja ocenili výšku dopadu kybernetických hrozieb na zdravotnícke zariadenie.

Druhou hypotetickou organizáciou, ktorú sme v praktickej časti diplomovej práce analyzovali bola súkromná výrobná organizácia pôsobiaca v strojárenskom priemysle. Na základe vykonanej analýzy sme aj v tomto prípade identifikovali aktíva spoločnosti a tri najnebezpečnejšie kybernetické hrozby. Ako ďalší krok sme aj tu spracovali scenár vývoja bezpečnostnej situácie a pomocou vhodného postupu ocenili výšku dopadov na aktíva strojárskej firmy pre tieto tri najnebezpečnejšie kybernetické hrozby v jednotlivých fázach vývoja.

Ocenenie výšky dopadov kybernetických hrozieb na hypotetické organizácie v našej diplomovej práci nám ukazuje, že kybernetické hrozby by organizácie nemali podceňovať. Dopady niektorých kybernetických hrozieb môžu byť pre organizácie pôsobiace v súkromnom a verejnom sektore veľmi zásadné, až likvidačné. Aj tie menej závažné dopady kybernetických hrozieb na organizácie spôsobujú škody, ktoré zhoršujú ich ekonomickú situáciu a často vedú k problémom v ich fungovaní. Ako jedno z riešení sa ukazuje zvyšovať povedomie zamestnancov o nebezpečenstvách kybernetických hrozieb spolu s investíciami do zaisťovania kybernetickej bezpečnosti technickými prostriedkami.

ZOZNAM POUŽITEJ LITERATÚRY

1. DĚDINA, Jiří a Václav CEJTHAMR. *Management a organizační chování: manažerské chování a zvyšování efektivity, řízení jednotlivců a skupin, manažerské role a styly, moc a vliv v řízení organizací*. Praha: Grada, 2005. Expert (Grada). 340 s. ISBN 8024713004.
2. VEBER, Jaromír. *Management: základy, moderní manažerské přístupy, výkonnost a prosperita*. 2., aktualiz. vyd. Praha: Management Press, 2009. 736 s. ISBN 9788072612000.
3. STRECKOVÁ, Yvonne a Ivan MALÝ. *Veřejná ekonomie: pro školu i praxi*. Praha: Computer Press, 1998. Business books (Computer Press). 226 s. ISBN 8072261126.
4. KÚTIK, Ján a Martina KLIEROVÁ. *Verejný sektor*. 1.vydanie. Trenčín: Trenčianská univerzita Alexandra Dubčeka, 2013. 190 s. ISBN 9788080755973.
5. NR SR. *Zákon č. 523/2004 Z.z. o rozpočtových pravidlách verejnej správy a o zmene a doplnení niektorých zákonov.*
6. NR SR. *Zákon č. 176/2004 Z.z. o nakladaní s majetkom verejnoprávnych inštitúcií a o zmene a doplnení niektorých zákonov.*
7. NR SR. *Zákon č. 111/1990 Z.z. o štátnom podniku.*
8. NR SR. *Zákon č. 213/1997 Z.z. o neziskových organizáciách poskytujúcich všeobecne prospešné služby.*
9. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). 309 s. ISBN 8086898385.
10. KOSTRECOVÁ, Eva. *Informačná bezpečnosť*. Bratislava: Slovenská technická univerzita, 2013. 83 s. ISBN 9788022739276.
11. LUKÁŠ, Luděk. *Teorie bezpečnosti I*. Zlín: Radim Bačuvčík - VeRBuM, 2017. 220 s. ISBN 9788087500897.
12. VACULÍK, Juraj. *Manažment bezpečnosti informačního systému*. Žilina: EDIS, 2018. 288 s. ISBN 9788055414621.
13. DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM*. 2., přeprac. vyd. Praha: Professional Publishing, 2011. 286 s. ISBN 9788074310508.

14. LUKÁŠ, Luděk. *Konvergovaná bezpečnost*. Zlín: Radim Bačuvčík - VeRBuM, 2019. 206 s. ISBN 9788087500996.

15. ČERMÁK, Miroslav. *Informační bezpečnost vs. kybernetická bezpečnost.* In: *CleverandSmart.cz* [online]. 2014, 26.11.2014, aktualizované 25.08.2015, [Cit. 12.5.2020]. Dostupné z: http://www.cleverandsmart.cz/information-security-vs-cybersecurity/

16. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. 220 s. ISBN 9788072513970.

17. NR SR. *Zákon č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov.*

18. PAVLÍK, Lukáš. *Návrh algoritmu pro stanovení pojistné hodnoty z pohledu kybernetické bezpečnosti*. Dizertačná práca. Zlín: Univerzita Tomáše Bati ve Zlíně, 2019. Školiteľ dizertačnej práce doc. Ing. Luděk Lukáš, CSc.

19. SVAČINA, Pavel. *Oceňování nehmotných aktiv*. Praha: Ekopress, 2010. 214 s. ISBN 9788086929620.

20. CVEČKOVÁ, Mária. Nehmotné aktíva podľa IAS 38 s príkladmi. Právny stav od 1.1.2014 do 31.12.2016. In: *Daňovécentrum.sk* [online]. ©2010-2020 [Cit. 26.4.2020]. Dostupné z: https://www.danovecentrum.sk/odborny-clanok/nehmotne-aktiva-podla-IAS-38-s-prikladmi.htm

21. MÚČKOVA, Barbora. *Ohodnocovanie dlhodobého nehmotného majetku* [online]. 2011 [Cit. 28.5.2020] Dostupné z: http://is.ambis.cz/th/tto5f/. Bakalárska práca. Vysoká škola regionálneho rozvoje a Bankovní institut - AMBIS, Bankovní institut vysoká škola SK. Vedúci bakalárskej práce prof. Ing. Štefan Cisko, CSc.

22. MALÝ, Josef. *Oceňování průmyslového vlastnictví: nové přístupy*. V Praze: C.H. Beck, 2007. C.H. Beck pro praxi. 182 s. ISBN 9788071794646.

23. NR SR. *Zákon č. 431/2002 Z.z. o účtovníctve.*

24. MLÁDEK, Robert. *IFRS and US GAAP: accounting policies and procedures = IFRS a US GAAP : postupy účtování*. Praha: Leges, 2017. Praktik (Leges). 400 s. ISBN 9788075021946.

25. ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015. ISBN 9788073959531.

26. ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. Brno: Tribun EU, 2009. Knihovnicka.cz. 134 s. ISBN 978-80-7399-731-1.

27. Sociálne inžinierstvo. *CSIRT.SK: Jednotka pre riešenie počítačových incidentov* [online]. Bratislava, ©2020. [Cit. 25.3.2020]. Dostupné z: http://www.csirt.gov.sk/bezpecnostna-studovna/bezpecnostne-hrozby-a-zranitelnosti/socialne-inzinierstvo-812.html

28. *IBM.COM: IBM Security: Cost of a Data Breach Report 2020* [online] ©2020. [Cit. 22.6.2020] Dostupné z: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

ASA	Adaptive Security Apliance (Adaptívne bezpečnostné zariadenie)
CAD	Computer Aided Design (Počítačom podporovaný návrh)
CGM	Compu Group Medical (Softvérová spoločnosť)
CNC	Computer Numeric Controll (Počítačové číselné riadenie)
CT	Computer Tomography (Počítačová tomografia)
DDoS	Distributed Denial of Service (Distribuovaný útok odmietnutie služby)
DMZ	Demilitary zone (Demilitarizovaná zóna)
DNS	Domain Name System (Systém názvov domén)
DoS	Denial of Service (Odmietnutie služby)
ESET	Softvérová spoločnosť
EUR	Euro (Európska spoločná mena)
FIFO	Firs In - First Out (Prvý dnu - Prvý von)
HELIOS	Ekonomický softvér
HMI	Human - Machine Interface (Rozhranie človek - stroj)
IAS	International Accounting Standards (Medzinárodný účtovný štandard)
IBM	Počítačová firma
ICT	Information and Communication Technologies (Informačné a komunikačné technológie)
IFRS	International Financial Reporting Standards (Účtovné zásady)
IOS	Internetwork Operating Systém (Sieťový operačný program)
IS	Informačný systém
IT	Information Technologies (Informačné technológie)
KNIS	Komplexný nemocničný informačný systém
LIFO	Last In - First Out (Posledný dnu - Prvý von)
LINUX	Počítačový operačný systém

NO	Nezisková organizácia
OBERON	Ekonomický softvér
PA	Per Annum (Ročne)
PACS	Picture Archiving and Communication Systém (Systém na správu, distribúciu a archiváciu obrazovej zdravotnej dokumentácie)
PC	Personal computer (Osobný počítač)
RESP	Respektíve
RTG	Röntgen
S4M	Zdravotnícky softvér
SCADA	Supervisory Control And Data Acquisition (Dispečerské riadenie a zber dát)
SQL	Structured Query Language (Štruktúrovaný dopytovací jazyk)
T-FLEX	Počítačový program na tvorbu parametrických modelov
TJ	To je
SRO	Spoločnosť s ručením obmedzeným
UPS	Uninterruptible Power Supply (Zdroj neprerušovaného napájania)
USB	Universal Serial Bus (Univerzálna sériová zbernica)
USD	United States Dollar (Americký dolár)
USG	Ultrasonograf
US GAAP	United States Generally Accepted Accounting Principles (Účtovné zásady)
VEMA	Softvérová spoločnosť, názov personálneho a mzdového softvéru
VLAN	Virtual Local Area Network (Virtuálna lokálna sieť)
Wi-Fi	Wireless Fidelity (Súbor štandardov pripojenia k bezdrôtovým sieťam)
ZZ	Zbierky zákonov

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK