Ochrana datové infrastruktury podniku

Bc. Bohuslav Beran

Diplomová práce
2019

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2018/2019

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Bohuslav Beran**
Osobní číslo:	**A17310**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Ochrana datové infrastruktury podniku**
Téma anglicky:	**The Protection of an Enterprise's Data Infrastructure**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Analyzujte současnou legislativu, bezpečnostní situaci a používané bezpečnostní modely.**
3. **Popište bezpečnostní hrozby a trendy útoků na datovou infrastrukturu podniku.**
4. **Představte podnik a použitý podnikový informační systém (ERP) a jeho nasazení.**
5. **Uveďte příklady možných současně známých útoků a případné dopady na chod podniku.**
6. **Analyzujte stav zabezpečení podnikové infrastruktury a podnikového informačního systému, definujte možné hrozby, prověřte silné a slabé stránky.**
7. **Na základě získaných poznatků navrhněte vhodná protiopatření pro posílení ochrany datové infrastruktury a vyhodnoťte jejich přínos v podniku.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **JAŠEK, Roman a David MALANÍK. Bezpečnost informačních systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013. ISBN 978-80-7454-312-8.**
2. **STAUDEK, Jan a Petr HANÁČEK. Bezpečnost informačních systémů. 1. vyd. Praha: Úřad pro státní informační systém, 2000. 127 s. ISBN 80-238-5400-3.**
3. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 8025101061.**
4. **BARTONĚK, Dalibor a Robert JURČA. Informační systémy. Kunovice: Evropský polytechnický institut, 2014. ISBN 978-80-7314-322-4.**
5. **DOBDA, Luboš. Ochrana dat v informačních systémech. 1. vyd. Praha: Grada Publishing, 1998, 286 s. ISBN 80-716-9479-7.**
6. **GDPR: Obecné nařízení o ochraně osobních údajů prakticky. 2017. Dostupné z: https://www.gdpr.cz/.**

Vedoucí diplomové práce: **doc. Ing. Martin Hromada, Ph.D.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **30. listopadu 2018**

Termín odevzdání diplomové práce: **17. května 2019**

Ve Zlíně dne 14. prosince 2018

L.S.

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně, dne …….

podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá firemní datovou infrastrukturu, riziky a hrozbami, kterým může být vystavena. Teoretická část uvádí základní pojmy, představuje prvky datové infrastruktury, možné hrozby podnikový informační systém a metody analýzy rizik. Praktická část se zabývá analýzou rizik, návrhem na jejich ošetření a případné posílení ochrany datové infrastruktury ve společnosti Agrotec a.s.

Klíčová slova:

DATA, FIRMA INFORMACE, INFORMAČNÍ SYSTÉM, OCHRANA

ABSTRACT

The diploma thesis deals with corporate data infrastructure, risks and threats that it might be exposed to. The theoretical part specifies basic terms, presents the elements of data infrastructure, potential threats, company information system and methods of risks analysis. The practical part deals with risks analysis, proposal for their treatment and possible reinforcement of data infrastructure protection in the company Agrotec a.s.

Keywords:

COMPANY, DATA, INFORMATION, INFORMATION SYSTEM, PROTECTION

Poděkování:

Rád bych na tomto místě poděkoval doc. Ing. Martinu Hromadovi, Ph.D., vedoucímu této diplomové práce, za konzultace, pomoc a trpělivost při jejím vypracování.

Také bych chtěl poděkovat Ing. Miroslavu Štolpovi, Ph.D., vedoucímu oddělení informačních a komunikačních technologií, a Petru Čankymu, vedoucímu SAP oddělení ve společnosti Agrotec a.s., a dále ing. Tomáši Pokornému ze společnosti IBM za poskytnutí informací, podkladů, rad a odborných konzultací při tvorbě praktické části této diplomové práce.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Význam počítačové a komunikační techniky v současnosti rapidně roste ve všech oblastech běžného života a zásadně se dotýká i provozu a fungování prakticky všech dnešních podniků. Digitalizace pronikla prakticky do všech oborů a není možné se jí vyhnout. Přinesla s sebou dříve těžko představitelné výhody, mezi jednu z hlavních je možné uvést prakticky okamžitou dostupnost informací v reálném čase, stačí jen vědět, kde se informace nacházejí, a mít potřebné online připojení.

Za okamžitou dostupností informací se skrývá neviditelná, pro mnoho lidí možná i nepředstavitelná flotila vzájemně propojených a komunikujících počítačů a jiných síťových či datových prvků schopných uchovávat, přenášet a poskytovat zadané informace všem návštěvníkům, kteří přistoupí k některému konkrétnímu zdroji v dané síti, obvykle známému Internetu. Dostupnost připojení do této sítě zásadně změnila způsob přenosu informací a jejich sdílení, zejména v oblasti medií, sociální komunikace nebo vzdělávání došlo k určitému velkému třesku, kdy je množství snadno dostupných, často ale protichůdných informací či sdělení natolik velké, že je nutné získané informace dále filtrovat a ověřovat.

Kromě volně šiřitelných a veřejně dostupných informací nadále existují oblasti, ve kterých je nutné informace centralizovat, sdílet a dále s nimi pracovat pouze v užším spektru zainteresovaných osob, kdy dostupnost všem je nežádoucí. Nemusí se jen jednat o prostředí tajných služeb či bezpečnostních složek, ale i soukromých firem. Každá organizace disponuje informacemi, které je třeba vhodným způsobem ochránit a zajistit tak, že nebude volně přístupná komukoliv, kdo projeví zájem. V prostředí digitální doby to znamená zejména ochránit datovou infrastrukturu, která tyto informace uchovává, přenáší a poskytuje určenému okruhu osob před neoprávněným přístupem k datům a informacím.

S ohledem na stále rostoucí množství a objem zpracovávaných dat rostou i nároky na zajištění funkční a bezpečné datové sítě. Zejména středně velké a velké podniky tak musejí hledat cesty a způsoby, jak zajistit bezpečnost svých dat a informací, jejichž hodnota může zejména u vývojově či výrobně zaměřených produktů nabývat těžko vyčíslitelných hodnot.

Tato diplomová práce vysvětluje, co se skrývá pod obecným pojmem datová infrastruktura, shrnuje aktuální rizika a hrozby, kterým může být vystavená podniková datová infrastruktura, a hledá vhodná opatření, která mohou působení rizik a hrozeb snížit.

I. TEORETICKÁ ČÁST

1 INFORMAČNÍ BEZPEČNOST

Rostoucí význam informací se dotýká do všech oblastí lidského života. Ve vojenských operacích rozhoduje kvalita informací a jejich vhodné využití o průběhu či výsledku konfliktu, ve firemní sféře pak vlastnictví určitých informací ve vhodnou dobu může znamenat výrazný potenciál pro další rozvoj podniku. I nejmenší organizace tak čelí nutnosti získávat, zpracovávat a uchovávat informace, ke kterým by neměly mít přístup neoprávněné osoby.

Brigádní generál Armády ČR Karel Řehka definuje pojem informační bezpečnost takto: *„Jejím cílem je chránit uložené, zpracovávané nebo přenášené informace a jejich hostitelské systémy proti ztrátě důvěrnosti, celistvosti a dostupnosti prostřednictvím různého procedurálního, technického a administrativního řízení.“*[1]

V obecné rovině se tak informační bezpečnost zabývá postupy a opatřeními pro zajištění utajení určitých informací. Zároveň je nutné zachovat požadovanou úroveň rozhodování či dostupnosti a sdílení těchto informací. Příliš vysoké utajení informací může mít stejně negativní dopady jako nedostatečné utajení. [1]

Současný význam informační bezpečnosti v jakékoliv oblasti výrazně ovlivňuje fakt, že se z informací stalo žádané a obchodovatelné zboží. Zejména ve firemním prostředí tak případná ztráta dat či informací může mít velmi vážné dopady na další fungování podniku.

1.1 Základní pojmy

V oblasti bezpečnostních systémů a bezpečnostní politiky se užívají tyto pojmy:

Aktivum:

„Aktivum je všechno, co má pro subjekt hodnotu, která může být zmenšena působením hrozby. Aktiva se dělí na hmotná (například nemovitosti, cenné papíry, peníze apod.) a na nehmotná (například informace, předměty průmyslového a autorského práva, morálka pracovníků, kvalita personálu apod.). Aktivem ale může být sám subjekt, neboť hrozba může působit na celou jeho existenci.“[2]

[1] KAREL ŘEHKA – Informační válka, str. 155
[2] VLADIMÍR SMEJKAL a KAREL RAIS - Řízení rizik ve firmách a jiných organizacích. 4., aktualizované. a rozšířené vydání, str. 82

Hodnota aktiva představuje cenu nebo ocenění daného aktiva. U hmotných aktiv ji lze obvykle stanovit na základě pořizovací ceny, u nehmotných aktiv nemusí být možné finanční hodnotu přesně stanovit. Ta může být navíc rozdílná pro majitele podniku či možného útočníka. [3]

Každý podnik by měl znát hodnoty svých aktiv, na základě které lze posoudit význam jejich přiměřené ochrany.

Hrozba:

„*Hrozba je síla, událost, aktivita nebo osoba, která má nežádoucí vliv na bezpečnost nebo může způsobit škodu. Hrozbou může být například požár, přírodní katastrofa, krádež zařízení, získání přístupu k informacím neoprávněnou osobou, chyba obsluhy, ale i kontrola finančního úřadu nebo růst české koruny vzhledem k evropské měně apod*.“[3]

Škody na informačních systémech jsou často obtížně prokazatelné, může se jednat o porušení integrity (celistvosti) dat a informací nebo jejich záměrné pozměnění či zničení, ztrátu dostupnosti či důvěrnosti dat nebo ztrátu autentičnosti dat. [3]

Pro identifikaci hrozeb či jejich dopadů lze využít hodnocení expertních týmů, auditů či vlastních zkušeností. Zásadní vliv představuje stanovení nákladů na odstranění hrozby.

Zranitelnost:

„*Zranitelnost je nedostatek, slabina nebo stav analyzovaného aktiva (případně subjektu nebo jeho části), který může hrozba využít pro uplatnění svého nežádoucího vlivu. Tato veličina je vlastností aktiva a vyjadřuje, jak citlivé je aktivum na působení dané hrozby.*“[4]

Zranitelnost působí na každé aktivum, míru zranitelnosti pak určují různé vlivy. Důležité je stanovení náchylnosti aktiva vůči poškození konkrétní hrozbou (označovaná jako citlivost) v kombinaci s významem aktiva pro subjekt (označované jako kritičnost). [2, 3]

---

[3] VLADIMÍR SMEJKAL a KAREL RAIS - Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání, str. 82

[4] VLADIMÍR SMEJKAL a KAREL RAIS - Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání, str. 83

Protiopatření:

„*Protiopatření je postup, proces, procedura, technický prostředek nebo cokoliv, co bylo speciálně navrženo pro zmírnění působení hrozby (její eliminaci), snížení zranitelnosti nebo dopadu hrozby. Protiopatření se navrhují s cílem předejít vzniku škody nebo s cílem usnadnit překlenutí následků vzniklé škody.*“[5]

Zvolené protiopatření tak může aktiva chránit úplně, případně zmírňovat působení hrozeb a vznik možných škod. [3]

Výběr vhodného protiopatření obvykle znamená hledání optimálního řešení v kombinaci s přijatelnými náklady na jeho realizaci.

Riziko:

„*Riziko vzniká vzájemným působením hrozby a aktiva. Hrozba, která nepůsobí na žádné aktivum, nemusí být při analýze rizik brána v úvahu. Aktivum, na které nepůsobí žádná hrozba, není předmětem analýzy rizik.*“[6]

Příkladem rizika v podnikovém prostředí může být vznik potenciální ztráty či výskyt situace s negativním dopadem na stanovené cíle. Míru rizika lze snížit jeho identifikací, analýzou a řízením. Riziku se lze vyhnout, může to ale znamenat ztrátu možné příležitosti.

Riziko bývá často zaměňováno s nejistotou. Oproti riziku stojí ale nejistota, přestavuje zejména nemožnost nebo neschopnost spolehlivého odhadu dalšího vývoje rizikových faktorů, oproti rizikům ji lze pouze snížit, nikdy ji ale nelze zcela eliminovat.

Data a informace:

Často nesprávně zaměňované pojmy. Data jsou chápána jako statický, časově nezávislý údaj, který je často sám o sobě pro příjemce nesrozumitelný. Po metodickém zpracování dat je možné vytvořit informaci, která již pro uživatele má požadovanou odpovídající hodnotu s vlivem na rozhodovací proces. Informace mají určitou vypovídající a často také pořizovací hodnotu, která může být pro různé strany odlišná. [3, 4]

---

[5] VLADIMÍR SMEJKAL a KAREL RAIS - Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání, str. 83

[6] VLADIMÍR SMEJKAL a KAREL RAIS - Řízení rizik ve firmách a jiných organizacích. 4. aktualizované a rozšířené vydání, str. 83

Pro získání informace musí zpracovatel dat disponovat určitými znalostmi, obvykle získanými na základě předchozího vzdělání nebo zkušeností. Bez těchto znalostí zůstávají jen data bez další informační hodnoty.

Citlivá data a informace:

Jsou data a informace vyžadující s ohledem na jejich hodnotu ochranu před vlivem hrozeb. V oblasti informačních a komunikačních technologií se jedná např. státní či služební tajemství, personální informace, osobní údaje, finanční a účetní výkazy, klientské databáze apod. Ztráta, poškození nebo zničení těchto dat má obvykle negativní dopad na chod organizace, proto je vhodné určit, co přesně před čím bude chráněno, a za jakou cenu, žádná skutečná ochrana není zadarmo. [3]

Informační systém:

Informační systém (dále jen IS) představuje soubor technického i netechnického vybavení, technologií a pracovníků užívaných pro správu informací. [3]

1.2 Informační cyklus

Každá informace prochází během své životnosti postupně několika různými fázemi, dohromady tvořícími tzv. informační cyklus, který je možné rozdělit do následujících kategorií:

- Získání informací – schopnost získat nebo se včas dostat ke správným informacím představuje v současné době jednu z významných vlastností úspěšné firmy. Informace jsou obvykle získávány osobně prostřednictvím zaměstnanců firmy, případně využitím tzv. zpravodajství z otevřených zdrojů (anglicky OSINT – Open Source Inteligence). Mezi hlavní zdroje tak můžeme zařadit různé veřejné rejstříky a databáze, sociální sítě, veřejné knihovny, volně dostupné televizní nebo rádiové zpravodajství, denní tisk, internetové diskuse atd.
- Uchování informací – získanou informaci je nutné vhodným způsobem uchovat, aby byla přístupná i ostatním pracovníkům, mezi jejichž kompetence a pravomoci daná informace spadá. Pro uchování informace je nutné zajistit datové uložiště s přístupem oprávněných uživatelů. Ve firemním prostředí se informace obvykle ukládají do specializovaných podnikových informačních systémů.

- Zpracování a využití informací – Získat včas vhodné informace je zcela určitě výhodou, neméně podstatné je ale získané informace zcela přesně pochopit a využít k požadovaným účelům. K pochopení informace pomáhají různé analytické nástroje, odborné diskuze a hodnocení, týmové workshopy atd.
- Archivace – každá informace postupně ztrácí svoji hodnotu, ať již tím, že stárne, stane se obecně volně dostupnou, nebo již došlo k jejímu uplatnění v praxi. V takovém případě by neměla sdílet stejný prostor s aktuálními informacemi, ale je vhodné ji přesunout do archivu. Je pak zřejmé, o jakou informaci se jedná, jakým způsobem byla využita, přičemž je ale oddělena od aktuálních informací.
- Likvidace – poslední životní fází je odstranění informace z informačního systému.

Bezpečnost a ochrana informací musí být zajištěna po celou dobu jejich životnosti, způsob ochrany vychází z hodnoty dat. Vhodné řízení životního cyklu informací zajišťuje nejen jejich přiměřenou ochranu, zároveň ale zároveň dle analýzy společnosti Deloitte snižuje množství nepotřebných či zastaralých informací, usnadňuje práci s informacemi, a přispívá tak k vyšší efektivitě práce. Ve výsledku tak nabízí významnou úsporu celkových nákladů i vyšší kvalitu nabízených služeb vůči zákazníkům. Důležitá je i aktualizace dat, dle odhadu společnosti Deloitte je 80% dat ve výrobně zaměřených podnicích již zastaralých. [5]

1.3 Druhy informační bezpečnosti

Informační bezpečnosti není možné zajistit univerzálním způsobem. Během svého životního cyklu jsou informace zaznamenány na několika úrovních, které je třeba chránit. Jedná se o:

- Fyzickou bezpečnost – představenou hardwarem, tedy datovými médii, počítači, servery a dalšími zařízeními, na kterých se data nacházejí. Tato zařízení musí být zajištěna proti odcizení, přístupu nepovolaných osob či působení před přírodními nebo jinými hrozbami. Obvykle se využívá pro tento účel vytvořených prostor.
- Personální bezpečnost – lidský faktor, zejména vlastní zaměstnanci, představuje dle uváděných informací největší riziko pro zajištění informační bezpečnosti. Pro zajištění dostatečného zabezpečení je tak nutné nejen vybírat kvalitní pracovníky, ale i zajistit, aby měl každý přístup jen k takovým informacím, které vyžaduje v souvislosti se svou pracovní pozicí.
- Komunikační bezpečnost – data musejí být s ohledem na svoji dostupnost přenášena v rámci počítačových sítí. Během přenosu může dojít k jejich zachycení, poškození,

změně nebo ztrátě, tento stav je samozřejmě nežádoucí. Komunikační bezpečnost tak zajišťuje, aby byl přenos dat úplný a co nejvíce eliminoval výše uvedené hrozby.

- Logická bezpečnost – spočívá v zajištění vhodného softwaru, užívaného pro práci s daty. Obvykle se jedná o operační systém, podnikový informační systém, databázový software a další nástroje. V rámci informační bezpečnosti je nutné mít dostatečně zajištěný nejen samotný software, ale i přístup k němu.
- Organizační bezpečnost – neboli administrativní bezpečnost. Tvoří ji soubor standardů, procesů, pravidel, norem a nařízení, kterými se daný podnik řídí.

Pro zajištění komplexní informační bezpečnosti je nutné aplikovat vhodná bezpečnostní opatření pro jednotlivé úrovně. Ke komplexnímu posouzení bezpečnostních opatření je vhodné použít některou z dostupných analýz rizik, vytvořenou interními nebo externími pracovníky podniku. [6]

1.4 Právní rámec v ČR

V roce 2015 vstoupil v platnost zákon č. 181/2014 Sb., o kybernetické bezpečnosti, který upravuje práva a povinnosti osob a pravomoci a působnosti orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon byl v roce 2017 dvakrát novelizován, a to prostřednictvím zákonů č. 104/2017 Sb. a č. 205/2017 Sb. Hlavním cílem tohoto zákona je:

- Stanovit základní úroveň bezpečnostních opatření
- Vylepšit detekci kybernetických bezpečnostních incidentů a zavést jejich hlášení
- Zavést systém opatření k reakci na kybernetické bezpečnostní incidenty

Dále byla v roce 2018 vydána vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti, na neoprávněný přístup k datům pamatuje i zákon č. 40/2009 Sb. Trestní zákoník, nyní č. 58/2017 Sb. V rámci ČR je ústředním správním orgánem pro kybernetickou bezpečnost, včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany, Národní úřad pro kybernetickou a informační bezpečnost, který vznikl v roce 2017 na základě již zmíněného zákona č. 205/2017 Sb. Ředitel tohoto úřadu je členem výboru pro kybernetickou bezpečnost a pravidelně se též účastní jednání Bezpečnostní rady státu, není ale jejím členem. Tento úřad zajišťuje zejména prevenci před kybernetickými hrozbami, řešení kybernetických bezpečnostních incidentů, vzdělávací činnost, výzkum a vývoj v této oblasti, pořádání národních i mezinárodních cvičení či spolupráci s dalšími orgány působícími v oblasti kybernetické bezpečnosti. [7, 8, 9]

Data, informace, jejich získávání, předávání, zpracování, aplikace, uchovávání či aktualizace mají zásadní význam v téměř všech oblastech běžného života, z čehož vyplývá také potřeba jejich ochrany před ztrátou, odcizením, zneužitím nebo narušením. V případě vlastních dat či informací je pro soukromou osobu čistě na vlastním zvážení, zda je chránit, jakým způsobem a za jakou cenu. U státních organizací, bezpečnostních složek či soukromých podniků už je logicky objem takových dat a informací mnohonásobně vyšší a jejich ochrana se stává nezbytnou. Možností je mnoho, jejich účinná aplikace do praktického života není vůbec snadná.

2 DATOVÁ INFRASTRUKTURA

Termínem datová infrastruktura lze vyjádřit množství vzájemně funkčně propojeným prvků, zajišťujících používání, ukládání a zabezpečení požadovaných dat pro poskytování informačních služeb. V současné moderní době se jedná o jeden z klíčových typů infrastruktur, splňující kritéria pro zařazení mezi kritickou infrastrukturu. Možný výpadek tak představuje hrozbu pro fungování celé ekonomiky i společnosti. Ve firemním prostředí jsou následky možného výpadku zejména ekonomické, mohou se ale projevit i poškozením dobrého jména společnosti.

2.1 Prvky datové infrastruktury

Jednotlivé části datové infrastruktury jsou závislé na její architektuře, nasazení, velikosti a dalších faktorech. Obecně se lze vždy setkat s těmito vzájemně spolupracujícími prvky:

- Datová uložiště – představují média pro fyzické ukládání dat. S ohledem na stále rostoucí datové a informační objemy a požadavek okamžité dostupnosti je nutné zajistit dostatečnou kapacitu i rychlost datových uložišť a to prostřednictvím lokálního řešení nebo cloudu. S ohledem na náročné požadavky na spolehlivost a dostupnost uložišť se využívá specializovaných služeb významných výrobců komponent datové infrastruktury (např. Dell EMC), které jsou schopné nabídnout návrh a výstavbu datového uložiště přesně dle požadavků konkrétního podniku.
- Hardware – zahrnuje veškeré komponenty nutné pro provoz počítačové sítě zajišťující dostupnost spojení a přenos informací. Jednotlivé komponenty se liší dle použité síťové architektury, v obecné rovině se jedná o routery, přepínače, servery, síťovou kabeláž, zesilovače signálu, vzdálené přístupové body a další technická zařízení.
- Software – jedná se o programové nástroje určené pro zajištění provozu sítě. Do této kategorie můžeme zařadit jak příslušné databázové nástroje, tak aplikace pro monitorování stavu sítě, její správu či řízení.
- Síťové uspořádání – architektura sítě definuje použité síťové prvky, jejich vzájemné propojení a závislosti k zajištění funkčního celku.
- Fyzické prostory – jedná se o místa s fyzickou alokací síťových komponentů. Zejména u serverů a datových uložišť by se mělo jednat o prostory schopné zajistit dostatečnou bezpečnost před neoprávněným přístupem, schopnou odolat hrozbám přírodního či umělého charakteru.

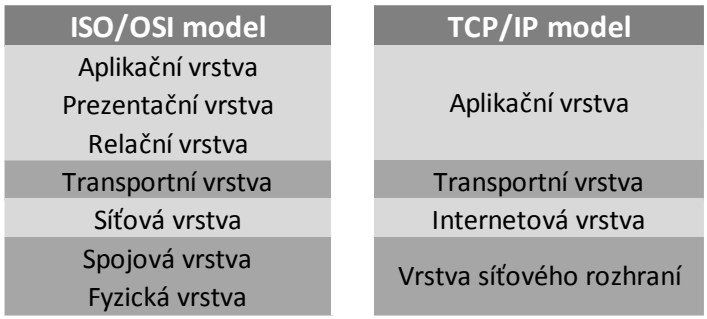
- Lidé – všichni uživatelé s přístupem do dané sítě na různé úrovni (od běžných uživatelů až po správce sítě). Každý uživatel by měl mít v rámci svého přístupu definována jen taková oprávnění, která mu umožňují plnění svěření pracovních úkolů. Nadbytečná oprávnění nejsou kvůli riziku zneužití vhodná.

S ohledem na složitost celkové sítě je nutné zajistit, aby jednotlivé prvky byly v rovnováze. Návrh a výstavbu sítě by měli provádět zkušení pracovníci, případně specializovaná externí firma, u které se předpokládají vyšší znalosti aktuálních technologií a možností řešení.

2.2 Síťová architektura

Síťová architektura představuje velice složitý soubor různých prvků, které je nutné vhodně propojit tak, aby byla zajištěna vzájemná spolupráce. Jednotlivé síťové protokoly jsou proto uspořádány do tzv. vrstev, zajišťujících provedení určitých činností pomocí služeb vrstvy bezprostředně pod sebou. Tyto vrstvy jsou zajištěny pomocí softwarových (dále jen SW) či hardwarových (dále jen HW) prvků nebo jejich kombinací. Původní model síťové architektury byl vypracován organizací pro standardizaci ISO již v sedmdesátých letech dvacátého století a je označován podle výboru založeného touto organizací jako OSI (Open ® Interconnection). Model OSI pracuje se sedmi vrstvami (aplikační, prezentační, relační, transportní, síťová, linková a fyzická vrstva).

V sedmdesátých letech dvacátého století byl vytvořen jiný síťový model pracující s jednotlivými vrstvami, označovaný jako TCP/IP (Transmition control protocol/Internet protocol), zohledňující práci s protokoly v rámci internetu a dalších sítí. Tento model pracuje na rozdíl od ISO/OSI modelu pouze se čtyřmi vrstvami (aplikační, transportní, internetová a vrstva síťového rozhraní). Na obrázku níže je vidět vzájemné srovnání těchto vrstev. [10, 11]



Obr. 1 - Srovnání síťových modelů [6]

Aplikační vrstva:

Nejvyšší vrstva zajišťuje přenos zpráv síťových aplikací pomocí různých protokolů. Mezi nejznámější protokoly patří ®, SMTP, FTP, Telnet nebo DNS. Protože jsou tyto protokoly vždy předávány na několik koncových systémů, mohou si tímto způsobem vzájemně předávat informace, pro tuto vrstvu označovanou jako zprávy. Tyto protokoly určují, jaké zprávy si jednotlivé aplikace na koncových systémech vzájemně předávají. [10]

Dle statistik společností SAP a IBM Security jsou případné útoky na datovou infrastrukturu ve více než 80% všech případů prováděny právě na této vrstvě.

Transportní vrstva:

Tato vrstva slouží pro přepravu zpráv aplikační vrstvy mezi koncové body aplikací, a to pomocí dvou protokolů – TCP a UDP. Protokol TCP prostřednictvím spojované služby řídí datový tok a zaručuje doručení zpráv z aplikační vrstvy do cíle. V případě přehlcení sítě umí snížit přenosovou rychlost mezi vysílacím a přijímacím bodem. Protokol UDP je oproti tomu nespojovaný, nezaručuje tedy spolehlivé doručení paketů, ani neumožňuje řídit datový tok v případě zahlcení. Je vhodný pro použití v případech, kdy se počítá se ztrátou datagramů (např. hlasové VoIP přenosy). [10, 11]

Síťová vrstva:

Bývá také někdy označována jako internetová nebo jen IP vrstva, podle nejznámějšího protokolu pracujícího na této vrstvě. Dále obsahuje také směrovací protokoly určující trasy datagramů mezi zdrojovými a cílovými body napříč sítí. Najdeme ji jak ve směrovačích, tak

v koncových zařízeních. [10, 11]

Vrstva síťového rozhraní:

Hierarchicky nejnižší vrstva umožňující přístup do sítě pomocí určitých přenosových médií (ethernet, optické vlákno, wifi…). [11]

Pochopení funkčnosti modelu síťové architektury umožňuje definovat vhodné zabezpečení sítě a zaměřit se na klíčové vlastnosti jednotlivých vrstev.

Síťová architektura představuje složitý systém složený obvykle z velkého množství vzájemně propojených komponent. Tak jako v jiných oblastech zde platí, že míra spolehlivosti či zranitelnosti celé sítě je dána jejím nejslabším prvkem. Případní útočníci obvykle nezkouší náhodné útoky, ale zkoušejí, např. pomocí tzv. skenování portů, jednotlivé síťové prvky a služby s cílem najít právě nejvhodnější a nejzranitelnější místo a dle toho pak volí způsob útoku. U malých a jednoduchých domácích wifi sítí se obvykle jedná o jeden wifi router, ve firemním prostředí je ale situace obrácená. Celá firemní síť by tak měla být navržena a vybudována i s ohledem na vyváženost jednotlivých částí.

3 BEZPEČNOSTNÍ HROZBY A ANALÝZA RIZIK

Veškerá informační bezpečnost podniku je zajištěna a zároveň ohrožena lidským faktorem. Lidé či skupiny mohou mít ale rozdílné zájmy, zejména v době, kdy více než kdy dříve platí, že informace = zboží, což může být pro některé jedince z různých důvodů zajímavým lákadlem.

3.1 Bezpečná organizace

Každá komerční i nekomerční organizace pracující s aktivy v oblasti informačních a komunikačních technologií (dále jen ICT) by měla pro zajištění své informační bezpečnosti mít určitou vizi doplněnou zpracovanou a průběžně aktualizovanou analýzou možných rizik s návrhem protiopatření vůči působení hrozeb na chráněná aktiva. V rámci bezpečnostní politiky firmy pak je možné určit bezpečnostní cíle a postupy, jak je zajistit. V rámci bezpečnostní politiky se lze setkat s těmito pojmy:

- Aktivní bezpečnostní politika – zodpovídá na základní bezpečnostní otázky, tedy co chránit, proč chránit a před čím, jak zjistit, že nastavená ochrana opravdu funguje, a co se stane v případě selhání. Bezpečnostní politika definuje soubor pravidel a nařízení, která určují, jak je organizace chráněna jako celek. Tato opatření musí být průběžně analyzována, vyhodnocována, aktualizována a implementována do firemního prostředí.
- Bezpečnostní audit – posuzuje skutečný stav v oblasti bezpečnostní politiky podniku na základě definovaných standardů. Cílem je definice rizik a slabých stránek bezpečnostní politiky a návrh opatření pro splnění stanovených cílů. V oblasti ICT se jedná zejména o audit procesních a technických částí datové infrastruktury.

Přístupy k bezpečnostní politice firmy se obvykle pohybují mezi dvěma přístupy:

- Vše je povoleno – liberální přístup k bezpečnostní politice, který povoluje každému uživateli, co sám chce. Jakékoliv zabezpečení obvykle není aplikováno, důvodem může být neznalost, naivita nebo nedostatek finančních zdrojů k zajištění vyšší úrovně zabezpečení.
- Vše je zakázáno – paranoidní přístup, zajišťující nejvyšší úroveň ochrany, např. omezením přístupu do vnější sítě, používáním přenosných paměťových médií či dalšími parametry. Využívá se v organizacích pracujících s utajovanými informacemi, výzkumnými pracovišti či prostředí s vysokou hrozbou průmyslové špionáže. V rámci

běžného firemního prostředí je toto nastavení spíše omezením pro vykonávání běžné pracovní činnosti.

Přístup k bezpečnostní politice firmy je obvykle ovlivněn znalostmi, zkušenostmi a celkovým nastavením managementu společnosti k řízení rizik.

3.2 Vnitřní hrozby

Bezpečnostní útoky prováděné uvnitř organizace představují významné riziko, dle odhadů je 80% případů úmyslného či neúmyslného porušení ochrany informací způsobeno vlastními pracovníky organizace, lidmi s přístupem do interní sítě. Mezi obvyklé důvody je možné zařadit nedostatečnou odbornost, lidské selhání, nezájem, ale i pomstychtivost nebo ziskuchtivost. Pracovníkům podniku již z podstaty věci nelze zamezit k přístupu ke všem důležitým informacím, neměli by ale mít volný přístup k datům nebo informacím bezprostředně nesouvisejícími s jejich pracovním uplatněním. Důležitý je vhodný výběr interních i externích pracovníků, důraz na vzájemnou komunikaci a průběžné vyhodnocování spokojenosti zaměstnanců. Klíčovou roli s největším vlivem na spokojenost zaměstnanců má vždy jejich přímý nadřízený. [3, 4]

Vhodným nástrojem pro řízení práv pro práci v IS je tzv. matice neslučitelných pravomocí, umožňující pomocí definovaných pravomocí spravovat přístupová oprávnění a účty uživatelů přistupujících do IS a tím definovat nežádoucí kombinace oprávnění pro jednotlivé pracovní pozice zaměstnanců.

Pro komplexnější IS existují vhodné SW nástroje umožňující sledování a vyhodnocování činnosti zaměstnanců, jejich přihlašování do systémů či sledování činností, které mohou způsobit nestandardní nebo mimořádnou událost.

3.3 Vnější hrozby

Jedinec nebo skupina, která nemá přímý přístup do interní sítě a pro uplatnění svých hrozeb, tak musí překonávat nastavená bezpečnostní opatření. V dnešní době je možné provádět tyto útoky prakticky z libovolného místa, jedinou obranou je funkční zabezpečení IS a využití vhodných protiopatření. Vnější útočníky můžeme dle jejich odbornosti rozdělit na amatéry a profesionály. Mezi tyto organizace mohou být zařazeny i vládní organizace či tajné služby kteréhokoliv státu. [12]

3.4 Způsoby útoků

S rozvojem internetu je pro potenciální útočníky mnohem snadnější získat znalosti či nástroje schopné proniknout do cizí počítačové sítě. Hrozby v oblasti digitální bezpečnosti pocházejí z mnoha různých zdrojů, které se mohou objevovat náhle a bez předchozího varování. Typy útoků se v průběhu času mění a známé útoky jsou nahrazeny novými. Mezi nejčastější typy útoků zaznamenané v posledních třech letech patří:

Vydírání – neboli Ransomware, tedy software šířitelný různými způsoby, napadající klienta s účelem zamezení přístupu k jeho datům, obvykle jejich šifrováním nebo uzamčením. Cílem tohoto typu útoku je získat od poškozeného klienta výkupné výměnou za obnovení funkčnosti napadených dat. Velmi známým příkladem Ransomware je WannaCry, který v roce 2017 napadl více než 200 tisíc počítačů a stal se tak historicky nejrozšířenějším počítačovým virem v historii. Dosud neznámý útočník, neoficiálně se spekuluje o severokorejské hackerské skupině Lazarus, využil zranitelnosti protokolu SMB1, standardně používaném pro komunikaci se síťovými zařízeními, a pronikl do počítačů vybavených operačním systémem Windows. Ransomware WannaCry se choval jako červ a využil dvou typů útoků dříve vyvinutých americkou bezpečnostní agenturou NSA (Eternalblue a Doublepulsar). Po průniku do systému došlo k zašifrování dat velmi silným šifrovacím mechanismem AES-128 v kombinaci s RSA-2048 a znemožnění k přístupu k nim, pro jejich dešifrování byla požadována platba částky zhruba 300 USD v kryptoměně Bitcoin, uhrazené během tří dnů – po uplynutí této doby byla vyžadována platba dvojnásobné částky. K hromadnému napadení počítačů došlo v pátek 12. května 2017, třídenní termín tak běžel i během víkendu, kdy mnoho obětí nemělo o napadení ani tušení. Sledování toku bitcoinu směrem k účtu příjemců ale neukázalo o extrémní výdělečnost – během prvních čtyř dnů se mělo jednat o cca 72 000 USD, což je s ohledem na množství infikovaných stanic poměrně nízká částka.

WannaCry nebyl primárně určen k obohacení útočníků, mimo soukromé osoby však napadal i celé sítě, mezi jeho oběti se tak řadí banky, státní a zdravotnická zařízení, telekomunikační či technologické firmy či významní průmysloví hráči na trhu. Odhaduje se, že virus byl rozšířen ve více než 150 zemích a mimo finanční škody měl výrazný dopad i na chod kritické infrastruktury v některých státech, například omezení lékařské péče v zasažených nemocnicích. Celkové škody, které tento útok napáchal, jsou tak odhadovány na více než 8 miliard USD. Použitý útok EternalBlue byl znám již před samotným útokem WannaCry, v březnu

2017 vydala společnost Microsoft bezpečnostní aktualizaci, která měla odstranit právě zranitelnosti protokolu SMB1. I tak byl počet napadených počítačů obrovský a potvrdil, že ne všichni uživatelé přistupují k bezpečnostním aktualizacím zodpovědně. [13, 14]

Dalším známým zástupcem Ransomware útoků je Petya, po průniku do systému šifruje hlavní tabulku souborů a blokuje tak přístup k souborům uloženým na pevnému disku. [13]Dle společnosti Symantec byla většina Ransomware útoků v období do roku 2017 mířena na účty soukromých uživatelů. V roce 2017 nastala rovnováha mezi množstvím útoků na soukromé i firemní účty a od loňského roku směřovalo 81% známých útoků právě na firemní klientelu. Zatímco celkový počet zaznamenaných útoků klesl o 20 %, množství známých útoků na firemní počítače narostlo o 12 %. [13]

Nedostupnost služby – neboli tzv. DDoS attacky (z anglického Distributed Denial of Service), poměrně jednoduchý, ale účinný způsob útoku spočívající v koordinovaném útoku vedeném z několika různých bodů na jednu konkrétní službu za účelem jejího znepřístupnění ostatním uživatelům, nebo jako kamufláž při provádění jiného souběžně probíhajícího útoku, kdy se IT pracovníci věnují vyřešení DDoS útoku a nevšimnou si, či nemají kapacitu řešit další právě běžící aktivity útočníka. Cílem se může stát kterékoliv zařízení připojené k internetu, obecně ale útočníci preferují významnější cíle, před soukromou webovou stránkou neznámého blogera tak spíše cílí na atraktivnější služby, např. poskytovatele internetového připojení, vládní instituce, infrastrukturu, komerční eshopy nebo aktivistické stránky. Útok si může prostřednictvím specifických nástrojů typu Tor objednat prakticky kdokoliv pomocí různých skupinových fór či přímo webových služeb černého trhu, tento způsob komunikace zajišťuje, že se jak zadavatel útoku, tak jeho organizátor nemusí osobně znát a jejich identita je velmi obtížně zjistitelná. Platba za službu probíhá obvykle prostřednictvím kryptoměn, zadavatel pak může dostat report o úspěšnosti provedeného útoku. Náklady, které musí zadavatel za provedený útok zaplatit, se liší dle délky trvání, složitosti útoku či lokality, ve které mají být provedeny. Obecně se pohybují v řádech jednotek až desítek USD na hodinu, což je činí poměrně dostupnými. [15]

Většina DDoS útoků probíhá na síťové nebo aplikační vrstvě. Dle společnosti Cisco vykazuje v současnosti větší procento útoků aplikační vrstva, nejčastěji pomocí ®, HTTPS, DNS, SMTP či VoIP protokolů. Oproti tomu útoky na síťové vrstvě nejčastěji využívají spojení TCP-SYN flood, protokolů UDP, ICMP, Ipv6 a další. Slabinou pro útočníky je skutečnost, že délka těchto útoků je časově omezena, obvykle se pohybuje v řádech několika minut či

hodin. I tak ale umí tento typ útoku napáchat škody s významnými ekonomickými dopady, přičemž možnosti obrany jsou omezené. [13, 16, 17]

Útok na dodavatelské řetězce – neboli supply chain attack. Tento typ útoků je zaměřen zejména na poskytovatele finančních, vývojových, výrobních, obchodních nebo jiných profesionálních služeb s cílem dostat se k jejich datům, či datům dalších navázaných spolupracujících článků, jako jsou další dodavatelé, zákazníci či uživatelé. Obvykle je využíváno nežádoucích služeb nebo produktů třetích stran, které jsou zamaskovány nebo podsunuty za účelem získání určitých dat nebo služeb, například formou vytvořených skriptů, aktualizací či nelegální úpravou původního softwarového kódu užívaného produktu. Dalším způsobem je zneužití nainstalovaných softwarových nástrojů, se kterými uživatel běžně pracuje pomocí skriptů, či tzv. shell kódů. Díky tomu mohou útočníci napadnout daný zdroj a dále provádět další akce. Tento způsob útoku bývá označován jako „Living off the Land“

Aktuálně se dle společnosti Symantec jedná o aktivitu, jejíž rozvoj byl v roce 2018 velmi výrazný – meziroční nárůst činil 78 %, známé jsou zejména útoky na velké telekomunikační společnosti. [13, 17]

Těžba digitálních měn – alias coin mining je způsob získávání virtuálních měn prostřednictvím výkonu počítačů a vhodného SW zápisem těžby do speciální databáze, tzv. blockchainu, jakési účetní knihy, evidující uživatelem provedené transakce virtuální měny. Mezi v současnosti nejznámější a nejrozšířenější kryptoměny patří tzv. Bitcoin, který lze využít pro platby i mimo virtuální svět. Využití počítačů pro těžbu kryptoměn vyžaduje velké nároky na výkon počítače a zdroj elektrické energie. Samotná těžba není nelegální, neměla by ale být prováděna bez vědomí uživatele, což se ale často děje. Nejvíce pokusů o zneužití počítače pro těžbu kryptoměn bylo zaznamenáno v posledních měsících roku 2017, kdy strmě rostl kurz bitcoinu. V září 2017 byl také představen JavaScript Coinhive, který umožňoval návštěvníkům stránek těžit virtuální měnu Monero. Tento script bylo možné umístit na webové stránky, jejichž návštěvníci pak pomocí svých počítačů prováděli těžbu výměnou za určitou provizi z vytěžené částky. Problémem bylo, že návštěvníci nebyli vždy informováni o přítomnosti sctiptu na navštívené stránce, o probíhající těžbě (tzv. cryptojackingu) se tak nemuseli vůbec dozvědět, přestože na zasaženém počítači dojde ke snížení jeho výpočetního výkonu a navýšení spotřeby elektřiny. [13, 17]

Internet věcí – označovaný též jako IoT (z anglického Internet of Things) představuje síť fyzických zařízení vybavených elektronikou, softwarem nebo jinými prvky, připojenou do

sítě a schopnou datové komunikace. Každé připojené zařízení pracuje samostatně, je ale v rámci sítě identifikovatelné. Takto připojená zařízení lze dálkově ovládat či z nich získávat zaznamenaná data nebo ovlivňovat jejich funkcionalitu. V domácím prostředí se jedná např. o chytré televize, ledničky nebo sportovní testery, ve firemním prostředí nachází široké využití v logistice (řízení skladů a zásob), zdravotnictví (sledování zdravotního stavu pacienta), personalistice (docházka zaměstnanců), infrastruktuře a dalších odvětvích.

Dle údajů společnosti Symantec byl počet útoků na zařízení Internetu věcí v roce 2018 stejný jako v roce 2017 (respektive poklesl o 0,2 %). I tak ale představuje jednu z významných současných hrozeb, útoky v 75 % případů mířily na síťové routery a bezpečnostní kamery. Známý DdoS útok zaměřený na Internet věcí, Mirai, byl v roce 2018 stále aktivní, přestože byl objeven již v roce 2016, problémem je celkové zabezpečí zařízení Internetu věcí a zejména nedostatečná, často nulová možnost upgradu použitého firmware na novější verze. [13, 17]

Útoky na cloudová uložiště – využití cloudových služeb představuje model, kdy je požadovaný SW nebo služba dostupná pomocí vzdáleného přístupu v rámci internetu, namísto disku lokálního počítače. Přístup k této službě pak probíhá pomocí internetového prohlížeče nebo jiné specializované aplikace. Některé cloudové služby jsou volně dostupné, jiné pak placené, uživatel platí za užívání požadované služby, nikoliv za samotné vlastnictví SW. Možnou slabinou cloudových uložišť je pak jejich zabezpečení, které uživatel služby nemá šanci ovlivnit, a musí se tak spolehnout na dostatečné zabezpečení ze strany poskytovatele služeb. Slabě zabezpečená služba tak představuje pro soukromého či firemního uživatele hrozbu. Dle společnosti Symantec uniklo v roce 2018 z uložiště S3 (Simply Storage Service), které provozuje společnost Amazon, více než 70 milionů záznamů právě díky nedostatečnému zabezpečení služby. Společnost Amazon je přitom jedním z největších světových hráčů na poli e-comerce. O rok dříve bylo pomocí Ransomware napadeno během jednoho víkendu více než 26 tisíc databází služby Mongo DB, jejichž přístup do databáze byl zablokován, za opětovný přístup útočník nebo skupina útočníků požadovali zaplacení bitcoinové částky odpovídající 650 USD. [13, 17, 18]

Útoky na mobilní zařízení – rozvoj rychlého mobilního internetu a dostupnost WiFi připojení změnila nutnost připojení do vnější sítě ze stolních počítačů, stále více uživatelů nyní přistupuje k internetu z mobilních zařízení, jako jsou mobilní telefony nebo tablety. Mobilní zařízení tak nezůstávají stranou zájmů potencionálních útočníků, ale představují další možnost, jak získat data uživatelů nebo přístup do interních sítích. Dominantními hráči na trhu

operačních systémů pro mobilní zařízení je Google se svým Androidem a Apple s iOS. Zatímco iOS je obecně považován za uzavřenější, a tedy bezpečnější systém, Android je vyvíjen a distribuován jako otevřený (Open Source) systém, který může při dodržení licenčních podmínek využívat kterýkoliv jiný poskytovatel. Výrobci mobilních zařízení s OS Android tak mají obvykle vlastní verze tohoto OS, doplněné o vlastní funkce či úpravy. Velkým problémem tak u Android zařízení zůstává pravidelnost aktualizací, za které je zodpovědný výrobce zařízení. Právě neaktuální firmware, bez nejnovějších zabezpečení, představuje velké riziko pro uživatele – dle společnosti Symantec pouze 20 % uživatelů OS Android používá aktuální nejnovější verzi tohoto OS. Aktualizaci přitom uživatelé často nemohou ovlivnit, její četnost je zcela v rukou výrobců mobilních zařízení. Další hrozby představuje instalace aplikací do těchto zařízení, které mohou obsahovat podvodný mallware, trojské koně, virusy nebo jiné škodlivé kódy. Některé z nich mohou být v daném zařízení již z výroby a uživatel má minimální šanci na jejich odhalení, nejsou součástí oficiálního OS, ale byly přidány v rámci dodavatelského řetězce. Hrozby představují zejména zneužití bankovních informací klientů, skryté zasílání dat uživatelů na zadaná cílová místa či možnost zneužití k těžbě kryptoměn. Nebezpečí představují i reklamní bannery, po jejichž otevření může dojít k průniku do systému. Dostatečné zabezpečení mobilních zařízení tak představuje stejnou nutnost, jako je tomu u stolních stanic. [17]

Všechny tyto popsané způsoby útoků nejsou samozřejmě jedinými aktuálně používanými. Stejně tak je většina současných útoků vedena nikoliv jen jedním popsaným způsobem, ale kombinací několika z nich.

3.5 Možné cíle útoků

Zdatný útočník obvykle nezkouší proniknout do systému bez konkrétního cíle. Ví, co chce získat, a podle toho volí vhodný postup. Mezi nejčastější cíle útočníků lze zařadit:

- Neoprávněný přístup do systému – nejcennější data a informace se nacházejí v podnikovém informačním systému. Útočník může získat přístup k externímu přístupu do tohoto systému, případně být i jeho uživatelem, pracovníkem společnosti, a tím získat požadovaná data. Jedním ze základních prvků zabezpečení proti neoprávněnému přístupu je přidělení pravidel pro ověření identity uživatele, tedy jeho identifikace, autorizace a autentizace. To probíhá formou zadání uživatelského jména (identifikace), hesla (autorizace) a definovaného oprávnění pro práci v rámci IS (autenti-

zace). Externí útočník se může k těmto údajům různým způsobem dostat (např. formou sociálního inženýrství či útoku hrubou silou), interní je má přiděleny zaměstnavatelem.

- Převzetí uživatelského účtu – umožňuje útočníkovi získat přístup k aplikacím, které uživatel běžně využívá (např. informační systém, elektronická pošta, bankovní aplikace, komunikační nástroje a další) a tím získat nejen požadované informace, stejně jako zneužít dané systémy (např. peněžní převody, nevhodná či nevyžádaná komunikace a další). Ochranou může být vícestupňové zabezpečení u důležitých aplikací.
- Změna integrity dat – představuje úmyslné či neúmyslné narušení celistvosti dat, jejich správnosti či úplnosti. Výsledkem pak je, že organizace využívá pro svoji práci nevhodná data a tím i nesprávné informace, což má, zejména v dlouhodobém horizontu, velmi negativní dopady. Riziko úmyslné změny lze snížit důkladným zabezpečením systému a omezením přístupu běžných uživatelů (mohou data pouze prohlížet, nikoliv upravovat), neúmyslné změny lze odhalit sledováním pravidelným sledováním provedených změn jednotlivými uživateli s aktivním oprávněním pro tuto činnost.
- Průmyslová špionáž – cílem této aktivity je získání dat a informací, které jsou následně využity pro konkurenční, obvykle komerční, účely. Jedná se o jeden z velmi častých typů útoků, směřující zejména proti výzkumně nebo výrobně orientovaným společnostem.

V souvislosti s celkovým zabezpečením datové infrastruktury se může útočníkům podařit několik úspěšných výše uvedených cílených útoků, nejen pouze některý z nich. [19]

3.6 Oblasti útoků

Dle celosvětového hodnocení společnosti IBM směřovaly v loňském roce útoky na datovou infrastrukturu a jiné bezpečnostní incidenty ve firemním prostředí nejčastěji na podniky působící v těchto prostředích:

- Finančnictví a pojišťovnictví – s 19 % celkových útoků se jedná dlouhodobě o nejčastější cíl útočníků. Obvykle se útočníci snaží získat přístupové údaje k bankovním účtům či platebním kartám za účelem převodu peněžních toků na jiné účty nebo zneužití k vlastním platbám. I tak patří technické zabezpečení v tomto oboru mezi nejlépe hodnocené a nejvíce progresivní.

- Doprava – s 13 % podílem ze všech zachycených útoků představují dopravní služby, jako je letecká, silniční nebo námořní doprava, druhé místo v žebříčku. Tento sektor patří mezi kritickou infrastrukturu každého státu, motivací pro útok tak kromě zneužití údajů z platebních karet či věrnostních programů dopravních společností patří i útoky na satelitní komunikační systémy, radary, řízení leteckého či námořního provozu a další kritické systémy. Dopady se tak projevují nejen na potenciální cestující a zainteresované podniky, ale i na celkovou ekonomiku daného státu.
- Sektor služeb – 12 % zaznamenaných útoků mířilo do segmentu zastupovaného právními službami a poradenstvím, účetnictvím, audity, či architekturou. Jedná se tedy o lukrativní odvětví, které z pohledu zabezpečení obvykle nedosahuje úrovně předchozích dvou oblastí.
- Prodej výrobků – s 11 % útoků patří čtvrtá pozice prodejním službám, od potravin přes elektroniku, oblečení, nábytek či automobily. Útočníci ve stále větší míře zneužívají online prodejních služeb, hledají informace o zákaznících, dodavatelských řetězcích, bankovních účtech a dalších zneužitelných údajích.
- Výroba – 10 % útoků mířilo do výrobního sektoru, představovaného útoky na společnosti zaměřené na produkci rozlišného zboží nebo materiálů. Ve světovém měřítku tak tento segment dosáhl na páté místo, v rámci EU se ale pohybuje dle IBM ještě o dvě příčky výše. Útoky byly zaměřeny na obchodní tajemství, duševní vlastnictví, patenty, důvěrnou firemní komunikaci, firemní bankovní účty, lze očekávat i útoky na Internet věcí nasazený v průmyslové výrobě.

Na dalších příčkách žebříčku se dle IBM umístily oblasti médií (8 % útoků), státní správy (8 %), zdravotnictví (6 %), vzdělávání (6 %) a energetiky (6 %).

Uvedené oblasti útoků nejsou ve statistikách dále rozváděny do jednotlivých regionů, nelze tedy přesně určit, odpovídají-li celosvětová čísla i skutečné situaci v České republice. Dle oslovených IT odborníků jsou ale reálné předpoklady k tomu, aby se situace v ČR od těchto čísel výrazně nelišila. [20]

3.7 Analýza rizik

Předmětem analýzy rizik je pojmenování konkrétních rizik, posouzení pravděpodobnosti jejich vzniku s hodnocením následných dopadů na konkrétní subjekt. Získaným výstupem jsou materiály pro rozhodování o možných rizicích, obvykle tedy co může nastat, s jakou pravděpodobností se tak skutečně může stát a jaké škody mohou být daným rizikem způsobeny.

Pro zpracování analýzy rizik je možné použít následující typy metody:

- Kvalitativní – tyto metody využívají matematických a statistických metod, výsledné hodnoty jsou tak číselné. Výhodou je vyšší přesnost, obvykle se proto využívají i v rámci finančních analýz. Nevýhodou pak náročnost na kvalitu a množství vstupních dat a náročnost zpracování.
- Kvantitativní – tento způsob analýzy rizik naopak využívá odborných znalostí pro určení možného dopadu rizika a pravděpodobnosti, že riziko nastane. Těmto parametrům jsou přiřazeny číselné nebo slovní hodnoty. Jedná se tak o obvykle méně náročný způsob analýzy, více zaměřený na subjektivní pocity a znalosti hodnotitelů.
- Kombinované – využívají vzájemného propojení obou výše uvedených metod.

Velký význam při zpracování analýzy rizik má též přístup managementu, obvykle se lze setkat s následujícími variantami:

- Základní přístup – analýza rizik jako taková se neprovádí, dodržují se obecně známá doporučení a pracovní postupy.
- Formální přístup – klade důraz na podrobné zpracování analýzy rizik, využívají se pokročilé matematické či statistické metody, analýza rizik se provádí opakovaně.
- Neformální přístup – spíše pragmatický způsob zpracování analýzy rizik, preferuje se využití méně detailních způsobů analýz.
- Kombinovaný přístup – využívá napříč více metod, obvykle ze základní analýzy rizik vybírá na základě dalších metod (např. Paretova pravidla) konkrétní rizika, která jsou dále detailněji zpracovány a vyhodnoceny.

3.8 Metoda KARS

Výběr vhodného přístupu k analýze rizik je ovlivněn několika faktory, zejména cílem, kterého má být v rámci analýzy rizik dosaženo, významem aktiv, jejich hodnotou a účelem, zásadní je také posouzení celkových nákladů na analýzu a ošetření rizik vůči hodnotě samotného aktiva, na které rizika mohou působit. Jednou z možných metod analýzy rizik je metoda KARS (Kvantitativní Analýza Rizik s použitím jejich Souvztažnosti), kterou ve své dizertační práci na téma „Analýza rizik, jeden ze základních nástrojů krizového managementu při řešení nevojenských krizových situací“ v roce 2007 vypracoval Ing. Štefan Pacinda, Ph.D. Tato metoda slouží k určení primárních (takových, kterými je nutné se zabývat v první řadě) a sekundárních rizik (tedy těch, kterými je možné se zabývat až následně, jako druhými

v pořadí) a je založena na vzájemném působení rizik mezi sebou (tzv. souvztažnosti rizik). Metoda je tak vhodná pro analýzu rizik v systémech, ve kterých působí více různých typů rizik. Díky rozdělení na primární a sekundární rizika tak vypracovaná analýza umožňuje určit ta rizika, kterými je nutné se zabývat a dále je třeba rozpracovat či vyhodnotit dalšími známými metodami. [21]

Bezpečnostní politika podniku představuje komplexní oblast, kombinující poznatky, metody a nástroje několika oborů. S měnící se bezpečnostní situací by podniky měly brát, a objektivně většinou často i skutečně berou, v potaz i rostoucí počet hrozeb, se kterými je možné se setkat, či jim dokonce čelit. Pojmenování možných rizik, pravděpodobnosti, že skutečně nastanou, a určení možných protiopatření je základním předpokladem jejich ošetření. Metod a způsobů, jak dosáhnout snížení míry rizika, je mnoho. Každý podnik by se měl analýzou rizik a jejími dalšími fázemi zabývat pravidelně, jednorázové vypracování není dostačující. Rizika, pravděpodobnost vzniku i odhadované dopady se mění v čase. Tento krok znamená výrazný posun v aktivní bezpečnostní politice podniku a dává tak firmě šanci lépe čelit možným hrozbám.

4 PODNIKOVÝ INFORMAČNÍ SYSTÉM

Tento typ SW představuje pro každý střední a větší podnik klíčový nástroj pro jeho provoz, neboť svým zaměřením integruje různé vzájemně spolupracující oblasti nezbytné pro fungování firmy. Správcům a uživatelům tak umožňuje mít veškerá nezbytná data v jednom systému, díky čemuž lze poměrně přehledně sledovat aktivity a dosažené výsledky v jednotlivých částech podniku, od nákupu materiálu přes výrobu, prodej zboží a jeho expedici.

4.1 Historie ERP

Za vznikem ERP (z anglického „Enterprise Resource Planning“, v češtině je používán nepřesný překlad „Podnikový informační systém“ nebo „Systém pro plánování podnikových zdrojů“) systémů stojí potřeba významných globálních výrobců k využití celopodnikových informačních systémů v průběhu šedesátých let 20. století. Tyto systémy se zaměřovaly převážně na plánování zásob a skladů a byly vyvíjeny v tehdy rozšířených programovacích jazycích. Postupem času, v sedmdesátých letech, vyvinula společnost IBM systém pro materiálové plánování výroby, označovaný jako MPR I, který byl o dekádu později představen ve druhé verzi jako MPR II a vyznačoval se integrací výrobní činnosti podniku. Skuteční předchůdci dnes známých ERP systémů, vykonávající a automatizující větší část firemních procesů přichází na scénu na přelomu osmdesátých a devadesátých let. Nejsou již vyvíjeny jen pro použití v konkrétních podnicích, ale nabízeny jako komerční řešení, které je možné implementovat v rámci jiných firem. Nabídka zefektivnění firemních procesů a snížení nákladů společně s klesajícími cenami IT služeb znamenaly jasný signál pro využití ERP systémů, dosud využívanými zejména největšími korporacemi, i v rámci menších, lokálních podniků. [22]

V současnosti patří mezi nejvýznamnější hráče na trhu s nabídkou ERP systémů společnosti SAP, FIS Global, Oracle či Microsoft.

4.2 SAP R/3

Německá společnost SAP SE patří mezi nejznámější výrobce podnikového ERP systému, označovaného dle názvu firmy SAP. Verze R/3 byla uvolněna počátkem devadesátých let, jedná se o aplikaci typu klient – server. Tato architektura označuje model, kdy klient (např. uživatel systému) přistupuje pomocí síťové architektury k jinému počítači (serveru) nabíze-

jícímu určité požadované služby. Výhodou této architektury je centralizace uložiště, umožňující snadnější správu a údržbu, možná i vyšší bezpečnost. Nevýhodou je naopak riziko přetížení sítě. V případě výpadku serveru pak nejsou požadované služby dostupné.

Označení R/3 odkazuje na model aplikace pracující v reálném čase ® a třívrstvou architekturou systému (3). Jedná se o tyto vrstvy:

- Prezentační vrstva – slouží jako uživatelské rozhraní, využívající grafického rozhraní SAP GUI (Graphical User Interface) pro komunikaci mezi uživatelem a samotným systémem SAP. Posílá uživatelské požadavky na server a zobrazuje přijaté odpovědi.
- Aplikační vrstva – komunikuje s oběma dalšími vrstvami a zajišťuje tak běh jednotlivých programů. Obvykle je tvořena jedním nebo více aplikačními servery zajišťujícími provoz nezbytných služeb.
- Databázová vrstva – je určena pro ukládání dat a jejich volání, obsahuje tak veškerá systémová data. Je podporována většina standardně používaných databázových nástrojů jako je Microsoft SQL, Oracle, lze ale použít i vlastní databázový systém.

Zjednodušeně lze říci, že je systém SAP tvořen pomocí programů využívajících a vytvářejících vhodná data, nacházející se v tabulkových databázích. Programy tak mají poměrně rychlý a spolehlivý přístup k požadovaným datům, a mohou tak provádět zadané úkony.

Pro přístup klienta je nutné jeho přihlášení, v systému musí mít vytvořený uživatelský profil s odpovídajícími oprávněními pro přístup k jednotlivým funkcím systému. Přihlášení lze provést pomocí speciálního softwaru (SAP GUI) instalovaného na OS Microsoft Windows, zajišťujícího grafické rozhraní systému. Tento způsob zajišťuje nejvyšší úroveň služeb, SAP GUI ale vyžaduje instalaci na lokálním disku. Stanice s jiným OS než je MS Windows lze přihlásit pomocí zvláštního JAVA GUI, další variantou je připojení pomocí webového prohlížeče.

Systém SAP využívá pro programování jednotlivých transakcí vlastní programovací jazyk označovaný jako ABAP. Znalost tohoto jazyka umožňuje programátorům rozšíření a modifikaci systému dle vlastních požadavků. [23, 24]

4.3 Moduly SAP

SAP R/3 je tvořen několika vzájemně propojenými moduly. Každý modul zastupuje určitou oblast, ve které se podnik může, ale nemusí pohybovat. Je tak na každém podniku, jaké moduly pro svou práci a agendu využívá. Mezi hlavní moduly patří:

- FI – Financial accounting – slouží pro řízení finančních transakcí podniku a jeho účetnictví. Umožňuje evidovat a řídit pohledávky, závazky, úvěry, bankovní účty, platby či majetek podniku.
- CO – Controling – využívá informace ze všech ostatních modulů k řízení a reportingu finančních operací. Sleduje tak interní a externí náklady, výnosy či výkonnost jednotlivých středisek a dále s těmito výstupy pracuje v rámci ucelených reportů a analýz. Díky zpracování nezbytných dat umožňuje vnímat rozdíly mezi plánovanými a skutečně dosaženými hodnotami a tím i efektivní finanční řízení podniku.
- SD – Sales and distribution – je určen ke zpracování odbytových a prodejních transakcí, jako jsou obchodní poptávky, nabídky, objednávky či prodejní zakázky. Umožňuje definovat prodejní parametry, jako jsou ceny výrobků a materiálů, rabatové podmínky pro jednotlivé zákazníky a spravovat navázaná data využitelná pro podporu prodeje.
- PP – Production planning – modul zaměřený na plánování, realizaci a řízení výroby a výrobních procesů, včetně nástrojů pro plánování samotné výroby a reálného odhadu odbytu vyprodukovaného materiálu nebo produktů. Vhodné pro společnosti zaměřené na sériovou výrobu. Podporuje i koncept Kanban, zaměřený na zeštíhlení výroby, a Just In Time model výroby.
- MM – Material management – nezbytný pro řízení skladů a skladových zásob materiálů v podniku. Zastřešuje aktivity, jakými je evidence skladových materiálů, příjem materiálu na sklad, jeho výdej a vystavení nezbytných účetních dokladů. Při vhodném nastavení jej lze využít pro plánování nezbytných skladových zásob a řízení dodavatelských řetězců.
- QM – Quality management – používá se k řízení kvality procesů napříč celou organizací. Tento modul je úzce navázán na ostatní moduly (MM, PP, SD…), díky čemuž umožňuje efektivně a přehledně nastavovat firemní procesy a podpůrné činnosti.
- HR – Human resources – zaměřený na řízení lidského kapitálu ve společnosti. Umožňuje nastavení personálních procesů, řízení náboru a hodnocení pracovníků, vytváření modelů vzdělávacích a rozvojových aktivit či zpracování mezd pracovníků.

Mimo tyto zmíněné moduly existují ještě další moduly, pokrývající další podnikové oblasti. Je na zvážení každého podniku, využívající ERP SAP, které moduly skutečně potřebuje pro svoji práci a které finálně implementuje. Jak je již z principu modulárního systému zřejmé,

jednotlivé moduly nemusí být pořízeny jednorázově při prvotní implementaci SAPu, ale mohou být pořízeny dodatečně až v případě přímé potřeby. Výhodou tak je, že si každý podnik může svůj vlastní ERP systém uzpůsobit na míru dle vlastních požadavků, nevýhodou přílišné customizace pak je náročnost na údržbu systému. [24, 25]

4.4 SAP BASIS

Pro potřeby vzájemné komunikace mezi operačním systémem, jednotlivými databázovými rozhraními, komunikačními protokoly či SAP moduly slouží soubor nástrojů a programů nazvaný SAP BASIS (Business Application Software Integrated Solution), v současnosti je používán název Netweaver. Díky tomu mohou být jednotlivé moduly spuštěny a provozovány v různých, zejména serverových, operačních systémech (Windows server edition, Unix, AS400…), podporována je i široká základna databázových systémů (Oracle, Microsoft SQL server, DB2…). SAP Basis je tak vlastně operačním systémem pro SAP aplikace a ABAP, a jako takový zajišťuje komunikaci s ostatními OS, přístup do databáze, správu paměti, spuštěných procesů a aplikací či práci s daty. [24]

4.5 Technologické požadavky SAP

Základním komponentem pro implementaci SAP ERP je vhodný hardware, skládající se z těchto prvků:

- Servery – obvykle se jedná o lokální servery umístěné v podnikovém datovém centru, existuje ale i možnost využití hostování serveru u externího poskytovatele nebo využití cloudového řešení. Zásadní jsou hardwarové parametry serverů, aby byl zajištěn dostatečný výpočetní výkon. Ten lze objektivně změřit pomocí měřítka výkonu označovaného jako SAPS (SAP Aplication Performance Standard). Jedná se o měření navržené přímo pro srovnání výkonu systému SAP, a to pomocí transakce v odbytovém (SD) modulu. Dle platného standardu tak 100 SAPS jednotek odpovídá množství 2000 zpracovaných prodejních zakázek za hodinu, kdy je každá zakázka tvořena pěti položkami. Pomocí tohoto měření je tak možné porovnat různé konfigurace serverů a posoudit jejich odhadovaný výkon například ve vztahu k pořizovacím nákladům. Mezi nejznámější výrobce serverů patří významní hráči na trhu, jako jsou společnosti DELL, IBM, Hewlett Packard a další.
- Disková uložiště – systémy diskových uložišť lze přirovnat ke skříním určeným k provozu většího počtu pevných disků, i v tomto případě lze pro ukládání dat ale

využit cloudová řešení. Na těchto uložištích se nacházejí databáze a veškeré instalační a spustitelné soubory, včetně souborů s operačním systémem. Zásadními parametry diskových uložišť jsou jejich rychlost a dostupnost. Výkonné řešení představuje uložiště typu SAN (Storage Area Network), umožňující provozovat v jedné skříni řádově až stovky pevných disků, propojených s databázovým systémem systému SAP pomocí specializovaných karet označovaných jako HBA (Host Bus adapter). Zásadním parametrem pro určení výkonu diskového uložiště je počet zvládnutelných vstupně-výstupních operací, které zvládne uložiště zpracovat v kombinací s jeho datovou propustností – objemem dat udávaným v MB/s. Neméně významným parametrem je pak dostupnost dat a provozuschopná doba uložiště. Samozřejmostí je nutnost zajištění dostatečné kapacity uložiště, jelikož v celém systému pravidelně roste počet uložených dat, řádově o desítky GB za měsíc.

- Síťová zařízení – představují síťové prvky, jako jsou routery, switche či firewally.

Výběr vhodných technologických komponent je obvykle velmi náročnou aktivitou, s ohledem na množství různých produktů na trhu je v případě výběru HW pro ERP SAP, v případě, že podnik nemá dostatek vlastních zkušeností, je vhodné oslovit odborné poradce nebo konzultanty. [24]

Podnikový ERP systém představuje pro každou firmu nejdůležitější a také nejcennější zdroj dat. Jeho funkční provoz a samozřejmě i zabezpečení tak musí mít pro zodpovědné pracovníky jednu z nejvyšších priorit. Pořízení ERP systému znamená investici na mnoho dalších let, přičemž je třeba počítat s nutností naddimenzování celé systémové infrastruktury. Dále je nutné zajistit údržbu, uživatelské licence a zabezpečení po celou dobu životního cyklu podnikového informačního systému. Vhodně vybraný a implementovaný ERP pak nabízí podniku výraznou přidanou hodnotu v možnosti efektivnějšího zpracování interních procesů a tím i značnou úsporu časových či finančních nákladů. Samotná implementace je činností natolik náročnou, že je obvykle prováděna externími konzultantskými firmami schopnými nabídnout dostatek zkušeností i doporučení.

5 ZPŮSOBY OCHRANY

S ohledem na množství hrozeb, se kterými se lze dnes setkat, není možné zvolit jednoduchý a univerzální způsob zabezpečení datové infrastruktury. Již z prostého důvodu, že útočníci jsou vždy krok napřed před svými lovci, v tomto případně bezpečnostně-technologickými firmami, je nutné volit kombinaci preventivní ochrany a aktivních bezpečnostních prvků.

5.1 Proaktivní ochrana

- AntiMalware – tento typ software poskytuje ochranu před infikací počítače nežádoucím nebo škodlivým kódem (tzv. malware, z anglického malicious software) jako jsou trojské koně, červi, spyware, či nevhodné doplňky internetových prohlížečů. V některých případech bývá AntiMalware součástí antivirového programu, pro domácí použití jsou nabízeny některé účinné nástroje zdarma. V rámci komerční sféry se obvykle jedná o placený nástroj.
- Antivirové nástroje – je určen pro identifikaci a likvidaci škodlivých počítačových virů, čímž brání vzniku možných škod. Kontroluje operační paměť či jednotlivé soubory na disku a hledá podezřelé kódy, které by mohly odpovídat definovaným virům v databázi. Zároveň sleduje spustitelné soubory a jejich chování při spuštění, v případě podezření (např. při zápisu kódu do jiného souboru) jej může označit jako virus. Některé antiviry mohou zároveň fungovat jako Antimalware, ve firemním prostředí se obvykle jedná o placené nástroje.
- Detekce anomálií a analýza chování sítě – systémy známé také pod anglickým označením „Network Behavior Anomaly Detection“ představují doplňkovou službu zabezpečení počítačové sítě. Toto řešení pomocí určité umělé inteligence a strojového učení sleduje v reálném čase síťový provoz a probíhající komunikaci a hledá a analyzuje podezřelé chování. Umožňuje tak zachytit i hrozby, které se vyhnuly tradičním bezpečnostním prvkům (jako je např. firewall).

Tyto nástroje jsou nasazeny jak na serverech, tak na koncových stanicích. Aplikace na koncových stanicích by z důvodu bezpečnosti neměly mít možnosti vypnutí nebo omezení funkčnosti ze strany uživatele. Na trhu je obvykle několik dostupných produktů v různé kvalitě, rozhodně je vhodné připlatit si za kvalitní a vyzkoušené produkty nabízející požadovanou úroveň kvality i následných služeb (např. technická podpora, aktualizace…). [25, 26]

5.2 Preventivní ochrana

Tento způsob ochrany vyžaduje aktivní zapojení uživatele, který mu ale nemusí být, zejména ve firemním prostředí, vůbec nakloněn. Tato opatření je nutné nejen dodržovat, ale i pracovat na jejich průběžné aktualizaci.

- Aktualizace systému – velmi důležitý prvek, který zajišťuje, že operační systém, antivir, internetový prohlížeč, emailový klient, kancelářský balíček či jiný používaný software je chráněn proti aktuálně známým bezpečnostním hrozbám. Nemusí zcela zabránit potenciálním útočníkům napadení počítače, jejich práci ale to ale může výrazně ztížit.
- Dodržování základních bezpečnostních zásad – předpokládá určitou obezřetnost na straně uživatele, který se snaží předcházet případným hrozbám. Může se jednat o kvalitní hesla, důsledné neotevírání neznámých příloh, nepoužívání maker, mazání nevyžádaných a podezřelých emailů, nepoužívání přenosných datových médií z neověřených zdrojů a další kroky, které mohou výrazně snížit šanci pro úspěšný útok. Problémem bývá i tzv. sociální inženýrství, kdy se útočníkům podaří různými způsoby dostat z uživatele požadované údaje, jako jsou přístupová hesla, PIN kódy platebních karet či jiné citlivé údaje.
- Zálohování – pravidelná záloha důležitých dat umožňuje v případě zašifrování disku nebo jiné ztráty dat jejich obnovení. Důležitá je pravidelná frekvence zálohování, které může být na jedné straně vhodné provádět co nejčastěji, což ale nese ruku v ruce vyšší náklady na dostatečnou kapacitu datové infrastruktury. Pro tyto účely lze využít serverových disků, lokálních externích disků nebo cloudových uložišť. Výhodou serverových disků je jejich snadná a rychlá dostupnost, i u nich ale hrozí napadení a ztráta dat. Použití lokálních externích disků v kombinaci s vhodným SW lze využívat i k automatickému zálohování. Cloudová uložiště se ve firemním prostředí v ČR nesetkávají s příliš velkou náklonností ze strany možných klientů. Firmy nerady sdílí svá produkční data, složitá je i otázka legislativy, zabezpečení dat je pak zcela mimo dosah uživatele. Nevýhodou může být v případě nutnosti přístupu k většímu množství dat (stovky GB až jednotky TB) nízká propustnost dat a tím i pomalý přístup k těmto datům. Otázkou je také nákladová stránka takového způsobu zálohování, coudové uložiště s přijatelným způsobem zabezpečení není levná záležitost. Zálohovaná data mohou být samozřejmě šifrována, vhodné je i jejich umístění do prostor odolávajících živelným nebo jiným pohromám.

- Matice neslučitelných oprávnění – definuje, které pravomoci a oprávnění vyžaduje pracovník pro plnění stanovených úkolů v rámci své pracovní pozice a které by naopak vykonávat neměl, aby nevznikl tzv. kritický konflikt. Pomocí tzv. kritického oprávnění (SOD - Segregation of duties) lze určit jednotlivé činnosti, jejichž vykonávání jednou osobou současně může vést ke zneužití, a pomocí nepřidělení oprávnění lze těmto situacím zabránit. Příkladem může být účetní, která by neměla mít přístup k pořízení faktury a zároveň k její platbě, aby nedošlo k nežádoucímu zpracování a proplácení účetních dokladů.
- Přihlašovací údaje, role a pravomoci uživatele – zajišťují, aby uživatelé měli přístup jen k takovým datům, které vyžadují pro svoji pracovní náplň. Každý uživatel tak má definované své přihlašovací jméno (ID) a heslo, pod kterým je prostřednictvím logu dohledatelná jeho činnost. Pro jednotlivé SAP aplikace lze definovat tzv. role, usnadňující definici přístupových pravomocí pro jednotlivé skupiny uživatelů dle zastávané pracovní pozice (např. účetní, skladník, plánovač atd.). Uživatel pak má oprávnění spustit pouze transakce přidělené této roli, do ostatních je mu zamítnut přístup. Systém rolí usnadňuje správu jednotlivých uživatelských oprávnění oproti manuálnímu nastavení pro každého jednotlivého uživatele. V případě potřeby je samozřejmě možné konkrétnímu uživateli přiřadit potřebná oprávnění nad rámec definovaný jeho rolí.

5.3 Technické prostředky

Představují souhrn prostředků a služeb pro zajištění bezpečnosti digitální infrastruktury. Lze použít tyto nástroje a jejich vzájemné kombinace:

- Zajištění fyzické bezpečnosti – soubor pravidel a prostředků, umožňující ochránit prostory s prvky datové infrastruktury před působením nežádoucích přírodních hrozeb (povodeň, požár…), stejně jako v omezení přístupu nepovolaných osob do těchto vymezených prostor. Obvykle jsou realizovány kombinací vhodných stavebních řešení, mechanických a elektronických zabezpečovacích systémů a kamerových systémů.
- Firewall - představuje kombinaci SW a HW umožňující blokovat příchozí a odchozí pakety a tím dává možnost správci sítě kontrolovat a řídit přístup do vnitřní sítě. Firewall je umístěn mezi spravovanou sítí a vnější sítí (např. internetem), a veškerý

datový provoz tak prochází obousměrně přes toto zařízení, které propustí pouze autorizovanou komunikaci, neautorizovaná se tak do vnitřní sítě nedostane. Jakožto síťové zařízení je nutné dbát na správné navržení a instalaci, v opačném případě nasazení firewallu vzbuzuje pouze falešný pocit bezpečí. Tento stav může být z pohledu datové infrastruktury nebezpečnější než úplná absence firewallu. Firewall lze rozdělit do tří skupin:

Paketový filtr – je provozován na síťové vrstvě a filtruje všechny datové pakety přicházející z vnější sítě do vnitřní sítě nebo odcházející obráceným směrem na základě jejich záhlaví. Paketový filtr pak buď umožňuje jednotlivým datagramům průchod, nebo je na základě správcem určených pravidel z komunikace vyřadí. Obvykle se posuzují zdrojové a cílové IP adresy, typy použitých protokolů, zdrojové a cílové porty a další parametry. Konfigurace firewallu vychází z bezpečnostních zásad a firemní politiky organizace.

Stavový paketový filtr – pracuje na transportní vrstvě a oproti paketovému filtru nesleduje samostatně každý přenesený paket dat, ale sleduje navázané relace protokolů TCP a UDP. V rámci těchto jednotlivých relací posuzuje stavy paketů a propouští jen ty pakety, které spadají mezi povolené relace, ostatní jsou zamítnuty.

Aplikační brána – nachází se na nejvyšší, tedy aplikační vrstvě a na rozdíl od výše uvedených filtrů dokáže pracovat za záhlavím IP/TCP/UDP, propouští nebo zamítá datagramy na základě aplikačních dat, která přes tuto bránu musí projít. Vnitřní sítě mohou mít několik aplikačních bran pro různé protokoly (HTTP, FTP, emailová komunikace a další), z čehož plynou i nevýhody v podobě nutnosti udržovat samostatnou aplikační bránu pro každou aplikaci. Předávání dat přes aplikační bránu také snižuje výkon celé sítě, zejména v případě, kdy více uživatelů používá bránu umístěnou na stejném počítači. [11]

Správně nainstalovaný, nastavený a pravidelně aktualizovaný firewall představuje jeden ze základních bezpečnostních prvků síťové infrastruktury, který ale může být ze strany některých správců sítě podceňován.

5.4 Speciální softwarové nástroje

Pro analýzu a řízení rizik v ERP systému existují i specializované SW nástroje. Přímo v nabídce společnosti SAP je produkt SAP GRC (z anglického Governance, Risk, Compliance),

skládající se z několika modulů zaměřených na analýzu a řízení rizik v nežádoucích či neoprávněných operacích v prostředí ERP. Produkt je tvořen mnoha moduly zaměřenými na jednotlivé oblasti řízení rizik, mezi nejčastěji využívané patří:

- SAP Risk Management – nástroj první linie pro oblasti podnikového řízení rizik umožňuje managementu společnosti analyzovat, hodnotit a ošetřovat případná rizika. Modul obsahuje známé metody analýzy rizik, umožňuje definovat What-If scénáře (co se stane když…) a to v reálném čase. Pomáhá tak včasné identifikaci možných rizik, a dává tak možnost včasného zavedení nástrojů pro snížení míry dopadu rizik.
- SAP Access Control – SW pro řízení přístupů a oprávnění digitálních identit jednotlivých uživatelů do systému SAP. Umožňuje definovat a nastavovat konfliktní matice a neslučitelná oprávnění v rámci podniku a jejich snadné přiřazení jednotlivým uživatelům, která lze řídit a sledovat mnohem efektivněji než pomocí externě vytvořené matice. Systém dokáže v reálném čase sledovat aktivity uživatelů či upozorňovat na konflikty v kritických oprávněních, které zároveň monitoruje a reportuje správci systému. Tyto aktivity probíhají automaticky, nikoliv namátkově, a není tak vyžadováno zapojení personálu. Veškeré kroky jsou auditovány, a slouží tak jako případné podklady pro management společnosti.
- SAP Enterprise Threat Detection – zástupce pro prevenci, detekci a řízení bezpečnostních hrozeb v reálném čase. Aplikuje forenzní nástroje pro práci v prostředí počítačové sítě a umožňuje automatickou detekci možných průniků do systému či jiných nestandardních a nežádoucích aktivit.

Zásadní výhodou SAP GRC je komplexnost celého systému, modulární nasazení umožňuje podniku vybrat si pouze ty modely, které potřebují pro svoji činnost. Zároveň se jedná o oficiální produkt společnosti SAP, čímž je usnadněno jeho nasazení a implementace v rámci podniku a zajištěna dostatečná úroveň poprodejních služeb. Jedinou, nicméně významnou, nevýhodou jsou náklady na pořízení tohoto programu, které se v rámci středně velkého podniku mohou pohybovat v rámci desítek milionů korun. [28, 29, 30, 31]

Nástroje uvedené v této kapitole představují nejčastěji využívané a vyzkoušené způsoby ochrany datové infrastruktury. Ani v této oblasti neexistuje univerzální způsob ochrany dat, je proto nutné zvolit efektivně fungující kombinaci těchto nástrojů v kombinaci s odborně znalým personálem zodpovědným za správu a řízení datové infrastruktury.

6 SHRNUTÍ TEORETICKÉ ČÁSTI

Obsah teoretické části poskytuje seznámení s prostředím datové infrastruktury podniku, jejím významem pro fungování celého podniku a možnými riziky či hrozbami a jejich případnými dopady na činnost podniku. Představuje možná protiopatření, která působení rizik či hrozeb snižují. Z poznatků získaných v této části diplomové práce lze usuzovat, jakým hrozbám může podnik čelit a jaké úsilí, znalosti či schopnosti musí mít potenciální útočník, aby se dostal k požadovaným datům.

Obecně je zřejmé, že kybernetická kriminalita není na ústupu a lze očekávat, že bude nadále posilovat a zaměřovat se více na firemní klientelu, u které lze v případě úspěšného útoku očekávat vyšší zisky. Nelze přesně stanovit pravděpodobnost napadení konkrétního podniku, ani dopady možných škod, i tak je však v zájmu každé firmy, aby chránila svá aktiva a citlivá data. Odhad možných škod nelze přesně vyčíslit i z toho důvodu, že napadené firmy obvykle informace o útocích, jejich provedeních a způsobených škodách nezveřejňují. Ve statistikách světových výrobců IT technologií a poskytovatelů služeb nefiguruje Česká republika jako samostatný stát, proto nelze použít ani tento odhad možných škod.

Data a informace představují pro podnik jeden z hlavních nemovitých majetků a nástrojů know how. Zároveň platí, že v současné době více než kdy dříve představují informace i zboží, pro které může být na trhu poptávka ze strany jiných zákazníků. Ochrana těchto dat tak musí být jednou z hlavních bezpečnostních priorit v rámci bezpečnostní politiky firmy. Hlavním zdrojem citlivých dat je pak podnikový informační systém (označovaný jako ERP), se kterým běžně pracují zaměstnanci firmy a v rámci svých pracovních náplní mají přístup k různým částem tohoto systému. Riziko interních hrozeb je tak řádově vyšší než možná externí rizika způsobená vnějšími útočníky, ti musejí pro přístup do systému překonat podstatně více překážek. Pro ochranu proti interním úrokům tak musí existovat jasná pravidla pro přístup k těmto datům, včetně kontrolních mechanismů pro uživatele s patřičnými oprávněními.

Ochranu dat před externími hrozbami je nutné neustále modernizovat a zdokonalovat, neboť motivovaní útočníci jsou vždy nejméně o krok napřed před svými strážci, není možné se spokojit se stavem, kdy dosud k žádnému vážnějšímu útoku nedošlo, a stávající bezpečnostní opatření jsou tak dostatečná, či dokonce zbytečná. I podniky, které zatím nemají vlastní zkušenosti s útokem na datovou infrastrukturu, musejí počítat s tím, že tato situace může nastat a pravděpodobně i v budoucnosti nastane, v lepším případě zůstane u pokusu o

útok. Univerzální způsob ochrany zároveň neexistuje, vždy se jedná o kombinaci několika různých prvků společně tvořících funkční celek.

Zároveň je třeba brát v potaz vyváženost mezi nastavenou bezpečnostní politikou a možnými hrozbami tak, aby přílišné zabezpečení nemělo negativní vliv na běžný provoz podniku, nebo aby celkové náklady vynaložené na zabezpečení systému nepřevyšovaly možné ztráty na podnikových aktivech.

V rámci praktické části této diplomové práce jsou zařazeny návrhy a vyhodnocení možných opatření pro datovou infrastrukturu konkrétního podniku.

II. PRAKTICKÁ ČÁST

7 PŘEDSTAVENÍ PODNIKU

Praktická část této diplomové práce se zabývá datovou infrastrukturou, jejím stavem a ochranou, použitou v akciové společnosti Agrotec. Tato společnost vznikla krátce po sametové revoluci a sídlí v Hustopečích u Brna, kde patří k jednomu z nejvýznamnějších regionálních zaměstnavatelů. Od svého počátku se zaměřuje na obchodní činnosti spojené s prodejem, servisem a jinými poprodejními službami zemědělské techniky, osobních či nákladních automobilů a také stavebních strojů. Společnost působí prostřednictvím svých dceřiných společností i na slovenském a maďarském trhu a celkově aktuálně zaměstnává více než 1000 zaměstnanců. V rámci ČR patří dlouhodobě mezi největší prodejce pozemní techniky, celkový obrat dosažený v roce 2018 se pohyboval těsně pod 9 miliardami Kč, přičemž od roku 2011 dochází každoročně k mírnému nárůstu dosaženého obratu. Ten je tvořen zhruba ze dvou třetin aktivitami spojenými ze zemědělskou a stavební technikou, zbývající třetinu pak zajišťuje automotive část a další nabízené služby zákazníkům.

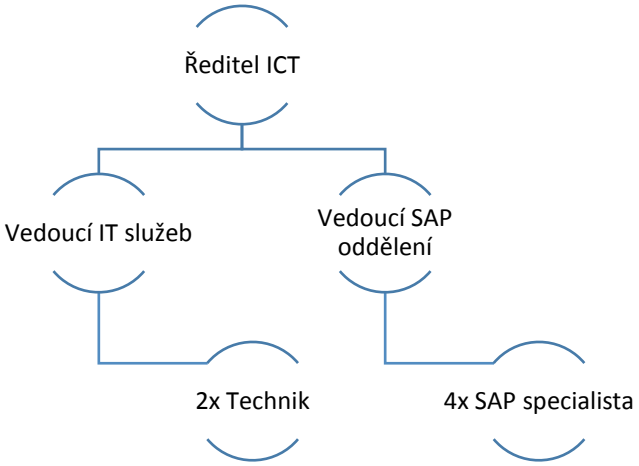
7.1 Organizační a majetková struktura

Společnost byla založena již v roce 1990 panem Karlem Losenickým, svým zaměřením se specializovala na dovoz zemědělských strojů Fiat Agri a prodej a servis osobních aut Fiat a Škoda. V dalších letech přibyly do portfolia nákladní automobily značky Iveco, stavební stroje New Holland a CASE či osobní automobily Kia. V roce 2007 došlo k akvizici a začlenění podniku do portfolia společnosti Agrofert, která se stala jejím novým, 100% vlastníkem. V rámci svých obchodních aktivit a jednotlivých regionů je firma rozdělena do několika divizí, doplněných dceřinými společnostmi. Každá tato divize nebo dceřiná společnost má své vlastní obchodní aktivity, plány a je plně zodpovědná za dosažené výsledky. Mimo jednotlivé divize a dceřiné společnosti stojí správní část podniku, která zajišťuje administrativní a podpůrné aktivity v rámci celé skupiny. Aktuální organizační struktura je zobrazena v příloze této práce. U společnosti Agrotec a.s. lze očekávat další rozšiřování na některém ze zastupovaných trhů, aktuálně použitá data a informace tak odpovídají těm, které jsou v platnosti v době psaní této práce.

V rámci vstupu společnosti do koncernu Agrofert se skupina Agrotec stala dodavatelem pozemní techniky v rámci celého koncernu, společnost tak roste nejen ekonomicky, zvyšuje se ale i celkový objem dodaných strojů klientům.

7.2 Správa informačních a komunikačních technologií

Oddělení Informačních a komunikačních technologií (dále jen ICT) zastřešuje provoz a údržbu veškerých informačních a datových služeb v rámci celé skupiny Agrotec. Pracovníci mají své zázemí na centrále společnosti v Hustopečích, při správě běžných provozních záležitostí na vzdálených pobočkách tak mohou využívat služeb externích lokálních dodavatelů. Organizačně je toto oddělení rozděleno do dvou částí, první se zabývá hardwarem, druhou skupinu tvoří SAP specialisté zodpovědní za chod podnikového ERP. Struktura oddělení je zobrazena na následujícím obrázku:



Obr. 2 - Struktura ICT oddělení [Zdroj: Vlastní]

Oddělení IT služeb zajišťuje kompletní technickou stránku provozu počítačové sítě, instalaci SW na jednotlivé pracovní stanice, dodávku nových počítačů, mobilních telefonů nebo jiného hardwaru či zajištění chodu periferních zařízení. Úlohou SAP oddělení je implementace, správa a vývoj interního ERP systému, kterým aktuálně je SAP R/3. V rámci ERP také přidělují přístupny novým uživatelům a udržují pracovní role, u kterých definují oprávnění pro přístup do jednotlivých transakcí systému.

Pro zajištění komunikace a sdílení obecných dat je vyhrazen firemní Sharepoint, veškeré IT požadavky na provoz HW, instalaci SW, mobilní telefony, interní aplikace nebo ERP jsou zakládány elektronickou formou přes helpdeskové rozhraní na Sharepointu. Tento systém umožňuje evidovat veškeré vzniklé požadavky, sledovat jejich množství a určení, přiřazovat jednotlivé typy požadavků konkrétním zodpovědným osobám či sledovat reakční dobu a způsob vyřešení požadavku. Zavedení systému zvýšilo efektivitu jednotlivých pracovníků,

zároveň v případě zjištění nedostatečné kapacity pracovníků slouží jako podklad pro případné jednání o nových pracovních pozicích v tomto oddělení.

V rámci citlivosti použitých postupů, metod, technologií či bezpečnostních opatření nejsou v rámci této práce uváděny vždy přesné označení zařízení, popisy zabezpečení či jednotlivých bezpečnostních prvků.

Autor této diplomové práce je více než 10 let zaměstnancem společnosti Agrotec nebo některé z jejích dceřiných společností. Informace zpracované v praktické části jsou tak čerpány z konzultací s kolegy, zejména IT odborníky, a z jeho vlastních zkušeností získaných v průběhu zaměstnání ve firmě.

Společnost Agrotec je středně velkou, stále rostoucí firmou, která musí pro svoji efektivní činnost plně využívat dnešních informačních a komunikačních technologií a dále investovat do jejich rozvoje a nasazení. Spolehlivost datové sítě a ochrana proti možným výpadkům či útokům je tak jednou z důležitých podmínek provozu firmy.

8 ANALÝZA RIZIK

Pro provedení analýzy rizik datové infrastruktury v podniku byla vybrána metoda KARS, umožňující objektivně posoudit, jaká rizika jsou v dané oblasti pro společnost nejvyšší a měla by tak mít nejvyšší prioritu při ošetření rizik. Soupis rizik a jejich vzájemné souvztažnosti je uveden v následující tabulce:

Tab. 1 - Analýza rizik pomocí metody KARS [zdroj: Vlastní]

Riziko		1	2	3	4	5	6	7	8	9	10	∑
1	Požár	X	1	0	0	0	0	0	1	0	0	**2**
2	Výpadek proudu	1	X	0	1	0	0	0	1	0	0	**3**
3	Krádež zařízení	0	1	X	1	0	1	0	1	0	1	**5**
4	Interní sabotáž	1	1	1	X	1	1	1	1	0	1	**8**
5	Nadbytečná oprávnění	0	0	1	1	X	1	0	1	0	1	**5**
6	Nedostatečné zálohování	0	0	0	0	0	X	0	0	1	0	**2**
7	Slabá hesla	0	0	0	1	1	0	X	1	1	1	**5**
8	Nedostupnost služby	1	1	1	1	1	0	1	X	0	0	**6**
9	Externí kybernetický útok	0	1	0	0	0	1	0	1	X	1	**4**
10	Internet věcí	0	1	0	0	1	0	1	0	0	X	**3**
∑		**3**	**6**	**3**	**5**	**4**	**4**	**3**	**7**	**2**	**5**	

V uvedené tabulce tak lze vidět 10 rizik a jejich vzájemné vztahy. Pokud může riziko číslo 1, v tomto případě požár, vyvolat některé z dalších uvedených rizik, je u daného rizika v tabulce doplněna hodnota „1“. Naopak, pokud reálná možnost vyvolat další uvedené riziko neexistuje, je do příslušného pole zanesena hodnota „0“. Z tabulky je tak zřejmé, že uvedený požár může vyvolat výpadek proudu, ale nemůže vyvolat krádež zařízení. Stejná logika pak platí pro ostatní uvedená rizika v tabulce.

Výsledné hodnocení vzájemného působení rizik je nakonec jak v jednotlivých řádcích, tak sloupcích sečteno a doplněno celkové hodnocení daného rizika. Pravděpodobnost vzniku jednotlivých rizik lze pak vyjádřit matematicky pomocí tzv. koeficientů aktivity a pasivity.

Koeficient aktivity (KAR) vyjadřuje procentuálně počet rizik, která mohou být vzájemně vyvolána, pokud uvedené riziko nastane, zatímco koeficient pasivity (KPR) vyjadřuje počet všech vytypovaných rizik, která mohou následně vyvolat konkrétní riziko R_i. Výpočty lze provést pomocí těchto rovnic:

$$KAR_i = \frac{\sum R_i}{x-1} * 100$$

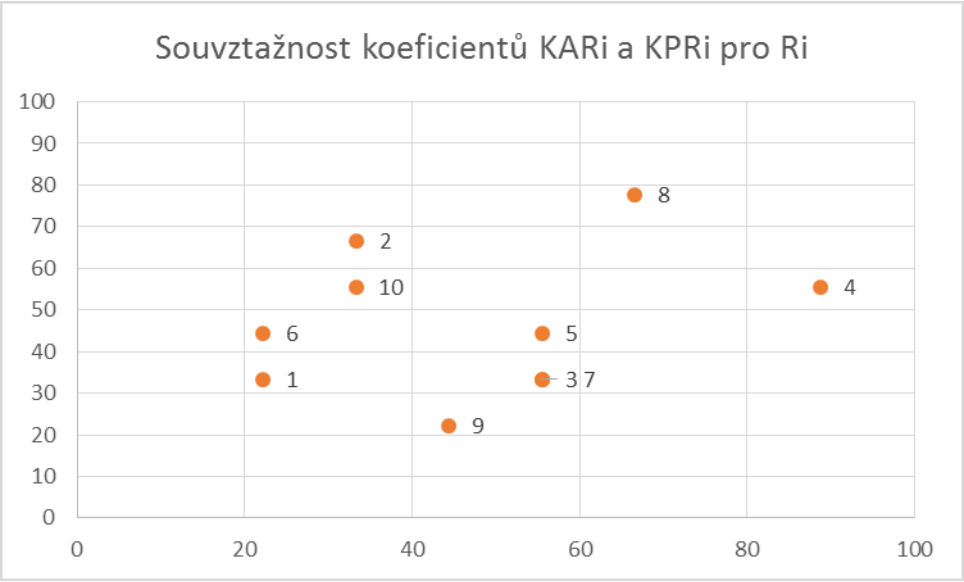
$$KPR_i = \frac{\sum R_j}{x-1} * 100$$

Kde R_i je celkový součet rizik v daném řádku, R_j v daném sloupci a x představuje celkový počet uvedených rizik. Každé z rizik uvedených v tabulce č.1 je charakterizováno dvojicí koeficientů, jejichž hodnoty jsou po dosazení do výše uvedených vzorců následující:

Tab. 2 - Vyhodnocení koef. aktivity a pasivity metodou KARS [Zdroj: Vlastní]

Riziko Ri	1	2	3	4	5	6	7	8	9	10
KARi [%]	22,2	33,3	55,5	88,8	55,5	22,2	55,5	66,6	44,4	33,3
KPRj [%]	33,3	66,6	33,3	55,5	44,4	44,4	33,3	77,7	22,2	55,5

Pro přehlednější zpracování lze data z tabulky zanést do grafu, kde jsou na jednotlivých osách zobrazeny vypočítané hodnoty koeficientů aktivity a pasivity. Body v oblasti grafu pak značí jednotlivá rizika.



Obr. 3 - Graft souvztažnosti koeficientů metodou KARS [zdroj: Vlastní]

Pro přesné určení významu nebezpečnosti daných rizik lze graf rozdělit na čtyři kvadranty:

- I. kvadrant – oblast primárně a sekundárně nebezpečných rizik
- II. kvadrant – oblast sekundárně nebezpečných rizik
- III. kvadrant – oblast primárně nebezpečných rizik
- IV. Kvadrant – oblast relativně bezpečná

Rozdělení jednotlivých kvadrantů probíhá pomocí výpočtů osy 0_1 a 0_2, dle Paretova pravidla je stanovena hodnota, že se 80% rizik má dostat do I. kvadrantu. Pro výpočet hodnot je nutné stanovit si maximální rozsahy hodnot získaných v tabulce vyhodnocení koeficientů v řádcích pro jednotlivé koeficienty. Z hodnot v tabulce vyplývají intervaly:

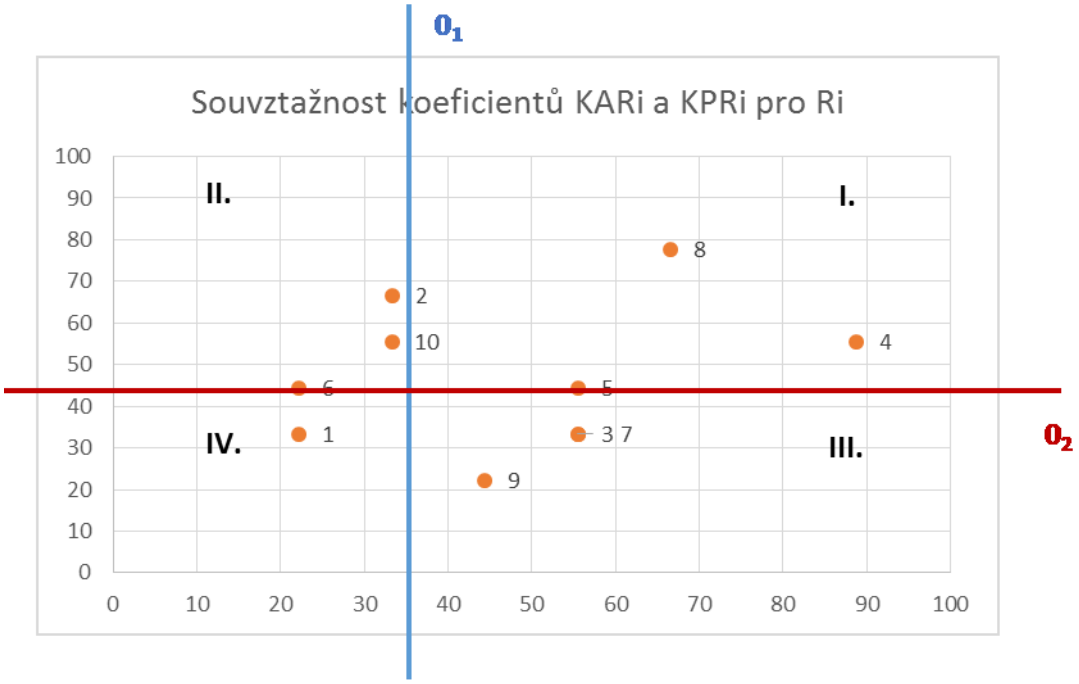
$$KAR_i = [22{,}2; 88{,}8], KRP_j = [33{,}3; 77{,}7]$$

Pro výpočet osy 0_1 a 0_2 tedy platí:

$$0_1 = K_{Amax} - \frac{(K_{Amax} - K_{Amin})}{100} * 80 = 88{,}8 - \frac{88{,}8 - 22{,}2}{100} * 80 = 88{,}8 - 0{,}666 * 80 = 88{,}8 - 53{,}28 = 35{,}52$$

$$0_2 = K_{Pmax} - \frac{(K_{Pmax} - K_{Pmin})}{100} * 80 = 77{,}7 - \frac{77{,}7 - 33{,}3}{100} * 80 = 77{,}7 - 0{,}444 * 80 = 77{,}7 - 35{,}52 = 42{,}17$$

Po zanesení os 0_1 a 0_2 do grafu tak vzniknou kvadranty s jednotlivými riziky:



Obr. 4 - Vyhodnoceního grafu souvztažnosti metody KARS [zdroj: Vlastní]

Na základě uvedeného grafu lze analýzu rizik metodou KARS vyhodnotit následovně:

Tab. 3 - Vyhodnocení rizik dle jejich důležitosti metodou KARS [zdroj: Vlastní]

Kvadrant	Popis rizik
I.	Interní sabotáž (4), Nadbytečná oprávnění (5), Nedostupnost služby (8)
II.	Výpadek proudu (2), Nedostatečné zálohování (6), Internet věcí (10)
III.	Krádež zařízení (3), Slabá hesla (7), Externí kybernetický útok (9)
IV.	Požár (1)

Výhodou použité metody analýzy rizik je přijatelná vypovídající hodnota nevyžadující použití složitých matematických či statistických metod. Ze získaných výsledků lze určit, na která rizika se mají zodpovědní pracovníci dále zaměřit, případně je detailněji analyzovat jinými metodami analýzy rizik.

Z analýzy rizik metodou KARS vyplývá, že společnost by se měla primárně zaměřit na rizika spojená s interní sabotáží, nadbytečnými oprávněními uživatelů a nedostupností služby, případně krádeží zařízení, slabými uživatelskými hesly a externím kybernetickým útokem. Tento závěr kombinuje jak interní rizika, plynoucí ze strany zaměstnanců, tak rizika externí. Oběma typy se detailněji zabývají následující kapitoly, v rámci firmy pak mohou být využity další metody analýzy rizik, zaměřené již na tato konkrétní zjištěná rizika.

9 ERP SYSTÉM

Společnost Agrotec změnila v roce 2007 používaný podnikový systém a implementovala moderní ERP systém SAP R/3, který je využíván dodnes. Tento systém logicky představuje hlavní zdroj firemních dat, v brzké budoucnosti je plánováno jeho nahrazení novější verzí SAP S4 HANA. Jak již bylo zmíněno v rámci teoretické části, ERP systém obsahuje citlivá data společnosti, která je třeba chránit. Tato kapitola se tak zabývá tím, jaká data chránit a jakým způsobem může být jejich ochrany dosaženo.

9.1 Použité moduly

Systém SAP je v rámci podniku tvořen těmito moduly:

- CO – kontrolingový modul představuje hlavní nástroj pro řízení ekonomiky podniku. Zodpovědní ekonomové díky tomu mohou pravidelně sledovat dosažené výsledky jednotlivých středisek, porovnat je se stanoveným plánem a včas analyzovat případné problémy. Přístupem do tohoto modulu tak uživatel získá přehled o finančních kondicích podniku v jednotlivých obdobích a jeho kompletních výsledcích. Má zásadní vliv na řízení celého cash flow společnosti.
- FI – finanční modul umožňuje práci správu celé externí účetní agendy společnosti. Najdeme zde veškeré vystavené účetní doklady, jako jsou faktury, dobropisy či přijaté platby od zákazníků. Dovoluje prohlížet bankovní účty společnosti, zadávat platební příkazy pro platby dodavatelům, evidovat účetní majetek společnosti, sledovat aktuální finanční stav firmy, její pohledávky či stav materiálového hospodářství. Všechny v tomto modulu zaúčtované výnosy a náklady jsou automaticky transferovány do modulu CO, kde jsou přiřazeny konkrétnímu profit centru.
- SD – odbytový modul shromažďuje kompletní informace o uskutečněných prodejích zákazníkům. Jsou v něm evidovány kmenové záznamy odběratelů, jejich dosažené obraty, veškeré prodané či vrácené zboží. Dále jsou v tomto modulu udržovány kompletní prodejní ceníky materiálů a prodejní podmínky jednotlivých zákazníků, včetně nastavených slev na jednotlivé materiály.
- MM – modul pro řízení materiálů umožňuje spravovat veškerou agendu s jednotlivými materiály a sklady v rámci podniku. Najdeme zde tak kompletní data o všech materiálech, které historicky prošly skladem, jejich aktuálním stavem a umístěním,

historickými pohyby, nákupními infozáznamy jednotlivých dodavatelů či přesnými nákupními podmínkami.

- HR – zpracování personální agendy je řešeno pomocí tohoto modulu. Najdeme tak zde veškeré osobní informace o zaměstnancích, personálních požadavcích, výběrových řízeních, absolvovaných školeních či kurzech. Tento modul je také využíván pro evidenci a vyplácení mezd jednotlivých pracovníků.
- CS – tento modul slouží k potřebám jednotlivých servisů automobilové, stavební a zemědělské techniky. Evidují se zde veškeré přijaté stroje, provedené předprodejní, servisní, garanční nebo reklamační zakázky, včetně rozsahu práce a materiálů použitých pro opravu. Podle výrobního čísla daného stroje tak lze v tomto modulu najít veškerou servisní historii daného stroje. Dále je používán pro plánování práce jednotlivých mechaniků.
- PM – modul údržby je využíván zejména oddělením zodpovědným za správu budov v celé společnosti. Umožňuje plánovat, řídit a reportovat jednotlivé investice a opravy do strojů či nemovitostí, a to včetně jejich plánovaných a skutečných nákladů.
- PS – modul pro projektové řízení umožňuje plánování a řízení marketingových kampaní, projektů či vedení jednotlivých týmů. V rámci společnosti není tento modul s ohledem na náročnost použití prakticky využíván.

Jednotlivé moduly jsou vzájemně propojeny, někteří uživatelé vyžadují pro splnění své pracovní náplně přístup do více modulů. Vazby mezi moduly jsou natolik integrované do celého systému, že běžný uživatel ani nemusí vědět, v jakém modulu přesně pracuje. Řeší jen přístup do transakcí, ke kterým má nastavena oprávnění.

9.2 Citlivá data v jednotlivých modulech

V každém modulu se nacházejí data či informace, které lze zařadit do kategorie citlivých dat. Ochrana těchto dat pak spočívá v jejich dostupnosti pouze těm uživatelům, kteří s těmito daty nutně pracují v rámci své pracovní náplně a mají ve svých pracovních smlouvách ošetřeno, jak s takovými daty nakládat. Naopak v případě dostupnosti těchto citlivých dat ostatním zaměstnancům mohou podniku vzniknout ztráty a to jak ekonomického charakteru, tak např. poškození dobrého jména společnosti. Přílišná otevřenost v klasickém korporátním prostředí v podmínkách ČR, na rozdíl od některých oblíbených startupů, není zcela vhodná. V tabulce níže tak lze najít typy dat, které v rámci jednotlivých modulů mohou být zařazeny do kategorie citlivých dat.

Modul	Citlivá data
CO	Finanční výsledky jednotlivých interních středisek, informace o cash flow společnosti
FI	Výpisy z bankovních účtů, evidence příchozích a odchozích plateb, zadávání platebních příkazů, přehled vzájemného salda
HR	Pracovní smlouvy a platební výměry jednotlivých pracovníků, zpracování mezd
SD	Evidence prodejů zákazníkům, evidence zákazníků, vytváření a úprava prodejních ceníků zboží a služeb, vytváření nákupních podmínek zákazníků

Obr. 5 - Citlivá data v některých SAP modulech [zdroj: Vlastní]

Citlivá data jsou uložena i v ostatních modulech, které nejsou v tabulce uvedeny. Jejich kompletní uvedení a zpracování přesahuje možnosti i rozsah této práce, proto jsou vybrány moduly a data s nejvyšší prioritou.

9.3 Typy uživatelů systému SAP

V rámci obchodní firmy je definováno několik typů uživatelů s různým rozsahem předpokládaných činností a tím i nezbytných oprávnění a pravomocí:

- Běžný uživatel – nejčastější typ uživatele, jehož oprávnění pro přístup do systému je definován jeho pracovní náplní, další oprávnění jsou nežádoucí.
- Technický pracovník – tento přístup umožňuje uživateli vykonávání pravidelných jobů či nastavení komunikace mezi jednotlivými systémy. Vyžaduje hlubší znalosti systému, přičemž každému technickému pracovníkovi je přiřazen jeho vlastník, který může sledovat jeho veškeré prováděné činnosti.
- Konzultant – může být interní či externí IT pracovník s vývojářskými nebo systémově administrátorskými znalostmi. Jedná se o nejvyšší typ oprávnění, i toho je ale možné omezit nastavením oprávnění pouze pro přístup k určitým okruhům.

Toto rozdělení umožňuje vytvořit odpovídající skupiny pracovníků, kterým jsou následně definovány jejich systémové role. O zařazení do jednotlivých skupiny rozhoduje zodpovědný IT pracovník.

9.4 Přihlášení do systému a autorizace

Každý uživatel musí mít pro přihlášení do SAPu vytvořen v tomto systému svůj uživatelský profil s definicí oprávnění pro přístup do jednotlivých částí a transakcí systému. Tento systém brání uživatelům v přístupu k datům či systémovým funkcionalitám, které jim nepřísluší. Důvody tohoto omezení jsou zejména:

- Zajištění bezpečnosti a stability systému
- Výkonnost systému
- Integrita a ochrana dat a informací

Identifikace uživatele v prostředí SAPu je zajištěna unikátním přihlašovacím jménem v kombinaci s uživatelským heslem. Samotné heslo zná jen konkrétní uživatel, v případě jeho ztráty či opakovaného chybného zadání je nutné provedení resetu hesla příslušným systémovým administrátorem. Síla hesla je určena minimálním počtem znaků a kombinací malých a velkých písmen, čísel a speciálních znaků. Udržována je i tzv. Tabulka zakázaných hesel, která nese informaci o heslech, která nemůže uživatel použít, obvykle z důvodu jejich snadného uhodnutí (např. jméno firmy). Přihlašovací jméno je navázáno na tzv. kmenový záznam uživatele, který eviduje tyto uživatelské informace:

- Osobní data uživatele – jméno, adresa, kontakt, společnost, jazyk pro komunikaci
- Pevné hodnoty – struktura úvodního menu, přihlašovací jazyk, tiskárna, formát zobrazení číselných hodnot, data a času
- Parametry – hodnoty parametrizovaných rolí
- Role – definice přiřazených rolí s nastavenou dobou platnosti
- Data licencí – informace o přiřazené licenci pro přístup do systému SAP

Každé přihlášení uživatele do systému je ověřováno a logováno, což umožňuje sledovat jeho chování v systému. Vícenásobné přihlášení uživatele do produktivního systému není povoleno a uživatel jej nemůže provést. Vždy je tak logován právě jeden přístup konkrétního uživatele.

Základním parametrem pro určení oprávnění do jednotlivých transakcí je tzv. Role uživatele, která je charakterizována jako:

- Představuje souhrn profilů oprávnění ke schváleným činnostem určeným pro výkon konkrétní pracovní pozice (např. prodejce, přijímací technik, vedoucí servisu, personalista atd.)

- Je udržována systémovými IT administrátory, případně pověřenými SAP konzultanty
- Nové role musí být vždy nejprve otestovány v rámci vývojového systému a teprve následně mohou být přesunuty do testovacího nebo produkčního režimu. Tento systém brání možnosti nefunkčního nasazení v „ostrém“, tedy produkčním systému.
- Přiřazení jednotlivých rolí je definováno podle tzv. Rozdělení pravomocí (SoD – z anglického Segregation of Duties). U koncových uživatelů musí být standardně vždy deaktivovány jakákoliv oprávnění související s přístupem do SAP Basis administrace (označení BC_A) či centrálních funkcí (označení BC_C), neboť se u běžných uživatelů jejich využívání nepředpokládá.

Hlavním významem rolí je usnadnění správy oprávnění jednotlivých uživatelů, je zcela jistě snadnější řešit přístupy několika desítek vytvořených rolí, specifických pro konkrétní pracovní činnosti, než několika set či tisíc možných uživatelů. Jednotlivé role se dále dělí na několik typů:

- Master role – tzv. mateřské role, definují seznamy menu, transakcí a autorizačních objektů. Jejich používání je na rozdíl od ostatních rolí povinné. Tyto role jsou dodané od externích SAP konzultantů, zodpovědných za implementaci ERP.
- Derivované role – neboli odvozené role, vycházejí z výše uvedených master rolí. Na rozdíl od nich jsou ale doplněny o platné organizační oblasti, tedy účetní okruhy, prodejní organizace, závody, nákupní organizace a další podsystémy SAPu. Zjednodušeně se jedná o mateřské role přenesené do konkrétního podnikového prostředí, např. doplněním o oprávnění ke konkrétní prodejní organizační organizaci nebo skladu.
- Kompozitní role - slouží ke zjednodušení přiřazení rolí, a jsou tak v podstatě seznamem jednotlivých rolí.

Každá role má po vytvoření svého vlastníka zodpovědného za její správu. Celkem evidují správci SAPu 111 027 jednotlivých transakcí. Takto velké množství transakcí není možné přiřazovat uživatelům jednotlivě, proto je význam rolí pro nastavení přístupových oprávnění zásadní.

9.5 Matice neslučitelných pravomocí

Hlavním pracovním i bezpečnostním rizikem je přístup pracovníků do systémových transakcí, které nejsou vyžadovány pro jejich běžnou práci. Uživatel s přístupem mimo svoji pracovní agendu může vědomě či nevědomě disponovat znalostí interních informací, které mu nejsou určeny, a v nejhorším případě tyto informace předávat dál, ať už v rámci firmy, či mimo ni. Nejčastější důvody neoprávněného přístupu k informacím jsou:

- Uživateli byly dočasně přiděleny přístupy, které mu ale po skončení stanovené nezbytné doby nebyly odebrány. Příkladem může být rozšíření oprávnění v rámci zastupitelnosti kolegů (např. při dovolených, nemoci atd.).
- Uživateli se zkopíruje šablona oprávnění na základě oprávnění jiného kolegy pracujícího na stejné pozici. Není ale dále zkoumáno, jestli kolega, jehož oprávnění byla použita jako vzor pro přidělení jinému pracovníkovi, nedisponuje unikátními oprávněními, kterými by ostatní disponovat neměli.
- Uživatel přejde z jedné pracovní pozice na jinou, zůstanou mu ale aktivní oprávnění související s původní pozicí.

Každá společnost by proto jako prevenci před interním zneužitím informací měla mít vytvořenou tzv. Matici neslučitelných pravomocí, která v rámci ERP systému jasně definuje:

- Seznam pracovních pozic v rámci společnosti
- Přiřazení pracovních pozic do jednotlivých SAP modulů
- Přiřazení standardních rolí k jednotlivým profesím
- Oprávnění do jednotlivých SAP transakcí pro jednotlivé profese
- Oblast, do které jsou dané transakce zařazeny

Vytvoření a následná údržba této matice pomáhá standardizovat oprávnění jednotlivých pracovníků, které je možné systémově udržovat. V případě, že má některý uživatel nadstandardní oprávnění nad rámec zřízených rolí, je definováno, pro jakou činnost je oprávnění dané a jaký kontrolní mechanismus bude aplikován jako prevence před zneužitím.

V kapitole 7.2. byla definována citlivá data v jednotlivých modulech, přístup k nim probíhá pomocí jednotlivých transakcí, ke kterým musí mít pouze zaměstnanci v odpovídajících pracovních pozicích, ostatním je zamítnut. Společnost Agrotec aktuálně eviduje celkem 99 různých pracovních pozic, s ohledem na takto vysoký počet zde nebudou uváděny všechny pozice, pracovníci na některých pozicích navíc přístupem do ERP nedisponují. SAP disponuje

možností přiřazení různého rozsahu pracovních činností v rámci každé činnosti, uživatel tak může být omezen nejen přístupem ke konkrétní činnosti, ale i tím, že nemá možnost práce v plném rozsahu. Administrátor má možnost přiřazení oprávnění pouze k transakcím, které umožňují tyto činnosti:

- Založení/vytvoření – uživatel má v rámci přístupných transakcí vytvářet doklady, prodejní či nákupní podmínky, provádět účetní operace nebo zadávat nová data do SAPu. Každý takový krok je logován a je dohledatelné vše, co daný uživatel prováděl.
- Editace – uživatel má možnost měnit již vytvořené zakázky, doklady, parametry jednotlivých podmínek či nezaúčtované doklady. Každá provedená změna je opět logována a je tak dohledatelné, kým a kdy byla změna provedena.
- Zobrazení – uživatel má možnost pouze prohlížet již vytvořené systémové záznamy, doklady či podmínky, nemá ale možnost vytvořit cokoliv nového či změnit stávající.

Nastavení rozsahu oprávnění činností k přístupu do jednotlivých transakcí je opět na správci systému. Dále je pro zpracování matice nutné definovat tyto parametry:

- Název role – systémové označení role přidělené jednotlivým uživatelům
- Navázaný modul – modul, v rámci kterého je role aktivní
- Pracovní pozice – definuje možné pracovní pozice s oprávněním k dané transakci
- Organizační úroveň – definují a upřesňují oblasti dat v jednotlivých modulech, v každém modulu se může jednat o jiné označení úrovní, vždy je ale víceúrovňové
- Popis transakce – definuje účel transakce
- Kód transakce – kód transakce pro spuštění v prostředí SAPu

Návrh této matice pro jednotlivé, z pohledu citlivých dat kritické, moduly vypadá následovně:

Modul SD:

Pro práci v SD modulu (zaměřeném na prodej a odbyt) jsou klíčová data související se zákazníky, nastavenými obchodními podmínkami a nezbytnými účetními doklady.

Ve svých pracovních kompetencích mají definován přístup do odbytového modulu tyto pracovní pozice:

Vedoucí skladu, Vedoucí aktivity (VA), Asistent (AS), Analytik (AN), Účetní (Ú), Interní auditor (IA), Referent náhradních dílů (RND), Referent servisu (RS), Referent prodeje (RP),

Účetní specialista (ÚS), Vedoucí servisu (VS), Vedoucí prodeje (VP), Vedoucí prodeje náhradních dílů (VPND) a Technik náhradních dílů (TND).

V rámci přehlednosti při zpracování matice v omezeném prostoru této práce jsou jednotlivé pozice nahrazeny zkratkami uvedenými u každé pozice. V reálné tabulce, která není omezena formátem A4, je pro přehlednost vhodnější pozice jednotlivě vypsat.

Organizační úrovně jsou tvořeny těmito parametry a podmínkami:

- 1. úroveň – definuje účelovost transakce, v tomto případě to jsou kategorie:
    - Kmenová data – Statické záznamy nezbytné pro prodej materiálu, např. data o zákaznících, prodejních cenách, slevových podmínkách atd.
    - Prodej – transakce určené pro práci s prodejními zakázkami, tedy s vazbou na materiály, prodejní ceny a podmínky.
    - Expedice – transakce určené pro zajištění činností spojených s fyzickou dodávkou zboží (např. potvrzení o vyskladnění zboží, vytvoření dodacího listu…).
    - Fakturace – transakce určené pro vytvoření účetních dokladů spojených s prodejem zboží (faktury, dobropisy atd.).
    - Bonus – transakce ke sledování obchodních smluv a podmínek, obchodních plánů jednotlivých dodavatelů a jejich průběžného plnění.
- 2. úroveň – určuje oblasti, ke kterým vede přímá vazba z první úrovně. Jedná se o:
    - Business partner – zákazník společnosti
    - Cenové podmínky – vazba na prodejní ceny a podmínky pro konkrétní zákazníky či materiály.
    - Dodávka – systémové potvrzení o expedici zboží.
    - Faktura – transakce spojené s vystavením nezbytných účetních dokladů
    - Infosystém – transakce spojené s finančními atributy zákazníka.
    - Informační systém – transakce spojené se zobrazením souhrnných dat a reportů spojených s odbytovými a prodejními operacemi.
    - Intrastat – informace o materiálech a jejich celním zařazení
    - Kontrakt – zákaznická smlouva spojená s odbytem materiálu
    - Materiál – vazba na materiál, který je předmětem některé z odbytových operací a prodejních operací.
    - Nabídka – prodejní nabídka konkrétního materiálu zákazníkovi.

  - Skladový příkaz – transakce navázané na skladové operace spojené s fyzickým a účetním výdejem materiálu.
  - Smlouvy – kontrakty spojené s bonusovými podmínkami odběratelů.
- 3. úroveň – definuje cílového příjemce volené podmínky, služby nebo parametru:
  - Cenové podmínky – parametry ovlivňující prodejní cenu materiálu či služby.
  - Dodávka – doklad potvrzující provedení fyzického vyskladnění požadovaného ze skladu či poskytnutí služby.
  - Faktura – závazný účetní doklad za provedenou práci nebo dodané zboží.
  - Fyzická osoba – koncový zákazník společnosti.
  - Intrastat – celní zařazení materiálu dle mezinárodního celního systému sledování obchodu a pohybu zboží mezi jednotlivými zeměmi.
  - Kontaktní osoba – konkrétní osoba zajišťující vzájemnou komunikaci.
  - Kontrakt – typ založené kupní smlouvy.
  - Kusovníky – kategorii definující strukturu a zařazení materiálu.
  - Materiál – zboží, které je předmětem kupní smlouvy se zákazníkem.
  - Nabídka – dokument s nabídkou zboží zákazníkovi včetně ceny a dodacích podmínek. Z akceptované nabídky je možné vytvořit prodejní zakázku a tím realizovat domluvený prodej.
  - Infosystém – systémová či jiná opatření a vazby nastavená a provedená v rámci ERP.
  - Právnická osoba – firma s určitou právní subjektivitou, zákazník společnosti.
  - Příjemce faktury – fakturační adresa společnosti dle zápisu v obchodním rejstříku.
  - Příjemce materiálu – dodací adresa společnosti, pokud je rozdílná od fakturační adresy (např. právnická osoba má více poboček).
  - SD zakázky – parametry mající dopady na vytvoření prodejní zakázky.
  - Sériové číslo – VIN stroje nebo jiný unikátní identifikátor materiálu či služby.
  - Skladový příkaz – dokument určený pro fyzický výdej ze skladu
  - Smlouvy – právní dokument potvrzující určitou dohodu mezi dvěma či více společnostmi včetně přesných podmínek této dohody.
- 4. úroveň – definuje úroveň oprávnění jednotlivých uživatelů, tedy možnost vytváření, editace nebo prohlížení v rámci daných transakcí. U některých položek může být možná pouze některá z těchto aktivit.

Návrh Matice neslučitelných pravomocí pak vypadá následovně:

Název role	1. úroveň	2. úroveň	3. úroveň	4. úroveň	Transakce	Popis transakce	Pracovní pozice
Z_SD_Prodej_zpracování	Prodej	Zakázka	Prodejní zakázka	Založení	VA01	Založení prodejní zakázky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zpracování	Prodej	Zakázka	Prodejní zakázka	Změna	VA02	Změna prodejní zakázky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zpracování	Prodej	Zakázka	Prodejní zakázka	Zobrazení	VA03	Zobrazení prodejní zakázky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zobr	Prodej	Zakázka	Prodejní zakázka	Zobrazení	VA03	Zobrazení prodejní zakázky	AN, AS, IA, RND, RP, RS, TND, Ú, ÚS, VA, VPND, VS, VS
Z_SD_Prodej_zpracování	Prodejj	Nabídka	Cenová nabídka	Založení	VA21	Založení cenové nabídky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zpracování	Prodej	Nabídka	Cenová nabídka	Změna	VA22	Změna cenové zakázky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zpracování	Prodej	Nabídka	Cenová nabídka	Zobrazení	VA23	Zobrazení cenové nabídky	AS, RND, RP, RS, TND, VA, VPND, VP, VS
Z_SD_Prodej_zobr	Prodej	Nabídka	Cenová nabídka	Zobrazení	VA23	Zobrazení cenové nabídky	AN, AS, IA, RND, RP, RS, TND, Ú, ÚS, VA, VPND, VS, VS
Z_SD_Kmen_Data_CenPodm_údržba	Kmenová data	Cenové podmínky	Cenové podmínky	Založení	VK11	Založení cenové podmínky	VA, VS, VP, VPND
Z_SD_Kmen_Data_CenPodm_údržba	Kmenová data	Cenové podmínky	Cenové podmínky	Změna	VK12	Změna cenové podmínky	VA, VS, VP, VPND
Z_SD_Kmen_Data_CenPodm_údržba	Kmenová data	Cenové podmínky	Cenové podmínky	Zobrazení	VK13	Zobrazení cenové podmínky	VA, VS, VP, VPND
Z_SD_Kmen_Data_CenPodm_Zobr	Kmenová data	Cenové podmínky	Cenové podmínky	Zobrazení	VK13	Zobrazení cenové podmínky	AN, AS, IA, RND, RP, RS, TND, Ú, ÚS, VA, VPND, VS, VS

Obr. 6 - Návrh Matice neslučitelných oprávnění v SD modulu [zdroj: Vlastní]

Z výše uvedeného návrhu je zřejmé, že pro uvedené role mají oprávnění pouze zaměstnanci na určitých pozicích. Je vidět, že např. pracovní role „Z_SD_Prodej_zpracování“ umožňuje přiděleným uživatelům zakládat, měnit a prohlížet prodejní zakázky, zatímco uživatelé s oprávněním plynoucím z pracovní role „Z_SD_Prodej_zobr“ mohou tyto zakázky pouze prohlížet, nemohou ale vytvořit novou či změnit již existující zakázku. V rámci jednotlivých rolí zde nejsou uvedena veškerá oprávnění do jednotlivých transakcí, např. zmíněná role „Z_SD_Prodej_zpracování“ má mimo uvedenou možnost založení zakázky přiřazeno dalších více než 20 možných transakcí. Celkově je pak jen pro zmíněný SD modul vytvořeno 13 různých rolí s oprávněním pro vytváření či změnu dat, nabídek, zakázek nebo jiných činností. Dalších 13 rolí je pak definováno pro stejné činnosti, bez možnosti zakládání nebo změny, povoleno je pouze prohlížení založených záznamů. Kompletní matice tohoto modulu tak čítá 174 řádků pro výkonné role a 66 řádků pro role s omezením oprávnění pouze pro zobrazování založených záznamů a dat. Kompletní zpracování této matice pro daný modul

tak přesahuje rozsah této diplomové práce, pro praktické nasazení ve společnosti je ale nezbytné.

Modul FI:

Dalším příkladem Matice neslučitelných oprávnění je modul zaměřený na finance podniku. V rámci tohoto modulu jsou interně definovány tyto pracovní pozice:

Finanční Contoler (FC), Interní auditor (IA), Účetní (Ú), Účetní specialista (ÚS), Vedoucí účtárny (VÚ).

V rámci přehlednosti jsou jednotlivé pozice v tabulce nahrazeny pouze zkratkami, ve finálním interním dokumentu jsou uvedeny v plném znění.

Organizační úrovně jsou v tomto modulu tvořeny těmito parametry a podmínkami:

- 1. úroveň – definuje nejvyšší strukturu účetního dokumentu nebo operace.
  - Banky – určuje operace a transakce spojené s bankovnictvím.
  - Dodavatelé – finanční transakce spojené s dodavateli či dodavatelskými řetězci společnosti.
  - Hlavní kniha – nejvyšší účetní doklad společnosti zahrnující definovaná pole jako je číslo dokladu, číslo série, datum účtování, bilance má dáti/dal či jiné parametry.
  - Odběratelé – finanční transakce spojené se zákazníky společnosti.
- 2. úroveň – určuje typ provedených operací:
  - Aktuální nastavení – uložení parametrů současného nastavení účetních dat a parametrů v systému (účetní období, měnové kurzy, úrokové podmínky atd.).
  - Doklad – určuje typ pořízeného dokladu, jednotlivé typy jsou dále rozlišeny v následující úrovni.
  - Hlášení – povinná hlášení a reporty, dále jsou opět rozlišeny další úrovní.
  - Kmenová data – Systémově nastavená a ošetřená data s vazbou na jednotlivé účetní operace a doklady.
  - Informační systém – systémová či jiná opatření a vazby nastavené a provedené v rámci ERP
  - Kmenová data – upřesňující bankovní údaje (čísla účtů, bank, IBAN, SWIFT atd.)
  - Korektury – opravné operace již vytvořených dokladů a účetních operací.

  - Odeslání – operace spojené s bankovními platbami.
  - Periodické práce – určuje opakující se účetní operace či práce, dále jsou upřesněny v další úrovni.
  - Příjmy – operace spojené s plusovými pohyby na bankovních účtech.
  - Účet – transakce spojené s bankovními účty.
  - Účtování – metodické potvrzení konkrétní účetní operace.
  - Tisk korespondence – transakce spojené s tiskem a zasíláním finančních reportů a výkazů.
- 3. úroveň – dále upřesňuje některé operace ze druhé úrovně:
  - Archivace – systémové operace spojené s archivací účetních dokumentů.
  - Centrální údržba – transakce pro údržbu systémových dat.
  - Doklad hlavní knihy – typ dokladu s vazbou na hlavní knihu.
  - Doklad – účetní doklad, který nemá vazbu na hlavní knihu.
  - Dokumentování – operace spojené s pohyby v rámci hlavní knihy.
  - Firemní banky – transakce spojené se správou firemních bank.
  - Hlášení – typy povinných hlášení a reportů.
  - Hlášení DPH – konkrétní typ povinného hlášení pro finanční úřad.
  - Nástroje – transakce s vazbou na vytvořené reporty a jiné nástroje v rámci SAPu, tzv. Query
  - Kmenová data – záznamy s informacemi o odběratelích či dodavatelích, bankovních záznamech a parametrech.
  - Kontrola/Výpočty – zkontrolování a odsouhlasení vytvořených účetních dokladů, platebních příkazů, legislativně závazných hlášení apod.
  - Korespondence – požadavky na systémovou rozesílku vystavených dokladů, potvrzení o provedených účetních operacích, vzájemných zápočtech a dalších dokumentech.
  - Odeslání platby – operace nutné pro zadání a odeslání bankovní platby.
  - Online platby – transakce spojené se zadáním a příjmem online plateb.
  - Operace hlavní knihy – účetní operace s vazbou na hlavní knihu.
  - Operace přesahující rámec podniku – vazba na externí podniky pro usnadnění zadávání plateb
  - Ostatní – funkce nespadající do žádné z uvedených kategorií.
  - Platební avízo – informace o zaslané platbě či výzvě k fakturaci.

- Potvrzení zůstatku – odsouhlasení vzájemného salda s odběrateli a dodavateli.
- Požadavky na platbu – souhrn zadaných požadavků na provedení odchozích plateb.
- Profit centrum – vazba na konkrétní středisko v rámci organizační struktury SAPu, definuje zejména přiřazení nákladů a výnosů danému středisku (např. servis, prodej či jiná aktivita).
- Předběžné pořízení – způsob zpracování určitých účetních dokladů.
- Příjmy – operace spojené s příjmovými pohyby na bankovních účtech.
- Souhrnná hlášení EU – konkrétní typ povinného hlášení.
- Storno – typ operace, týká se např. storna vytvořeného dokladu.
- Storno dokladu – operace vedoucí ke stornování vystaveného účetního dokladu.
- Tisk korespondence – fyzické vystavení účetních dokladů či reportů či tisk do PDF souboru.
- Účtování – účetní zpracování dokladu nebo účetní operace.
- Výkazy k účetnictví odběratelů – transakce s vazbou na konkrétní výkazy spojené s jednotlivými odběrateli, jako jsou obraty, analýzy splatnosti, seznamy otevřených faktur a vzájemných zápočtů a jiných výkazů.
- Výkazy pro účetnictví dodavatelů – transakce s vazbou na konkrétní výkazy spojené s jednotlivými dodavateli, viz. Výkazy k účetnictví odběratelů.
- Výpis z účtu – informace o stavu konkrétního bankovního účtu.
- Záloha – požadavky ze strany dodavatelů na úhradu zálohových faktur.
- Závěrka – operace s vazbou na výkazy či výstupy nezbytné ke zpracování účetní závěrky podniku.
- Zobrazení změn – prohlížení provedených změn v rámci účetních dokladů či účetních operací, kmenových záznamů odběratelů či dodavatelů nebo jiných systémových infozáznamů.

- 4. úroveň – definuje úroveň oprávnění jednotlivých uživatelů, tedy možnost vytváření, editace nebo prohlížení v rámci daných transakcí.

Matice Neslučitelných pravomocí pak vypadá následovně:

Název role	1. úroveň	2. úroveň	3. úroveň	4. úroveň	Transakce	Popis transakce	Pracovní pozice
Z_FI_HK_DOKLAD_XXX	Hlavní kniha	Doklad	Doklad HK	Založení	FB01	Založení dokladu hlavní knihy	Ú, ÚS, VÚ
Z_FI_HK_DOKLAD_XXX	Hlavní kniha	Doklad	Doklad HK	Změna	FB02	Změna dokladu hlavní knihy	Ú, ÚS, VÚ
Z_FI_HK_DOKLAD_XXX	Hlavní kniha	Doklad	Doklad HK	Zobrazení	FB03	Zobrazení dokladu hlavní knihy	Ú, ÚS, VÚ
Z_FI_HK_Z_DOKLAD_XXX	Hlavní kniha	Doklad	Doklad HK	Zobrazení	FB03	Zobrazení dokladu hlavní knihy	FC, IA, Ú, ÚS, VÚ
Z_FI_BANKY_KMEN_DATA_XXX	Banka	Kmenová data	Firemní banky	Založení	FIBHU	Správa firemních banlk	FC, ÚS, VÚ
Z_FI_BANKY_KMEN_DATA_XXX	Banka	Kmenová data	Firemní banky	Zobrazení	FIBHS	Zobrazení firemních bank	FC, ÚS, VÚ
Z_FI_BANKY_Z_KMEN_DATA_XXX	Banka	Kmenová data	Firemní banky	Zobrazení	FIBHS	Zobrazení firemních bank	FC, Ú, ÚS, VÚ
Z_FI_ODB_UCTOVANI_XXX	Odběratel	Účtování	Platební avízo	Založení	FBE1	Založení platebního avíza odběrateli	Ú, ÚS, VÚ
Z_FI_ODB_UCTOVANI_XXX	Odběratel	Účtování	Platební avízo	Změna	FBE2	Změna platebního avíza odběrateli	Ú, ÚS, VÚ
Z_FI_ODB_UCTOVANI_XXX	Odběratel	Účtování	Platební avízo	Zobrazení	FBE3	Zobrazení platebního avíza odběratele	Ú, ÚS, VÚ
Z_FI_ODB_Z_UCTOVANI_XXX	Odběratel	Účtování	Platební avízo	Zobrazení	FBE3	Zobrazení platebního avíza odběratele	FC, IA, Ú, ÚS, VÚ
Z_FI_DOD_KM_DATA_UDRZBA_XXX	Dodavatel	Kmenová data	Kmenová data	Založení	FK01	Založení účetních dat dodavatele	Ú, ÚS, VÚ
Z_FI_DOD_KM_DATA_UDRZBA_XXX	Dodavatel	menová dat	Kmenová data	Změna	FK02	Změna účetních dat dodavatele	Ú, ÚS, VÚ
Z_FI_DOD_KM_DATA_UDRZBA_XXX	Dodavatel	Kmenová data	Kmenová data	Zobrazení	FK03	Zobrazení účetních dat dodavatele	Ú, ÚS, VÚ
Z_FI_DOD_KM_DATA_Z_UDRZBA_XXX	Dodavatel	menová dat	Kmenová data	Zobrazení	FK03	Zobrazení účetních dat dodavatele	FC, IA, Ú, ÚS, VÚ

Obr. 7 – Návrh Matice neslučitelných pravomocí v FI modulu [zdroj: Vlastní]

Stejně jako v návrhu matice v rámci SD modulu lze na obrázku výše vidět jednotlivé role přiřazené pracovním pozicím s oprávněním pro přístup do FI modulu. Pro role s oprávněním založení či změny záznamu, podmínky nebo dokladu tak mají přístup pouze někteří pracovníci, zatímco prohlížet již vytvořené údaje a doklady mohou i pracovníci na jiných pozicích. V rámci FI modulu je definováno celkem 51 rolí s pravomocemi založení a změny a 31 rolí s oprávněním zobrazení. Správa jednotlivých rolí a transakcí, ke kterým mají mít přístup, je v tomto modulu poměrně rozsáhlá a čítá celkem 1016 tabulkových řádků.

Výhodou implementace této Matice neslučitelných pravomocí je její univerzálnost, nemusí být vázána nejen na ERP, dá se pojmout plošně v rámci firmy. Její vytvoření je kladně hodnoceno i auditory, kteří každoročně sledují činnosti podniku a hodnotí je dle stanovených kritérií. Matice je vytvořena interními pracovníky, není tak nutné oslovovat externí firmy, její aplikace do praktického využití není až tak složitá. Nejobtížnější část, a to zejména z důvodů časové náročnosti, je tak nutnost jejího pečlivého vytvoření a zapojení všech možných

vazeb mezi jednotlivými pozicemi, jejich pracovní náplní a práci v ERP. Matici není možné vytvořit pouze jedním pracovníkem, jedná se tak o práci v širším týmu, který musí mít zástupce za každý SAP modul, znalého práce v tomto modulu, pracovní aktivity jednotlivých pracovníků a dopadů jejich činnosti. Samotné vytvoření matice je tak záležitostí několika měsíců, implementace do praxe je pak již spíše předmětem ověření její funkčnosti a rozhodnutí vedení společnosti o jejím nasazení.

Nevýhodou naopak je fakt, že samotná Matice nepředstavuje žádné systémové řešení, náročná je i následná údržba, která probíhá manuálně. Katalog jednotlivých rolí se mění v čase, obvykle roste, údržba matice probíhá skokově, nikoliv průběžně, může docházet k vytváření vícenásobných pracovních účtů. Nepodléhá tzv. User lifecycle, jakékoliv proběhlé změny řízení pracovníka, dočasný zástup, odchod na mateřskou dovolenou či jiné ne zcela rutinní situace musí být ošetřeny vždy individuálně, IT správce je provádí na základě pokynů jiných kolegů, může dojít ke zpoždění předání informací nebo k informačnímu šumu.

I když tedy Matice neslučitelných pravomocí znamená posun ve směru zabezpečení ERP proti nadměrným oprávněním, pro ošetření těchto rizik je vhodnější implementovat nástroje

9.6 Nástroje Identity managementu

Nástroj SAP GRC není aktuálně ve společnosti vůbec využíván. Jeho nasazení bylo předmětem interních analýz a návrhů, nicméně s ohledem na cenovou nabídku a celkové náklady, které by implementace tohoto systému vyžadovala, není v současné době pořízení tohoto systému reálné. I když nástroj nabízí zřejmě nejlepší možnost ošetření rizik spojených s nadbytečnými oprávněními uživatelů a sledování jejich chování v rámci ERP, celkové pořizovací a provozní náklady v současnosti převyšují odhadovaný přínos. Výše uvedená rizika tedy musí být ošetřena jiným způsobem.

Další variantou mimo společnost SAP může být jiný nástroj tzv. Identity managementu, nástroj Identity Governance and Intelligence (dále jen IGI) od společnosti IBM. Tento SW umožňuje spravovat společně oprávnění rolí pro SAP, stejně jako jiných obvykle používaných aplikacích, což pro podnik znamená výraznou výhodu. Řízení přístupových práv a identit uživatelů tak probíhá na více úrovních, což omezuje možnost negativních dopadů lidských chyb, vnitřního konfliktu pravomocí nebo zneužití nadbytečných oprávnění. Zároveň IGI umožňuje snižovat dopady, které mohou nastat při zneužití přístupu některých uži-

vatelů. Systém pomocí umělé inteligence vyhodnocuje, do jakých systémů (v SAP pak transakcí) se uživatel přihlašuje, a pracuje s nimi, v případě pokusů o přihlášení do jiných systémů či SAP transakcí pak vyhodnocuje možná rizika a v reálném čase upozorňuje zodpovědné osoby na možné nebezpečí. Umožňuje tak odhalit možné případy zneužití identity uživatele mnohem dříve, než je tomu u standardního logování přístupů v jednotlivých systémech, u kterého může odhalení trvat několik měsíců až let, či dokonce zůstat neodhaleno. Pokud by tedy potenciální útočník zjistil a zneužil virtuální identitu a přístupy některého ze zaměstnanců, má podnik díky IGI výrazně vyšší šance na minimalizaci dopadů takového útoku.

Nastavení uživatelských práv pak probíhá systémem „Privacy by default" kdy má uživatel na počátku pouze minimální oprávnění, která mu jsou v případě potřeby rozšířena. Adaptivní řízení přístupu vyhodnocuje opět pomocí umělé inteligence a adaptivního učení z jakých zařízení se uživatel do systému připojuje, v případě přístupu z podezřelého zařízení či internetového prohlížeče není přístup umožněn. Prakticky to znamená, že připojoval-li se dosud uživatel do některé firemní aplikace vždy z interní sítě nebo v rámci ČR a najednou se připojuje např. z Číny, může to znamenat určité ohrožení a kontrolní mechanismus neumožní připojení do systému bez dalšího vícekrokového ověření identity uživatele. Oproti tomu, pokud se uživatel přihlašuje z ověřené interní sítě a ověřeného zařízení, může proběhnout přihlášení bez jakékoliv autorizace.

Bariérou nasazení IGI může opět být jeho cena, která by ale měla být oproti produktům společnosti SAP akceptovatelnější, nabízí také komplexní ochranu před neoprávněným přístupem do systému a omezuje nadbytečná uživatelská oprávnění i mimo ERP.

Jako u všech komplexních systémů je nutné před případnou implementací zvážit připravenost společnosti na tento typ SW. Dle zodpovědného senior consultanta ze společnosti IBM představuje IGI modulární systém, který lze provázat s jednotlivými interními systémy. Společnost musí mít jasno, jaké moduly využít a v jakých interních systémech chce otázku identity managementu řešit a ověřit, případně přizpůsobit tomuto systému své interní nastavení a procesy. Samotný produkt tvoří 20% celého identity managementu, 80% zastřešují interní procesy a organizační nastavení v podniku. Jako u všech dalších informačních systémů platí, že nelze mít vše, podnikové zdroje, a to jak finanční, tak lidské, jsou omezené, a je tak nutné vhodně vybrat nejdůležitější věci s největším dopadem a přínosem. S analýzou těchto dopadů a integrací systému je schopná pomoci dodavatelská firma, která by měla mít s podobnými záležitostmi více zkušeností než samotný podnik.

Před samotnou implementací nástrojů pro řízení identity uživatelů musí podnik ve spolupráci s dodavatelem vyřešit tyto záležitosti:

- Identifikace sponzorů a stakeholderů – je nutné jasně vědět, kdo má celou implementaci zastřešovat, financovat a kdo tvoří zainteresované strany. Právě zapojení zainteresovaných osob (obvykle budoucích uživatelů systému) je velmi důležité, umožňuje pochopit požadavky na systém z různých úhlů a vytvořit si tak komplexní obraz toho, co vlastně podnik požaduje.
- Definice motivace – proč chce vlastně podnik nástroj implementovat a co je cílem tohoto kroku, jaký má být konečný stav po implementaci nástroje.
- Identifikace a popis prostředí – zmapování aktuálně používaných interních systémů, nástrojů, analýza oblasti podnikání.
- Popis současného stavu – definice aktuálního skutečného stavu v podniku.
- Popis očekávání – určení, co přesně od nasazení nového systému podnik očekává, posouzení reálnosti těchto očekávání a dopadů, které bude implementace mít na další pracovní činnost pracovníků.
- Definice rozsahu – vyhodnocení a odhad velikosti celého systému, posouzení náročnosti implementace a to nejen finanční, ale i časové.
- Identifikace a popis technologií – jaké technologie jsou, či v budoucnu budou podnikem využívány v rámci životního cyklu nového systému.
- Identifikace priorit, závislostí a omezení – komplexní posouzení priorit podniku, vazeb mezi jednotlivými systémy, jejich dopadů a případných omezení v dalším provozu, které mohou po implementaci Identity managementu nastat. Omezení mohou být i na straně uživatelů těchto systémů, kteří obvykle další bezpečnostní opatření nevnímají příliš pozitivně.
- Odsouhlasení projektové dokumentace – v rámci životního cyklu produktu vždy nastane situace, kdy bude třeba řešit nová doplnění, upgrade, rozšíření možností a další funkcionality. Bez vhodně vytvořené produktové dokumentace nelze objektivně posoudit veškeré možné dopady a tento krok se může snadno stát noční můrou.

Příprava na samotnou implementaci systému je velmi důležitým krokem už z toho důvodu, že jakékoliv změny nebo úpravy realizované později při samotné realizaci přinášejí s sebou velmi vysoké dodatečné náklady.

Aktuálně používaný ERP systém, SAP R/3, lze hodnotit jako bezpečný systém, u kterého lze pravděpodobnost hrozby externích útoků na databázovou vrstvu hodnotit jako přijatelnou. Oproti tomu je riziko interních hrozeb poměrně vysoké, zaměstnanci mají přístup i k datům a informacím, které bezprostředně nesouvisí se zastávanou pracovní pozicí. Tato skutečnost neznamená, že se některá citlivá data a informace dostanou mimo firemní prostředí, jejich zneužití může mít negativní dopady i v případě, že jimi disponují zaměstnanci, kteří tyto informace mít nesmí.

V rámci společnosti tak budou v průběhu letošního roku v souvislosti s přechodem na novou verzi SAP S4/HANA vypracována nová pravidla pro přístup do jednotlivých částí ERP, která odstraní nedostatky a chyby způsobené původní strukturou stávajícího ERP. Míra zabezpečení vůči vnitřním i vnějším útokům tak bude posílena.

Kladně lze hodnotit, že si podnik stávající nedostatky uvědomuje a vyvíjí aktivity pro jejich odstranění nebo alespoň snížení na hranici akceptovatelného rizika. Do budoucna lze ale s ohledem na velikost podniku i význam interních informačních systémů a jiných IT aplikací doporučit nasazení některého z nástrojů pro řízení uživatelských identit.

10 INTERNÍ BEZPEČNOST

Dle zkušeností IT odborníků představují interní hrozby pro datovou infrastrukturu vyšší riziko nežli hrozby externí, a to zejména ve středních a větších firmách. Hrozby pro data uložená v ERP byla popsány v jedné z předchozích kapitol, obsahem této kapitoly tak jsou možná bezpečnostní opatření mimo ERP.

10.1 Školení a vzdělávání zaměstnanců

Každý nový zaměstnanec společnosti, zařazený do kancelářské pracovní pozice, absolvuje po svém nástupu do společnosti tzv. adaptační proces. Účelem tohoto procesu je získat přehled o činnostech a náplních jednotlivých odděleních společnosti, ve kterých zaměstnanec stráví vždy určitý vyhrazený čas. Jedním z těchto oddělení je i oddělení informačních a komunikačních technologií, kde se nový pracovník seznámí s jednotlivými informačními systémy a aplikacemi, se kterými bude v rámci své náplně pracovat. Získá také základní školení o informační bezpečnosti.

Další vzdělávání v oblasti informační bezpečnosti není dále pro pozice mimo IT oddělení realizováno. V rámci společnosti je aktivně provozována aplikace e-learningu, běžící v prostředí Microsoft SharePoint, využívaná zejména pro technická a obchodní školení a vzdělávání, včetně závěrečných testů doplněných v případě úspěšného splnění certifikátem o absolvování školení. V rámci průběžného vzdělávání zaměstnanců je proto vhodné využít tento způsob vzdělávání i o aktivity v oblasti IT bezpečnosti. Příprava těchto kurzů vyžaduje:

- Vytvoření školících materiálů – vytvoření školících materiálů, ze kterých pak uživatel čerpá požadované informace. Tyto materiály, obvykle ve formátu pdf, jsou dostupné online v rámci vytvořeného školícího kurzu, účastník kurzu si je může vytisknout či otevřít online v příslušeném prohlížeči.
- Vytvoření zkušebních testů – absolvování kurzu je podmíněno splněním závěrečného testu, který musí školitel vytvořit. Rozsah testu a minimální hranice pro jeho úspěšné splnění je plně v pravomoci školitele, stejně jako způsob vyhodnocování. Obvykle se volí způsob několika možností, ze kterých pak účastník kurzu volí jednu nebo více správných odpovědí.
- Certifikát o absolvování kurzu – v případě úspěšného absolvování je účastníkovi kurzu vygenerován certifikát potvrzující úspěšné zakončení kurzu.

Výhodou e-learningových kurzů je zejména možnost poměrně rychlého vytvoření příslušného kurzu, který zaměstnanci mohou absolvovat v rámci své pracovní doby na svých pracovištích, čímž je oproti klasickým školením dosaženo i časové úspory. Vyhodnocení probíhá systémově, školitel se jím nemusí zabývat, získá ale zpětnou vazbu o chybně zodpovězených otázkách, na které se pak může zaměřit v dalších kurzech nebo rozvojových aktivitách. Zaměstnavatel naopak získává jistotu, že zaměstnanci byli seznámeni s problematikou kurzu a v rámci možností jí rozumí. Přijatelné jsou rovněž náklady na přípravu i absolvování školení, které jsou spíše časové než ekonomické.

10.2 Instalace softwaru

Každý pracovník má dle své role definován pracovní software, který je nezbytný pro plnění pracovních povinností. Standardně se jedná zejména o balíček Microsoft Office, zajišťující emailového klienta či tabulkový a textový editor, přístup do ERP systému SAP R3, internetové prohlížeče a jiný univerzální software. Samotný pracovník nemá možnost instalace jiného softwaru, ta musí být provedena pověřeným pracovníkem IT oddělení. Tato ochrana tak zamezuje jednak instalaci nelegálního softwaru, jehož není podnik vlastníkem, ale brání tak i instalaci dalších nežádoucích nástrojů, které by mohly být zneužity k získání citlivých informací pracovníky.

Na jednotlivých stanicích jsou prováděny pravidelné audity, sledující veškerý spustitelný nainstalovaný SW na konkrétním počítači. Audity jsou prováděny vzdáleně, zodpovědný pracovník IT oddělení tak může kdykoliv získat aktuální výstup, stačí mu fyzické připojení konkrétního počítače do interní podnikové sítě.

10.3 Oprávnění pro pohyb v prostorách firmy

V předchozích letech byl v rámci centrály společnosti a vybraných stávajících budov implementován systém elektronického zabezpečení proti neoprávněnému fyzickému přístupu do budov a jednotlivých částí budov. Každý zaměstnanec tak má v rámci interního zabezpečovacího systému přidělen pomocí vstupní karty přístup jen do těch budov, kanceláří nebo jiných prostor, ke kterým má přidělena vhodná oprávnění. Obvykle jsou tato oprávnění omezena na turniket v hlavní budově, budovu, ve které pracující vykonává svoji pracovní činnost a jeho konkrétní kancelář. Návštěvy si mohou na recepci oproti podpisu vypůjčit návštěvnické vstupní karty, opravňující je pouze k průchodu hlavním turniketem. Do specializova-

ných prostor, např. s informačními a komunikačními zařízeními tak mají přístup pouze pracovníci oddělení ICT, případně jejich doprovod. Ve vybraných částech budov je instalován dohledový kamerový systém, umožňující sledovat tyto prostory na dohledovém pracovišti ostrahy.

Tento systém brání volnému přístupu zaměstnanců do prostor, které nesouvisí s jejich pracovní náplní, a slouží tak jako účinné preventivní i bezpečnostní oprávnění proti tomu, aby se zaměstnanci dostali k materiálům, technologiím nebo zařízením, které nesouvisí s přímým výkonem jejich pracovní činnosti.

10.4 Provoz a zajištění fyzické ochrany datové infrastruktury

Nejdůležitější částí firemní datové infrastruktury jsou datová centra. Z bezpečnostních důvodů není v této práci uváděna přesná lokalita těchto datových center, ani jejich přesná struktura. Použitá datová centra splňují certifikát vyspělosti na úrovni Tier III, který zaručuje dostupnost služby ve výši 99,98%, redundantní napájení i chlazení a nezávislé zálohování. Výměny komponent mohou probíhat za provozu centra. Zajištění fyzických prostor odpovídá normě EN 50600. Fyzický přístup do prostor datových center je elektronicky zabezpečen a sledován a je povolen jen úzkému okruhu oprávněných osob.

10.5 Zálohování dat

Zaměstnanci mají možnost pořízení firemních externích hard disků pro zálohování vlastních dat, nicméně se jedná jen o jejich vlastní aktivitu a nelze tak příliš spoléhat na to, že zálohování skutečně probíhá v pravidelných časových intervalech, ani jaká data zaměstnanec vlastně zálohuje. Pro skutečnou ochranu dat a jejich obnovení, např. v případě úspěšného ransomware útoku, který může na poškozeném počítači zašifrovat část dat, je nutné systémové zálohování. Na druhou stranu je faktem, že ztráta dat z koncového počítače může být velmi nepříjemná pro konkrétního uživatele, z pohledu kompletní datové infrastruktury a celkového chodu podniku se ale nejedná o nic zásadního. Primární je tedy záloha dat z ERP nebo jiných firemních aplikací, kde by výpadek těchto dat znamenal zásadní, v určitých případech kritický, problém. Oproti zálohování dat z koncových stanic probíhá zálohování dat z ERP systémově a to ve dvou úrovních:

- Kompletní systémová záloha – zahrnuje kompletní zálohu dat včetně všech nastavení systému, protokolů transakcí a přesné kopie databázového nastavení. Umožňuje kompletní obnovu systému do stavu odpovídajícího datu a času provedené zálohy.

Nevýhodou tohoto typu zálohy je jeho vysoká náročnost na diskovou kapacitu i dlouhá délka zálohování. Z tohoto důvodu je frekvence zálohování určitým kompromisem.

- Datová záloha – obsahuje pouze samotná data, v záloze tak nejsou systémová nastavení a další faktory. Umožňuje obnovení dat, což je dostačující v případě, že nedošlo k systémovým změnám v systému. Výhodou je menší náročnost na rychlost zálohy i požadovanou kapacitu paměťových médií.

Součástí zálohování SAPu je i kontrola konzistence databází, během které je provedena revize databázových indexů a jejich propojení. Tato kontrola umožňuje odhalit případné problémy před tím, než by bylo použito obnovení z chybných záloh. S ohledem na význam ERP dat je zálohování prováděno vícenásobně, aby při ztrátě nebo poškození jedné zálohy byly negativní dopady co nejmenší.

Hlavní hrozbu pro interní bezpečnost podniku představuje sám zaměstnanec, firma bez zaměstnanců ale už z podstaty věci fungovat nemůže, nebo jen ve velmi omezeném rozsahu (obvykle pouze v rámci živnostníků). Interní rizika tak není možné zcela eliminovat, existují pouze způsoby, metody a nástroje, jak tuto skupinu rizik snížit na přijatelnou úroveň. Základním faktorem je pečlivý výběr zaměstnanců a jejich prověření před nástupem, ať už formou referencí u předchozích zaměstnavatelů, možném okruhu známých osob nebo shlédnutím profilů a aktivit na populárních sociálních sítích, mnoho osob je dnes schopných sdílet ve virtuálním prostředí překvapivě mnoho osobních informací. U nových pracovníků je vhodné přiřadit jim po nástupu některého ze zkušenějších kolegů, kteří novému zaměstnanci pomohou se zapracováním, zároveň ale dohlíží na jeho pracovní činnost, sledují jeho aktivitu, návyky a chování, a mohou tak včas zachytit některé varovné signály.

Z technických prostředků lze pro zabezpečení vnitřní bezpečnosti aplikovat omezení veškerých přístupových práv, jak fyzických, tak virtuálních, na nezbytně nutnou úroveň. Omezení přístupu do fyzických prostor znesnadňuje možnost úmyslného poškození, krádeže nebo zneužití firemních nástrojů k vlastním účelům, u IT systémů pak tento faktor výrazně zjednodušuje práci systémovým administrátorům. Vždy se snáze kontroluje malá skupinka uživatelů než možný dav.

V případě skutečného vzniku možných hrozeb je nutné dostat co nejdříve zpět maximální možný objem dat, který v systému byl před působením hrozeb. Obnovení činnosti systému a minimalizaci možných ztrát pomáhá zálohování.

V rámci společnosti Agrotec a.s. jsou již aplikovány způsoby zabezpečení pomocí omezení přístupových fyzických i virtuálních práv, funguje zde i pravidelné zálohování dat. Výběr vhodného personálu a práce se stávajícími zaměstnanci je dalším krokem, který pomůže snížit rizika interních hrozeb v této společnosti.

11 EXTERNÍ BEZPEČNOST

K zajištění bezpečnosti vůči externím hrozbám vůči datové infrastruktuře je využito několika nástrojů. Společně mají chránit „perimetr“ společnosti proti možným hrozbám. Všechny uvedené nástroje tak tvoří ucelený řetězec bezpečnostních opatření. Některé bezpečnostní prvky jsou nasazeny výhradně ve vlastní síti, některé společnost sdílí v rámci síťové architektury s mateřským koncernem Agrofert. Některé bezpečnostní hrozby tak mohou být zachyceny a zastaveny v rámci zabezpečení této vyšší úrovně sítě.

11.1 Sledování chování datové sítě

Pokročilé sledování aktivity v rámci interní sítě probíhá pomocí nástroje Flowmon. Tento komplexní systém umožňuje mít neustálý přehled o datovém toku v rámci celé sítě i jednotlivých poboček a v případě podezřelé aktivity získat obratem bližší informace o tom, kde dochází k nestandartnímu chování či zvýšenému datovému zatížení sítě.

Systém je schopen pomocí aktivních čidel monitorovat datovou zátěž 24 denně a vyhodnocovat nežádoucí provoz či operace, ke kterým může v rámci síťového provozu docházet a odhalit tak i aktivity, které projdou firewallem. Umožňuje tak zachytit jak externí útoky typu DDos, Botnet či dalšími útoky, stejně jako sleduje chování interních pracovních stanic připojených do lokální sítě a jejich síťové aktivity.

Hlavním monitorovacím prostředím je tzv. Dashboard – domovská stránka, umožňující sledovat pomocí upravitelných widgetů základní nástroje síťového provozu, jako jsou aktuálně běžící služby a protokoly, doba odezvy serveru, objem přenášených dat a další parametry. U každé zobrazené aktivity lze nastavit přesný časový horizont v řádu několika posledních hodin až třech měsíců a tím omezit nebo naopak rozšířit objem zobrazených informací. Další nástroje Flowmon ADS (Anomaly Detection Systém) a APM (Application Performance Monitoring) pomáhají pomocí umělé inteligence ochranu proti Malware, DDoS či jiným útokům na aplikační nebo síťové vrstvě. V případě nestandardního chování je spuštěn varovný systém, který správce upozorní na možný útok, a umožní tak reagovat bez zbytečné časové prodlevy.

Příklad systému Flowmon lze prezentovat na příkladu neobvykle vysokého datového toku na jedné z koncových stanic v podnikové síti:

Tento příklad má reálný základ a nastal začátkem března letošního roku. Při automatické systémové analýze datového toku byl zaznamenán neobvykle vysoký obousměrný datový

tok z pracovní stanice jedné ze slovenských dceřiných společností. Report celé události je vzhledem ke své velikosti součástí přílohy této práce, v příloze P2 tak lze vidět, že v rámci celé datové komunikace celé pobočky komunikoval firemní počítač s IP adresou 10.146.37.123 se servery na zdrojových adresách ec2-107-21-218-60.compute-1.amazonaws.com a ec2-107-20-234-220.compute-1.amazonaws.com. Vzájemná komunikace probíhala dle reportu téměř týden a přenesla skoro 60GB dat, což bylo téměř 40% celkového datového toku v daném týdnu. Jak již bylo zmíněno, komunikace byla oboustranná, nejednalo se tedy o samotné stahování dat zaměstnancem, ani o jednostranné posílání dat na server z firemního počítače. Odpovědný IT pracovník tak může při zachycení takto neobvyklého datového toku poměrně v krátké době prověřit, jedná-li se o žádoucí, nebo nežádoucí komunikaci, a přijmout nápravná opatření. Datové toky lze sledovat zpětně pomocí reportů, možností je i nastavení alertu při překročení stanovených parametrů nebo systémového vyhodnocení podezřelého chování, kdy dojde k automatickému upozornění. Ukázka běžného datového toku bez neobvyklého chování nebo událostí je pak součástí přílohy P3. Výhoda celého systému spočívá zejména v jeho fungování v reálném čase, zpětná analýza není vždy s ohledem na časové a lidské kapacity proveditelná, navíc umožňuje reagovat na vzniklé situace až se zpožděním.

Příklad DDoS útoku bohužel nebylo možné použít, reálný útok v době tvorby této diplomové práce nebyl zachycen, a simulovaný útok s odpovídajícím výsledkem se nepovedlo věrohodně v dostatečné síle provést.

11.2 Firewall

Ochranu proti útoku na služby, které se nacházejí mimo interní síť, což je webový server, DNS, VoIP brána, nebo tzv. webové služby, zajišťuje vytvoření tzv. demilitarizované zóny (dále jen DMZ), která přidává do interní LAN sítě další vrstvu, na které jsou tyto služby provozovány. Případný útok přes zmíněné služby vede pouze na zařízení umístěné v této DMZ, ale nikoliv na ostatní uložené mimo vytvořenou zónu. V rámci DMZ je provozován zdvojený firewall, kdy front end kontroluje provoz v rámci DMZ a back end zajišťuje kontrolu oblastí mezi DMZ a vnitřní sítí. Toto řešení je obecně považováno za spolehlivé, přesné výstupy a nastavení nejsou s ohledem na veřejnou dostupnost této práce zveřejněny.

11.3 Antivir a Anti malware

Pro ochranu pracovních stanic je v rámci celé společnosti na jednotlivých počítačích aktuálně provozován antivirový systém Symantec Endpoint Protection, verze 14. Obecně je tento SW považován za jeden z nejlépe hodnocených antivirových programů na trhu. Instalace SW probíhá povinně na každém nově pořízeném počítači, běží na pozadí a koncový uživatel nemá oprávnění jeho funkcionalitu vypnout. Součástí Symantec Endpoint Protection jsou tyto služby:

- Ochrana proti počítačovým virům, spyware, malware a ransomware
- Proaktivní detekce hrozeb
- Whitelist

Symantec Endpoint Protection nabízí pokročilou detekci hrozeb, využívající aktivního skenování operační paměti, systémových registrů či jednotlivých souborů ke sledování a vyhodnocování běžících procesů. Dokáže zachytit podezřelé aktivity, a zabránit tak možným útokům, a to i v případě, že se jedná o útoky, které ještě nejsou obecně známé (tzv. Zero Day útoky), a není tak proti nim uvolněna účinná ochrana, obvykle formou aktualizace.

Z bezpečnostních důvodů není uváděno ošetření na straně serveru, informace IT odborníků nicméně potvrzují skutečnost, že k většině (uvádí se 80%) externích útoků na datovou infrastrukturu podniku dochází průnikem přes koncové stanice, nikoliv přímo na server. Toto tvrzení dokazuje, jak je nutné chránit i běžné počítače připojené do interní sítě, protože jsou obvykle zranitelnější než servery, čehož potenciální útočníci rádi využijí.

11.4 Mobilní zařízení

V rámci společnosti nejsou pro přístup do podnikové datové infrastruktury využívány jen klasické počítače, ale i mobilní zařízení, umožňující přístup k některým službám i mimo běžný počítač. Jedná se zejména o:

- Mobilní telefony – většinově založené na operačním systému Android, v menší míře pak na iOS od společnosti Apple. Prakticky každý dnes využívaný firemní mobilní telefon umožňuje uživateli přístup k firemnímu emailovému účtu prostřednictvím služeb Exchange serveru, pomocí webového prohlížeče pak přístup k běžným internetovým stránkám a aplikacím.
- Tablety – využívají prakticky pouze operační systém iOS a jsou jimi vybaveni jen někteří pracovníci společnosti.

V rámci těchto mobilních zařízení není možné přímo přistupovat do ERP systému či jiných aplikací. Instalace aplikací na tato zařízení není omezena uživatelskými právy, jako je tomu u instalace SW do běžných pracovních stanic. U každého mobilního přístroje je vyžadována ochrana proti nežádoucímu přístupu pomocí zámku obrazovky prostřednictvím číselného kódu, otisku prstu uživatele či zvoleného gesta. S ohledem na to, že mobilní zařízení neumožňují přímý přístup do firemních aplikací, není další způsob zabezpečení vyžadován. Podcenění zabezpečení tak je rizikem spíše pro ty uživatele firemních telefonů a tabletů, kteří na uvedených zařízeních využívají i aplikace pro soukromé účely, příkladem může být mobilní bankovnictví. Právě uživatelé soukromých mobilních zařízení v rámci firemní sítě mohou představovat rizika, protože provozují na jednom zařízení soukromé i firemní aplikace a data. Možností, jak snížit rizika, je zavedení Mobile Device Managementu (dále jen MDM). Tento způsob umožňuje stanovit pravidla bezpečnostní politiky a nastavit parametry pro její fungování. Služba může být řešena vlastním softwarem, či externě, obvykle ji za poplatek nabízejí i příslušní mobilní operátoři.

V případě zavedení nástrojů pro řízení uživatelských identit může firemní mobilní telefon nebo jiné mobilní zařízení sloužit jako prvek vícestupňové autorizace pro přihlášení do interních aplikací či systémů. Podobně dnes funguje internetové bankovnictví, kdy nelze uživatele přihlásit jen po zadání přihlašovacích údajů.

11.5 Internet věcí

Internet věcí představuje moderní trend zejména v oblasti automatizace výroby, skladového hospodářství a dalších činností, ve kterých chytré stroje, zařízení a technologie zefektivňují či přímo nahrazují lidskou práci. Tyto technologie ve společnosti Agrotec v rámci jejího provozu aktuálně implementovány nejsou.

V rámci firmy jsou provozovány IP kamery, v případě zneužití by tak potenciální útočník mohl být schopen získat na základě těchto dat přehled o tom, co se děje ve sledovaných prostorách.

S využitím internetu věcí se lze setkat v produktech, které společnost na trhu nabízí v rámci výbavy osobních či nákladních aut i zemědělských a stavebních strojů. Moderní technologie tak umožňují přesně sledovat polohu stroje, jeho spotřebu, analyzovat v reálném čase data o

zařízení, hlásit případné poruchy či další funkce. Tyto technologie jsou přímo vyvíjeny výrobci strojů či jejich subdodavateli, společnost Agrotec tak nemá možnost jakkoliv ovlivnit jejich nastavení či zabezpečení, které je plně v odpovědnosti daného výrobce.

11.6 Cloud

Cloudová uložiště ani aplikace nejsou ve společnosti Agrotec provozována, ani se s tímto způsobem provozování informačních a komunikačních služeb či zálohování dat v brzké budoucnosti nepočítá.

Posouzení externích hrozeb nelze zcela obsáhnout v rozsahu této práce, s ohledem na to, že se jedná o bezpečnostní otázky, navíc není možné zveřejnit všechna aplikovaná bezpečnostní opatření. Adekvátní a komplexní odpověď na otázku skutečného zajištění bezpečnosti by přinesl pouze bezpečnostní audit. V rámci celé společnosti platí striktní dodržování tzv. Best Practices, tedy doporučení vývojářů používaného SW, v tomto případě zejména společností SAP a Microsoft, jako je šifrování MD5, práce s bezpečnostními certifikáty a další opatření dle vydaných tabulek a pokynů. Dodržování vydaných Best Practices taktéž výrazně přispívá ke snížení možných rizik.

Ze získaných poznatků ale lze usuzovat, že společnost Agrotec klade zajištění bezpečnosti své datové infrastruktury přiměřený význam a investuje do jejího zajištění, které je aktuálně na odpovídající úrovni. Pro další posílení je nutné pečlivě stanovit očekávané přínosy a možné dopady, celkové náklady i vliv na stávající datovou infrastrukturu.

Zcela jistě mohou nastat situace, kdy dojde k prolomení perimetru z vnějšího prostředí, proti těmto hrozbám není imunní prakticky žádná společnost. Aktuální zabezpečení by ale mělo minimálně snížit dopady současně známých hrozeb.

12 SHRNUTÍ PRAKTICKÉ ČÁSTI

Praktická část představuje společnost Agrotec, firemní datovou infrastrukturu a nástroje, které podnik používá pro její ochranu před vnitřními či vnějšími hrozbami k ochraně svých aktiv.

Jak již bylo uvedeno v předchozích kapitolách, citlivá data jsou obsažena zejména ve firemním ERP systému, kterým je aktuálně SAP R3. Tento systém je v rámci své architektury uznáván jako dobře chráněný systém před možnými vnějšími útoky, v rámci diskuzí s externími nezávislými SAP konzultanty či interními SAP specialisty nebyl potvrzen případ, kdy by došlo k neoprávněnému přístupu do databázové vrstvy tohoto systému z vnějšího prostředí. Tento fakt je sám o sobě povzbuzující, zcela jistě ale případného odhodlaného zkušeného útočníka neodradí, jen mu ukáže, že jistější variantou může být jiný typ útoku. Největší úspěšnost pro jeho provedení tak představuje interní útok pomocí některého ze zaměstnanců firmy, který dobrovolně, či nedobrovolně získá požadovaná data nebo zajistí přístup k nim. Společnost Agrotec nemá v současné době aplikovanou tzv. Matici neslučitelných pravomocí nebo Matici kritických oprávnění, která by definovala, k jakým částem ERP má daný uživatel přístup. I když probíhá přidělování oprávnění, není zcela systémově ošetřeno, a může tak dojít k neoprávněnému přístupu.

Společnost Agrotec přechází ve druhém pololetí letošního roku na novou verzi ERP, kterým je SAP S4 HANA. Tento krok dává možnost restartovat stávající přístup k uživatelským oprávněním a přístupům do jednotlivých transakcí a nastavit jej nově tak, aby byl efektivnější a účinnější. Příkladem toho, jak může být Matice neslučitelných pravomocí zpracována, může být i tato práce. Z pohledu bezpečnostní politiky firmy by nejvyšší úroveň ochrany před neoprávněnými přístupem k citlivým datům zajistila implementace některých modulů systému SAP GRC, s ohledem na celkové pořizovací a provozní náklady ale tento krok v nejbližší době realizován nebude. Za zvážení stojí posouzení možnosti implementace konkurenčního nástroje pro řízení Identity managementu, možnosti, které tento nástroj přináší, výrazně převyšuje jakoukoliv Matici neslučitelných pravomocí už jen proto, že umožňuje centrálně a systémově spravovat přístupy do více systémů, nejen ERP, a zároveň v reálném čase vyhodnocuje chování uživatele, čímž významně zvyšuje úroveň firemní bezpečnostní politiky.

Zabezpečení proti externím útokům je aktuálně na dostatečné úrovni, což neznamená, že nemůže dojít ke změně situace. Kombinace použitého firewallu, pokročilého sledování síťového provozu i antivirového programu s antimalware a antiransomware se ukazuje jako dostatečná bariéra proti současným útokům. Zodpovědní pracovníci ani vedení společnosti by se touto skutečností neměli nechat zcela uspokojit, protože, jak již bylo zmíněno, motivovaní útočníci jsou vždy o krok napřed a mohou využít i dosud neobjevených slabin bezpečnostního systému.

Pro komplexnější posouzení stávajícího stavu IT bezpečnosti by bylo vhodné absolvování komplexního bezpečnostního auditu zajištěného externí firmou, který by obsáhl i rizika, hrozby a možná protiopatření, která nejsou součástí této diplomové práce.

ZÁVĚR

Pokrok, který během uplynulé dekády nastal v oblasti digitalizace, zcela mění jak běžné lidské životy, tak i firemní prostředí. Je obtížné vyhnout se mu a ještě obtížnější jít zcela proti proudu, což právě ve firemním prostředí, hledajícím rovnováhu mezi požadavky zákazníka a vlastním fungováním, platí o to více. Tlak na výkon, efektivitu i co nejnižší provozní náklady nutí management společností přemýšlet co dělat jinak, lépe a hlavně jakým způsobem.

Datová infrastruktura podniku dnes vzdáleně připomíná nervovou soustavu, zodpovídá za přesný a rychlý přenos informací z jednoho místa na druhé. Představuje tak vysoce funkční celek, jehož složitost a náročnost není lehké si představit, natož ji detailně rozumět. Pro každý podnik dnes ale představuje jeden ze základních pilířů, bez kterého nedokáže dlouhodobě vůbec fungovat, krátkodobě pak jen s výraznými omezeními a z toho plynoucími ztrátami. Je tak zřejmé, že zájmem každé firmy je, aby byla právě tato datová infrastruktura co nejlépe chráněna před možnými hrozbami a podvědomě tak fungovala právě jako zmíněná nervová soustava.

Teoretická část této práce slouží jako určitá rešerše základních pojmů a problematiky datových přenosů, představuje aktuální bezpečnostní hrozby a možnosti ochrany proti jejich působení, případně alespoň snížení dopadů těchto hrozeb. Poskytuje informace o možných způsobech zajištění bezpečnosti podniku a posuzuje, co je nutné k dosažení přijatelného stavu bezpečnosti zajistit.

Praktická část se zabývá posouzením ochrany datové infrastruktury v konkrétním podniku, společnosti Agrotec. Analyzuje možná rizika a jejich možné dopady na chod podniku, hledá způsoby a řešení, jak tato rizika ošetřit, nebo snížit na přijatelnou úroveň. Provedení těchto kroků ukazuje, že hlavním cílem společnosti by mělo být zaměření na posílení interní bezpečnosti, zejména na hrozby související se zneužitím virtuálních identit pracovníků a jejich nadbytečným oprávněním v práci s interními IT aplikacemi a systémy, především ERP. Nástroje, které mohou být pro zvýšení míry bezpečnosti v tomto segmentu využity, existují, nicméně s ohledem na komplexnost problematiky není jejich okamžitá implementace možná ani technicky, ani časově. Firma by tak měla v určitém časovém horizontu zvážit možnost nasazení některého ze systémů tzv. Identity managementu a zvážit poměr mezi náklady, provozem a přínosy, co tento systém pro podnik znamená. I když nelze přesně vyčíslit ztráty, které mohou společnosti vzniknout při uskutečnění některého interního útoku, dopady jsou

vždy nejen přímé, ale zejména nepřímé, poškozující dobré jméno společnosti u svých zákazníků či dodavatelů. Přesně to jméno společnosti, které se obvykle velmi dlouho a obtížně buduje.

Samotné hrozby nepřicházejí jen zevnitř samotného podniku, ale lze je najít i ve vnějším prostředí. Z této stránky se v současnosti společnost jeví jako poměrně dobře zabezpečena, což ovšem nemusí znamenat, že tomu tak bude i nadále. Komplexní možnosti posouzení externích útoků navíc přecházejí možnosti této diplomové práce a skutečné ověření v praxi tak vyžaduje opakované provádění bezpečnostních auditů včetně penetračních testů, objektivně posuzující míru zabezpečení na reálnou úroveň.

I když je společnost Agrotec čistě obchodní společností, a nemá tak vlastní produkt či vlastní vývojové centrum a navazující výrobu, což by ji činilo možným kandidátem pro průmyslovou špionáž, disponuje zcela jistě dostatečným množstvím materiálů, technologií, postupů a dalších faktorů, které spadají do kategorie citlivých, a ty je nutné chránit. Existuje mnoho důvodů, proč i obchodní společnosti mohou být zajímavým cílem jakéhokoliv útoku na datovou infrastrukturu a ztráta, zneužití či změna celistvosti firemních dat a informací může znamenat velmi vážné hrozby pro další působení společnosti na trhu.

Na základě poznatků a informací získaných při tvorbě této diplomové práce, ale s ohledem na bezpečnost nebylo možné všechny uvést, lze konstatovat, že společnost Agrotec je firmou s aktivní bezpečnostní politikou, vědomou si možných rizik a hrozeb, které mohou nastat. Společnost se snaží přijímat taková opatření, která přispějí ke snížení těchto rizik, a lze předpokládat, že v tomto směru bude úspěšná a zůstane nadále aktivní. Možní útočníci jsou totiž vždy o krok napřed a obvykle vědí, co chtějí, a jak těchto cílů dosáhnout.

SEZNAM POUŽITÉ LITERATURY

[1] ŘEHKA, Karel. *Informační válka*. Praha: Academia, 2017. XXI. století. ISBN 978-80-200-2770-2.

[2] SMEJKAL, Vladimír a Karel RAIS. *Řízení rizik ve firmách a jiných organizacích*. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.

[3] DOBDA, Luboš. *Ochrana dat v informačních systémech*. Praha: Grada, 1998. ISBN 80-716-9479-7.

[4] POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. Vysokoškolské učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.

[5] Information Life Cycle Management (ILM). *Deloitte* [online]. 2019 [cit. 2019-03-17]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-advisory-information-lifecycle-management.pdf

[6] ČERMÁK, Miroslav. Informační bezpečnost. *CleverAndSmart* [online]. Miroslav Čermák, 2019, 14.4.2011 [cit. 2019-04-05]. Dostupné z: https://www.cleverandsmart.cz/informacni-bezpecnost

[7] Aktuální legislativa. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2019-04-05]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/legislativa/

[8] O úřadu. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2019-04-05]. Dostupné z: https://nukib.cz/cs/o-nukib/o-uradu/

[9] Co je NCKB. *Národní centrum kybernetické bezpečnosti* [online]. [cit. 2019-04-05]. Dostupné z: https://www.govcert.cz/

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

[11] KUROSE, James F. a Keith W. ROSS. *Počítačové sítě*. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

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

[13] Internet Security Threat Report: Volume 24. *Symantec* [online]. Symantec Corporation, 2019 [cit. 2019-03-03]. Dostupné z: http://app.mktgassets.symantec.com/e/er?aid=elq_19296&s=912704989&lid=30169&elqTrackId=a9ac2bb6ba194c278bb4b16dae858794&elq=c8d4339874584609baef813b069e7a1c&elqaid=19296&elqat=1

[14] WannaCry. Avast [online]. *Avast Software*, 2019 [cit. 2019-03-03]. Dostupné z: https://www.avast.com/cs-cz/c-wannacry

[15] MAKRUSHIN, Denis. The cost of launching a DDoS attack. *Securelist* [online]. Kaspersky Labs, 2019, 23.3.2017 [cit. 2019-03-03]. Dostupné z: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

[16] Cisco 2018: Annual Cybersecurity Report. *Cisco* [online]. Cisco, 2018 [cit. 2019-03-03]. Dostupné z: https://www.cisco.com/c/dam/m/hu_hu/campaigns/security-hub/pdf/acr-2018.pdf

[17] Internet Security Threat Report volume 23. *Symantec* [online]. Symantec Corporation, 2019 [cit. 2019-03-13]. Dostupné z: https://www.symantec.com/content/dam/symantec/docs/reports/istr-23-2018-en.pdf

[18] TUNG, Liam. MongoDB ransacking starts again: Hackers ransom 26,000 unsecured instances. *ZD Net* [online]. CBS Interactive, 2019, 5.9.2017 [cit. 2019-03-13]. Dostupné z: https://www.zdnet.com/article/mongodb-ransacking-starts-again-hackers-ransom-26000-unsecured-instances/

[19] IBM X-Force Threat Intelligence Index 2018. *IBM* [online]. [cit. 2019-04-15]. Dostupné z: https://www.ibm.com/downloads/cas/MKJOL3DG

[20] IBM X-Force Threat Inteligence Index 2019. *IBM* [online]. [cit. 2019-04-05]. Dostupné z: https://www.ibm.com/downloads/cas/ZGB3ERYD

[21] PACINDA, Štefan. *Analýza rizik, jeden ze základních nástrojů krizového managementu při řešení nevojenských krizových situací: disertační práce*. Brno: Univerzita obrany, 2007. DKZ.

[22] Historie ERP systémů. *ERP Systémy* [online]. 2018, 1.5.2011 [cit. 2018-12-29]. Dostupné z: http://erp-systemy.cz/historie-erp-systemu/

[23] SAP R/3 Architecture tutorial. *Guru99* [online]. Guru99, 2019 [cit. 2019-04-05]. Dostupné z: https://www.guru99.com/learning-sap-architecture.html

[24] ANDERSON, George W. *Naučte se SAP za 24 hodin*. Brno: Computer Press, 2012. ISBN 978-80-251-3685-0.

[25] SAP Modules – SAP FI, SAP CO, SAP SD, SAP HCM and more. *Simplilearn* [online]. [cit. 2019-04-05]. Dostupné z: https://www.simplilearn.com/sap-modules-sap-fi-sap-co-sap-sd-sap-hcm-and-more-rar111-article

[26] Malware. Avast [online]. *Avast*, 2019 [cit. 2019-04-14]. Dostupné z: https://www.avast.com/cs-cz/c-malware

[27] BHATTACHARYYA, Dhruba K. *Network anomaly detection: a machine learning perspective*. Boca Raton, [2014]. ISBN 978-146-6582-088.

[28] Enterprise Risk Management Software. *SAP Software Solutions* [online]. [cit. 2019-04-20]. Dostupné z: https://www.sap.com/products/risk-management.html

[29] Access Control Software. *SAP Software Solutions* [online]. [cit. 2019-04-20]. Dostupné z: https://www.sap.com/products/access-control.html

[30] Neutralize cybersecurity threats with real-time SIEM intelligence. *SAP Software Solutions* [online]. [cit. 2019-04-20]. Dostupné z: https://www.sap.com/products/enterprise-threat-detection.html

[31] Securing SAP Systems from Cyber Attacks. *Deloitte* [online]. [cit. 2019-04-20]. Dostupné z: https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-sap-governance-risk-compliance-sap-cyber-security-brochure-2018.pdf

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

DMZ Demilitarizovaná zóna

ERP Podnikový informační systém

ICT Informační a komunikační technologie

IS Informační systém

HW Hardware

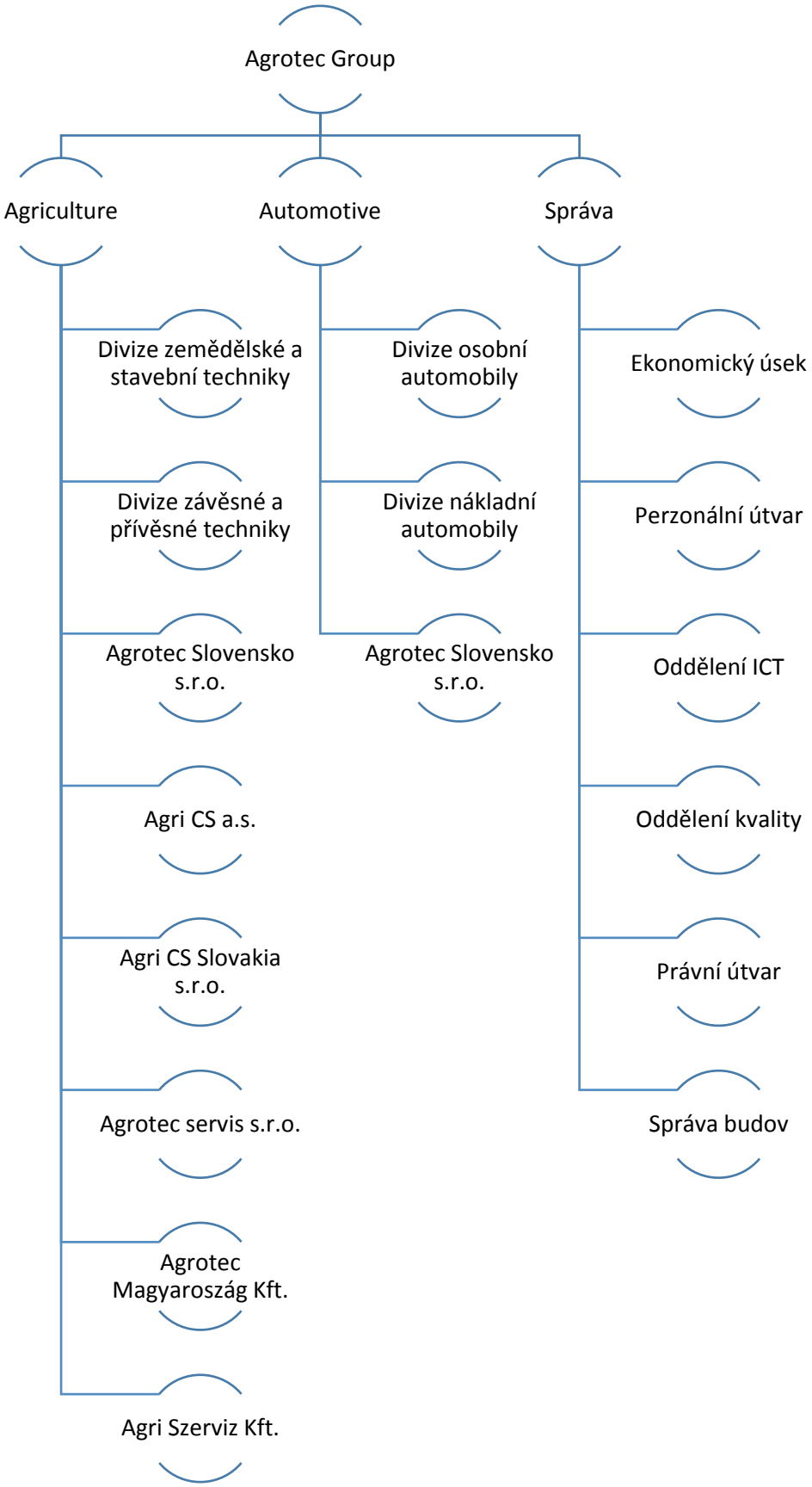
SW Software

SEZNAM OBRÁZKŮ

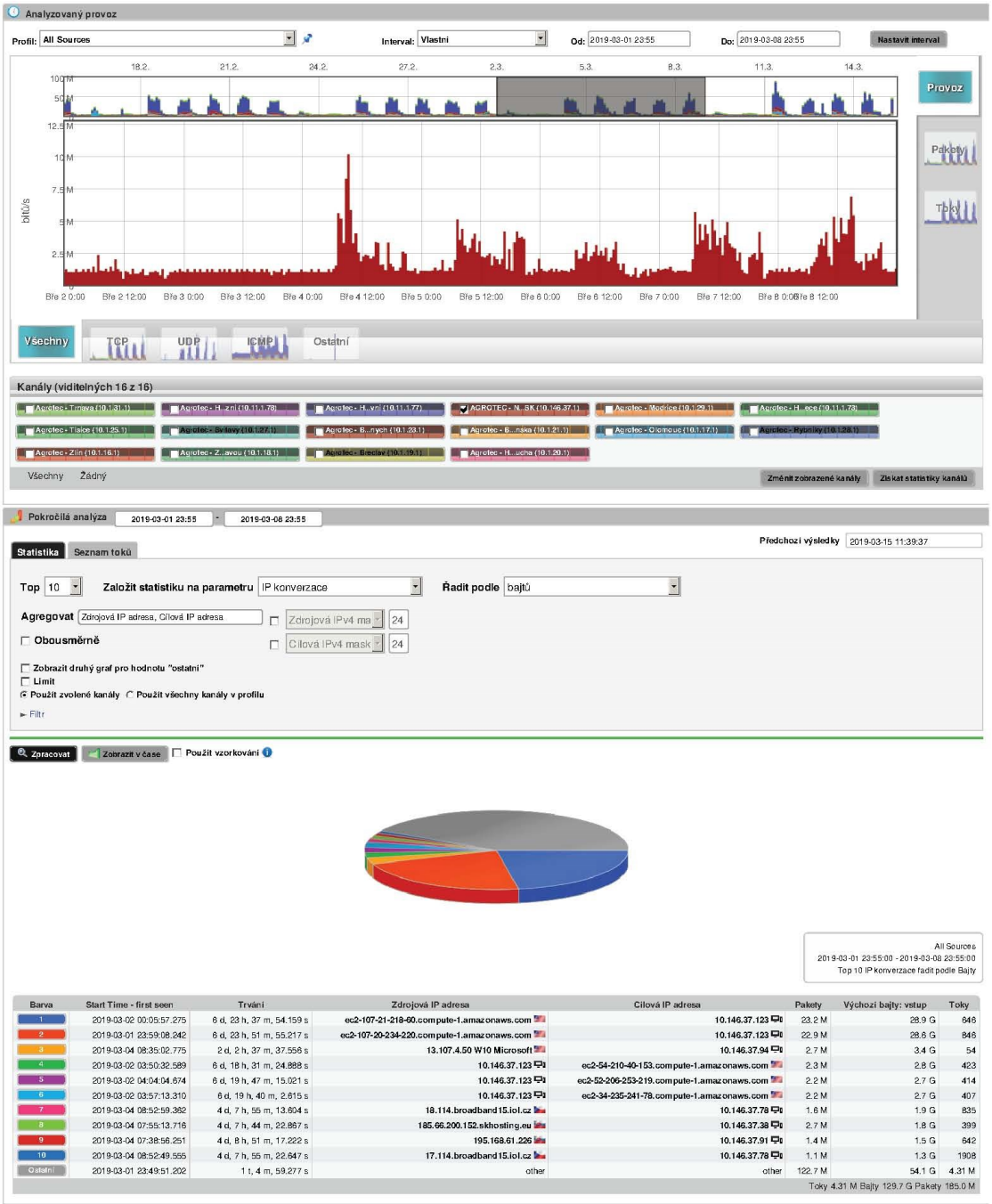
SEZNAM TABULEK

SEZNAM PŘÍLOH

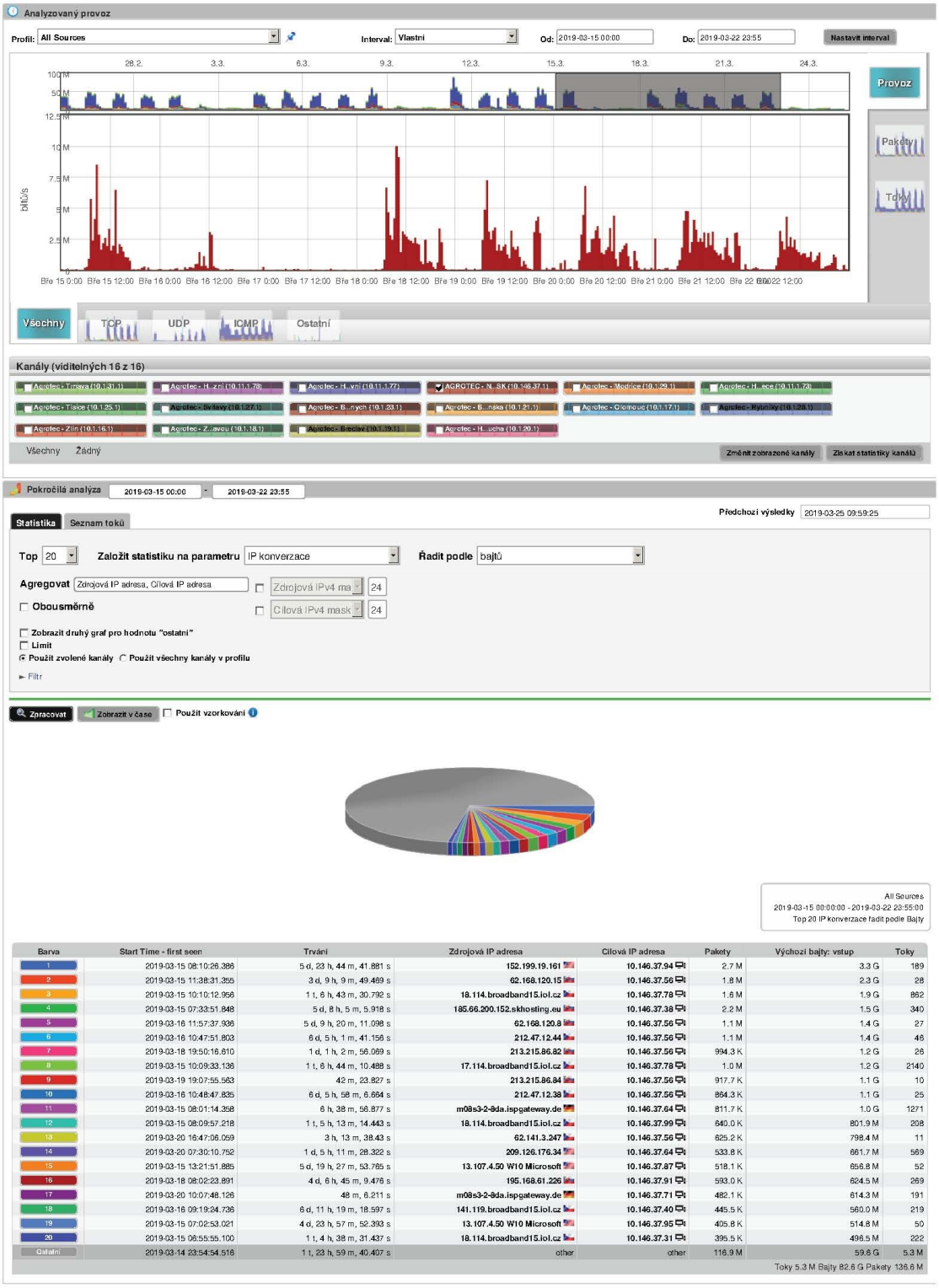
PŘÍLOHA P1: ORGANIZAČNÍ STRUKTURA SPOLEČNOSTI AGROTEC



PŘÍLOHA P 2: NEOBVYKLÝ DATOVÝ TOK V SW FLOWMON:



PŘÍLOHA P 3: BĚŽNÝ DATOVÝ TOK V SW FLOWMON



Barva	Start Time - first seen	Trvání	Zdrojová IP adresa	Cílová IP adresa	Pakety	Výchozí bajty: vstup	Toky
1	2019-03-15 08:10:26.386	5 d, 23 h, 44 m, 41.881 s	152.199.19.161	10.146.37.94	2.7 M	3.3 G	189
2	2019-03-15 11:38:31.355	3 d, 9 h, 9 m, 49.469 s	62.168.120.15	10.146.37.56	1.8 M	2.3 G	28
3	2019-03-15 10:10:12.956	1 t, 6 h, 43 m, 30.792 s	18.114.broadband15.iol.cz	10.146.37.78	1.6 M	1.9 G	882
4	2019-03-15 07:33:51.848	5 d, 8 h, 5 m, 5.918 s	185.66.200.152.skhosting.eu	10.146.37.38	2.2 M	1.5 G	340
5	2019-03-16 11:57:37.936	5 d, 9 h, 20 m, 11.098 s	62.168.120.8	10.146.37.56	1.1 M	1.4 G	27
6	2019-03-16 10:47:51.803	6 d, 5 h, 1 m, 41.156 s	212.47.12.44	10.146.37.56	1.1 M	1.4 G	46
7	2019-03-18 19:50:16.810	1 d, 1 h, 2 m, 56.069 s	213.215.86.82	10.146.37.56	994.3 K	1.2 G	26
8	2019-03-15 10:09:33.136	1 t, 6 h, 44 m, 10.488 s	17.114.broadband15.iol.cz	10.146.37.78	1.0 M	1.2 G	2140
9	2019-03-19 19:07:55.563	42 m, 23.827 s	213.215.86.84	10.146.37.56	917.7 K	1.1 G	10
10	2019-03-16 10:48:47.835	6 d, 5 h, 58 m, 6.664 s	212.47.12.38	10.146.37.56	864.3 K	1.1 G	25
11	2019-03-15 08:01:14.398	6 h, 38 m, 56.877 s	m08s3-2-8da.ispgateway.de	10.146.37.64	811.7 K	1.0 G	1271
12	2019-03-15 08:09:57.218	1 t, 5 h, 13 m, 14.443 s	18.114.broadband15.iol.cz	10.146.37.99	640.0 K	801.9 M	208
13	2019-03-20 16:47:06.059	3 h, 13 m, 38.43 s	62.141.3.247	10.146.37.56	625.2 K	798.4 M	11
14	2019-03-20 07:30:10.752	1 d, 5 h, 11 m, 28.322 s	209.126.176.34	10.146.37.64	533.8 K	661.7 M	569
15	2019-03-15 13:21:51.885	5 d, 19 h, 27 m, 53.765 s	13.107.4.50 W10 Microsoft	10.146.37.87	518.1 K	656.8 M	52
16	2019-03-18 08:02:23.891	4 d, 6 h, 45 m, 9.476 s	195.168.61.226	10.146.37.91	593.0 K	624.5 M	269
17	2019-03-20 10:07:48.126	48 m, 6.211 s	m08s3-2-8da.ispgateway.de	10.146.37.71	482.1 K	614.3 M	191
18	2019-03-16 09:19:24.736	6 d, 11 h, 19 m, 18.597 s	141.119.broadband15.iol.cz	10.146.37.40	445.5 K	560.0 M	219
19	2019-03-15 07:02:53.021	4 d, 23 h, 57 m, 52.393 s	13.107.4.50 W10 Microsoft	10.146.37.95	405.8 K	514.8 M	50
20	2019-03-15 08:55:55.100	1 t, 4 h, 38 m, 31.437 s	18.114.broadband15.iol.cz	10.146.37.31	395.5 K	496.5 M	222
Ostatní	2019-03-14 23:54:54.516	1 t, 23 h, 59 m, 40.407 s	other	other	116.9 M	59.6 G	5.3 M
					Toky 5.3 M Bajty 82.6 G Pakety 136.6 M		