UNIVERZITA PARDUBICE

FAKULTA EKONOMICKO-SPRÁVNÍ

BAKALÁŘSKÁ PRÁCE

2022 VOJTĚCH KRÁL

Univerzita Pardubice

Fakulta Ekonomicko-správní

Zabezpečení IT infrastruktury a vybraného informačního systému ve vybrané organizaci

Bakalářská práce

2022 Vojtěch Král

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: 2021/2022

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Vojtěch Král**
Osobní číslo:	**E19288**
Studijní program:	**B0688A140004 Informatika a systémové inženýrství**
Specializace:	**Informační a bezpečnostní systémy**
Téma práce:	**Zabezpečení IT infrastruktury a vybraného informačního systému ve vybrané organizaci**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování

Cílem práce je provedení průzkumu a vyhodnocení aktuálního zabezpečení IT infrastruktury a vybraného informačního systému ve vybrané organizaci a z těchto dat vyvodit doporučení ke zlepšení.

Osnova:
- Úvod do problematiky bezpečnosti IT infrastruktury a informačních systémů.
- Popis vybrané organizace a průzkum aktuálního stavu zabezpečení IT infrastruktury a souvisejícího vybraného informačního systému.
- Výsledky průzkumu a vyhodnocení možných hrozeb.
- Návrhy pro zlepšení zabezpečení ve vybrané organizaci.

Rozsah pracovní zprávy: **cca 35 stran**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

KIZZA, Joseph Migga. Guide to computer network security. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5
PETROVIČ, Michal a Michal KOSTĚNEC. CISCO NETWORKING ACADEMY PROGRAM. Bezpečnost počítačových sítí. Plzeň: Západočeská univerzita v Plzni, 2012. ISBN 978-80-261-0117-8
POŽÁR, Josef. Manažerská informatika. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9. Dostupné také z: https://ndk.cz/uuid/uuid:0b511f50-6cac-11e7-94b3-005056825209
SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7
ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2018. ISBN 978-80-7380-737-5

Vedoucí bakalářské práce: **Ing. Renáta Máchová, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. září 2021**
Termín odevzdání bakalářské práce: **30. dubna 2022**

L.S.

prof. Ing. Jan Stejskal, Ph.D. v.r.
děkan

RNDr. Ing. Oldřich Horák, Ph.D. v.r.
vedoucí ústavu

V Pardubicích dne 1. září 2021

Prohlašuji:

Práci s názvem *„Zabezpečení IT infrastruktury a vybraného informačního systému ve vybrané organizaci“* jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Beru na vědomí, že v souladu s § 47b zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších předpisů, a směrnicí Univerzity Pardubice č. 7/2019 Pravidla pro odevzdávání, zveřejňování a formální úpravu závěrečných prací, ve znění pozdějších dodatků, bude práce zveřejněna prostřednictvím Digitální knihovny Univerzity Pardubice.

V Pardubicích dne 30. 11. 2022

Vojtěch Král

PODĚKOVÁNÍ

Tímto bych rád poděkoval vedoucí mé bakalářské práce Ing. Renátě Máchové, Ph.D., za všestrannou pomoc, množství cenných a inspirativních rad, podnětů, doporučení, připomínek a zároveň za velkou trpělivost s obdivuhodnou ochotou při konzultacích poskytnutých ke zpracování této práce.

ANOTACE

Bakalářská práce je zaměřena na bezpečnost IT infrastruktury a vybraného informačního systému ve vybrané organizaci. Obsahem je úvod do problematiky datových sítí, informačních systémů a vysvětlení pojmů souvisejících s jejich bezpečností. To vše je využito při průzkum, vyhodnocení a návrhu na zlepšení ve vybrané organizaci.

KLÍČOVÁ SLOVA

Bezpečnost, informatika, systém, počítač, síť, IT infrastruktura

TITLE

Security of IT infrastructure and selected information system in a selected organisation

ANNOTATION

The bachelor thesis is focused on the security of IT infrastructure and selected information system in a selected organization. The content is an introduction to the topic of data networks, information systems and an explanation of terms related to their security. All this is used in research, evaluation and suggestion for improvement in the selected organization.

KEYWORDS

Security, informatics, system, computer, network, IT infrastructure

OBSAH

SEZNAM ILUSTRACÍ A TABULEK

SEZNAM ZKRATEK A ZNAČEK

ASP Aplication service providers

ARP Address resolution protocol

BIOS Basic Input-Output System

CAD Computer aided design

CCTV Closed-circuit television

DB Databáze

DHCP Dynamic host configuration protocol

DNS Domain name system

EDI Electronic data interchange

EIS Executive information systém

EPS Elektronický protipožární systém

EZS Elektronický zabezpečovací systém

GIS Geografical information systém

HW Hardware

IAAS Infrastructure as a service

IMAP Internet message access protocol

IP Internet protocol

IS Informační systém

ICT Information and communication technologies

IAAS Infrastructure as a service

KII Kritická informační infrastruktura

LAN Local area network

LDAP Lightweight Directory Access Protocol

MAC Media access control (adress)

MAN Metropolitan area network

MIS Management information system

MS Microsoft

NAS Network attached storage

NIC Network interface card

OIS Office information system

PAAS Platform as a service

PAN Personal area network

PC Personal computer

PCO Pult centrální ochrany

PIS Personální informační systém

RAID Redundant array of inexpensive disks

SAAS Software as a service

SŘBD Systém řízení báze dat

SMTP simple mail transfer protocol

SNMP Simple network management protocol

SQL Structured Query Language

SSH Secure shell

SW Software

TCP Transmission control protocol

UML Univesal modelling language

UPS Uninterruptible power supply

USA Spojené státy americké

USB Universal serial bus

VLAN Virtual local area network

VIS Významný informační systém

WAN Wide area network

ZKB Zákon o kybernetické bezepečnosti

ÚVOD

Správné zacházení s daty, informacemi a informačními technologiemi jsou pro úspěch organizace v dnešní době třetí průmyslové revoluce a neustálého konkurenčního boje jedním ze zásadních pilířů fungování podniku, firmy, státní správy a dalších tržních subjektů. Díky digitalizaci se stále více údajů zpracovává na počítačích v podobě binární soustavy jedniček a nul, přenáší ke koncovým uživatelům pomocí různých datových sítí a ukládá na digitální média. Již nestačí uložit smlouvu sepsanou na papíře do archivu ve sklepení, který má kvalitně zabezpečený vchod zámkem a opatřený nápisem „zákaz kouření“. V digitálním světě je možné informace nejen lehce uložit, ale také o ně stejně lehce přijít, nebo je modifikovat do požadovaného tvaru. Velkým tématem je proto v posledních letech téma bezpečnosti, které s každým rozšířením zprávy o novém útoku na jedince, organizaci či stát narůstá na důležitosti. Zabezpečení dat důležitých pro organizaci se může odehrávat na různých úrovních s různým stupněm bezpečnosti. Je nutné je chránit po celou dobu, po kterou mají hodnotu nebo nejsou zničena. Pro dosažení takové bezpečnosti je potřebné, aby organizace měla povědomí o svých významných statcích a znalosti z oboru bezpečnosti pro specifikaci co, proč a jak chránit.

Cílem této bakalářské práce je provedení průzkumu aktuálního stavu zabezpečení IT infrastruktury a informačního systému ve vybrané organizaci a z těchto dat vyvodit doporučení ke zlepšení. Dílčími cíli práce je seznámit čtenáře s problematikou tématu bezpečnosti IT infrastruktury a informačních systémů, popis vybrané organizace a průzkum aktuálního zabezpečení v této organizaci. Z výsledků průzkumu vyhodnotit možné hrozby a navrhnout, jak by vybraná organizace mohla své zabezpečení vylepšit.

1. ÚVOD DO PREOBLEMATIKY BEZPEČNOSTI IT INFRASTRUKTURY A INFORMAČNÍCH SYSTÉMŮ

Pro vyřešení bezpečnosti jakéhokoliv prostředí je nutné pochopit jeho základní fungování. Bezpečnost má základní prvky a jejich popsáním lze definovat bezpečnost nebo prvky, které mají být chráněny. Úvod do problematiky slouží pro zorientování se v aspektech bezpečnosti informačního systému (IS) a IT infrastruktury.

1.1 Data, informace

Pojmy, které se často zaměňují, přitom každý z nich má svoji definici. Oba pojmy mají úzkou souvislost v podobě znalostního řetězce. Data díky kontextu tvoří informaci a pomocí určení souvislostí mezi informacemi lze získat znalost, která může sloužit např. jako konkurenční výhoda.

Data

U informačních technologií byla data vždy chápana jako něco, co reprezentuje fakta či děj, které jsou zaznamenávány. Lze je rozdělit na strukturovaná (zachycují vlastnosti, fakta, atributy, popisují objekty aj.) a nestrukturovaná, kdy jsou vyjádřeny jako tok bitů (video, obrázek, textový dokument). Daty lze tedy označit zvuky, obrázky, texty a další vjemy určené pro zpracování počítačem. [1]

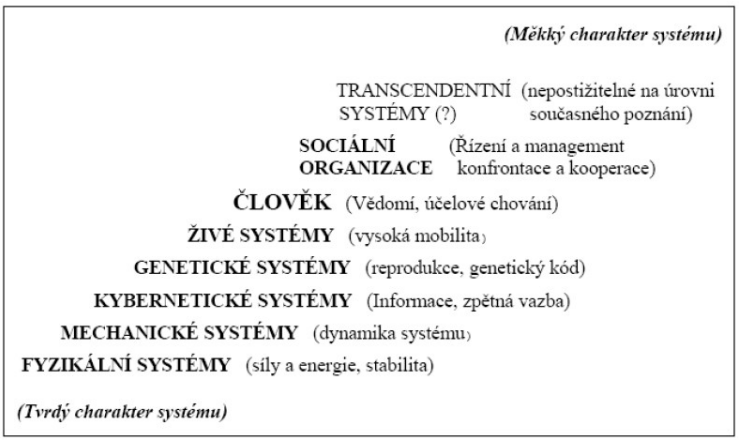
Informace

Pojem informace je multioborový, a patří mezi nejvíce obecné pojmy, kdy každý obor používá různě odlišný přístup k jejímu zkoumání. Teorie informace vytvořená pány C. E. Shannonem a N. Wienerem říká, že *„informace o nějakém jevu, je jistá veličina, která nám snižuje dosavadní neurčitost, neznalost právě o onom jevu.“* [2] Vhodným příkladem pro vysvětlení, odvozeným od Sklenáka [1] může být číslo 00420111222333 (data), které je ale užitečné pouze tomu, kdo hledá telefonní číslo a ví, že 00420 je předvolba pro Českou republiku a 111222333 tvoří telefonní číslo (informace).

Pro práci s informacemi je zapotřebí kvalitní informační základna, která následně tvoří podporu rozhodování a předvídání budoucí situace ve vnějším i vnitřním prostředí podniku. Vnitřní informační základnu dle Součka [3] tvoří informační technologie, specializované databáze a vzájemné propojení technologií uvnitř i s okolím (internet, dodavatelé).

1.2 Systém

Obecná teorie systémů hovoří o systému jako o na potřebnou (rozlišovací) úroveň zjednodušeném prostředí, které je jasně ohraničeno, ve kterém pomocí vazeb probíhá komunikace mezi jeho prvky a mezi systémem a jeho okolím mohou probíhat interakce. Tedy ne každý objekt je systém, ale existence systému neznamená že nejde o objekt – například stůl systémem není, zatímco auto ano. Částmi, které systém vytvářejí, jsou dle Jančíkové [4, s. 7-10]: **prvek** je na dané rozlišovací úrovni dále nedělitelná část systému, ale zároveň může tvořit další samostatný systém, který poté nazýváme **subsystémem**. Prvky mezi sebou komunikují pomocí **vazeb**. Jde o způsob propojení tvořící jeho uspořádání, tedy **systémovou strukturu** mezi prvky nebo spojení prvků a okolí systému, kdy takové propojení může být vnitřní či vnější a dle způsobu propojení jde o vazby sériové, paralelní nebo zpětně zapojené. Vazby jsou také různě ohodnocené pomocí parametrů, které mohou udávat rychlost propojení, násobnost vazby apod. Prvky, které nejsou součástí systému, ale vykazují k němu důležité vazby tvoří **okolí systému**. Množina vazeb, kterými systém působí na okolí, se nazývá **výstupy**. Okolí působí opačným směrem pomocí **vstupů**. Při hodnocení **času odezvy** se hovoří o uplynulém čase, který je potřebný k zpracování vstupu na výstup. Jako další složky uvádí Komárková a kolektiv [5, s. 10] **parametry** jako proměnné přiřazené prvkům a vazbám, a **transformační funkce** určující jejich hodnoty.



Obrázek 1 - Bouldingovo rozdělení systémů

Zdroj: [5, s. 11]

Systémy díky multiplatformitě a různé škále objektů a situací, které můžou popisovat, získaly několik klasifikací a rozdělení. Nejčastěji se uvádí rozdělení popsané ekonomem K. Bouldingem zobrazené na Obrázek 1, který rozděluje systémy mezi tvrdé a měkké dle jejich předvídatelnosti a chování. Čím měkčí charakter, tím je těžší předvídání chování systému a tím více čerpají ze systémů nižších (tedy tvrdších), které řeší problémy specifické a dobře

strukturované. Pokud je na firmu použit systémový přístup, výsledkem je mnoho procesů, které by bylo dobré automatizovat, sloučit s dalšími částmi a vytvořit tak ucelený systém. Pokud je systém zpracováván jako SW a je podpořen vhodným HW, lze hovořit o informačním systému jako podpoře potřebného odvětví firmy, začlenitelného do vnitřní IT infrastruktury.

1.3 Informační systém

Jedna z definic hovoří obecně o IS právě tehdy, pokud jde o vzájemné propojení informací a procesů které s těmito informacemi pracují (zpracovávají je z informací do systému vstupujících na informace vystupující). [6, s. 129] Pro lepší pochopení je vhodnější definice dle Laudona [7, s. 37], který hovoří o *„souboru vzájemně propojených komponent, které shromažďují (nebo načítají), zpracovávají, ukládají a distribuují informace za účelem podpory rozhodování, koordinace a řízení v organizaci.“* Nejde tedy o jednoduchý SW používaný v organizaci, ale o mnohem komplexnější systémy, sdružující takové nástroje, které mají vliv na chod organizace. Jako komponenty informačního systému uvádí Danel [8, s. 6]:

- software a hardware,
- databáze, datové zdroje (dataware),
- lidskou složku (peopleware),
- organizační uspořádání firmy (orgware),
- kontext IS – reálný svět.

1.3.1. Komponenty IS

Čtyři základní komponenty tvořící systém, jsou ovlivněny reálným okolím, do kterého jsou umístěny. To tvoří exogenní vlivy, které předvídat nelze a jejich popis je velmi obtížný (mohou se neustále objevovat, měnit, mizet). Zbylé prvky lze určit lépe, a to pomocí analýz stávajícího a budoucího stavu, aplikováním systémových přístupů, nebo pouhým pozorováním.

Software a hardware

Jako **software** lze popsat samotný informační systém, ale může do něj také zasahovat jiné programové vybavení firmy, které se stane součástí IS, nebo ho využívá ke svému chodu. Jedná se o různé operační systémy, programy obsluhující databáze a například i ovladače HW, které mohou ovlivňovat chod IS - např. grafické zobrazení.

Jako **hardware** lze považovat veškeré komponenty IT infrastruktury, které ovlivňují chod IS. Jde o servery, PC, síťové prvky (routery, switche). Hardwarem jsou i další síťové prvky jako kabeláž, zásuvky, tiskárny apod. Jde vždy o část, kterou IS využívá pro svůj chod. Tyto

technologie může firma provozovat na vlastních komponentách (i existujících) v uzavřeném a díky tomu kontrolovatelném prostředí. Tento způsob je nejvíce bezpečný a ovšem vyžaduje vlastní ICT oddělení a hrozí konflikt s případným dodavatelem SW. Další možností je některá z forem outsourcingu – pronájem virtuálního prostředí, nebo celého zařízení (serveru), který může být provozován uvnitř firmy nebo vzdáleně v housingu[1] poskytovatele. Je možné také využít možností pronájmu infrastruktury (IAAS), kdy je zpoplatněn přístupový čas k poskytnutým prostředkům a zákazník si pronajímá výpočetní výkon.

Databáze, dataware

Jedná se o jednu z nejdůležitějších částí IS. Zabezpečuje ukládání dat do souborů s pevně daným uspořádáním. Pokud tvůrce zvolí nesprávný návrh a technologii databáze, bude celý systém degradován. Pokorný [9, s. 33-45]definuje databázi jako „*systém sloužící k modelování objektů a vztahů reálného světa (včetně abstraktních nebo fiktivních) prostřednictvím digitálních dat uspořádaných tak, aby se s nimi dalo efektivně manipulovat, tj. rychle vyhledat, načíst do paměti a provádět s nimi potřebné operace – zobrazení, přidání nových nebo aktualizace stávajících údajů, matematické výpočty, uspořádání do pohledů a sestav apod.*“ I přes uvedení databáze jako systému, se mezi databází a tazatelem nachází další ovládací prvek, systém řízení báze dat (SŘBD), který má na starosti právě řízení přístupu k datům a práce s nimi, snižuje duplicitu dat, umožňuje simultánní přístup aj.

Peopleware

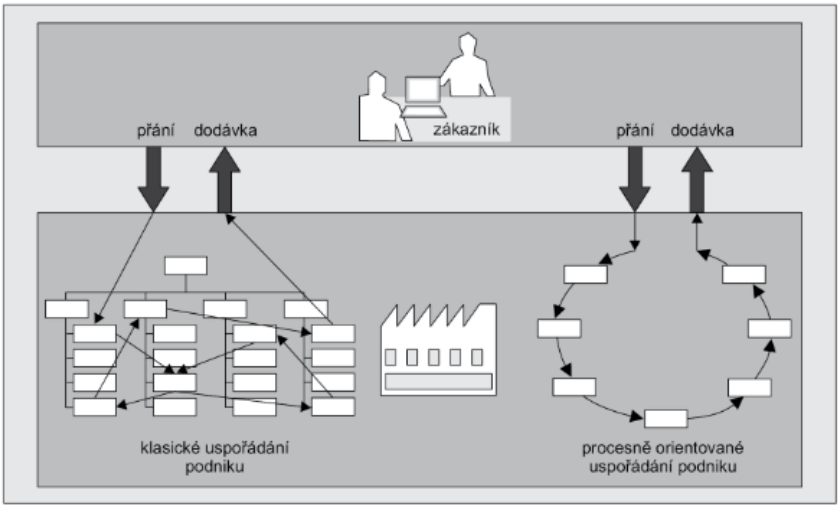
Termín, který poprvé použil P. G. Neumann v roce 1976, odkazuje na fakt, že lidé jsou stejně důležití jako SW nebo HW, protože bez nich by nedošlo k použití ani ke vzniku IS a spolu tvoří koncepční trojúhelník. Lidé se objevují v rolích uživatelů, projektových týmů, administrátorů, vývojářů, zákazníků i jako okolí v podobě útočníků či konkurence [10]. IS je navíc budován na základě pohledů na fungování mezi zadavatelem, projektantem IS a uživatelem. Požár [6, s. 138] upozorňuje že právě díky odlišným postojům a chybám v dorozumívání, nebo nepochopení obsluhovaných dat může být systém i několikrát opravován, než dojde k jeho plnému nasazení.

Organizační uspořádání

Prukner [11] definuje organizační strukturu jako „*organizovaný systém, ve kterém je práce rozdělena, seskupena a koordinována*“. Velmi dobře pro základní pochopení shrnuje problematiku Cejthamr s Dědinou [12, s. 203], kteří popisují organizaci takového systému jako

[1] Server housing – pronájem fyzického serverového prostoru, nebo celého serveru

uplatňování rozhodovacích pravomocí a sdružování činností, které tvoří obsahovou náplň lidí či organizačních jednotek. To nejlépe tak, aby byl brán ohled na velikost a zaměření podniku. Dle rozhodovacích pravomocí dělíme organizační struktury na tři základní typy: liniovou, štábní nebo jejich kombinaci (liniově štábní, maticové, projektové…). Jako ukázku obsahových náplní uvádějí Cejthamr a Dědina [12, s. 214] základní nezbytné funkce průmyslového odvětví pro odbyt produktu: výroba, marketing, finance, účetnictví a personalistiku. Procesní přístup k rozdělení podniku, zobrazený na Obrázek 2, je velmi dobře aplikovatelný na IS. Lze díky němu vytvořit procesní mapu a lépe stanovit jednotlivé úkoly, oprávnění a povinnosti k určitým oddělením nebo odpovědným osobám.



Obrázek 2 - Rozdíl mezi klasickým a procesním uspořádáním podniku

Zdroj: [13, s. 114]

1.3.2. Zdroje informací pro IS

Data ukládaná v IS můžou mít různý původ, kvalitu i reprezentační schopnost. Základní rozdělení uvádí Basl [13, s. 52] a rozlišuje data dle druhu nosiče informací na:

- informace již zapsané v databázích, která vylučují přímou účast člověka,
- informace uložené na jiných „klasických" nosičích – různé doklady, formuláře, předpisy a další formou dané dokumenty (většinou v papírové podobě),
- informace od odborníků, zkušenosti, které nejsou nikde zaznamenané (uložené v hlavách zaměstnanců).

IS se dělí podle zdroje informací na **interní** a **externí**. Interními zdroji může být strategický plán organizace, různé předpisy, zápisy z porad, obchodní smlouvy, metodické přípisy, výplatní pásky aj. Jako externí zdroje lze označit veřejně dostupné zdroje (zákony, vyhlášky, úřední

výstupy, mapy…), web (zejména po nástupu webu 2.0 - sociální sítě, sdílený obsah) a konkurenční zpravodajství. Brabec [2, s. 212] uvádí nejčastější původ informací v podnikové praxi:

- z oboru podnikání – zejména interní typ informací, pokud vnější, dotýkají se přímo oboru podnikání (návody, pracovní postupy),
- právní – nezbytné právní předpisy, opět týkající se směru podnikání,
- ekonomické – účetní a daňové informace, zejména se vztahem k finančnímu úřadu,
- z trhu – různé tržní inzerce, reklamy, vývoj technologií, marketing apod.,
- obchodní – jde o různé obchodní smlouvy,
- organizační, personální, všeobecné, specifické.

Informace prochází v IS životním cyklem zobrazeným na Obrázek 3, ze kterého vyplívá neustálý koloběh informace systémem. Její načítání, zobrazování, ukládání i případné vymazání. Ve všech těchto situacích musí být brána v potaz bezpečnost.

Obrázek 3 - Životní cyklus informace

Zdroj: [14]

1.3.3. Pořízení a provoz IS

Pořízení IS v organizaci provází mnoho kroků, od uvědomění si jeho potřeby, přes analýzu, návrh, pořízení, implementaci, zpětnou kontrolu a případné upravení nebo rozhodnutí o dalším použití. K jeho pořízení musí vést určitý motiv. Nejčastěji se jedná o požadavky v organizaci, kde se již s výpočetní technikou pracuje a je žádoucí zavést jistý druh automatizace procesů, které probíhají v analogové podobě, nebo pokud chce podnik zvýšit svoji efektivitu vnitřních procesů, kooperaci s okolím nebo soupeřit s konkurencí pomocí zavedení inovací. Pořízení může probíhat formou použití **hotového řešení**, případně rozšířením již stávajícího řešení, kdy se organizace částečně přizpůsobuje vybranému IS. Může být také přizpůsobeno hotové **řešení na míru**, což je nákladnější. Je možné kompletní naprogramování **vlastními silami** (využití

vlastního IT oddělení), což je oproti předchozím metodám náročné na personální zdroje a čas. Varianty shrnuje Basl [13] v Tabulka 1.

Tabulka 1 – Varianty řešení IS

Varianty řešení	Pro	Proti
Rozvoj existujícího systému	- maximální využití existujících zdrojů - z krátkodobého hlediska lacinější a rychlejší - uspokojení okamžitých potřeb	- nemusí odpovídat všem budoucím požadavkům - celkové náklady mohou být vyšší - výsledkem může být méně kvalitní systém
Vývoj nového systému na míru	- Může přesně odpovídat potřebám podniku - řízený vývoj	- celkově dražší řešení - časově náročné řešení - riziko negarantovaného konečného produktu a jeho vývoje
Nákup hotového řešení	- dlouhodobě finančně méně náročný - rychlejší zavedení - zaručená funkčnost a další vývoj	- nemusí přesně splňovat všechny požadavky uživatele - závislost na dodavateli

Zdroj: [13, s. 55]

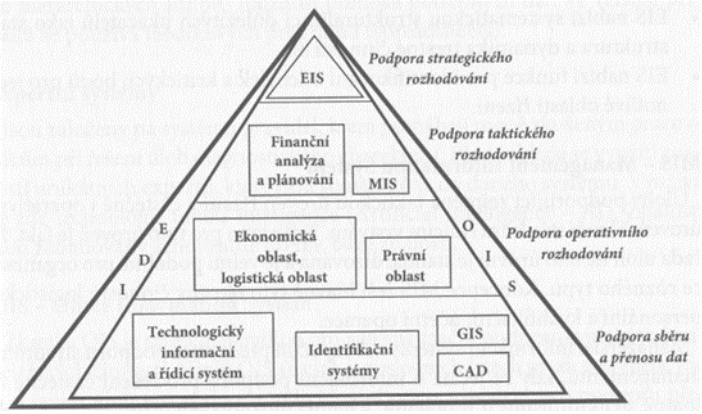
Podobně jako je tomu u pořízení, lze IS provozovat několika způsoby. Lze je provozovat uvnitř firmy vlastními silami, nebo je pořídit také jako služby – PAAS (je poskytována celá platforma, zákazník pouze zajišťuje samotný software), SAAS (uživatel si pronajímá licence, nestará se o programové ani technické vybavení, neřeší zabezpečení) nebo ASP, která je asi největším uzpůsobením pro firmu (vlastní nastavení a provoz oddělený od ostatních, sdružuje všechny předchozí možnosti), ale může také znamenat pomalou odezvu na problémy díky více zainteresovaným stranám.

1.3.4. Druhy IS

Všeobecně lze rozdělit IS do dvou základních kategorií, kterými jsou podnikové systémy a veřejné informační systémy. Podnikové lze dále rozdělit na univerzální, které mají největší množství využití (ekonomické, fakturační), pro specifické účely a informační systémy [15] na míru (například „PID lítačka“ – IS pražské integrované dopravy). Dále je možné je rozdělit do základních typů dle využití a vztahu k řízení podniku [6, s. 133]:

- systémy pro podporu strategického rozhodování (EIS),
- systémy taktického rozhodování (finanční IS, MIS),
- systémy pro operativu (logistika, právní oblast),
- systémy pro podporu sběru a přenosu dat (technologie, GIS, CAD).

Spolu s uvedenými systémy existuje OIS a EDI vrstva. OIS jsou systémy, které používají všechny skupiny systémů a jsou jim společné. Jde zejména o podpůrné kancelářské balíky jako MS Office. EDI je systém, který zajišťuje komunikaci mezi jednotlivými systémy i vrstvami a propojuje je. [6, s. 135]



Obrázek 4 - Druhy informačních systémů

Zdroj: [16, s. 182-193]

1.4 IT infrastruktura

Procházka [17] definuje IT infrastrukturu jako *„technologie a prvky nutné k provozu IT, jedná se nejen o vlastní využívaný software, hardware (datová centra, servery, počítače, notebooky), základní software (operační systémy, databáze), sítě a síťové prvky, ale také o periferie (monitory, tiskárny, skenery), telefony a telefonní ústředny“* a která slouží pro uchování, zpracování a zobrazování dat. Protože je infrastruktura nedílnou součástí IS, základní informace o jejích součástech jsou uvedeny v oddílu 1.3.1 o komponentách IS.

1.4.1. Síťové prvky

Jde o všechny prvky, které jsou do sítě zapojené nebo slouží k jejímu chodu, tedy přijímají, vysílají nebo přenáší data. Stryhal [18] je rozděluje na **aktivní,** které působí na přenášené signály a vyžadují elektrické napájení, a **pasivní**, které napájení nevyžadují a slouží k přenosu dat. Aktivními prvky jsou osobní počítače a servery, což jsou počítače přizpůsobené pro nepřetržitý běh, které simultánně obsluhují více uživatelů nebo procesů. Sosinky [19, s. 128] uvádí pět základních typů serverů – **souborový / tiskový**, **aplikační** (pro databáze, webové služby, e-mail či software), **zálohovací**, **síťový** (poskytující směrovací a identifikační funkce jako např DHCP, DNS) a **doménový** (jako základ pro rozsáhlé sítě). Dle Štráfeldy [20] může jako server sloužit nainstalovaný SW, který se po nastavení chová jako fyzický stroj, díky čemuž předchozí typy serverů nahradí jeden fyzický provozující několik virtuálních služeb. Dalšími nejčastějšími aktivními prvky jsou repeater, switch, hub a router. Pasivní prvky

v podobě zásuvek, konektorů a přenosových medií doplňují různé typy rozvaděčů (racky, patchpanely). „*Přenosovým médiem jsou média schopná přenášet elektromagnetický signál*“. [19, s. 28]

Hub (rozbočovač)

Jednoduché pasivní zařízení provozované na fyzické vrstvě, sloužící pouze k prodloužení dosahu sítě. Do signálu nijak nezasahují, pouze ho rozešlou dál do všech směrů.

Repeater (opakovač – aktivní rozbočovač)

Jde o napájený zesilovač, který příchozí signál na fyzické vrstvě vytvoří znovu a přeposílá dál se stejnými parametry. V pevných LAN sítích se téměř nepoužívá, smysl má zejména u bezdrátových sítí, které mají omezený dosah. [19, s. 202]

Bridge (most)

Vychází z opakovače, je ale mnohem sofistikovanější. Zatímco opakovač pouze propojí dvě části (sběrnice) a neřeší co a kam je posíláno, most ze zprávy získá informace o cíli a předá ji pouze v případě jeho existence. Komunikace na jedné straně neovlivní stranu druhou, pokud to není vyžádáno. [21, s. 154].

Switch (přepínač)

Sosinky [19, s. 203] uvádí, že jde o aktivní zařízení, které spojuje minimálně dvě sítě na dvou a více vrstvách, ale že jeho definice není pevně stanovena. Uvádí také, že dnes switche plní mnoho dalších funkcí, které nahrazují jiné prvky jako mosty, rozbočovače a jiné. Dnes se jedná o multiplatformní zařízení, které dokáže obsáhnou vlastnosti potřebné pro obsloužení všech vrstev síťové komunikace (filtrování, VLAN, velké množství portů atd).

Router (směrovač)

„*Směrovač je zařízení, které propojuje různé sítě. Rozděluje kolizní domény, filtruje a rozděluje všesměrové vysílání a zjišťuje optimální trasu pro směrování paketů (zpráva rozdělená do malých částí) k cíli*“. [19, s. 207] Funguje na síťové vrstvě. Většina routerů má v dnešní době integrovány další služby jako DHCP nebo DNS.

1.4.2. Komunikace v síti

Komunikace mezi zařízeními může probíhat analogově nebo digitálně. Vzhledem k rozšířenosti digitálních technologií, by pro analogový přenos bylo zapotřebí použít digitální převodníky, které by snižovaly největší konkurenční výhodu analogové technologie – rychlost. Proto dále není analogový přenos zohledněn. Pro komunikaci v digitálním prostředí se nejčastěji používá

přenos binárních hodnot (dvojková číselná soustava v hodnotách 1 a 0). Tyto hodnoty spolu s Booleovou logikou[2] tvoří dnešní základ výpočetních technologií. Dle rozsahu se dělí sítě na **rozlehlé** (WAN), někdy definované jako síť ze sítí, **lokální** (LAN), které jsou tvořeny od dvou propojených PC v jedné místnosti až do spojení několika budov. Jako hlavní oddělující prvek sítí LAN je považován vložený router nebo bridge. Třetím typem sítě je **metropolitní** (MAN) nebo **univerzitní** (CAN), které jsou nejčastěji uváděny příkladem spojení poboček jedné společnosti na větší vzdálenosti pomocí páteřního spojení (např. optickým kabelem). Jako nejmenší je uváděna **personální** síť (PAN), která slouží pouze pro uživatele, například mezi počítačem a datovým úložištěm (NAS). Každá taková síť tvoří určitou topologii zapojení. Kizza [22, s. 13] dělí topologie na:

- **Typ síť (mesh)** – vzájemné propojení nejbližších prvků, jde o odolné řešení při výpadku jednoho spojení ho lze nahradit „jiným“ – používá se zejména v MAN,
- **typ strom (tree)** – připomíná kořeny stromu, kdy v hierarchické struktuře je na vrcholu dominantní prvek sítě a ostatní pod ním paralelně připojeni v několika větvích – problémem jsou poruchy, kdy porucha uprostřed způsobí výpadek pro podřízený zbytek dané větve,
- **typ sběrnice (bus)** – všechny prvky sítě jsou postupně připojeny k centrálnímu páteřnímu vedení – řešení náročné na antikolizní mechanismy – pouze jeden element má v daný okamžik nad sběrnicí kontrolu a určuje pořadí ostatních [22, s. 14],
- **typ hvězda (star)** – Používané zejména u LAN, všechny prvky jsou přímo připojené do prvku centrálního. Po centrálním prvku je požadována vysoká režie (výkon), navíc jeho selhání má za následek rozpad celé sítě,
- **typ kruh (ring)** – prvky jsou připojeny do kruhové topologie, tedy k informaci se může dostat kterýkoliv z nich, stejně tak je připojen řídící prvek (server). Kdo vysílá je řízeno systémem tokenů.

Aby přenos v síti nebyl chaotický a měl svá daná pravidla (také aby byl univerzální), vznikla iniciativa standardizační komise (jak správně uvádí Sosinky [19, s. 44] vzniklo obdobným způsobem mnoho dalších standardů, jako například webový W3C nebo standardizační ISO). Ta stanovila základní model komunikačního protokolu, nazvaného **ISO/OSI**. Ten určuje 7 vrstev modelu: fyzickou, linkovou, síťovou, transportní, relační, prezentační a aplikační jejichž použití shrnuje Tabulka 2. V praxi se síť používající tento model nevyskytuje. Je

[2] Booleova logika – založena na pravdivosti nebo nepravdivosti, které může nabývat logický výrok založený na binárních hodnotách. Vztahy mezi proměnnými se vyjadřují operátory AND, OR, NOT.

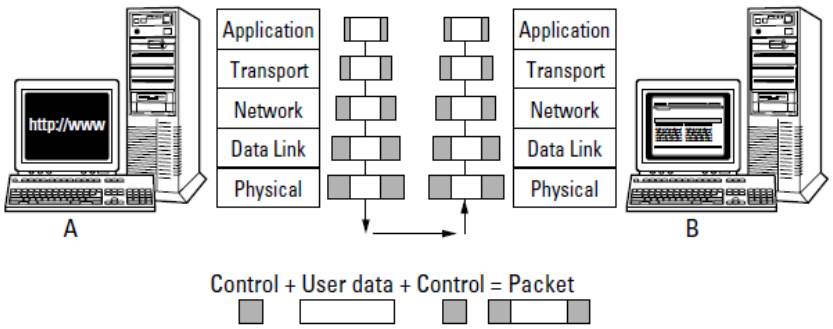
důležitý pro základní pochopení, protože ostatní modely z něho vycházejí, ale díky agregaci různých vrstev je složitější z nich pochopit základy.

Tabulka 2 - Vrstvy modelu ISO

Vrstva	Způsob přenosu	Funkce
Aplikační	Data	Zajišťuje síťové spojení mezi aplikací a sítí
Prezentační	Data	Formátují se zde data do podoby zpracovatelné příjemcem
Relační	Data	Zakládá unikátní spojení mezi aktéry přenosu a zajišťuje korektnost dat
Transportní	Segmenty nebo datagramy	Řídí hlavní aspekty přijímání a odesílání dat
Síťová	Pakety	Řeší adresaci systémů, mezi kterými dochází k výměně dat
Linková	Rámce	Adresace hardwaru
Fyzická	Bity	Definuje přenosové médium (kabely, radiové vlny…)

Zdroj: [19, s. 45]

Pro datovou komunikaci je dnes nejrozšířenějším protokolem TCP/IP, jehož aktuální podoba vznikla v roce 1980 a na jeho největším rozšíření se podílelo ministerstvo obrany USA svým rozhodnutím o nasazení v armádě připojené v té době k ARPANETU [23], kdy postupně v devadesátých letech došlo k nasazení i v soukromé sféře. TCP/IP je na rozdíl od OSI modelu tvořen pěti vrstvami zobrazenými na Obrázek 5 : aplikační, transportní, internetovou a vrstvou síťového rozhraní. Leiden [24, s. 22] uvádí ještě fyzickou, jako pátou samostatnou vrstvu.

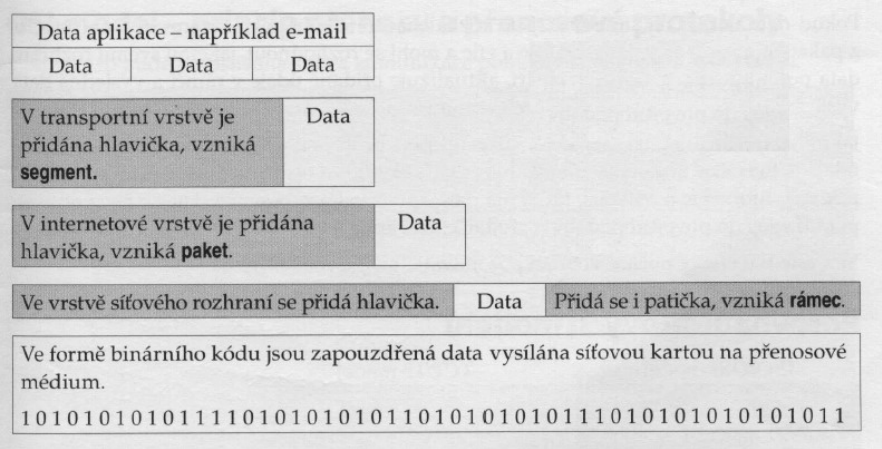


Obrázek 5 - Sestavení rámce v jednotlivých vrstvách TCP/IP protokolu

Zdroj: [24, s. 23]

Poslání dat v síti probíhá, obdobně jako na Obrázek 5, navázáním komunikace (datové spojení) mezi dvě zařízeními, kdy „počítač B“ požádá například o zobrazení emailu emailový server „počítač A“. „Počítač A“ připraví požadovaná **data** (aplikační vrstva) a předá je transportní vrstvě, která vytvoří **segment** přidáním hlavičky. Segment obsahuje informace o uspořádání a obsahu dat, aby data byla předána ve správné podobě (nic nebude ztraceno, pakety budou sestaveny ve správném pořadí). Segment je poté předán síťové vrstvě, která do hlavičky přidá adresy zdroje a cíle a vznikne tak **paket**. Paket je předán do vrstvy síťového rozhraní dalším

rozšířením hlavičky a přidáním patičky, do kterých jsou přidány informace o zdrojové a cílové MAC adrese a informace o síťové kartě (NIC). Takto zkonstruovaný **rámec** je po fyzické vrstvě odeslán do „počítače B“ kde jsou zpětnou konstrukcí data zobrazena v emailovém klientovi. Proces stavby rámce z dat je zobrazen na Obrázek 6.



Obrázek 6 - sestavení datového rámce v TCP/IP protokolu

Zdroj: [25, s. 37]

Přídomek IP v názvu protokolu TCP/IP znamená využití internetového protokolu, jehož smyslem je udržení propojení mezi koncovými body a je odpovědný za vytvoření rámců a jeho odeslání po IP síti za pomoci IP adresy. Tento protokol nemá žádné požadavky na typ přenosu. Proto ho lze velmi dobře využívat i v místech, kde se násobně mění typ spojení z kabelového na bezdrátový či optický.

1.4.3. Síťové protokoly a služby

Přes síť se v dnešní době přenáší velké množství informací a provozuje neméně služeb, pro které existují daná pravidla. Ta se nazývají síťové protokoly a vyskytují se na všech úrovních síťové komunikace. [26] S těmito protokoly souvisí i několik základních služeb, bez kterých by síť fungovala pouze v omezené míře. Při jejich znalosti, lze o síti získat velmi dobrý přehled, který lze využít pro snazší správu, nebo zneužít k nelegální činnosti.

DNS (domain name system)

Služba a protokol, která má na starosti překlad internetových jmen na IP adresy. Protože pamatovat si adresy, které mají číselný formát není snadné, byl vymyšlen systém přiřazených názvů jako www.upce.cz. Pokud si jej tedy klient vyžádá zadáním do prohlížeče, DNS server ze svých záznamů (nebo záznamů jiných DNS serverů) zjistí že má správně vyžadovat IP adresu 195.113.142.152 a přeloží ji síti pro uživatele. [25, s. 45]

ARP

Address resolution protocol (ARP) slouží k převodu síťové IP adresy na fyzickou MAC adresu jeho síťového rozhraní.

DHCP

Protokol dynamického a automatického přidělování adres. Pokud se počítač připojí do sítě, tento protokol a jemu nadřízená služba zařídí ověření, zda se může připojit (nebo zda je přístup umožněn komukoliv). Pokud ano, zda má již danou adresu nebo požaduje automatické přidělení. DHCP tedy eviduje přidělené IP adresy, MAC adresy zařízení, rozsah adres, které může přidělit. Automaticky připojenému zařízení přidělí IP adresu, masku podsítě, výchozí bránu, adresy serverů DNS.

SNMP

SNMP (Simple Network Management Protocol) Slouží pro správu zařízení a sítí. Každé zařízení podporující tento protokol je pomocí všesměrově posílaných dat schopné informovat o svém stavu (stav toneru v tiskárně, aktivní připojení switchů v síti apod).

SMTP, POP3, IMAP

Protokoly obsluhující elektronickou poštu. Simple mail transfer protocol (SMTP) je protokol pro přenos emailových zpráv mezi serverem a programy spravujícími e-mail, kterým se zabezpečuje spojení mezi klientem a serverem. POP3 následně slouží pro samotné stahování zpráv. Internet message access protocol (IMAP) umožňuje vzdálený přístup k uživatelově e-mailové schránce včetně pokročilé správy. [26]

PROXY

Jde o službu, někdy samostatný server, která má na starosti zprostředkování komunikace mezi LAN či MAN a internetem. Umožňuje filtrování komunikace na základě síťových portů, IP adres nebo celých služeb za použití předdefinovaných pravidel. Je možné nastavení odstranění webových reklam, blokování přístupu na webové stránky aj. [22, s. 260]

Telnet, SSH

Telnet protokol umožňuje za použití stejnojmenného programu vzdálené připojení k zařízení a jeho následné textové vzdálené ovládání. Komunikace v tomto protokolu není šifrována, je proto nahrazován protokolem Secure shell (SSH). Ten není pouze ovládacím, ale kompletním komunikačním protokolem pro komunikaci v nezabezpečené síti.

LDAP

Lightweight Directory Access Protocol (LDAP) je úložištěm, které uchovává a zpřístupňuje certifikáty, případně seznam odvolaných certifikátů. Usnadňuje přístup autentizovaného uživatele, který se nemusí znovu přihlašovat pod jedním účtem k více aplikacím. [22, s. 246]

1.4.4. Operační systémy

Brookshear [21, s. 122] definuje operační systém (OS) jako „*software, který řídí základní fungování počítače. Umožňuje uživatelům ukládat a načítat soubory, poskytuje rozhraní, aby mohl uživatel spouštět programy, a nabízí prostředí, které je potřebné k činnosti požadovaných programů*“. OS pomáhá uživateli ovládnout používaný HW a SW tak, aby vzájemné použití bylo co nejefektivnější s ohledem na zdroje. Tedy aby souběžně běžící programy běžely efektivně a dokázaly sdílet paměť, procesor a komunikovaly s okolím (zobrazování na obrazovce, posílání zpráv přes síť), aniž by zahltily poskytnuté prostředky. Klíčovým prvkem je virtualizace prostředí, která umožňuje poskytnout omezené fyzické zdroje více počítačům současně – OS poskytuje služby přidělování těchto zdrojů. Nejznámějšími operačními systémy jsou Windows, Linux a MacOS. Zároveň poskytuje pro uživatele a obsluhující první bezpečnostní bariéru díky bezpečnostním mechanismům, nebo nebezpečí v podobě neošetřených zranitelností OS. Většina operačních systémů již v základu obsahuje také sadu nástrojů pro základní práci. U desktopových verzí určených pro PC jde například o jednoduché textové a grafické nástroje, multimediální přehrávače nebo anti-malwarová řešení. U serverových distribucí se jedná o nástroj pro snazší administraci, logování a sledování jeho stavu. Některá rozšíření jako Active Directory, služba DHCP, DNS usnadňuje následnou činnost serveru v síti (administrátor je nemusí složitě instalovat a jsou dobře připravená k nastavení).

- Active Directory je adresářová služba fungující na protokolu LDAP, kterou vyvinula firma Microsoft a používá se pro autentizaci a autorizaci uživatelů a zařízení v síti. Všechny připojené prvky lze opatřit atributy a rozdělit je do domén, subdomén a skupin. Uvedenými technikami lze omezit přístup v síti i k souborům, distribuovat obsah a ověřovat uživatele při přístupu k různým aplikacím. Je většinou spravována doménovými administrátory nebo IT administrátory s omezením pravomocí na jejich subdoménu.

1.5 Bezpečnost

Bezpečnost je chápána jako stav ochrany prvků před útoky, hrozbami a riziky, která mohou hrozit a při nichž může dojít ke ztrátám. Jde o přípravu proti stavu, který může nastat a ohodnocení, zda je systém chráněn dostatečně (odvíjí se od jednotlivých potřeb a za ohodnocení jsou odpovědné příslušné osoby). Jako základ bezpečnostních pojmů je uváděna triáda CIA[3]. Ta je tvořena prvními písmeny anglických slov pro:

- **důvěrnost** – informace by měly být přístupné pouze těm, kdo mají oprávnění se s nimi seznámit,
- **integritu** – jinak řečeno úplnost dat. Se systémy a informacemi nebylo manipulováno a nebyly neoprávněně modifikovány,
- **dostupnost** – přístupnost informací a systémů v požadovaný čas a v co nejkratším čase.

K těmto třem přidávají některé zdroje **kontrolu** (ztráta dat znamená ztrátu kontroly a vlastnictví, ale nejde přímo o narušení důvěrnosti), **užitečnost** (např. uložená data ke kterým není známo heslo jsou sice dostupná, ale nejsou užitečná) a **autentičnost** (byla dodržena CIA, ale byl např. padělán elektronický podpis v dokumentu). Zachování důvěrnosti, integrity a dostupnosti informace je základní definicí **informační bezpečnosti**. Čapek a kolektiv [27, s. 19] uvádí, že mnoho autorů zaměňuje informační bezpečnost s dalšími druhy bezpečnosti v informatice – **bezpečností informačních a komunikačních technologií** (ICT) a **kybernetickou bezpečností**. Všechny jsou vzájemně propojeny, ale přistupují k bezpečnosti specifickými způsoby, ale jejich množiny mají jistý překryv [27, s. 11]. Někteří autoři spíše uvádějí že informační bezpečnost je nadřízená a ostatní typy jsou její podmnožinou [28]. Bezpečnost bude vždy velmi subjektivní, je tedy velmi obtížné určit výchozí stav, pokud se nejedná o zákonem chráněný systém jako jsou kritická informační infrastruktura (KII) nebo významný informační systém (VIS) které určují zákony. Pro všechny platí, že bezpečnost je nutné chápat jako **kontinuální proces** a musí být **nezávislá** (posuzování nesmí být závislé na vedení organizace), **řízená** (bezpečnost se nevyskytuje, ale někdo ji organizuje) a **oceňovaná** (míra bezpečí u stejných aktiv má pro každou organizaci jinou hodnotu). V rámci řešení bezpečnosti existují shodně používané základní pojmy [6, s. 252]:

- **aktiva** jsou hmotné (peníze, nemovitosti, HW) i nehmotné (informace/data, SW, know how) statky které mají pro majitele hodnotu,

[3] CIA – Confidentiality, Integrity, Availability

- **hrozba** je skutečnost, událost, síla nebo osoby, jejichž působením může vzniknout škoda (narušení bezpečnosti, porucha, poškození) na aktivech. Hrozby mohou být vnitřního nebo externího původu, náhodné nebo úmyslné způsobené přírodními, technickými nebo lidskými činiteli,
- **riziko** tvoří pravděpodobnost se kterou může konkrétní hrozba ohrozit konkrétní aktivum („*míra ohrožení aktiva*“ [6, s. 253]),
- **útok**em se rozumí úmyslné (využití zranitelného místa), nebo neúmyslné (zaviněný či nezaviněný výsledek činnosti), způsobení škody na aktivu,
- **zranitelnost** je slabina nebo nedostatek aktiva, jejímž využitím lze způsobit škodu při působení hrozby. Protože nelze domyslet veškeré působení světa, obsahuje zranitelnost každé aktivum. Některé zranitelnosti nelze odstranit, ale pouze snížit riziko nebo velikost škod při působení hrozby. Opatření aplikované pro snížení nebo eliminování dopadu hrozby se nazývá **protiopatření** [27, s. 8].

1.5.1. Informační bezpečnost

Udávaná definice bezpečnosti neřeší, o jaký typ informace jde (zda písemnou, ústní nebo elektronickou formu apod). Firmy se snaží zabezpečit všechny formy informací pomocí souboru opatření, během jejich životního cyklu, v přiměřené míře k povaze a důležitosti informací. Informace chráníme v prostorech podniku i mimo něj. Protože obsahem práce jsou IS a IT infrastruktura, řeší tato práce v dalších kapitolách bezpečnost kybernetickou.

1.5.2. Kybernetická bezpečnost

Digitální prostředí, ve kterém probíhá životní cyklus informace a je tvořený IS, digitálními službami a elektronickými sítěmi se nazývá **kybernetický prostor**. Jirásek a kol. [29, s. 69] definuje kybernetickou bezpečnost (KB) jako „*souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru*“. Dle Čapka a kol. [27, s. 19] se od informační bezpečnosti liší v přístupu k uživateli, kdy v KB je člověk brán nejen jako (zejména užívající) součást systému ale zároveň i část, která může být napadnuta útokem a je potřeba brát v potaz jeho zranitelnosti. Člověk je dnes ostatně označen jako nejslabší bezpečnostní článek systémů, ve kterých působí. V současné době KB slučuje a rozšiřuje základní opatření informační bezpečnosti dle Šulce [30, s. 101] na organizační a technická opatření. Další opatření, která Šulc uvádí, sjednocuje zákon o kybernetické bezpečnosti (ZKB) [31] pod dvě kategorie organizačních a technických opatření.

Organizační opatření

Organizační (v IB administrativní) opatření je systém daných pravidel, které upravují postupy práce při nakládání s utajovanými (chráněnými) informacemi nebo stanovují funkce s přidělením odpovědnosti za jednotlivé činnosti. Jde o soustavu předpisů, norem, zákonů a dalších dokumentů pocházejících zevnitř podniku nebo vycházející z platné legislativy [32, s. 73]. Organizační opatření také stanovují stupně důvěrnosti a ochrany jednotlivých informací a zahrnují školící aktivity v oblasti bezpečnosti informací. Mezi organizační opatření řadí ZKB [31] například řízení aktiv, organizační bezpečnost, řízení přístupů, řízení kontinuity činností, řízení rizik aj.

Technická opatření

Do technických opatření spadají fyzická a logická opatření IB. Pomáhají proti neoprávněnému přístupu, fyzickému zničení ale i zásahu vyšší moci[4]. **Omezení přístupu** slouží ke sledování pohybu osob a neoprávněnému přístupu k informacím (jejím nosičům), tedy vniknutí do objektu organizace (jejích částí) a fyzické manipulace jako výměna a odnesení nosiče, použití cizího zařízení v síti, zneužití firemního zařízení apod. Pro prokázání oprávnění k přístupu musí žadatel projít identifikací, autentizací a autorizací [33, s. 56]:

- **identifikace** probíhá prohlášením uživatele o své identitě. V nedigitálním světě se prokáže průkazem. Ve světě digitálním musí systému prokázat, že je to on podáním důkazu (nebo jejich kombinací). Mezi důkazní metody patří **znalost** (uživatel zná přístupové heslo), **vlastnictví** (např token, čipová karta, zvláštní soubor) nebo **vlastnost** (unikátní tělesná vlastnost – biometrika),
- **Autentizaci** provádí systém, jehož pomocí, nebo k němuž je požadován přístup. Ten porovná vložené autentizační údaje s těmi, které získal při jeho registraci,
- **autorizací** se rozumí umožnění přístupu, a poskytnutí dat, nebo jeho odmítnutí.

Základem omezení přístupu jsou systémy mechanických zábran, které tvoří konstrukce zařízení a objektů a jejich mechanická odolnost (čas a úsilí potřebné ke zničení / překonání – např. odolnost proti ohni, odolnost proti hrubé síle). Přístup se omezuje již před samotným objektem různými ploty – obvodová ochrana. Ta je prováděna různými fyzickými překážkami a zábranami, doplněné o kamerové systémy (CCTV). Fyzickou zábranu tvoří také konstrukce objektu jako stavebně technické prvky (zdi, okna, mříže aj.). Jako hlavní omezení přístupu před

[4] Zásah vyšší moci je nezaviněná, nepředvídatelná událost, kterou vlastník ohroženého aktiva nemůže kontrolovat – patří mezi ně např. epidemie, války, přírodní vlivy (katastrofy) aj.

neoprávněným přístupem uvádí Doseděl [33, s. 53] čtyři prvky k překonání: **ostrahu, dveře, zámky** a **trezory**. Ty tvoří plášťovou (ochrana vnějších částí) a předmětovou ochranu.

Ostrahou se rozumí různé hlídací služby, které za technologické podpory zabezpečovacích (EZS), protipožárních (EPS) a CCTV, které dle Brabce [2, s. 85] poskytují:

- Kontrolní propustkovou službu – brání neoprávněnému vstupu a kontrolují osoby a vozidla,
- kontrolní činnost – zabraňují rozkrádání, ničení a zneužití majetku,
- střežení objektů a prostor (strážní služba) – na stanovištích či pochůzkou
- realizaci bezpečnostních opatření v objektu – po dohodě s vlastníkem objektu či majetku jako doplňková služba
- realizace zásahu či pomoci při mimořádných událostech

EZS je tvořen soustavou čidel (optických, akustických) propojených do oddělených od ostatních rozvodů dokážou rozpoznat fyzické narušení objektu (rozbití skla, pohyb osob). Takto propojený systém je řízen centrální jednotkou EZS. Může být navíc použit pro rozdělení. Obdobně (ale opět odděleně) funguje EPS, které pomocí různých druhů čidel (teplotní, kouřové, spektrální) a hlásičů (tlačítkové, samočinné) nahlásí centrální jednotce EPS přesnou lokalizaci požáru. Oba systémy mohou být komunikačně provázány s pultem centrální ochrany (PCO). Jedná se o dispečerské stanoviště neustálého dohledu, které může v díky rychlému zpracování došlých zpráv koordinovat zabránění škod – při narušení objektu využívá vlastní zaměstnance k zásahu, informuje pověřené osoby vlastníka objekty a policii, při požáru informuje hasiče.

EPS již spadá do **ochrany před přírodními živly**. Doseděl [33, s. 54] zmiňuje živly, které mohou ohrozit IT infrastrukturu nebo IS: požár, vodu, zemětřesení či klima. Klima je uvedeno zejména z důvodu citlivosti výpočetní techniky na prostředí, ve kterém provozované. Důležité jsou zejména vlhkost a teplota.

Technickými opatřeními se také rozumí **kvalita technologií**, které jsou nasazeny k ochraně a provozu IT infrastruktury a IS, jejich ochrana proti možným technickým způsobům narušení jejich chodu a také jejich pravidelná revize, která potvrdí správnou funkčnost. Pod kvalitou technologií je myšleno použití a udržování ochranných a provozních technologií v takové kvalitě, která umožní dodržovaní nebo zlepšení nastavené úrovně bezpečnosti. Příkladem může být:

- rozlišení u bezpečnostních kamer, které umožní rozeznat obličej, mají dobrou noční viditelnost aj,
- použití EZS, s podporou různých typů čidel, nebo bude umět použití přístupových karet které umožní vedení vstupů či rozdělení budovy na bezpečnostní sekce,
- provozní server umožňující chod podporovaných operačních systémů, správný typ disků pro stabilní nepřetržitý chod apod.

Mezi ochranu proti technologickým narušením se řadí zejména ochrana proti nestabilitě a **výpadku elektrické energie**. Mezi nestabilitu řadíme podpětí, přepětí či proudové rázy. Napětí a přepětí jsou dlouhodobější odchylky od běžného napětí v energetické síti (230 V) vlivem poptávky po elektrickém proudu v distribuční síti. Hlavním řešením problémů s elektrickou sítí je akumulátorový zdroj (UPS) a generátor. UPS obsahuje akumulátor a je zapojen mezi elektrickou síť a obsluhované zařízení (i více). Při výpadku energie dokáže po určitý čas pokrýt období, než uživatel vhodným způsobem vypne zařízení, nebo než naskočí záložní generátor, který nahradí dodávky elektrické energie po dobu výpadku. UPS také dokáže pokrýt případné nestability sítě. [33, s. 54]

K technickým opatřením patří i ukládání dat na **disková pole** (RAID) a zálohování. RAID je označení technologie ukládání dat na dva a více nezávislých disků. Vytvoří z nich pro systém jedinou logickou jednotku a řadič následně řídí ukládání dat na tyto disky. Rozlišujeme několik základních typů – RAID 0, RAID 1, RAID 5 a další které jsou v úpravách modifikacemi nebo kombinacemi uvedených.

- RAID 0 potřebuje minimálně dva disky. Oba rozdělí na stejné části pevné velikosti, kdy následně využije všech pro cyklické ukládání dat. Data tedy prokládá na všechny disky – nejde tedy o plnohodnotný RAID – při poruše disku se nemají většinou jak obnovit. Umožňuje ale mnohem rychlejší zápis i čtení dat, používá se proto v kombinaci s dalšími (RAID 10, RAID 50)
- RAID 1funguje na principu zrcadlení – co je ukládáno na jeden disk je identicky uloženo i na druhý. Při výpadku jednoho disku pokračuje práce s druhým.
- RAID 5 požaduje k fungování minimálně tři disky. Data nejsou rozprostřena různě jako u RAID 0, ale střídavě na jeden z nich je vždy uložen samo opravný kód (kód parity). Při výpadku jednoho disku nehrozí ztráta dat.

Technická bezpečnost také zahrnuje **šifrování**, tedy zajištění důvěrnosti a integrity proti získání neoprávněného přístupu k datům a jejich přečten nebo modifikaci. Základním předpokladem je

použití bezpečného kryptografického algoritmu, která převádí text do šifrované podoby a zpět (dešifrování). Dle použití rozlišujeme šifrování symetrické a asymetrické (zda je k dešifrování použit sejný klíč jako k šifrování či nikoliv). O síle šifry také rozhoduje použitý typ šifrování a délka klíče. Protože asymetrické šifrování u delších textů by bylo složité, používá se z důvodu úspor systémových prostředků, lepší přenositelnost, symetrické šifrování textu za pomoci klíče s danou délkou. Tento klíč je následně zašifrován asymetricky. K nejbezpečnějším šifrám se dnes řadí algoritmy RSA, AES256 nebo TLS. [30]

1.5.3. Útoky

Protože zranitelnosti obsahují všechny aktiva, existuje v kyberprostoru i velké množství útoků, jejichž množství neustále narůstá. V dřívějších dobách ohrožovali organizace viry anebo nevyžádaná pošta v podobě emailů s velmi špatným jazykovým překladem, nad kterými se dnes spíše uživatelé usmějí. Dnešní útoky jsou velmi propracované a cílené. Základní skupiny útoků tvoří skenování sítě, útoky s cílem získání přístupu nebo informací a vyčerpání systémových prostředků. Sedlák [34, s. 109] jako nejčastější užívané kybernetické útoky řadí:

- **Nebezpečné programy (malware)** – velká „rodina“ škodlivých programů jako jsou viry, červi nebo trojské koně. Do této skupiny padají také aktuální hrozby v podobě **ransomware** (po infikování zařízení jej zašifruje s cílem získat výkupné) nebo cryptojacking (neoprávněná těžba kryptoměn). Pomocí malware lze vytvořit síť infikovaných strojů, tzv **botnet**,
- **webové útoky** – útoky pomocí infikovaných webových aplikací s cílem krádeže uživatelských dat (platební operace, přihlašovací údaje…) pomocí úpravy formulářů, přesměrování, podsunutí jiných než očekávaných informací.
- **phishing** – součást sociálního inženýrství s cílem získat osobní údaje (rodná čísla, hesla…), které mohou být následně zneužity. Zisk probíhá pomocí podvodných zpráv (imitace bankovních emailů, výzvy od úřadů apod.). Může vést ke **krádeži identity** použitím osobních údajů kompromitované osoby k obohacení útočníka (např. přístup k informacím, účtům),
- **DDoS** – útočník pomocí zahlcení prvků infrastruktury, nebo služby docílí její nedostupnosti,
- **vnitřní hrozba** – osoba zevnitř organizace s přístupem k aktivům způsobí jejich ohrožení nevhodným nakládáním s daty, prací pro externího útočníka apod.,
- **fyzická manipulace, zničení, krádež**,

- **kybernetická špionáž** – pomocí uvedených technik získání strategicky důležitých informací pro zisk politické, strategické či konkurenční výhody.

Kybernetické útoky mají jedno společné – jde většinou o soubor technik. Útoky na IT infrastrukturu bývají přímočařejší a jsou právě jedním z nástrojů kybernetických útoků. Mezi útoky Petrovič [35] řadí:

- **průzkum sítě** – slouží k neautorizovanému sběru informací, mapování topologie sítě a hledání zranitelností. Používá se hromadný ping, odchytávání paketů, skenování portů či zisk informací z registrace zařízení v síti.
- **skenování portů** – každá aplikace používá pro komunikaci v síti určitý port, který ji umožňuje rozlišit se v rámci PC (implicitně je například pro http port 80, pro http port 443 apod.), takto otevřené porty lze využít k následnému útoku (lze odvodit jaké aplikace jsou na PC nainstalovány, najít nejzranitelnější port…,
- **útoky na webové aplikace** – jde o narušení interpretace webových stránek s využitím chyb ve skriptech. Můžou směřovat na poškození funkčnosti, vzhledu nebo poskytnout údaje uživatelů,
- **SQLInjection** – využití standardního dotazovacího jazyka SQL pro vytvoření přístupu do databáze pomocí kódu vloženého do očekávané komunikace například z neošetřeného webového formuláře s databází.

1.5.4. Metody zjištění stavu bezpečnosti

Protože se v případě bezpečnosti jedná o nekončící a opakující se proces, je nutné mít v rámci organizace povědomí o jeho aktuálním stavu. Brabec [2, s. 56] uvádí, že *„smyslem a cílem komplexní (dílčí) bezpečnostní expertízy, při respektování strategického plánu a cílů organizace, je určit a navrhnout použití přiměřených bezpečnostních prostředků a opatření k účinnému a adekvátnímu řešení bezpečnostních problémů organizace s ohledem na její možnosti“.* Jako zdroj informací pro expertízu (v rámci práce se jedná o průzkum aktuální situace) slouží interní prostředí zkoumané organizace. Interními zdroji relevantních informací mohou být dokumenty vypovídající o aktuálním stavu organizace, vedoucí, odborní i běžní zaměstnanci organizace. Vnější prostředí může pomoci dokreslit některé interní souvislosti (např. informace od dodavatelů) a je zdrojem přepisů a zákonů ovlivňující organizaci.

Získané informace v podobě různých interních předpisů, smluv, finančních výkazů, pravidelných zpráv, rozhovorů se zaměstnanci a dodavateli, zjištěné vlastním pozorováním nebo rešerší z internetu je nutné utřídit, rozdělit je na relevantní a zbytečné a zkompletovat. Pro

samotné zjišťování stavu zabezpečení nebo jejich analýzu nejsou definovány žádné přesné metody. Využívá se proto zkušeností z jiných odvětví marketingu, ekonomie, matematiky a jiných dalších oborů. Jde například o tvorbu scénářů, expertní rozhovory, brainstroming, SWOT analýzu, PEST bodovou metodu „PNH“ či Paretovu analýzu. [2, s. 58]

Dalšími metodickými pomůckami při zjišťování hrozeb pro aktiva pracoviště může být mezinárodní norma ČSN ISO 27005 „Informační technologie – bezpečnostní techniky“. [36] Případně zákon č. 181/2014 Sb., o kybernetické bezpečnosti [31].

SWOT analýza

Jedná se zejména o marketingovou metodu používanou pro zjištění komplexního stavu organizace a umožňuje nalezení následných strategických postupů. Umožňuje také analýzu dílčích kroků (otevření pobočky, zavedení produktu, zjištění stavu zabezpečení). Pomocí zkoumání **vnitřního a vnějšího prostředí** zkoumaného subjektu jsou odhaleny čtyři faktory které ovlivňují další vývoj. Z vnitřního prostředí jsou to **silné (S) a slabé stránky (W)**. Z vnějšího prostředí jde o **příležitosti (O) a hrozby (T)**. Jednotlivé faktory se posoudí z hlediska významnosti a závažnosti pro organizaci (například kvantifikací – přiřazením váhy a bodového hodnocení, jejichž součinem se získá bodové skóre. Součet všech bodů tvoří celkové hodnocení kategorie). Vnitřní faktory jsou také posouzeny s těmi vnějšími v komparační matici tak, že jsou porovnány vzájemné vztahy, ze kterých vzniknou čtyři strategie – S-O, S-T, W-O a W-T. [37]

bodová metoda „PNH“

Metoda „PNH“ je polo-kvantitativním zhodnocením rizik (R) pomocí tří, předem stanovených, složek. Těmi jsou pravděpodobnost vzniku (P), míra či hodnota následků, nebo jejich vážnost pro zkoumaný objekt (N) a názor hodnotitelů (H), což je hodnocení míry a vážnosti následků. Pro každou jednotlivou složku metody se vytvoří ohodnocení na stupnici od 1 do 5. Vytvořenými stupnicemi se ohodnotí jednotlivé hrozby (Jaká pravděpodobnost hrozby? Jaká vážnost následků hrozby? Jaký názor hodnotitelů na hrozbu). Takto sestavené hodnoty se dosadí do vzorce R = P * N * H. [38]

Vypočítaná míra rizika R značí naléhavost aplikace protiopatření dle hodnotící stupnice zobrazené v Tabulka 6. [38]

2. POPIS VYBRANÉ ORGANIZACE A PRŮZKUM STAVU ZABEZPEČNENÍ VYBRANÝCH AKTIV

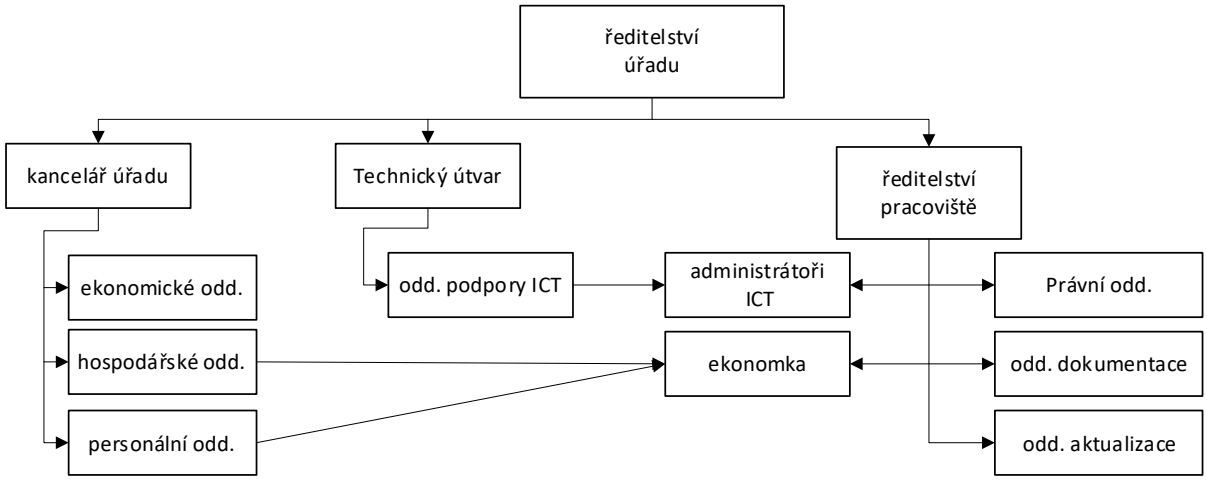
Kapitola obsahuje popis vybrané organizace a popis zjištění z průzkumu aktuálního stavu zabezpečení. Ze získaných poznatků jsou odvozeny zranitelnosti, které by mohli být zneužity hrozbami pro narušení kybernetické bezpečnosti. Zjištění jsou ještě doplněna SWOT analýzou, která pomůže organizaci ve výhledu na práci se zabezpečením na nejbližší období. Vše je shrnuto ve výsledcích průzkumu. Průzkum by vyhotoven zejména na základě normy ISO ČSN 27005 „Systémy řízení bezpečnosti – Požadavky“.

2.1 Popis organizace

Pracoviště vybrané pro analýzu zabezpečení, je věcně příslušný správní úřad, který vykonává správu příslušné agendy v České republice. Jeho vznik a působnost je vymezen zákonem. Pracoviště je členem resortní struktury jako poslední její článek. Hlavnímu úřadu se sídlem v Praze, podléhají úřady se sídlem v krajských městech, kterým je dána územní působnost. Každý krajský úřad je dále tvořen pracovišti, která sídlí ve větších městech příslušného kraje (včetně přímo města krajského).

Zákazníky tvoří ostatní orgány veřejné správy, se kterými sdílí informace, a veřejnost, která k němu činí podání ve formě dokumentů a získává platné i historické dokumenty a údaje. Důležitý je také soukromý sektor v podobě podnikatelů, který zastává roli nezávislého tvůrce podkladů a dat vedených úřadem. Vizí pracoviště je být moderní a důvěryhodnou organizací. Podpůrné cíle k dosažení vize jsou ochrana a poskytování správných informací v co nejefektivnější podobě a udržování pozitivní hodnocení úřadu u veřejnosti.

Na Obrázek 7 je znázorněno hybridní organizační schéma úřadu, jehož součástí je již pouze liniové uspořádání zvoleného pracoviště. To je tvořeno třemi odděleními – oddělení dokumentace, oddělení aktualizace a oddělení právní. Jako zvláštní funkce na pracovišti jsou vyčleněny pozice ekonomky a lokálních administrátorů ICT. Administrátoři ICT plní mimo běžnou práci úkoly zadané krajským oddělením podpory ICT (OPICT). Z pohledu funkčního, realizačního a částečně personálního je pracoviště samostatné, ale díky administrátorům ICT a OPICT je členem celé hybridní struktury. Výsledky a plněním úkolů odpovídá nadřízenému úřadu. Nadřízený úřad přes kancelář úřadu také poskytuje pracovišti ekonomické a hospodářské prostředky (rozhoduje o správě a rozdělení financí, počtech zaměstnanců, opravách budov, pořízení techniky). Celkem je na pracovišti zaměstnáno 61 zaměstnanců, z toho 3 administrátoři ICT.



Obrázek 7 - Organizační schéma úřadu

Zdroj: vlastní zpracování na základě konzultace s vedením pracoviště

2.2 Stávající zajištění bezpečnosti na vybraném pracovišti

Průzkum stávajícího stavu zabezpečení na pracovišti na technické, logické a organizační úrovni. Průzkum vyhotoven a konzultován ve spolupráci administrátory ICT. V rámci práce jsou popsána zejména taková zabezpečení, se kterými lze pracovat a mohou být zlepšena, případně stavy zabezpečení představující riziko.

Technické zabezpečení

Budova pracoviště je přístupná dvěma různými vchody. Hlavní vchod z přilehlé ulice s možností vstupu veřejnosti i zaměstnanců je tvořen automaticky otevíranými prosklenými dveřmi opatřenými elektromechanickým zámkem (zajišťují se elektricky s doplňkovým mechanickým zámkem). Druhý vchod je opatřen jednokřídlými prosklenými dveřmi s mechanickým zámkem, přístupné z uzavřeného dvora tvořeným blokem okolních domů s oploceným pozemkem s brankou. Hlavní vchod je střežen strážní službou zabezpečující kontrolní činnost pracoviště a střežení objektu, ale nezabezpečuje propustkovou službu s kontrolou osob. Slouží spíše jako informační bod pro vstupující, telefonní spojovatelka, zabezpečuje chod EZS a EPS. Po vstupu do budovy je k dispozici prostor se službami pro veřejnost, na který navazují prostory o třech patrech se zázemím pro aktiva, vybavení a zaměstnance pracoviště. Některá aktiva pracoviště jsou umístěna na chodbách (pasivní část LAN, kopírky) nebo v uzavřených kancelářích (pasivní část LAN, tiskárny, PC) a serverovně pracoviště. Všechny kanceláře využívající aktiva sídlí v třetím patře, serverovna se nachází v patře druhém. Všechny společné prostory pracoviště jsou dostupné veřejnosti s omezujícími upozorněními „nepovolaným vstup zakázán“. Prostory s aktivy:

- kanceláří je myšlena místnost s oknem, od společných prostor oddělená interiérovými dveřmi se zvýšenou odolnosti proti ohni a mechanickým zámkem,
- serverovna je umístěna za kanceláří OPICT v samostatné místnosti s oknem, nepřístupná ze společných prostor. Stěna mezi kanceláří OPICT a serverovnou je z velké části prosklená (pro možnost optické kontroly). Dveře mají zvýšenou odolnost proti mechanickému poškození a požáru, jsou opatřeny z vnější strany koulí a po otevření se samy zavírají. Klíče jsou vyloučeny ze systému klíčů, které pracoviště využívá. Serverovna je vybavena dvěma klimatizačními jednotkami s ručním ovládáním, rackovými rámy pro IT prvky (otevřené, bez stěn).

Elektrické zásuvky určené pro napájení IT infrastruktury jsou barevně odlišeny, umístěny na samostatném okruhu a chráněny přepěťovou ochranou. Servery a aktivní síťové prvky jsou napájeny pomocí UPS s dostatečnou kapacitou a bezpečnou dobou pro vypnutí (čas mezi výpadkem proudu a vybitím baterií UPS) v rozmezí 15 až 20minut dle aktuálního zatížení. Servery mají redundantní zdroje, PC a jiná zařízení jsou unifikována a není tedy problém s náhradou součástek. Budova pracoviště je střežena pomocí EZS a EPS. Prvky EZS jsou umístěny v prvním podlaží (pohybová, zvuková a magnetická čidla), které je přístupné z ulice u všech prvků plášťové ochrany, které je snadné překonat (typicky okna, dveře) nebo v místnostech na takový prostor bezprostředně navazující. U vyšších pater jsou chráněné již pouze prostory možného vniknutí (schodiště, střešní vstup, předvýtahové prostory…) a serverovna s kanceláří OPICT. EPS používá kouřovo-teplotní čidla a ruční hlásiče ve všech místnostech s vyšším rizikem vzniku požáru – serverovna, strojovna výtahu, archivy). Oba systémy jsou napojeny na PCO s dodavatelsky řešenou službou.

Na fyzickém serveru, který je provozován s operačním systémem Windows Server 2016 (v aktuální verzi) a je napojen na samostatné diskové pole v RAID 10, je instalován virtuální aplikační server. Ten je provozovaný na virtuálním prostředí Hyper-V s Windows Server 2008 R2. Fyzický přístup k serveru mají pouze zaměstnanci OPICT. Přístup k datům PIS je možný pouze přímo přes obslužnou aplikaci umístěnou na serveru nebo přes PC s nainstalovaným SW. Uživatelská PC jsou běžně na trhu dostupné počítače (USB rozhraní, video a audio výstup…). K těmto PC mají přístup všichni zaměstnanci, kteří mají klíč od příslušných kanceláří. Veškeré servery a PC jsou opatřeny SW pro vzdálenou správu, anti-malwarovým řešením a SW pro vzdálený dohled stavu. Pracoviště komunikuje v podnikové metropolitní síti, pomocí routeru s šifrovacím modulem a firewallem. Pracoviště nemá přímý přístup do internetu. Vnitřní

komunikaci v síti LAN mají na starosti switche se všemi porty aktivními a napojenými do sítě. Jsou vytvořeny některé VLANy pro rozlišení sítí (např. pro tiskárny, servery…).

Zálohy jsou umístněné na fyzickém serveru a jejich kopie je pravidelně zálohována na NAS umístěné v serverovně. NAS je diskovým polem v RAID 5, napájena je samostatnou UPS. Zálohy jsou prováděny každý den (přes noc).

Lidské zdroje jsou řízeny politikami a předpisy pracoviště. Oprávnění jsou přidělována dle organizačního zařazení na základě žádostí, dodavatel PIS nemá přístup do systémů. Všechny operace v PIS i jiných systémech jsou logovány (včetně přihlašování) a uživatel za ně nese odpovědnost. Přístup do systémů serverů mají pouze OPICT. Správu autentizace a autorizace provádí služba Active Directory a tvoří tak logická omezení přístupu jak na servery, tak i PC a SW. Přiřazování do bezpečnostních skupin probíhá pouze po schválení nadřízeného. K autentizaci se používá logovací jméno a heslo.

Organizační zabezpečení

Pracoviště má zpracované základní bezpečnostní politiky, některé další politiky a směrnice přebírá díky hierarchii od nadřízených úřadů. V dokumentech stanovuje aktiva, nastavuje odpovědné osoby (garanty) a jejich kompetence. Dalšími zpracovanými politikami jsou řízení lidských zdrojů, řízení rizik, plán kontinuity a politiku bezpečnostních incidentů. Z nich vyplívají veškeré povinnosti při práci s aktivy, jako administrace, přístupy, kontrolní mechanismy nebo logování. Všechny politiky a předpisy určující hierarchickou strukturu, bezpečnost při práci, únikový plán aj. jsou pravidelně kontrolovány a aktualizovány. Jsou také předepsány postupy hlášení bezpečnostních událostí a jejich zpracování. Zaměstnanci na odborných a vedoucích pozicích jsou o těchto politikách prokazatelně seznamováni a dle organizační struktury by měli předávat získané informace podřízeným. Je také předepsáno nakládání s informacemi po dobu jejich existence – tedy pořízení, uchování a skartace pro jednotlivé druhy informací. Dopsat co se řeší v organizační – školení, plánování rizik.

2.3 Aktiva pracoviště

Pro potřeby práce byla rozlišovací úroveň zjišťování aktiv pracoviště omezena na IT infrastrukturu a personální informační systém (PIS). Ze všech zjištěných aktiv byl vybrán reprezentativní vzorek důležitých aktiv pracoviště.

Tabulka 3 – Identifikovaná aktiva pracoviště s jejich odhodnocením

Aktiva pracoviště			Procesy, které plní	Vyšší hodnota následků (N)
IT infrastruktura	**A1**	**servery**	slouží pro chod virtuálních serverů v prostředí Hyper-V, je na něm provozována služba DHCP, provádí první úroveň zálohování,	4
	A2	**aktivní síťové prvky**	slouží jako koncový bod pro připojení do MAN resortu, obsahuje zároveň šifrátor a firewall,	2
	A3	**operační systémy**	serverové a uživatelské, slouží jako aplikační základna pro provoz obsluhu a chod HW, nasazeny jsou Windows 10 20H2, Windows Server 2008 R2 a Windows 2016	3
PIS	**A4**	**zálohy**	Zálohy OS, databází a uživatelských PC	5
	A5	**uživatelé s přístupem do PIS**	obsluha s omezenými právy, pracuje s daty v PIS (edituje a vytváří záznamy)	2
	A6	**SW PIS**	Obslužný SW pro práci s PIS na PC uživatelů	1
	A7	**databáze Oracle**	slouží pro ukládání dat PIS	5

Zdroj: vlastní zpracování

Při zjišťování byly použity vnitřní předpisy pracoviště a resortní politiky. Další informace nutné pro průzkum byly zjištěny díky spolupráci s administrátory ICT a vedoucími pracovníky pracoviště. Aktiva vybraných prvků jsou vypsána v Tabulka 3. Kromě popisu funkce aktiv na pracovišti, byla aktiva ohodnocena kvalitativním hodnocením převedeným na bodovou škálou od 1 do 5, přičemž vyšší hodnota znamená vyšší důležitost, vyšší hodnotu pro pracoviště a tím **vyšší hodnotu následků (N)** pro pracoviště.

Personální informační systém

PIS slouží pro jednotnou správu personální agendy, jako je evidence zaměstnanců, úvazků, mezd, záznamy o školeních (kurzech, kvalifikacích…), obstarává komunikaci se systémy ministerstva práce a sociálních věcí a další agendu spojenou s personalistikou. Každá resortní úroveň má svoji část tohoto decentralizovaného systému instalovanou na své infrastruktuře a všechna data jsou postupně „sbírána“ do centrálního systému. Systém je dodáván jako SaaS, běžící na prostředcích pracoviště. Případné požadované doplňky (např. pro elektronickou evidenci neschopenek) jsou dodávány pod samostatnými licencemi. Pro svou činnost využívá samostatnou relační databázi Oracle. Aktualizace jsou připraveny dodavatelsky, ale instalovat je musí lokální administrátor. Do PIS má přístup ředitel pracoviště, ekonomka, lokální administrátoři a z nadřízené organizace personální oddělení a OPICT na jejichž PC musí být instalován ovládací program přistupující k serverové části. Pomocí PIS se na pracovišti definují

základní uživatelské přístupy – díky zadání pracoviště, pozice, typu úvazku a dalších kritérií se uživateli založí účet, email a přidělí základní sada oprávnění pomocí Active directory.

Prvky IT infrastruktury

Mezi aktiva IT infrastruktury pracoviště, které lze identifikovat, patří aktivní prvky jako fyzický server, aplikační virtuální server běžící na fyzickém serveru, tiskárny a kopírky, osobní počítače a notebooky uživatelů, switch, router a pasivní část sítě. IT infrastruktura pracoviště také slouží jako HW složka PIS (proto není tato složka dále uváděna samostatně).

2.4 Hrozby pro aktiva pracoviště

Při určování hrozeb byly brány v potaz technický stav aktiv, kvalifikační zaměření pracoviště a aktuální trendy v kybernetické bezpečnosti. [39] Ze všech zjištění byl pro potřeby této práce vytvořen částečný výběr uvedený v Tabulka 4.

Tabulka 4 - Matice hrozeb a aktiv

	hrozby \ aktiva	Pravděpodobnost vzniku (P)	IT infrastruktura			PIS			
			servery	aktivní síťové prvky	operační systémy	zálohy	uživatelé s přístupem do PIS	SW PIS	databáze Oracle
			A1	A2	A3	A4	A5	A6	A7
H1	**ztráta dodávky energií**	2	X	X					
H2	**narušení fyzické bezpečnosti**	4	X	X		X	X		
H3	**nedostupnost**	2	X	X	X	X			X
H4	**škodlivý kód**	5	X	X	X	X		X	X
H5	**napadení komunikace**	4		X	X	X	X		
H6	**lidská chyba / selhání**	2	X			X	X	X	X
H7	**selhání hw**	1	X	X	X	X			

Zdroj: vlastní zpracování

Spolu s aktivy jsou hrozby umístěny do společné matice zobrazené v Tabulka 4 pro určení jejich průniku – která hrozba může ovlivnit které aktivum. Hrozby jsou stejně jako aktiva ohodnoceny stupnicí bodů od 1 do 5, kdy vyšší hodnota znamená pro pracoviště větší nebezpečí, pokud by byla hrozba přeměněna na útok, tedy vyšší míru ohrožení a nebezpečí pro pracoviště – **pravděpodobnost vzniku (P)**.

2.5 Zranitelnosti a výpočet metody „PNH“

Ze zkoumání pracoviště a seznamu nejběžnějších zranitelností [40, s. 1143] byly vybrány zranitelnosti každého aktiva sepsané do Tabulka 5. Tyto zranitelnosti byly ohodnoceny na stupnici od 1 do 5, kdy vážnou zranitelnost (možnost vzniku hrozby) znamená ohodnocení 5 body a větší vliv na **míru ohrožení (H)**.

Tabulka 5 - Matice zranitelností a hrozeb

zranitelnosti \ hrozby		Míra ohrožení (H)	ztráta dodávky energií	narušení fyzické bezpečnosti	nedostupnost	škodlivý kód	napadení komunikace	lidská chyba / selhání	selhání hw
	Označení hrozby		H1	H2	H3	H4	H5	H6	H7
Z1	nedostatečná kontrola fyzického přístupu k místnostem budově	1		X			X		
Z2	nechráněné komunikační linky	3			X	X	X		
Z3	nedostatečné bezpečnostní školení a povědomí zaměstnanců	4	X	X			X	X	X
Z4	nedostatečná ochrana HW	2	X		X	X	X	X	X
Z5	neaktuálnost SW	5			X	X	X		

Zdroj: vlastní zpracování

Aby bylo možné ohodnocení hrozeb, použije se výpočet míry rizika pomocí vzorce „PNH“ metody, tedy „R = P * N * H“. Kdy „P“ představuje ohodnocení hrozeb, „N“ představuje ohodnocení aktiv a „H“ je ohodnocení míry vlivu zranitelností. Pro svoji rozsáhlost je tabulka výpočtů uvedena v PŘÍLOHA A – . Míra rizika je hodnocena dle bodového rozpětí a vyjadřuje naléhavost aplikování protiopatření.

Tabulka 6 - Metoda "PNH": bodový rozsah pro určení míry rizika

Rizikový stupeň	R	Míra rizika
I.	>100	Nepřijatelné riziko
II.	51 <>100	Nežádoucí riziko
III.	11<>50	Mírné riziko
IV.	3<>10	Akceptovatelné riziko
V.	<3	Bezvýznamné riziko

Zdroj: vlastní zpracování dle [38]

2.6 SWOT Analýza zabezpečení

Pro zpřesnění, je v této kapitole bezpečnost pracoviště zpracována analýzou SWOT, která by měla pomoci určit oblasti k zabezpečení, které by v následujícím období měli být pro pracoviště stěžejní.

Silné stránky (S)

Jaké má pracoviště výhody v technologiích a zabezpečení. Jaké části zabezpečení lze vyzdvihnout?

S1. Pravidelně obměňované všechny aktivní prvky IT infrastruktury (aktuálnost řešení).
S2. Dostatečně velké personální zázemí pro správu, údržbu a evidenci technologií.
S3. Pravidelná školení odborných zaměstnanců.
S4. Dobře zpracovaná bezpečností politika, předpisy a prováděcí postupy a jejich aktuálnost.
S5. Provázanost s ostatními úřady a pracovišti v resortu – mnohá řešení jsou stejná nebo obdobná.

Slabé stránky (W)

Jaké z průzkumu vyplývají nedostatky a slabiny, které způsobují možné ohrožení, vznik zranitelností?

W1. Dlouhá doba testování a nasazení aktualizací SW a HW.
W2. Slabá proškolenost a informovanost běžných zaměstnanců na aktuální témata kyberbezpečnosti.
W3. Vysoká fluktuace zaměstnanců, zejména na odborných a IT pozicích.
W4. Pravidelná výměna HW a nutnost výběrových řízení znamená vysokou zátěž na znovu nasazení řešení od různých výrobců (chybí kontinuita).
W5. Omezené finanční prostředky neumožňují úplné plnění vnitřních bezpečnostních předpisů, což vede k vzniku výjimek.
W6. Mezery ve fyzickém zabezpečení.
W7. V PIS je mnoho záznamů, které mají různé hodnoty u stejných položek nebo záznamy obsahují chyby (např. název pracovní pozice, umístění zaměstnance…).

Příležitosti (O)

Jaké má organizace možnosti se rozvíjet? Jsou cesty ke zlepšení, o kterých pracoviště ví a mohly by vést ke zmírnění dopadů hrozeb?

O1. Aktuálně je vypsán vládní operační program, který při splnění podmínek, lze využít na zvýšení bezpečnosti organizace.
O2. Nabídka dodavatele EZS na zprovoznění systému přístupových karet.
O3. Školení kybernetické bezpečnosti, které poskytuje národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).
O4. Semináře, které výrobci technologií poskytují zdarma.
O5. Centralizace všech administrátorů ICT pod krajský OPICT pro lepší správu a vedení.

Hrozby (T)

Existují nějaké vlivy, které mohou nastat a zároveň budou mít nějaký negativní dopad na bezpečnost pracoviště?

T1. Aktuálně probíhající válka o Ukrajinské oblasti způsobující nepředvídatelné pohyby trhů, možnost rozšíření konfliktu.
T2. Probíhající masivní útoky na dostupnost pomocí DDoS na státní infrastrukturu, jehož je pracovitě součástí.
T3. Příchod nové legislativy Evropské unie pro kyberbezpečnost (NIS2) v roce 2023.
T4. Vznik nových druhů kybernetických útoků, sofistikovanější útoky, zlepšování a prohlubování detailnosti u aktuálně známých útoků.
T5. Nedostatek pracovníků díky malé nezaměstnanosti.
T6. Nedostatek čipů na trhu.

Dalším krokem je hledání souvislostí mezi SW a OT zpracovaných v Tabulka 7.

Tabulka 7 - SWOT analýza – souvislosti mezi SW a OT

		Interní analýza	
		Silné stránky (S)	**Slabé stránky (W)**
Externí analýza	**Příležitosti (O)**	**S-O strategie** Využití provázanosti úřadů a resortu pro snadné provedení semi-centralizace OPICT a administrátorů ICT – využití podobných akcí na jiných úřadech, využití potřeby znát podobné znalosti na všech úrovních resortu. Využití zpracovaného organizačního zabezpečení pro analýzu k přihlášce do vládního programu pro získání finančních prostředků. Ještě více prohloubit znalost zabezpečení u odborných uživatelů a vedoucích pomocí školení od NÚKIB.	**W-O strategie** Semináře externích firem využít k proškolení IT zaměstnanců pro lepší znalost nových technologií. Administrátoři zcentralizovaní do jednoho oddělení nebudou pod tlakem dvou nadřízených (ředitel pracoviště a vedoucí OPICT). Využití programu od NÚKIB k proškolení běžných zaměstnanců na kyberbezpečnost. Zlepšení fyzického zabezpečení za pomocí pořízení řízení přístupů a jasnou evidenci záznamů pomocí EZS čipových karet.
	Hrozby (T)	**S-T strategie** Díky dobře zpracované bezpečnostní politice by neměl být problém zapracovat NIS2. Díky dostatečnému počtu zaměstnanců na pozicích ovlivňující PIS a IT infrastrukturu by neměl být problém pokrýt středně dobý nedostatek pracovníků na trhu. Využít veškeré silné stránky pro rychlou identifikaci a omezení útoku typu DDoS.	**W-T strategie** Zvýšení pravděpodobnosti hrozby nově vzniklým útokem, nebo útokem na dostupnost služby, díky dlouhé době testování, nasazení nových updatů a technologií a podfinancováním v oblasti bezpečnosti. Nedostatek odborných pracovníků způsobených fluktuací zaměstnanců a jejich nedostatku na trhu práce. Mezery a výjimky v zabezpečení nemusí vyhovovat nově vzniklé evropské legislativě.

Zdroj: vlastní zpracování

Kvantifikace a komparační matice

Nejdříve byla všechna zjištění ohodnocena váhou, která udává, jak je zjištěná položka v dané kategorii důležitá – čím vyšší váha, tím vyšší důležitost. Poté je každá položka ohodnocena dle bodové stupnice 1 až 5 (5 = nejvyšší spokojenost s aktuálním stavem) s výpočty zobrazenými v Tabulka 8. Díky vložení celkového ohodnocení každé části do komparační matice, zobrazené v Tabulka 9, je možné získat jako výsledek jeden z kvadrantů určující budoucí strategii.

Tabulka 8 - Kvantifikace SWOT

	Silné stránky (S)	**Váha**	**hodnocení**	**součin**
S1	Pravidelná aktualizace technologií	0,3	5	1,5
S2	Robustní personální zázemí	0,15	2	0,3
S3	Pravidelná odborná školení	0,2	3	0,6
S4	Zavedená bezpečnostní politika	0,25	4	1
S5	Součinnost v resortu	0,1	2	0,2
celkem		**1**		**3,6**
	Slabé stránky (W)	**váha**	**hodnocení**	**součin**
W1	Pomalé nasazení aktualizací SW a HW	0,15	4	0,6
W2	Neinformovanost běžných zaměstnanců v KB	0,2	3	0,6
W3	Fluktuace zaměstnanců	0,15	2	0,3
W4	Neznalost nově nasazených technologií	0,1	2	0,2
W5	Výjimky z bezpečnosti díky omezeným financím	0,2	3	0,6
W6	Mezery ve fyzickém zabezpečení	0,15	3	0,45
W7	Chybné a nepřesné záznamy v PIS	0,05	1	0,05
celkem		**1**		**2,8**
	Příležitosti (O)	**váha**	**hodnocení**	**součin**
O1	Operační program pro zlepšení zabezpečení	0,3	3	0,9
O2	Vylepšení EZS o přístupové karty	0,15	2	0,3
O3	Školení od NÚKIB	0,2	3	0,6
O4	Semináře k technologiím od výrobců zdarma	0,25	4	1
O5	Sloučení administrátorů ICT do OPICT	0,1	2	0,2
celkem		**1**		**3**
	Hrozby (T)	**váha**	**hodnocení**	**součin**
T1	Válečný konflikt na Ukrajině	0,15	4	0,6
T2	Probíhající masivní útoky DDoS	0,15	2	0,3
T3	Nová bezpečnostní legislativa	0,1	2	0,2
T4	Zlepšení a vývoj kybernetických útoků	0,4	5	2
T5	Malá nezaměstnanost	0,1	1	0,1
T6	Nedostatek čipů na trhu	0,1	4	0,4
celkem		**1**		**3,6**

Zdroj: vlastní zpracování

Tabulka 9 - Komparační matice analýzy SWOT

		Silné stránky (S)	**Slabé stránky (W)**
	body	3,6	2,8
Příležitosti (O)	3		
Hrozby (T)	3,6	S-T strategie	

Zdroj: vlastní zpracování

2.7 Výsledky průzkumu a vyhodnocení možných hrozeb

Výsledkem nejrizikovějších hrozeb v rámci zkoumání **metodou „PNH“** se staly hrozby použití **škodlivého kódu**, **napadení komunikace** a **narušení fyzické bezpečnosti**. U všech tří hrozeb se v testování projevily nedostatky v aktualizacích SW, bezpečnostním školení zaměstnanců a špatné ochraně komunikačních linek. Nejvážnější výsledky, díky dosažení ohrožení I. a II. stupně dle Tabulka 6, jsou shrnuty v Tabulka 10. Tyto hrozby by měly být okamžitě řešeny a na daných aktivech minimalizovány užitím protiopatření tak, aby bylo možné dál aktiva bezpečně používat. Pokud by se pracoviště rozhodlo řešit bezpečnost komplexně, musí se věnovat všem výsledkům uvedeným v PŘÍLOHA A – Výpočet metody „PNH“ - například aplikací protiopatření, nebo za pomoci vhodného nástroje rizika alespoň sledovat, aby se nestalo kritickou hrozbou, pokud by došlo k navýšení rizika. Strategií vyplývající z analýzy SWOT je použití všech silných stránek k obraně před případnými útoky na dostupnost služeb pracoviště.

Tabulka 10 - metoda "PNH" shrnutí výsledků

aktivum	hrozba	zranitelnost	získané body	rizikový stupeň
zálohy	škodlivý kód	neaktuálnost SW	125	I.
databáze Oracle	škodlivý kód	neaktuálnost SW	125	I.
servery	škodlivý kód	neaktuálnost SW	100	II.
zálohy	napadení komunikace	neaktuálnost SW	100	II.
zálohy	napadení komunikace	nedostatečné bezpečnostní školení a povědomí zaměstnanců	80	II.
operační systémy	škodlivý kód	neaktuálnost SW	75	II.
zálohy	škodlivý kód	nechráněné komunikační linky	75	II.
databáze Oracle	škodlivý kód	nechráněné komunikační linky	75	II.
servery	narušení fyzické bezpečnosti	nedostatečné bezpečnostní školení a povědomí zaměstnanců	64	II.
servery	škodlivý kód	nechráněné komunikační linky	60	II.
operační systémy	napadení komunikace	neaktuálnost SW	60	II.
zálohy	narušení fyzické bezpečnosti	nechráněné komunikační linky	60	II.
zálohy	napadení komunikace	nechráněné komunikační linky	60	II.

Zdroj: vlastní zpracování

Výsledek použití **analýzy SWOT** bylo doporučení strategie S-T (max-mini). To pro pracoviště znamená využít své silné stránky v oblasti PIS a IT infrastruktury k minimalizaci hrozeb ohrožujících jejích aktiv. Očekávaný příchod nové legislativy NIS2 by nemělo být problematické zvládnout, pokud se i nadále bude pracoviště zaměřovat na kvalitu a rozsah bezpečnostních předpisů a v pravidelných intervalech revidovat jejich obsah.

Negativními zjištěními v oblasti zabezpečení aktiv, získanými provedeným **průzkumem na pracovišti** jsou:

- nedostatky fyzické ochrany v podobě neošetřených prosklených výplní ve vstupních dveřích a stěně serverovny, které lze snadno překonat rozbitím. Volný a nekontrolovaný pohyb veřejnosti mimo prostory veřejnosti určené. Díky otevřené serverové skříni je možné narušit chod serverů například nechtěným vytržením kabelu (datového, napájecího), lepé se ale chladí instalovaná technika,
- některé operační systémy používané organizací jsou zastaralé – Windows 10 ve verzi 20H2 nejsou od 10. 5. 2022 podporovány od výrobce (Microsoft), podobně je na tom i Windows server 2008, kterým v používané verzi končí podpora 10. 1. 2023,
- všechny datové zásuvky umístěné ve společných prostorách jsou aktivní a USB porty uživatelských počítačů nejsou omezeny,
- NAS, na který jsou ukládané druhotné zálohy („zálohy záloh“), je umístěn ve stejném prostoru s ostatními technologiemi, což neodpovídá principu zálohy, která by měla být co nejvíce odstíněna od stejných hrozeb, kterými ohroženy zálohovaná aktiva,
- pro identifikaci a autentizaci je použito pouze jednofaktorové přihlašování pomocí uživatelského jména a hesla. Tvorba účtů a přidělení přístupů je navíc přidělováno nevhodně pomocí PIS, do kterého mají přístup i jiné osoby než administrátoři ICT.

3. NÁVRH PRO ZLEPŠENÍ ZABEZPEČENÍ

Návrhy pro zlepšení zabezpečení jsou doporučeními, které by mělo pracoviště aplikovat pro zmírnění dopadu hrozeb. Hrozby byly zjištěny při analýze SWOT a bodovém odhadu „PNH“. Kapitola také obsahuje návrh pro zranitelnosti v podobě nedostatků v aktuálním zabezpečení zjištěných při průzkumu pracoviště, aby v budoucnu nedošlo k jejich ohrožení stejnými nebo v horším případě dalšími hrozbami.

Technická opatření

- Aplikování bezpečnostní fólie na prosklené plochy dosažitelné z okolí úřadu a zabránit tak jednoduchému rozbití těchto ploch.
- Omezení volného pohybu veřejnosti – omezení vstupu aplikováním pevné přepážky v podobě stěny s dveřmi. Lze použít komunikační nástroj v podobě elektronického vrátníka pro umožnění vstupu nebo využít služby strážní služby k evidenci vstupujících mimo veřejnosti přístupné prostory.
- Zajištění bezpečnosti sítě LAN pomocí vypnutí nepoužívaných portů na switchi, čímž dojde k deaktivaci nepoužívaných zásuvek. Porty switchů, které zůstanou aktivní, zabezpečit pouze na omezená zařízení pomocí filtrování pevných adres připojených zařízení
- Nevyužité USB porty na počítačích zaměstnanců ochránit před možným připojením cizího zařízení jejich softwarovým vypnutím na úrovni BIOS počítače.
- Pro identifikaci uživatelů v síti využít další ověřovací faktor, kterým může být biometrické údaje (např. otisk prstu) nebo token (čipová karta).
- Dodržet základní princip zálohování – záloha nemá být umístěna ve stejném místě jako zálohované zařízení nebo data. Doporučení je umístit záložní zařízení NAS do jiného prostoru, než je serverovna, nutností je dodržení všech bezpečnostních pravidel i v tomto odloučeném místě.

Organizační opatření

- Zlepšení organizace v testování a nasazení aktualizací aktiv definováním testovací skupiny s danými členy a odpovědností za testování. Pro instalace a kontrolu začít využívat prostředků centrálního dohledu, které jsou nainstalovány na počítačích a serverech. Do organizačních politik zavést pravidlo užití pouze aktuálního software s podporou.

- Upravit plány školení a zahrnout do nich bezplatné kurzy bezpečnosti, které pořádá NÚKIB, ty opakovat v pravidelném intervalu. Na intranet organizace pravidelně vyvěšovat informace o aktuálních nebezpečích hlášených od NÚKIB (aktuální SPAM, oznámené útoky na dostupnost…). Alespoň jednou ročně pořádat interní školení na téma bezpečnosti shrnující stálá pravidla a aktualizované o aktuální hrozby a změny předpisů.
- Změna používání PIS – v gesci personálního systému ponechat pouze tvorbu uživatelských účtů. Přidělení oprávnění uživatelům ponechat na administrátorech ICT a samotném Active Directory. Pracoviště by také mohlo jít cestou pořízení informačního systému správy identit. Tímto systémem by pracoviště mohlo vyřešit i chybné zápisy v PIS a splnění bezpečnostních předpisů v oblasti správy identit.
- Protože lidé jsou pro údržbu systémů stále potřeba, mělo by se pracoviště věnovat důsledně personální stránce a dostatečnému hodnocení práce svých podřízených, aby bylo možné zajistit stabilitu v dotčených odděleních (personální / ekonomka a administrátoři ICT), aby nemuselo řešit nedostatek odborníků na trhu práce.

ZÁVĚR

Protože bezpečnost je neustálý proces a žádné opatření nikdy nepokryje riziko hrozby v celém rozsahu (i při absolutní minimalizaci rizika hrozba stále existuje), může být pro pracoviště těžké identifikovat všechny hrozby bez určitého nadhledu, nebo posouzení nezávislou osobou. Práce řeší identifikaci hrozeb reálného pracoviště a vyhodnocení jejich působení na informační systém a IT infrastrukturu. Kapitoly a podkapitoly práce odkazují na jednotlivé body osnovy, jejichž obsah je rozveden na potřebnou úroveň pro pochopení tématu systémů, IT infrastruktury a jejich bezpečnosti. Na praktickém příkladu jsou získané znalosti aplikovány pro nalezení a vyhodnocení hrozeb pro bezpečnost v reálné organizaci.

Práce je rozdělena do tří částí, kdy v první si klade za cíl seznámit čtenáře se základními pojmy v oblasti informačních systémů a IT infrastruktury. Obě oblasti jsou, díky své rozsáhlosti, probírány zejména v tématech potřebných k získání přehledu o informacích, informačních systémech. První část rozebírá také téma bezpečnosti, které rozvíjí při popisu kybernetické bezpečnosti týkající se vybraných objektů průzkumu z prostředí informačních technologií. Součástí jsou také metody, kterými lze získat a vyhodnotit informace o zabezpečení.

Druhou kapitolu tvoří z části seznámení se se zkoumanou organizací a její obecný popis, který dotváří kontext dalším částem kapitoly. Na popis organizace navazují zjištění získaná průzkumem stávajícího stavu zabezpečení a jeho vlivu na vybrané oblasti. Pro další postupy jsou definována důležitá aktiva vybraná z obou oblastí a je jim přiděleno ohodnocení možného dopadu na organizaci při působení vybraných hrozeb, které byly taktéž ohodnoceny z pohledu pravděpodobnosti jejich výskytu. Pro působení hrozeb byly definovány zranitelnosti aktiv, které by mohly být využity a také došlo k jejich obodování. Takto obodovaná aktiva, hrozby a zranitelnosti byly použity pro výpočet míry rizika pomocí metody „PNH“. Výsledkem je tabulka míry rizika pro každou kombinaci aktivum x hrozba x zranitelnost. Výsledky byly rozděleny pomocí bodových intervalů do rizikových stupňů. Z výsledků byly vybrány nezávažnější případy pro zobrazení ve výsledcích. Pro lepší představu, jak postupovat v dalším zajištění bezpečnosti byla použita analýza SWOT. Zadáním slabých a silných stránek organizace a hrozeb a příležitostí z jejího okolí byly definovány možné strategie dalšího postupu v oblasti zabezpečení. Kvantifikací a výpočtem byla získána výsledná bezpečnostní strategie S-T (maximalizace silných stránek pro eliminaci hrozeb). Kapitolu uzavírá, uvedenými metodami vypočtené, vyhodnocení hrozeb a zjištěné výsledky průzkumu zabezpečení.

Třetí část navrhuje změny, které by organizace měla uplatnit jako protiopatření ke zmírnění rizika a pro zlepšení současné situace zabezpečení aktiv vyplývající ze zjištění v předchozí kapitole. Doporučení k zabezpečení jsou sepsána tak, aby bylo možné je ve vybrané organizaci použít, byla pro ni dosažitelná, srozumitelná a minimalizovala možnost zneužití zranitelností některou ze zjištěných hrozeb na minimální (akceptovatelnou) úroveň.

Pro sebe vidím přínosy práce v prohloubení stávajících a získání nových znalostí v oblasti zabezpečení, které jsou mi ku prospěchu v mém aktuálním zaměstnání. Pro případného čtenáře vidím přínos v možnosti ujasnění pojmů a získání návodu pro postup průzkumu zabezpečení, který se nemusí aplikovat jen na organizace. Protože metody jsou univerzální, lze je použít pro hodnocení bezpečnosti fyzické osoby nebo objektu.

Na základě výše uvedených závěrů, mohu konstatovat, že jsem splnil cíl práce formulovaný v úvodní části.

POUŽITÁ LITERATURA

[1] SKLENÁK, Vilém. *Data, informace, znalosti a Internet*. První. Praha: C.H. Beck, 2001. C.H. Beck pro praxi. ISBN 80-717-9409-0.

[2] BRABEC, František, Ivo LÁTAL, Rudolf MUSIL, Miloš URBAN a Tomáš VEJLUPEK. *Bezpečnost pro firmu, úřad, občana*. Praha: Public History, 2001. ISBN 80-86445-04-06.

[3] SOUČEK, Zdeněk. *Firma 21. století: (předstihněme nejlepší!!!)*. První. [Praha]: Professional Publishing, 2005. ISBN 80-864-1988-6.

[4] JANČÍKOVÁ, Zora. *Teorie systémů*. První. Ostrava: Vysoká škola báňská - Technická univerzita, 2012. ISBN 978-80-248-2561-8.

[5] KOMÁRKOVÁ, Jitka. *Úvod do informačních systémů: pro kombinovanou formu studia*. Vyd. 1. Pardubice: Univerzita Pardubice, 2006. ISBN 80-719-4870-5.

[6] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2010. ISBN 978-80-7380-276-9.

[7] LAUDON, Kenneth a Jane LAUDON. *Essentials of management information systems*. Thirteenth edition. New York: Pearson, 2019. ISBN 978-013-4802-756.

[8] DANEL, Roman. *INFORMAČNÍ SYSTÉMY*. První. Ostrava: Vysoká škola báňská – Technická univerzita Ostrava, 2013. ISBN 978-80-248-3051-3.

[9] POKORNÝ, Jaroslav. *Databázové systémy a jejich použití v informačních systémech*. Vydání 1. Praha: Academia, 1992. ISBN 80-200-0177-8.

[10] CHARLES, Michael. ManageEngine: Pitstop. In: *ManageEngine: Pitstop* [online]. Zoho Corp., 2022 [cit. 2022-10-15]. Dostupné z: https://pitstop.manageengine.com/portal/en/community/topic/term-of-the-day-peopleware

[11] PRUKNER, Vítezslav. *Manažerské dovednosti* [online]. První. Olomouc: Univerzita palackého v Olomouci, 2014 [cit. 2022-10-15]. ISBN 978-80-244-4329-4. Dostupné z: https://publi.cz/books/114/Cover.html

[12] CEJTHAMR, Václav a Jiří DĚDINA. *Management a organizační chování*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2010. Expert (Grada). ISBN 978-80-247-3348-7.

[13] BASL, Josef a Roman BLAŽÍČEK. *Podnikové informační systémy: podnik v informační společnosti*. 3., aktualiz. a dopl. vyd. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4307-3.

[14] ČERMÁK, Miroslav. Životní cyklus informace. In: *CLEVER AND SMART* [online]. 2022 [cit. 2022-10-15]. Dostupné z: https://www.cleverandsmart.cz/wp-content/uploads/zivotni-cyklus-informace.jpg

[15] KOĎOUSKOVÁ, Barbora. Informační systémy v kostce: ERP, CRM, implementace. In: *Rascasone* [online]. Praha: Rascasone, 2022 [cit. 2022-10-15]. Dostupné z: https://www.rascasone.com/cs/blog/informacni-systemy-erp-crm-implemetace

[16] ŽID, Norbert. *Orientace ve světě informatiky*. 1. Praha: Management Press, 1998. ISBN 80-859-4358-1.

[17] PROCHÁZKA, Jaroslav a Cyril KLIMEŠ. *Provozujte IT jinak: agilní a štíhlý provoz, podpora a údržba informačních systémů a IT služeb*. První. Praha: Grada, 2011. Průvodce (Grada). ISBN 978-80-247-7295-0.

[18] STRYHAL, Tomáš. 5. Síťová zařízení. In: *Tomáš Stryhal: Studijní materiály pro předmět Informatika a výpočetní technika* [online]. [cit. 2022-10-20]. Dostupné z: http://sites.cgym-kh.cz/stryhal/kvarta/pocitacove-site/sitova-zarizeni

[19] SOSINSKY, Barrie A. *Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]*. První. Brno: Computer Press, 2010. ISBN 978-80-251-3363-7.

[20] ŠTRÁFELDA, Jan. Server. In: *Jan Štráfelda* [online]. Praha/Mělník [cit. 2022-10-16]. Dostupné z: https://www.strafelda.cz/server

[21] BROOKSHEAR, J., David SMITH a Dennis BRYLOW. *Informatika*. 1. vydání. Brno: Computer Press, 2013. ISBN 978-80-251-3805-2.

[22] KIZZA, Joseph Migga. *Guide to computer network security*. Fourth edition. Cham, Switzerland: Springer-Verlag, 2017. Computer communications and networks. ISBN 978-3-319-55605-5.

[23] SMYSITELOVÁ, Lucie. Historie rozlehlých počítačových sítí. In: *FI MUNI: Masarykova univerzita Fakulta informatiky* [online]. Brno: Masarykova univerzita, 1999 [cit. 2022-10-23]. Dostupné z: https://www.fi.muni.cz/usr/jkucera/pv109/xsmysit.html

[24] CANDACE, Leiden a Marshall WILENSKY. *TCP/IP For Dummies®*. 6th ed. Indianapolis: Wiley Publishing, 2009. ISBN 978-0-470-45060-4.

[25] SPURNÁ, Ivona. *Počítačové sítě: praktická příručka správce sítě*. Vydání první. Kralice na Hané: Computer Media, 2010. ISBN 978-80-7402-036-0.

[26] POSPÍŠIL, Vojtěch. Nejčastěji používané síťové protokoly. In: *ZoneCloud: Magazín* [online]. Brno: Zoner, 2022 [cit. 2022-10-23]. Dostupné z: https://www.zonercloud.cz/magazin/nejcasteji-pouzivane-sitove-protokoly

[27] ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015. ISBN 978-80-7395-953-1.

[28] ČERMÁK, Miroslav. Informační bezpečnost vs. kybernetická bezpečnost. In: *CLEVER AND SMART* [online]. Zálepy, 2014 [cit. 2022-11-05]. Dostupné z: https://www.cleverandsmart.cz/information-security-vs-cybersecurity/

[29] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[30] ŠULC, Vladimír. *Kybernetická bezpečnost*. První. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o., 2018. ISBN 978-80-7380-737-5.

[31] *Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů: zákon o kybernetické bezpečnosti*. In: . Sbírka zákonů České republiky: Česko, 2014, ročník 2014, částka 75, číslo 181.

[32] RODRYČOVÁ, Danuše a Pavel STAŠA. *Bezpečnost informací jako podmínka prosperity firmy*. Praha: Grada, 2000. Manažer. ISBN 80-716-9144-5.

[33] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. První. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

[34] SEDLÁK, Petr a Martin KONEČNÝ. *Kybernetická (ne)bezpečnost: problematika bezpečnosti v kyberprostoru*. První. Brno: CERM, akademické nakladatelství, 2021. ISBN 978-80-7623-068-2.

[35] PETROVIČ, Michal a Michal KOSTĚNEC. CISCO NETWORKING ACADEMY PROGRAM. *Bezpečnost počítačových sítí*. Plzeň: Západočeská univerzita v Plzni, 2012, vi, ii, 214 s. : il. ; 21 cm. ISBN 978-80-261-0117-8.

[36] *ČSN ISO/IEC 27005. Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. Praha: Česká agentura pro standardizaci, 2019, 52 s. Třídící znak 36 9790.

[37] BLAŽKOVÁ, Martina. *Marketingové řízení a plánování pro malé a střední firmy*. První. Praha: Grada, 2007. ISBN 978-80-247-1535-3.

[38] ŠEFČÍK, Vladimír. *Analýza rizik*. První. Zlín: Univerzita Tomáše Bati ve Zlíně, 2009. ISBN 978-80-7318-696-8.

[39] *ZPRÁVA O STAVU KYBERNETICKÉ BEZPEČNOSTI ČESKÉ REPUBLIKY ZA ROK 2021* [online]. Praha: Národní úřad pro kybernetickou a informační bezpečnost, 2022 [cit. 2022-11-27]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/Zprava_o_stavu_kybernetick_bezpenosti_2021.pdf

[40] ČESKO. *Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů*. In: Sbírka zákonů České republiky, 2005. ISSN 1211-1244. Dostupné také z: http://aplikace.mvcr.cz/sbirka-zakonu/start.aspx

PŘÍLOHY

Příloha A – Výpočet metody „PNH“

PŘÍLOHA A – VÝPOČET METODY „PNH“

Tabulka s výpočty hodnocení rizika hrozby pro aktiva pomocí metody „PNH“.

aktivum	hrozby	zranitelnost	P	N	H	R
A1	H1	Z3	4	2	4	32
A1	H1	Z4	4	2	2	16
A1	H2	Z1	4	4	1	16
A1	H2	Z3	4	4	4	64
A1	H3	Z2	4	2	3	24
A1	H3	Z4	4	2	2	16
A1	H3	Z5	4	2	5	40
A1	H4	Z2	4	5	3	60
A1	H4	Z4	4	5	2	40
A1	H4	Z5	4	5	5	100
A1	H6	Z3	4	2	4	32
A1	H6	Z4	4	2	2	16
A1	H7	Z3	4	1	4	16
A1	H7	Z4	4	1	2	8
aktivum	**hrozby**	**zranitelnost**	**P**	**N**	**H**	**R**
A2	H1	Z3	2	2	4	16
A2	H1	Z4	2	2	2	8
A2	H2	Z1	2	4	1	8
A2	H2	Z3	2	4	4	32
A2	H3	Z2	2	2	3	12
A2	H3	Z4	2	2	2	8
A2	H3	Z5	2	2	5	20
A2	H4	Z2	2	5	3	30
A2	H4	Z4	2	5	2	20
A2	H4	Z5	2	5	5	50
A2	H5	Z1	2	4	1	8
A2	H5	Z2	2	4	3	24
A2	H5	Z3	2	4	4	32
A2	H5	Z4	2	4	2	16
A2	H5	Z5	2	4	5	40
A2	H7	Z3	2	1	4	8
A2	H7	Z4	2	1	2	4
aktivum	**hrozby**	**zranitelnost**	**P**	**N**	**H**	**R**
A3	H3	Z2	3	2	3	18
A3	H3	Z4	3	2	2	12
A3	H3	Z5	3	2	5	30
A3	H4	Z2	3	5	3	45
A3	H4	Z4	3	5	2	30

aktivum	hrozby	zranitelnost	P	N	H	R
A3	H4	Z5	3	5	5	75
A3	H5	Z1	3	4	1	12
A3	H5	Z2	3	4	3	36
A3	H5	Z3	3	4	4	48
A3	H5	Z4	3	4	2	24
A3	H5	Z5	3	4	5	60
A3	H7	Z3	3	1	4	12
A3	H7	Z4	3	1	2	6
aktivum	**hrozby**	**zranitelnost**	**P**	**N**	**H**	**R**
A4	H2	Z1	5	4	1	20
A4	H2	Z2	5	4	3	60
A4	H3	Z2	5	2	3	30
A4	H3	Z4	5	2	2	20
A4	H3	Z5	5	2	5	50
A4	H4	Z2	5	5	3	75
A4	H4	Z4	5	5	2	50
A4	H4	Z5	5	5	5	125
A4	H5	Z1	5	4	1	20
A4	H5	Z2	5	4	3	60
A4	H5	Z3	5	4	4	80
A4	H5	Z4	5	4	2	40
A4	H5	Z5	5	4	5	100
A4	H6	Z3	5	2	4	40
A4	H6	Z4	5	2	2	20
A4	H7	Z3	5	1	4	20
A4	H7	Z4	5	1	2	10
aktivum	**hrozby**	**zranitelnost**	**P**	**N**	**H**	**R**
A5	H2	Z1	2	4	1	8
A5	H2	Z2	2	4	3	24
A5	H5	Z1	2	4	1	8
A5	H5	Z2	2	4	3	24
A5	H5	Z3	2	4	4	32
A5	H5	Z4	2	4	2	16
A5	H5	Z5	2	4	5	40
A5	H6	Z3	2	2	4	16
A5	H6	Z4	2	2	2	8
aktivum	**hrozby**	**zranitelnost**	**P**	**N**	**H**	**R**
A6	H4	Z2	1	5	3	15
A6	H4	Z4	1	5	2	10
A6	H4	Z5	1	5	5	25
A6	H6	Z3	1	2	4	8

aktivum	hrozby	zranitelnost	P	N	H	R
A6	H6	Z4	1	2	2	4
A7	H3	Z2	5	2	3	30
A7	H3	Z4	5	2	2	20
A7	H3	Z5	5	2	5	50
A7	H4	Z2	5	5	3	75
A7	H4	Z4	5	5	2	50
A7	H4	Z5	5	5	5	125
A7	H6	Z3	5	2	4	40
A7	H6	Z4	5	2	2	20