Návrh a implementace bezpečnostní politiky v informačním a komunikačním systému organizace

Bc. Lukáš Pavlík

Diplomová práce
2015

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2014/2015

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

Jméno a příjmení:	**Bc. Lukáš Pavlík**
Osobní číslo:	**A13745**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh a implementace bezpečnostní politiky v informačním a komunikačním systému organizace**
Téma anglicky:	**The Design and Implementation of a Security Policy in the Information and Communication System of an Organization**

Zásady pro vypracování:

1. **Popište základní problematiku bezpečnostní politiky.**
2. **Vytvořte model komunikačního a informačního systému vybraného typu organizace.**
3. **Proveďte komplexní bezpečnostní analýzu organizace s důrazem na komunikační a informační systém.**
4. **Navrhněte a implementujte bezpečnostní politiku s ohledem na vnější a vnitřní rizika vyskytující se v dané organizaci.**
5. **Popište současné trendy a vývoj v oblasti bezpečnosti informačních a komunikačních systémů.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **Bílá, Jiří ŠMÍD, František KRÁL a Vladimír HLAVÁC. Informační technologie: Databázové a znalostní systémy. Praha: České vysoké učení technické, 2009, 126 s. ISBN 80-01-02790-2.**
2. **JASEK Roman, Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.**
3. **GÁLA Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2 vyd. Praha: Grada Publishing, a. s., 2009, 496 s. ISBN 978-80-247-2615-1.**
4. **VALOUCH Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 152 s. ISBN 978-80-7454-296-1. Dostupné z: https://dspace.k.utb.cz/handle/10563/25814.**
5. **POŽÁR Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. ISBN 80-8689-838-5.**
6. **LUDVÍK Miroslav. Teorie bezpečnosti počítačových sítí, Praha: Computer Media, 2008, 98 s. ISBN 80-86686-35-3.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **12. ledna 2015**

Termín odevzdání diplomové práce: **15. května 2015**

Ve Zlíně dne 6. února 2015

L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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/bakalářská 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/bakalářskou 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/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské 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/bakalářské 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/bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 29.4.2015

.....
podpis diplomanta

ABSTRAKT

Diplomová práce se zabývá problematikou bezpečnostní politiky v informačním a komunikačním systému vybrané organizace. Teoretická část je zaměřena na charakteristiku bezpečnostní politiky, formulování základních principů, struktury a její přínosy pro organizaci. Dále je zde rozpracována problematika informačních systémů a jejich rolí v informační společnosti. Praktická část poté obsahuje návrh a analýzu informačního systému, zahrnující komplexní posouzení bezpečnostní politiky. Závěr práce je věnován nejnovější trendům v této oblasti s možným vývojem do budoucnosti.

Klíčová slova: bezpečnost, riziko, informační systém, analýza, bezpečnostní politika, analýza rizik

ABSTRACT

This thesis deals with security policy in the information and communication system selected organizations. The theoretical part focuses on the characterization of security policies, formulating basic principles, structure and it‘s benefits for organizations. Furthermore, The issue of information systems and their role in the information society. The practical part includes the design and analysis of an information system with a comprehensive assessment of the security policy. The conclusion is devoted to the latest trends in this field with the development of the future.

Keywords: security, risk, information system, analysis, security policy, risk analysis

Děkuji panu doc. Ing. Jiřímu Gajdošíkovi, CSc. za odborné vedení a rady, které mi poskytl při zpracovávání mé diplomové práce. Dále bych rád poděkoval své rodině, za vytvoření vhodných podmínek pro mé studium.

Motto: Moudré je myslet skepticky a počínat si optimisticky.

[Hermann Hesse]

OBSAH

ÚVOD

Dnešní společnost lze nazvat „informační“ a proto jsou technologie, zaměřené na výměnu, zpracování a uložení dat velmi důležité. Informační systémy se využívají v nejrůznějších oborech lidské činnosti a jejich neustálý vývoj rozšiřuje možnosti jejich aplikace na další oblasti ve společnosti.

Jednou z těchto oblastí, jež je v současné době z pohledu informačních a komunikačních technologií předmětem výzkumu, je bezpečnost a bezpečnostní politika. Touto problematikou se zabývá jak soukromá, tak veřejná sféra a tak lze říci, že jde celosvětový trend. Tato diplomová práce je ovšem zaměřena na soukromou sféru a jejím cílem je vytvořit a zhodnotit informační systém vzhledem k bezpečnostní politice a rizikům, která lze při podrobné analýze v organizaci najít.

V teoretické části je vysvětleno, co je to bezpečnostní politika, jak se člení a jaké jsou zásady její tvorby. Důležitým bodem, této částí diplomové práce, jsou také nejčastější chyby při jejím vytváření. V další kapitole je rozpracována teorie informačních systémů a to včetně legislativy, vlastností samotných informačních systémů, jejich architektury a metod tvorby. Zde je také rozpracována oblast podnikových systémů, včetně integrace a různých úrovní managementu.

Praktická část je potom zaměřená na analýzu stávajícího informačního systému organizace včetně možných rizik, ohrožení a neefektivností, které jsou s tímto problémem spojeny. Poté jsou zde vytvořeny návrhy možných řešení, které by dané problémy odstranily. Dalším krokem je pak hodnocení a výběr vhodné varianty, která by byla pro organizaci tím nejlepším možným řešení s ohledem na její podstatu a fungování.

Tato část diplomové práce pak závěrem směřuje k předložení trendů v oblasti bezpečnostní politiky a informačních systémů v podobě aplikace nejvhodnějšího řešení s náznakem vědeckého rozvoje v následujících letech.

I. TEORETICKÁ ČÁST

1 BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Pojem bezpečnostní politika označuje dokument, který zajišťuje požadavky a nařízení, zajišťující bezpečnost konkrétního subjektu na všech jeho úrovních. Dříve tato problematika nebyla natolik předmětem zkoumání, jako je v dnešní době. Jelikož se ale rizika a hrozby v průběhu času mění, tak se začal z bezpečnostní politiky stávat celosvětový trend, který se neustále vyvíjí a zdokonaluje. O zavedení tohoto fenoménu do soukromé sféry se snaží čím dál více firem, protože si začínají uvědomovat, že se bez ní neobejdou a je pro jejich fungování a existenci velmi důležitá.

Bezpečnostní politika musí být v souladu s politikou celé organizace a musí jí respektovat, tj. definuje základní strategie, postoje, cíle, role, zodpovědností týkající se bezpečnosti a je závazná pro všechny zaměstnance. Poskytuje ochranu proti vloupání, zneužití, porušení, poškození a narušení fungování subjektu, což by mohlo mít za následek ohrožení nejen samotných aktiv, ale i celé organizace. [11]

Je důležité, aby dokument o bezpečnostní politice byl ve srozumitelné, přehledné, stručné a zároveň úplné formě a také řešil všechny otázky ohledně konfliktů a bezpečnosti dat, což není jednoduché. V praxi bývá problémem zkombinovat vyváženost stručnosti a pokrytí všech důležitých bodů. S touto překážkou si lze poradit tak, že v dokumentu lze používat odkazy na konkrétní normy, zákony a nařízení a tím dosáhnout požadovaného zestručnění informací. [11]

Základním podkladem pro tvorbu bezpečnostní politiky je analýza rizik. Ta má za úkol ohodnotit aktiva a s nimi spojené hrozby a rizika. Provádí se kvantitativní nebo kvalitativní metodou. Dále je zde důležitým bodem havarijní plán, který určuje postup při ohrožení nebo narušení fungování organizace a také obsahuje pokyny pro obnovu a nastolení rovnováhy. Nedílnou součástí je také bezpečnostní audit, který má za úkol kontrolovat bezpečnostní opatření a zodpovědnost za narušení bezpečnosti. Posledním bodem, který lze označit za důležitý pro bezpečnostní politiku jsou opatření, která slouží pro snížení zranitelnosti firmy a lze tyto zásady implementovat například do vnitřních norem, jako je pracovní řád, pracovní postupy, provozní předpisy apod. [11]

1.1 Principy zpracování bezpečnostní politiky

Vychází se především z:

- veškerých platných dokumentů organizace souvisejících s bezpečností (jako jsou BOZP a PO),
- systémových bezpečnostních požadavků,
- výsledků z analýzy rizik,
- požadavků na bezpečnost uvedených v normách, zákonech, vyhláškách apod. [11]

1.2 Legislativa související s bezpečnostní politikou

- zákon 365 / 2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů,
- zákon č. 127 / 2005 Sb. o elektronických komunikacích,
- zákon č. 101 / 200 Sb. o ochraně osobních údajů,
- zákon č. 227 / 200 Sb. o elektronickém podpisu,
- zákon č. 121 / 2000 Sb. zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon),
- zákon č. 480 / 2004 Sb. o některých službách informační společnosti,
- zákon č. 309 / 2006 Sb. v platném znění o zajištění podmínek BOZP,
- NV č. č. 378 / 2001 Sb., kterým se stanoví bližší požadavky na bezpečný provoz a používání strojů, technických zařízení, přístrojů a nářadí,
- vyhláška ÚOOÚ č. 366 / 2001 Sb. k zákonu o elektronickém podpisu,
- ISO / IEC 17799:2000, v této normě jsou zachyceny nejlepší praktiky v oblasti bezpečnosti pro komerční i státní organizaci, je převzata z Velké Británie,
- BS 7799-2:1999, zavedení této normy umožňuje organizaci prokázat, že její systém řízení bezpečnosti informací v organizaci byl zaveden správně, což jí umožňuje provést vlastní certifikaci,
- ISO / IEC 2700, slouží k samostatné specifikaci systému bezpečnosti informací,
- ISO / IEC 27002, doporučovaná opatření nutná pro systém řízení bezpečnosti informací,
- ISO / IEC TR 13335, slouží jako doplnění pro zavedení bezpečnosti organizace a pro podporu dalších metod, není plnohodnotnou normou jak například normy uvedené výše,
- další legislativa (vyhlášky, standardy atd.) MV ČR, ÚOOÚ, NBÚ apod.

1.3 Struktura bezpečnostní politiky

- stanovit účel bezpečnostní politiky v organizaci,
- určení zodpovědnosti za klasifikaci dat, přístupových práv a zaměstnanců,
- definice požadované úrovně bezpečnosti,
- normy chování zaměstnanců (zejména právní a etické aspekty),
- definice zodpovědnosti článků organizační struktury při řízení bezpečnosti,
- postupy a havarijní plány při budování bezpečnosti ICT v obecné rovině,
- podmínky auditu,
- definice zabezpečení a míry odolnosti v jednotlivých oblastech bezpečnosti (organizační, technická, personální apod.). [11]

1.4 Přínosy vytvoření bezpečnostní politiky pro organizaci

- zaměstnanci budou znát své povinnosti a odpovědnosti při práci s informacemi,
- v organizaci budou díky zavedení bezpečnostní politiky jasně formulovány základní principy řízení informační bezpečnosti,
- zavedením bezpečnostní politiky se zvyšuje kredit společnosti u spolupracujících subjektů a obchodních partnerů,
- jsou také definovány požadavky na chování vnějších subjektů v prostředí informačního systému organizace. [11]

1.5 Obsah kapitol dokumentu bezpečnostní politiky

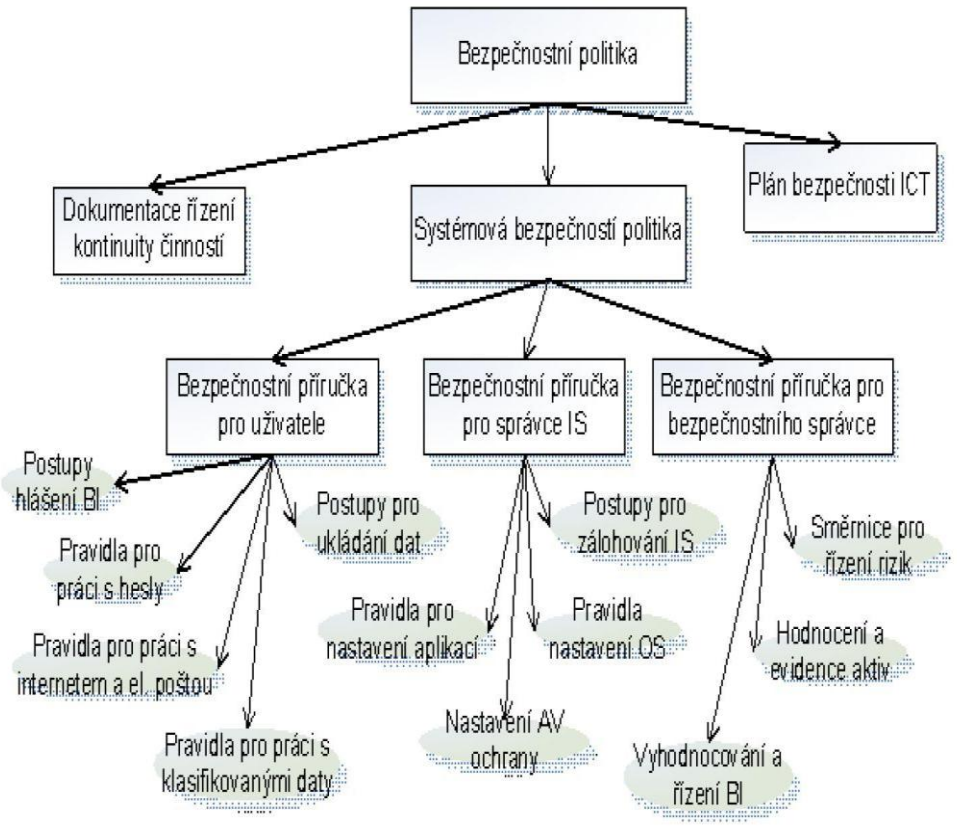
- organizační bezpečnost,
- bezpečnostní politika,
- bezpečnost prostředí a fyzická bezpečnost,
- personální bezpečnost,
- řízení a klasifikace aktiv,
- řízení přístupu,
- řízení provozu a komunikací,
- údržba a vývoj systémů,
- zajištění shody,
- zvládání bezpečnostních incidentů,
- řízení kontinuity činnosti. [12]

Bezpečnostní politika může být jednoduše formulována v rámci jediného dokumentu nebo může být vytvořena v rámci několika dokumentů vztahujícím se k celkové bezpečnostní politice ICT a navazující systémové bezpečnosti informačních systémů, kterých může být vypracováno více – pro každý informační systém. [12]

1.6 Dokumentace bezpečnosti

V rámci vytváření procesu bezpečnosti je potřeba definovat v dokumentu bezpečnostní politiky základní pravidla a předpisy. Bezpečnostní politika patří k základním zdrojům, které určují bezpečnost a pravidla v organizaci. Další dokumenty, které jsou k této problematice vázány, jsou jakýmsi doplněním pro upřesnění navazujících metodik a procesů.

Součástí základní bezpečnostní dokumentace a dokumentace bezpečnosti informačních procesů může být posloupnost několika dokumentů, které si může organizace rozvrhnout, podle svých potřeb, například takto [12]:



Obr. 1 Struktura bezpečnostní politiky [10]

Provozní směrnice, postupy a příručky navazují na již zpracovanou bezpečnostní politiku IS a stávají se tak nedílnou součástí komplexního řízení informační bezpečnosti. Navazující dokumenty více konkretizují problematiku bezpečnostní politiky, která zatím nebyla v základním dokumentu řešena.

Může se jednat například o:

1.6.1 Bezpečnostní příručka

Jsou zde určeny povinnosti a odpovědnosti uživatelů z pohledu bezpečnosti informací v rámci používání ICT organizace. [12]

1.6.2 Plán bezpečnosti ICT

Uvádí, bezpečnostní opatření, která je nutná provést vzhledem k bezpečnosti organizace. Tato část bezpečnostní politiky bývá určena na základně provedené analýzy rizik IS. V tomto plánu je stanoven harmonogram konkrétního opatření, který určuje časovou náročnost a implementaci tak, aby bylo dosaženo požadovaného cíle. Opatření, která jsou zde navrhnutá, se mohou týkat i jiných oblastí bezpečnosti, například personálních. Nemusí se jednat pouze o technické parametry IS. [12]

1.6.3 Směrnice pro bezpečnostního správce

Zde jsou charakterizovány jednotlivé činnosti, které jsou vykonávány bezpečnostním správcem ICT, jako například odpovědnosti, povinnosti a oprávnění při práci s informačními a komunikačními technologiemi. [12]

1.6.4 Směrnice pro IS, správce sítě, správce AV ochrany a správce zálohování

Týká se to zejména administrátorů různých oblastí IT a jejich činností v ICT.

1.6.5 Pokyny, návody a pracovní postupy

Určují postupy a povinnosti pro práci s prostředky ICT pro:

- práci s hesly,
- používání elektronické pošty,
- práci s notebooky,
- šifrování a práci s klíči, certifikáty,
- ukládání a zálohování dat, používání internetu atd.

1.6.6 Technická dokumentace

Týká se zejména nastavení firewallu, informačního systému, zálohovacího plánu, deníku správce sítě, záznamy o provozu atd.

Hlavními přínosy této dokumentace jsou:

- všichni zaměstnanci budou podrobně seznámeny se svými povinnostmi a odpovědnostmi při práci s ICT,
- sníží se riziko úniku dat,
- zvýší se povědomí uživatelů o informační bezpečnosti,
- bude snadnější zastupovat administrátory a správce,
- omezí se „absolutní moc“ administrátorů a správců. [12]

1.7 Problémy a chyby při tvorbě bezpečnostní politiky

Při tvorbě bezpečnostní politiky dochází často k různým nesrovnalostem a pochybením, které poté ovlivňují fungování celé organizace. Zde jsou nejčastěji se vyskytující problémy a chyby.

1.7.1 Velké množství kompromisů

Jedná se o častý problém, kdy postupným redukováním požadavků, zůstane jen část původního dokumentu. Nejdůležitější problémy, které měly být řešeny, byly přepsány nebo pozměněny a dané organizaci tak není umožněno řešit to, co je pro ni důležité. [3]

1.7.2 Nereálná bezpečnostní politika

Jde o velmi přísnou politiku, kdy současný stav společnosti v žádném bodě nevyhovuje dané politice. Zde je třeba definovat přechodné období a postupnou implementaci. Pokud se tak nestane, je velice pravděpodobné, že zaměstnanci budou celý proces bezpečnostní politiky vnímat odlišně od reality a toto nerespektování legislativy může vést k velmi závažným důsledkům. [3]

1.7.3 Neadekvátní rozsah politiky

Vedení managementu je předložena politika, která svým rozsahem značně znemožňuje se podrobně s celým dokumentem seznámit a pochopit tak význam jednotlivých ustanovení v organizaci. [3]

1.7.4 Podcenění propagace politiky

Je možné setkat se i s případy, kdy existence bezpečnostní politiky je před většinou zaměstnanců skrytá. Nebývá to z důvodu úmyslu, ale spíše nevhodnou a nezvládnutou komunikací směrem dovnitř firmy. Pokud s daným dokumentem nejsou zaměstnanci řádně seznámeni, těžko může být pro organizaci přínosem. [3]

1.7.5 Nekritické přebírání vzorců

Pokud nastane situace, že se bezpečnostní politika konkrétní firmy přenese na jinou firmu, nemusí být v praxi stejným přínosem, jako tomu bylo v prvním případě. Vylepšování původního „vzoru“, bez předchozí dostatečné analýzy, může přinést velmi špatný výsledek. [3]

Bezpečnostní politika je tedy souhrnem zásad a technických opatření, jejichž dodržování v praxi, vede ke zlepšení funkce organizace a k efektivnějšímu řízení bezpečnosti a rizik. V souvislosti s touto problematikou lze zmínit také bezpečnost informačních systémů, kterou se zabývá další kapitola.

2 BEZPEČNOST INFORMAČNÍCH SYSTÉMŮ

Pod tímto pojmem si lze představit komplexní ochranu informací a informačních technologií, které jsou touto formou přenášeny, uchovávány a zpracovávány. Tento druh bezpečnosti je dodržován zejména prostřednictvím technických, fyzických, logických a organizačních opatření, která chrání tyto informace před případným zneužitím odcizením nebo poškozením. Bezpečnost ICT také zahrnuje prevenci a zmírnění dopadů těchto hrozeb na informační systém a celou organizaci a proto je dle původu rizikových situací, můžeme rozdělit na [3]:

- napadení pracovních stanic,
- napadení na úrovni aplikací,
- napadení serverů,
- napadení síťové infrastruktury,
- odcizení soukromých dat,
- zablokování služeb,
- nežádoucí přednos dat. [3]

Dále je možné rizika ICT rozdělit na:

a) Vnitřní

- modifikace
- zničení
- ztráta
- kompromitace dat
- nedostupnost služeb způsobené chybou člověka

b) Vnější

- modifikace
- zničení
- ztráta
- nedostupnost služeb způsobená náhodnou nebo úmyslnou akci nepovolaných osob

Tyto druhy škod mohou nastat buď chybou systému, nebo chybou jednotlivce. Člověk je může páchat úmyslně, například cílenými penetračními testy, kdy se simuluje útok na systém (bez reálného poškození) nebo napadení informačního systému se záměrem odcizení a poškození dat. Dále je zde také možnost neúmyslného poškození a to zejména při programování, kdy může programátor zvolit nevhodné řešení apod. [9]

Bezpečnost informačních a komunikačních systémů se skládá z:

- kryptografické ochrany,
- počítačové a komunikační bezpečnosti,
- personální bezpečnosti,
- ochrany proti úniku elektromagnetického záření,
- fyzické bezpečnosti,
- administrativní bezpečnosti a organizačního opatření. [14]

Bezpečnostní informační systém, má-li splňovat svůj cíl a efektivitu, musí být řešen na těchto úrovních bezpečnosti:

2.1 Režimová bezpečnost

Tvoří základ pravidel a nařízení, která se vztahují k práci s daty a počítačovými a informačními systémy. Je nutné zejména kontrolovat jejich dodržování v praxi.

Režimová bezpečnost by se měla zabývat:

- přesným stanovením, jaké osoby mají přístup k určitému typu informací a určit jejich rozsah pravomocí,
- vymezit utajované informace a jejich stupně utajení,
- určit a vymezit pohyb zaměstnanců v prostorách organizace,
- stanovit režim a organizaci postupu při manipulaci s utajovanými informacemi firmy,
- zavést organizační řád. [13]

Pozn. O značení „režimová bezpečnost“ a „fyzická bezpečnost“ mohou být považovány za shodné, nicméně v některých zdrojích jsou tyto dva pojmy rozlišovány a proto se jejich význam liší i v této diplomové práci. [20]

2.2 Personální bezpečnost

Tato část bezpečnosti informací je zaměřena na prevenci hrozby, která může pocházet z řad vlastních zaměstnanců firmy. V praxi jsou to právě pracovníci, kteří potenciálně nejvíce ohrožují ICT. Proto se těmto nežádoucím situacím předchází různými prověrkami a testy, které jsou prováděny jak na budoucích zaměstnancích, tak na těch současných zaměstnancích. [2]

Pro výběr pracovníků, kteří budou mít za úkol správu informačního systému dané organizace, je potřeba vybírat kvalitní lidi, kteří budou pro firmu přínosem a nikoli nebezpečím. Z tohoto důvodu je třeba, aby byla personální bezpečnost nedílnou součástí bezpečnostní politiky a tím pádem byli vybíráni pouze takoví budoucí zaměstnanci, kteří nejsou pro ICT, žádným nebezpečím. [2]

2.3 Fyzická bezpečnost

Fyzická bezpečnost tvoří systém opatření, který má za úkol chránit data, jejich nosiče a informační zdroje před případnými fyzickými útočníky, kteří mohou odcizit nebo znehodnotit aktiva organizace. Prostory, kde se nacházejí důležité prvky ICT (jako jsou servery apod.), by měly být zabezpečeny perimetrickou ochranou s odpovídajícími bezpečnostními prvky a vstupy. Tato zařízení by měla být také chráněna proti neautorizovanému vstupu a zneužití. Pozornosti by také neměla uniknout ochrana podpůrných prostředků, jako jsou dodávka elektrické energie, popř. kabelové rozvody. [2]

2.4 Komunikační bezpečnost

Jedná se o zabezpečení informací během jejich přenosu informačními kanály, které mohou být odposlouchávány neznámými útočníky. Hlavním prostředkem zabezpečení tohoto procesu je například kryptografická ochrana a její detekování náhodné nebo záměrné změny. V tomto procesu výměny informací mezi různými subjekty dochází napřed k jejich autentizaci a identifikaci a poté ke komunikaci a přenosu informace. [8]

2.5 Administrativní bezpečnost

Administrativní bezpečnost má za úkol ochranu utajovaných listin, které obsahují utajované informace. Pro práci s těmito citlivými dokumenty je třeba stanovit určitý řád a postupy, které budou zahrnovat:

- tvorbu takových typů dokumentů,
- jejich příjem, zpracování a následné zařazení,
- evidenci, skartaci
- odesílání a přepravu,
- způsob přenášení,
- uložení, archivaci,
- popř. jiné nakládání. [2]

2.6 Bezpečnost hardwarových prostředků

Je zde řešena zejména problematika přístupu k technickým prostředkům, jejich ochrana proti elektromagnetickému záření, popř. zjišťování a odstraňování odposlechů. Tato činnost je zajišťována prostřednictvím pravidelných prohlídek s přesně stanoveným rozsahem nebo jednorázovými a neplánovanými prohlídkami vybavení a prostor pomocí zařízení, jako jsou šifrátory, šumové generátory apod., které slouží k rušení a zabránění odposlechů.

Vedle těchto kontrol, je potřeba provádět také prohlídky na specifických úsecích, které mají za úkol zaměstnanci, kteří jsou za ně zodpovědní.

Jedná se o zjišťování:

- funkčnosti technických prostředků bránící úniku informací,
- dodržování určitých organizačních opatření, která slouží k ochraně konkrétních úseků,
- provádění technických prohlídek pomocí zařízení, která slouží k detekci úniku informací. [17]

2.7 Bezpečnost softwarových prostředků

Do této problematiky lze zahrnou ochranu softwaru před případným zneužitím nežádoucími uživateli. Jde zde především o ověřování autentičnosti uživatele, jeho identifikování, rozdělení pravomocí jednotlivých uživatelů apod.

Bezpečnost těchto zařízení závisí na:

- šifrování
- antivirech
- firewallu

2.7.1 Šifrování

V praxi je nejvíce rozšířené symetrické klíčování, jedná se o klíčování založené na principu jednoho klíče, kterým lze data šifrovat i dešifrovat. Příkladem takové šifry je DES – Data Encryption Sandard. Od roku 1975 se také používá asymetrické šifrování, které je založeno na dvou odlišných klíčích, tj. veřejném a soukromém. [1]

2.7.2 Antiviry

Vzhledem k tomu, že počet virů stále roste a jedná se o čím dál tím více sofistikovanější programy, je na místě soustředit se také na antivirovou ochranu prostřednictvím kvalitního antiviru. Základem úspěšnosti a efektivnosti daného antiviru je jeho schopnost detekování nákazy. Antivirus tedy musí být schopen identifikovat různé druhy virů, jejich ž spektrum je stále rozmanitější. [1]

2.7.3 Firewally

Firewally slouží k zajištění datové bezpečnosti z pohledu odchozí a příchozí datové komunikaci. Jedná se ve své podstatě o „kontrolní bod“, který slouží k zajištění pravidel komunikace mezí sítěmi, které jsou oddělené. [1]

Firewall může být:

- **a)** Podnikový – jeden nebo více zařízení pro celou organizaci na důležitých přístupových bodech.
- **b)** Osobní – instalovaný na jednotlivých počítačích, pro každého uživatele jeden.
- **c)** Hardwarový – např. přímo v počítači.
- **d)** Softwarový – v proxy serveru. [1]

Bezpečnost informačních systémů a informací jako takových souvisí s mnoha oblastmi IS, jako například fyzickou ochranou serveru, ochranou utajovaných listin apod. K ochraně IS také slouží různé prostředky, jako šifrování, antiviry a firewally, které slouží k zabránění infiltrace nežádoucími programy, o kterých pojednává následující kapitola.

3 INFILTRACE DO INFORMAČNÍHO SYSTÉMU

Velké množství škod na programovém vybavení počítačů a na datech způsobují počítačové viry, což jsou programové moduly, které jsou připojeny k původnímu programu v počítači. Po načtení programu do paměti (při jeho spuštění), začne provádět virus činnosti, které nejsou žádoucí a uživatel je tudíž neočekává. Činnost viru může být aktivována bezprostředně po jeho zavlečení do operační paměti počítače nebo může být spuštěna jinými okolnostmi, například v určitý den nebo hodinu. [4]

V počítačové terminologii rozlišujeme:

3.1 Počítačové viry

Počítačový virus se kopíruje sám do sebe a do dalších programů, a tímto způsobem je infikuje. Ve své podstatě se jedná o malý kousek kódu, který se připojí ke kódům ostatních programů, které budou poté spuštěny. Viry útočí jen na některé typy souborů, jedná se většinou o spustitelné soubory. [4]

Účinky počítačových virů mají tyto charakteristické projevy:

- nestabilita programů (programy se „hroutí“),
- pomalejší chod počítače,
- modifikace dat,
- chyby v paměti počítače,
- odstranění dat,
- změna atributů souboru (změna velikosti a datumu souboru).

Existují tři hlavní typy počítačových virů:

a) Viry, **napadající spustitelné soubory,** buď určitého typu (.EXE, .COM) nebo jakékoliv jiné spustitelné soubory (.OVL, .SYS, PRG). Tyto soubory po napadení virem zvětšují svou velikost a tím je snadnější je identifikovat.

b) Viry, **napadající zaváděcí program operačního systému** v systémové oblasti disku (tzv. Master Boot Record – MBR). Tyto viry se přenášejí infikovanými nosiči, jako např. prostřednictvím CD a způsobují narušení operačního systému napadeného počítače.

c) Makro viry, **které napadají uživatelské programy** (např. MS WORD), které potom po spuštění začnou provádět úkony, které nebyly zadány uživatelem. [4]

Útoky na systém se klasifikují na:

a) **Pasivní**
   - realizované odposlechem toku informací v systému

b) **Aktivní**
   - realizované modifikací dat, přerušením informačního toku dat v systému apod. [5]

Absolutní prevence proti útoku není možná. Typickým postupem ochrany systému je detekování útoku, obnova činnosti informačního systému a vytvoření protiopatření k zamezení vzniku obdobného napadení. Útoky mohou být vedeny na:

a) **Důvěrnost**
   - zpřístupnění a narušení důvěrných dat neautorizovaným osobám

b) **Integritu**
   - narušení informačního systému, narušení celistvosti dat nebo bezpečnostního systému

c) **Dostupnost**
   - např. odmítnutí služby nebo přístupu. [4]

3.2 Trojské koně

Jedná se o programy, které se jeví jako jiné programy (vypadají velmi podobně) a po jejich spuštění získají osobní data a hesla uživatele, která poté zasílají autorovi trojského koně. Trojský kůň může být samostatný program, například spořič obrazovky nebo hra. Někdy se také trojský kůň vydává za malware (dokonce i jako takový může fungovat a odstraňovat konkurenční typ malware). [4]

3.3 Počítačoví červi

Jsou to programy, které se sami replikují, jiné programové vybavení počítače nemodifikují. Obvyklá cesta jejich šíření je elektronickou poštou (např. na všechny adresy v adresáři klientského programu).

Svým samostatným jednání se počítačový červ liší od počítačových virů. Někteří červi mohou být tzv. polymorfní, což znamená, že se liší od svého „rodiče“. Podstata šíření je obdobná, jako u počítačových virů, tedy zneužívání konkrétních bezpečnostních mezer v softwaru a operačním systému. [4]

Typy červů:

1) **E-mailoví červi**
- využívají ke svému šíření elektronickou poštu,
- poté, co infikují počítač, začnou se rozesílat na jiné e-mailové adresy, které získají buď z adresáře, nebo prohledáváním uložených souborů a jejich obsahu a extrahováním řetězců, které vyhovují tvaru e-mailové adresy,
- obsah zprávy, která je odeslána e-mailovým červem, obsahuje škodlivý program jako přílohu, popř. odkazuje na jiné internetové stránky, kde bude uživatel rovněž infikován. [21]

2) **Internetoví červi**
- internetový červ využívá všech dostupných síťových prostředků k tomu, aby našel počítač, který je zranitelný a tudíž náchylnější k útoku,
- v ideálním případě je schopen spuštění škodlivého kódů a vlastní instalace do systému bez vědomí uživatele. [21]

3) **IM a IRC červi**
- tyto druhy červů využívají pro své šíření sítě určené pro komunikaci v reálném čase,
- rozdíl je v tom, že IM červi obvykle rozesílají odkazy na webové stránky, oproti tomu IRC červi zasílají svůj program jako samostatně spustitelný soubor,
- IRC červi jsou tudíž méně nebezpeční, neboť v jejich případech musí dojít ke spuštění a instalaci souboru uživatelem,
- výhodou tohoto přístupu je, jako v případě počítačových virů, zasílání e-mailu jménem napadeného uživatele, což zvyšuje věrohodnost zprávy. [21]

4) **Červi využívající sdíleného souboru**
- tento druh počítačového červa kopíruje svůj program jako spustitelný soubor do sdílených umístění, většinou na sdílený prostor lokálního počítače nebo na vzdálený počítač, kde bývá tento soubor ke stažení,
- vzhledem k tomu, že sdílející sítě nabízejí většinou ke stažení nelegální soubory, je tedy snadnější, v případě vhodného pojmenování souboru, jeho rychlejší šíření. [21]

3.4 Phishing

Jedná se o druh počítačového podvodu, kdy se podvodníci snaží vylákat z uživatelů údaje, které slouží jako přístup k jejich bankovním účtům. K získání tohoto druhu informací se využívá zasílání e-mailů, které na první pohled vypadají tak, že jsou odesílány přímo z banky klienta. U tohoto druhu zprávy je vyžadováno, aby klient kliknul na odkaz a tím byl přesměrován na podvodné stránky, kde po něm budou vyžadovány osobní identifikační údaje. Nemusí se však jednat pouze o účty bankovní, ale také ostatních organizací, kde poté dochází k nedovolené manipulaci finančními prostředky. Příkladem může být třeba eBay, PayPal, Google, Skype. [18]

Základní znaky phishingového e-mailu:

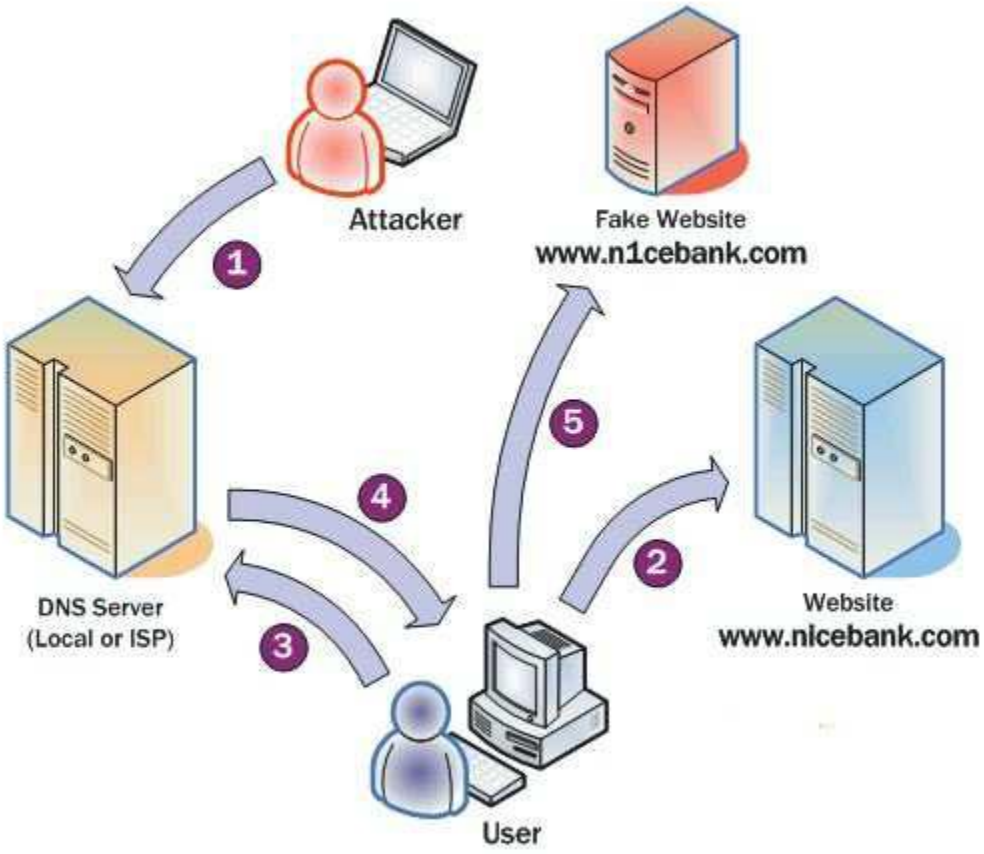
- snaží se vyvolat dojem, že byl odeslán „skutečnou“ organizací,
- tohoto dojmu se snaží tvůrce docílit pomocí grafiky a zfalšování adresy odesílatele,
- text může být formulován jako výzva k aktualizaci bezpečnostních údajů, jako informace o neprovedení platby, výzkum klientské spokojenosti, oznámení o dočasném zablokování klientské karty nebo účtu anebo jako elektronický bulletin určený pro klienty,
- v e-mailu je umístěn odkaz, který zdánlivě odkazuje na internetové stránky banky klienta, ale při jeho bližším prozkoumání se dá zjistit, že ve skutečnosti odkazuje na místo, kde jsou umístěny podvodné webové stránky. [18]

3.5 Pharming

Další metodou, která je zaměřena na nelegální získávání údajů od klienta, je pharming. V tomto případě není využíváno podvodných zpráv, jako je tomu u phishingu, ale uživatel je odkazován na podvodnou stránku přímo již při zadávání internetové adresy ve vyhledávači. Z těchto důvodů je velmi špatně rozpoznatelný. [15]

Princip fungování pharmingu:

1) Útočník zaměří (attacker) DNS spojení, které používá uživatel (user). Poté změní IP adresu např. www.dum.cz na falešnou IP adresu www.dum1.cz
2) Uživatel chce navštívit stránku www.dum.cz a zadá ji do prohlížeče.
3) Počítač uživatele předá žádost na DNS server pro IP adresu www.dom.cz
4) Pokud je DNS server již napadený, předá zpátky na počítač uživatele již IP adresu falešné stránky www.dum1.cz
5) Uživatel je odkázán na falešné stránky v domnění, že se jedná o stránky pravé. [15]



Obr 2. Princip pharmingu [15]

3.6 Spam

Ve své podstatě za spam můžeme označit zprávy (převážně komerčního charakteru), které jsou automaticky zasílané mnoha uživatelům, kteří si je neobjednali a nemají možnost tento nežádoucí odběr zrušit. Tyto zprávy chodí často stejným příjemcům, obsahují stejné informace, pouze se liší vnitřní úpravou tak, aby je filtr spamu nerozpoznal. [10]

Někdy se také jako o spamu mluví o hromadném přeposílání e-mailu se zábavným obsahem. Ale jelikož mají příjemci o tento druh e-mailů zájem a aktivně se podílejí na tomto procesu šíření, nelze v tomto případě o spamování hovořit. Z spam samozřejmě také nelze označit vyžádaný odběr např. akčních nabídek z konkrétního serveru apod. [10]

Základním principem spamu je šíření reklamy, nabídka produktů nebo propagace služeb. Spam ale také může být nosičem počítačového viru nebo trojského koně. Tyto trojské koně mohou mít např. funkci pro odposlouchávání hesel, které poté odesílají zpět autorovi e-mailu. [10]

Rozesílání spamu je pro obchodníky lákavé především tím, že jde o nenákladné využití informačních technologií a marketingu. V současné době jsou pro sparing využívány e-maily, blogy, diskusní skupiny, instant messengery (nejevíce Facebook, ICQ nebo Skype) a telekomunikační služby. [19]

3.7 Hoax

Pojmem hoax se označuje nevyžádaná e-mailová zpráva, která informuje o nebezpečí, žádá se v ní o pomoc, varuje před šířícím se virem, snaží se pobavit apod. V hoaxu bývá také obsažena výzva k jeho dalšímu přeposílání a proto se někdy také označuje pojmem „řetězový e-mail“. [19]

Škodlivost hoaxů lze spatřit zejména v:

1) **Obtěžování příjemců**
   - opakovaný příjem takových zpráv je pro uživatele velmi nepříjemný,
2) **Zbytečné zatěžování linek a serverů**
   - v době, kdy je jistý typ hoaxu velmi moderní, může jeho hromadné rozesílání zatěžovat počítačové servery a sítě,

3) **Nebezpečné rady**
   - některé hoaxy poskytují rady, které jsou nebezpečné, jako např. že se uživatel smazáním určitého souboru zbaví viru apod.
4) **Prozrazení důvěrných informací**
   - pokud je hoax rozesílán na mnoho dalších adres, jsou zde zachyceny adresy příjemců, které si mohou další příjemci tohoto e-mailu přečíst,
5) **Ztráta důvěryhodnosti**
   - odesílatel hoaxu ohrožuje svou důvěryhodnost, pokud odesílá zprávu z počítače, který je umístěn např. v jeho pracovní kanceláři,
   - z tohoto důvodu pak může být ohrožena dobrá pověst celé firmy nebo úřadu. [19]

Možností, jak infiltrovat IS je mnoho. V této kapitole byly uvedeny nejčastěji se vyskytující způsoby napadení a šíření škodlivého software. Jsou zde i nastíněny možnosti, jak takovým cíleným útokům předcházet a jak zvýšit svou bezpečnost v internetovém prostředí. Sledování této problematiky je důležité i pro úspěšné fungování podnikového informačního systému, kterým se dále podrobněji zabývám.

4 PODNIK A JEHO INFORMAČNÍ SYSTÉM

V dnešní době existují pojmy IS a komunikace v rámci jednoho systému, což v praxi znamená, že jsou tyto technologie integrovány ve společných zařízeních a technických prostředcích. Vždy tomu ale tak nebylo, ještě v 80-tých letech byly tyto problémy striktně rozděleny a ve firmách existovaly oddělení, které se zabývali IS a oddělení, které zajišťovaly komunikaci.

4.1 Struktura informačního systému v podniku

Pojem architektura se v informatice používá od 60-tých let a původně označovala uspořádání jeho hlavních komponent. Později se přidala architektura software, která je tvořena vrstvami vzájemně podřízených komponent operačního systému, kde každá nadřazená vrstva definuje své požadavky a využívá služeb podřízených vrstev.

Tento princip rozlišujeme na tři základní vrstvy:

1) **Vrstva technologická**
   Touto vrstvou rozumíme jednotlivé komponenty informačních technologií, zejména technických prostředků, základního software a jejich vnitřní struktury a vzájemné vazby.
2) **Vrstva aplikační**
   Do této vrstvy zahrnujeme veškerý aplikační software, datovou a funkční specifikaci, řešené projekty i jejich dokumentaci.
3) **Vrstva prostředí**
   Zde je obsaženo podnikatelské prostředí podniku, podnikové procesy, organizační struktura, personální kapacity a jejich kvalifikace a zkušenosti s řízením a provozováním IS/IT. [5]

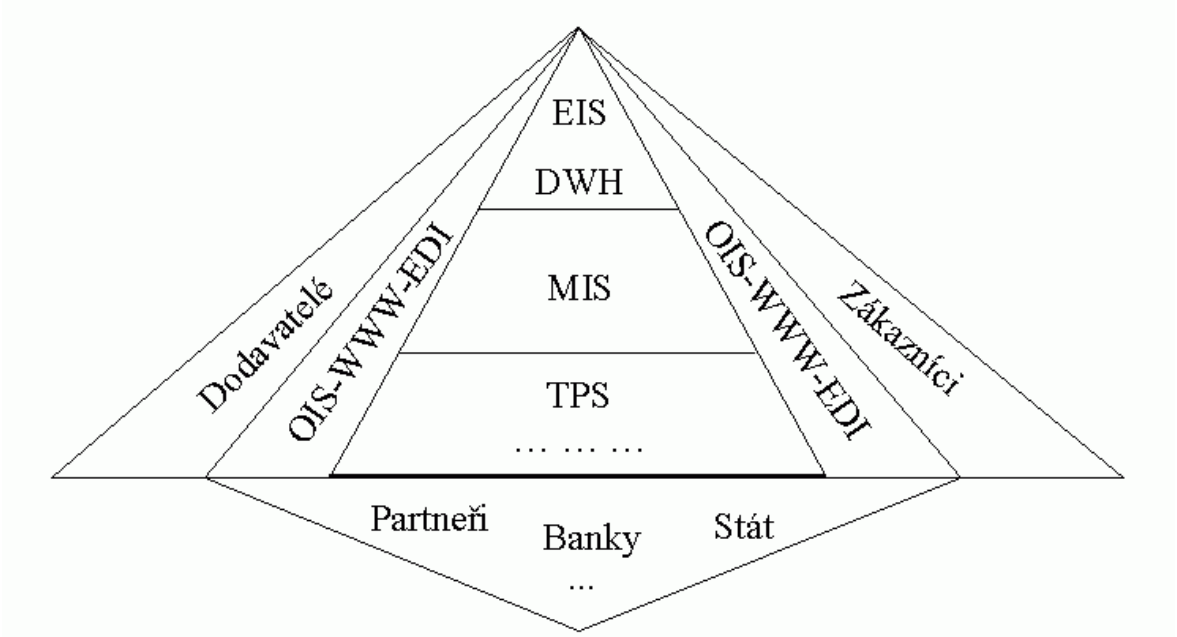
Jak jde vidět, vrstva technologická je nejnižší a vrstva prostředí nejvyšší. Znamená to, že vrstva prostředí zadává své požadavky na vrstvě aplikační, která pro uspokojení těchto požadavků vyžaduje využití vrstvy technologické. [5]

Typický informační systém moderního podniku se skládá z celé řady rozdílných aplikací IS/IT, které slouží k podpoře jeho různých oblastí. V rámci aplikační vrstvy se v podniku vyskytuje celá řada aplikací, které můžeme členit podle různých hledisek, které se vzájemně prolínají, a jejich vymezení není vždy jednoznačné.

Tyto aplikace se nacházejí v různých etapách své životnosti, a proto jsou některé z nich vyřazovány bez náhrady a některé z nich jsou nahrazovány novějšími verzemi. Také vznikají neustále nové aplikace na podporu podnikových procesů a tak je třeba se na informační systém dívat, jako na dynamicky se vyvíjející proces. [5]

4.1.1 Hlavní úrovně podniku – vertikální pohled

Z pohledu řízení je vhodné zobrazovat podnik v podobě pyramidy, jejichž jednotlivé úrovně představují různé stupně řízení. Tento model je v současné době velmi často nahrazován přístupy, které stimulují efektivnost činnosti týmů, flexibilitu pracovníků a vytvářejí důležité předpoklady pro celkovou odolnost podniku. [5]



Obr. 3 Hierarchická úroveň IS podniku [16]

Podle vztahu k úrovni řízení, se rozlišují aplikace IS/IT, zda jsou určené pro:

1) **Operativní úroveň řízení (TPS)**

Uživateli těchto aplikací jsou pracovníci, kteří mají za úkol zpracovávat data a vytvářejí v kancelářích zakázky, nabídky, připravují nové výrobky a služby pro další nabídky obchodníků a marketingu. [5]

2) Střední management (MIS)

Tuto úroveň představují pracovníci, kteří zajišťují včasnou, kvalitní a efektivní realizaci zakázek výrobků a služeb určených pro zákazníka. Tito pracovníci kladou velký důraz na kvalitu informací a jsou od nich vyžadovány také určité odborné znalosti. [5]

3) Vrcholový management (EIS)

Vrcholový management představuje nejvyšší úroveň řízení, určující podporující strategie a vize podniku, včetně informační, která je v souladu se zájmy jeho vlastníků. Zde jsou hlavním požadavkem zejména znalosti.

Pracovníci na jednotlivých úrovních podniku se odlišují nejenom svým postavením, ale i úkoly, které jsou s ním spojeny a kvalitními informacemi pro rychlejší rozhodování. Tomu odpovídají i softwarové a hardwarové prostředky. [5]

4.1.2 Hlavní podnikové funkce – horizontální pohled

V našich podnicích, bez ohledu na jejich skutečnou velikost, stále převládá standardní funkční uspořádání, které určuje i funkční architekturu jeho informačního systému. Tato funkční struktura je pak formalizovaná v podobě různých modulů a systémů, které slouží na podporu [5]:

- vytváření technologických postupů,
- marketingu,
- řízení výroby,
- plánování výroby,
- řízení prodeje a distribuce výrobků,
- řízení nákupu a skladů,
- řízení financí,
- řízení lidských zdrojů,
- řízení údržby a oprav technologického zařízení,
- řízení energetického hospodaření podniku atd.

Tyto vymezené prvky se nazývají vnitropodnikové útvary a vytvářejí dílčí funkční struktury (např. zásobovací, odbytové, výrobní apod.). V různých typech podniku jsou zastoupeny odlišné základní funkce respektující základní procesy v podniku.

Vedle těchto standardních funkčních oblastí aplikace IS/IT (marketing, finance apod.) v podniku, ještě členíme aplikace, které slouží pro podporu kancelářských prací (office automation), pro řízení technologických procesů (proces automation) nebo pro podporu řízení vlastního IS/IT v podniku (metainformation systems). [5]

4.2 Etapy životního cyklu IS/IT podniku

Je třeba si uvědomit, že IS/IT podniku není jediný osamocený produkt, ale že lze hovořit o jednotlivých složkách, které si do jisté míry žijí svůj vlastní autonomní život a jejich integrace je realizována pouze vzájemnou komunikací. Z hlediska aplikačního se jedná o celou paletu úloh a programů, které slouží k podpoře řízení různých oblastí podnikání a to z pohledu věcného i řídícího. Z hlediska funkčního, se pak jedná o komplex technických, programových, lidských a datových zdrojů, které dohromady vytvářejí informační strukturu podniku. [5]

Každá z těchto aplikačních či funkčních částí se může nacházet v různých etapách životního cyklu, který je zpravidla tvořen těmito částmi:

1) **Plánování**
   - jedná se o část, ve které se rozhodujeme CO? opravdu potřebujeme, JAK? to získat, k ČEMU to potřebujeme a jaký z toho budeme mít UŽITEK;
2) **Pořízení** (výstavba)
   - zde řešíme, jak pořídíme jednotlivé části IS/IT a to buď tím, že si požadovanou část zakoupíme, nebo si ji sami vyvineme, či vyrobíme;
3) **Zavádění** (implementace)
   - etapa, ve které je nakoupená nebo vyvinutá část IS/IT zaváděna do praxe, což bývá často spojeno s řadou procesních, organizačních i personálních změn v podniku;
4) **Rutinní provoz** (užívání)
   - tj. část, ve které užíváme zavedenou část IS/IT v provozu;
   - v průběhu tohoto procesu dochází většinou k postupnému „vylepšování“ systému tak, jak se objevují různé chyby a nedostatky během jeho užívání;
   - v některých případech vznikají také nové požadavky, které je třeba dosetému zpracovat;
   - proto se také často hovoří o etapě údržby systému;
5) **Likvidace**
   - v této etapě dochází k ukončení životního cyklu dané části IS/IT. [5]

Jednotlivé etapy životního cyklu zkoumáme ze tří různých hledisek a to z pohledu **věcného** (co všechno v nich lze vykonat), z pohledu **časového** (jak dlouho má daná etapa trvat), tak i z pohledu **ekonomického** (kolik budeme potřebovat finančních prostředků a jaký bude z dané etapy náš užitek). Průběh nákladů v čase je samozřejmě odlišný podle toho, zda si IS/IT pořizujeme dodavatelským způsobem, vlastním vývojem nebo určitou kombinací obou těchto způsobů. [5]

4.3 Vrstvená architektura a systémový integrátor

Vrstvená architektura IS/IT podniku má tu velkou výhodu, že lze vyměňovat zastarávající částí informačního systému, aniž by se to nějak významně dotklo funkce ostatních jeho částí. To umožňuje rozvíjet informační infrastrukturu podniku, což ovšem vyžaduje mít dobře zpracovanou **informační strategii podniku**, která určuje celkový charakter rozvoje informatiky v organizaci.

Systémová integrace slouží k tomu, aby všechny částí IS/IT podniku fungovaly jako jeden logický celek i v tom případě, že se jedná o produkty různých výrobců a různého funkčního určení. V případě důsledně vrstvené architektury, se jedná o problém rozhraní (interface) mezi jednotlivými částmi systému. Úloha systémové integrace se vyvíjela podle toho, jak se posunovala důležitost jednotlivých částí IS/IT směrem od vrstvy technologické k vrstvě prostředí. [5, 6]

Dnešní systémová integrace zahrnuje především:

- na strategické úrovni připojení podnikatelských záměrů do informační strategie (rozhraní mezi vrstvou prostředí a aplikační vrstvou);
- na projektové úrovni vytvoření konzistentní architektury a navržení procesů IS/IT (rozhraní mezi aplikacemi);
- na řídící úrovni optimalizaci organizace a řízení dodávek komponent IS/IT od všech subdodavatelů, včetně zákazníka (rozhraní mezi aplikační a technologickou vrstvou);
- na technicko-technologické úrovni propojování hardwaru a softwaru do komplexního celku (rozhraní mezi jednotlivými technologickými komponentami);

Úkoly systémové integrace jsou zajišťovány v podniku prostřednictvím **systémového integrátora.** Může jim být vlastní podnikový útvar pro IS/IT (interní systémový integrátor), pokud tedy disponuje příslušnými odborníky, ale častěji tuto úlohu plní jiné firmy (externí systémový integrátor). [7]

Podle toho, na jakou z těchto rovin systémové integrace dává systémový integrátor přednost, rozeznáváme tyto základní typy systémových integrátorů:

1) **Stratég**
   - jeho doménou je informační strategie;
   - měřítkem účelnosti projektů a aktivit je podpora podnikatelské strategie;
   - stratég se zaměřuje na to, proč a s jakými cíli je potřeba do IS/IT investovat;
   - u každého projektu vyhledává přínosy a snaží se je převést do měřitelných cílů;
2) **Projektant**
   - začíná systémově integrační projekty návrhem řešení, aniž by se zabýval širšími souvislostmi na jiné projekty nebo podnikatelské záměry;
   - jeho pojetí systémové integrace nejlépe odpovídá realizaci projektu, při kterém je na začátku projektu provedena analýza řešení až do úplného detailu, ta je akceptována a schválena vedením podniku, poté následují jednotlivé implementační kroky až po uvedení do provozu;
   - tím, že se na začátku jasně definuje cílový stav, je velmi obtížné provádět změny v průběhu realizace projektu;
3) **Manažer**
   - soustřeďuje se na řídící výstupy systémově integračních projektů, především na jejich nákladové a časové aspekty;
   - manažer definuje řídící struktury podniku, způsob řízení projektu, změnové řízení, řídící procedury s důrazem na zabezpečení kvality, předávací a reklamační procedury;
4) **Technik**
   - považuje propojení systémových komponent za jádro systémové integrace;
   - technik dá většinou uživateli k odzkoušení „nehotový“ prototyp systému a ten pak následně dle jeho připomínek „dodělává“. [5]

V praxi se samozřejmě tyto typy systémových integrátorů nevyskytují v čisté podobě, ale jedná se kombinaci všech těchto typů. Záleží na tom, který z nich se stane v podniku dominantním. [5]

Podnikový IS lze rozdělit do několika oblastí, pro které jsou přiřazeny různé přístupové úrovně i pravomoci, kterými jejich uživatelé disponují. Pro úspěšné fungování systému podniku je třeba znát jeho architekturu a různé principy integrace, která propojuje odlišné prvky různých systémů. Následující praktická část zahrnuje implementaci celé problematiky bezpečnosti IS na konkrétním příkladu firmy.

II. PRAKTICKÁ ČÁST

5 POPIS FIRMY

5.1 Charakteristika

Firma s.r.o., která je předmětem výzkumu v mé diplomové práci, provozuje 455 maloobchodních prodejen po celé České republice a její hlavní sídlo je v Ostravě – Martinov. Byla založena v roce 1992 a svou činnost provozuje až do současnosti. Za tuto dobu si tato společnost zajistila pevné místo na tuzemském trhu, o čemž svědčí roční obrat firmy, který za uplynulý rok činil přes 8 miliard korun. Základní kapitál, který je rozdělen mezi tři společníky, činí 78 000 000 Kč. Svou specializací firma se zaměřuje především na potravinářské zboží (tvoří cca 70 % sortimentu), ale také zboží nepotravinářského charakteru (tvoří cca 30 % sortimentu), jako je drogerie, domácí a kancelářské potřeby. Druhá hlavní pobočka této společnosti se nachází v Uherském Brodě, ze kterého je zásobována jižní a východní Morava.

Společnost také vlastní pekárnu, odkud distribuuje pečivo do svých maloobchodních jednotek a podílí se také na výrobě různých produktů, které jsou označeny logem firmy. Tyto produkty pro společnost ve vzájemné spolupráci vyrábí i jiné firmy. Zákazníci si tak mohou vybrat z celé řady kvalitních firemních výrobků.

Management řízení je hierarchicky rozdělen na dílčí řídící funkce, jako například ředitel maloobchodu, ředitel společnosti, finanční ředitel, ředitel nákupu a prodeje potravin, vedoucí velkoskladu, vedoucí IT a také různá oddělení, jako oddělení nákupu potravin, reklamační oddělení velkoskladu, přímé dodávky na MO, oddělení nákupu ovoce a zeleniny, oddělení nákupu drogerie, oddělení prodeje drogerie a oddělení velkoobchodního prodeje potravin.

Hlavním cílem společnosti je výroba a distribuce zboží v co nejvyšší kvalitě tak, aby byly uspokojeny potřeby zákazníků v co největší míře. Tento cíl je potřeba neustále zdokonalovat a vyvíjet ať už ze strany jakosti, tak i ze strany zaměstnanců, protože konkurenční vliv v tomto obchodním prostředí je velký.

5.2 Popis vnitřních informačních toků v organizaci z pohledu řízení

Firma je z hlediska organizační struktury rozdělena do několika úrovní a oddělení, která byla uvedena již v předchozí charakteristice. Mezi těmito odděleními fungují různé informační toky, které jsou realizovány s menší nebo větší efektivitou. Datové toky však neprobíhají pouze uvnitř firmy, ale také vně a to prostřednictvím dodavatelů a odběratelů, které lze v rámci obchodního styku zařadit mezi subjekty patřící do informačního systému firmy.

V rámci těchto probíhajících informačních toků mezi různými odděleními firmy je využíván informační systém, který byl navrhnut a naprogramován speciálně pro tuto organizaci a je tedy jakýmsi „vlastním produktem“, který je využíván pro výměnu a práci s daty. Struktura výměny dat je v této firmě realizována od nejvyšší úrovně vedení, tedy od vrcholového managementu přes střední úroveň řízení až po operativní úroveň řízení, jejichž pravomoci a práce s informacemi jsou velmi odlišené.

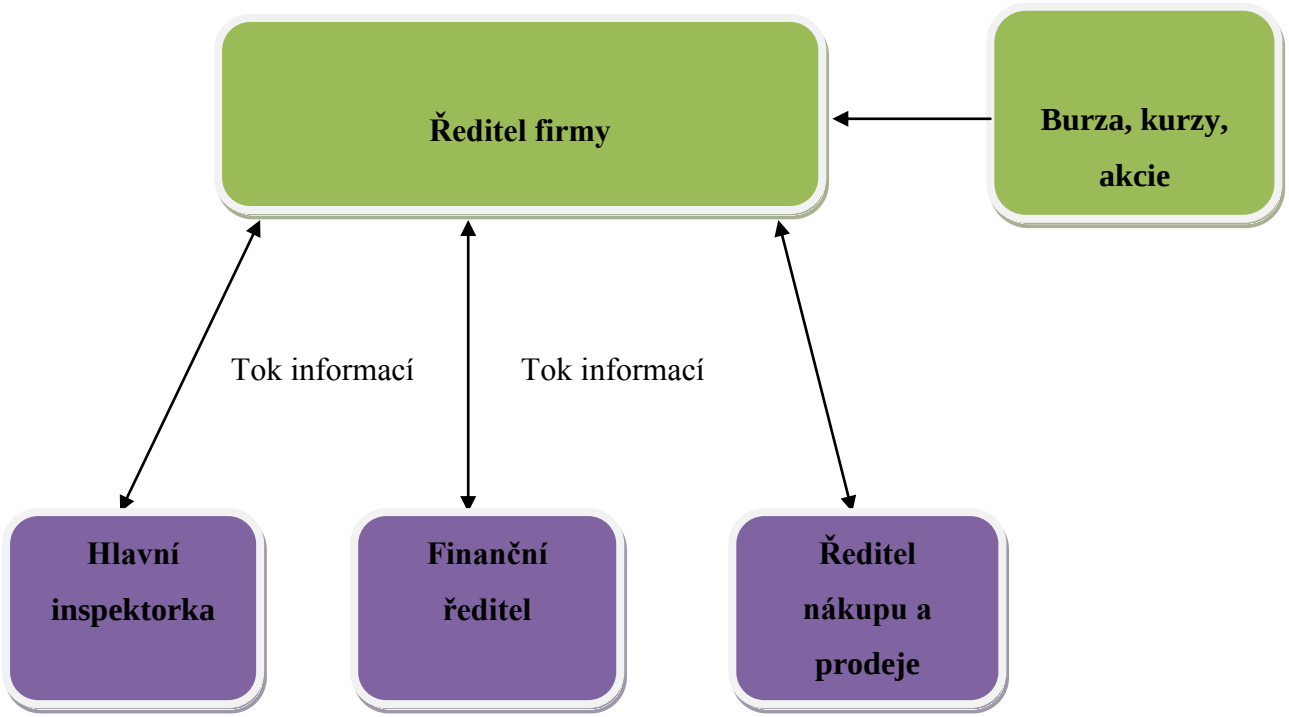
5.2.1 Vrcholový management

Tuto funkci zde plní ředitel firmy, který zodpovídá za fungování organizace jako celku a jsou mu podřízeny všechny nižší oblasti řízení, zejména strategická úroveň, která tvoří nejužší spolupráci s hlavním řízením firmy. Informace o stavu prodejen, měsíčních tržeb apod. jsou zde zprostředkovávány prostřednictvím hlavní inspektorky, která je zodpovědná za chod jednotlivých prodejen. Hlavní inspektorka je tím, kdo na pravidelných poradách prostřednictvím měsíčních výkazových správ předkládá informace, které jsou důležité pro rozhodování v oblasti marketingu, financování, reklamy a celkového budoucího vývoje firmy. Ředitel firmy získává také informace z vnějšího prostředí a to z burzy, kde musí sledovat investiční zdroje.

Hlavnímu vedení firmy jsou samozřejmě podřízeny i další vedoucí pozice na střední úrovni managementu, jako je finanční ředitel, který má za úkol ekonomickou a finanční prosperitu organizace a jeho největším úkolem je také posuzování rizikovosti různých investic a projektů, které chce firma realizovat.

Dalším, kdo se na této úrovni řízení nachází, je ředitel nákupu a prodeje potravin, který má ve své kompetenci tři hlavní úkoly:

a) rozhodovat o nákupu zboží, které bude pro organizaci co nejvíce ziskové;
b) vytvářet marketingovou strategii na nabídku akčního druhu zboží;
c) účastnit se měsíčních porad a seznamovat hlavní vedení organizace s možným budoucím vývojem co se týká nákupu a prodeje potravin.



Obr. 4 Informačního tok vrcholového managementu [zdroj: vlastní]

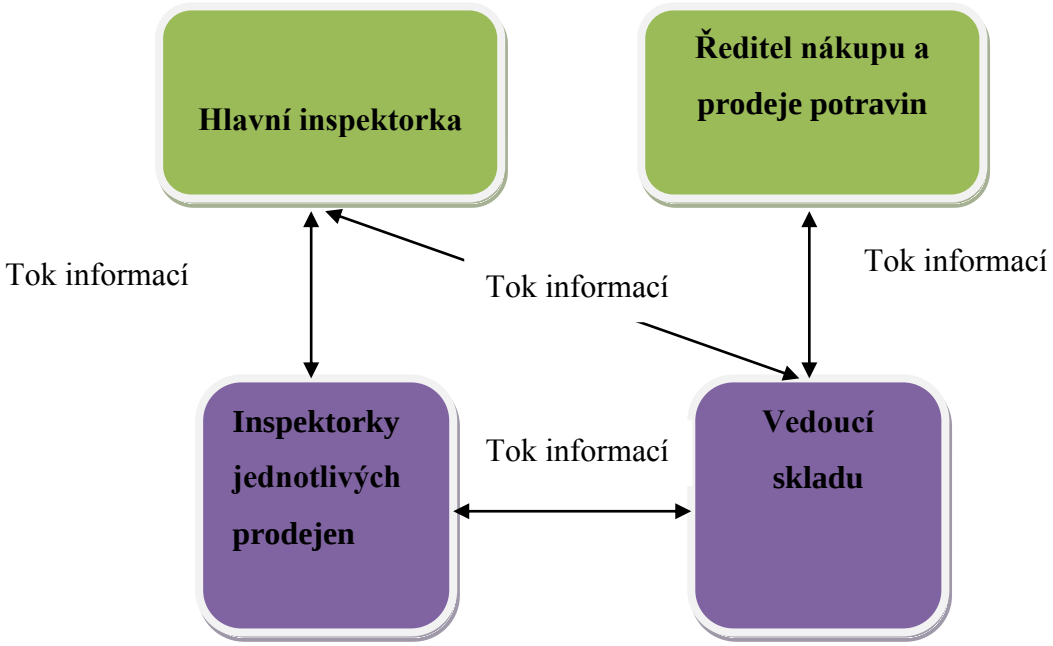
5.2.2 Střední management

Na této úrovni řízení se nachází inspektorky jednotlivých prodejen, mezi jejichž hlavní náplň patří koordinace a řízení jednotlivých maloobchodních jednotek, zpracovávání měsíčních správ pro hlavní inspektorku atd. Nejdůležitější komunikační vazbou je zde výměna informací mezi hlavní inspektorkou a inspektorkami jednotlivých prodejen.

Hlavní inspektorka nicméně komunikuje nejen se střední úrovní managementu, ale také s nejnižší úrovní managementu, tedy s operativním řízením, nicméně tato komunikace je velmi sporadická. Většina zástupců operativního řízení (jednotliví vedoucí prodejen),

komunikuje se svými inspektorkami, které jsou jim podle regionálního umístění přidělené a ty poté danou problematiku předkládají své hlavní inspektorce.

Posledním, kdo se na této úrovni řízení nachází, je vedoucí skladu. Tato pozice je vykonávána na dvou pracovištích a to jednak v hlavním sídle firmy v Ostravě – Martinov a také v Uherském Brodě, kde se rovněž nachází sklad firmy. Funkce vedoucí skladu slouží zejména pro řízení nákupu a uskladnění zboží, jeho kontrolu, odbyt a zásobování zbožím pro daný region. Vedoucí skladu je přímým podřízeným ředitele nákupu a prodeje potravin. V praxi jsou tyto dvě pozice úzce provázány, protože vzájemná komunikace a výměna informací jsou zde nezbytnou součástí dobře fungujícího skladového hospodářství. Vedoucí skladu má také za úkol, koordinovat a řídit své podřízené, kterými jsou zaměstnanci skladu, kteří plní funkce jako správné uskladnění zboží, nakládku zboží, kontrolu kvality a datumu spotřeby, úklid skladu apod.



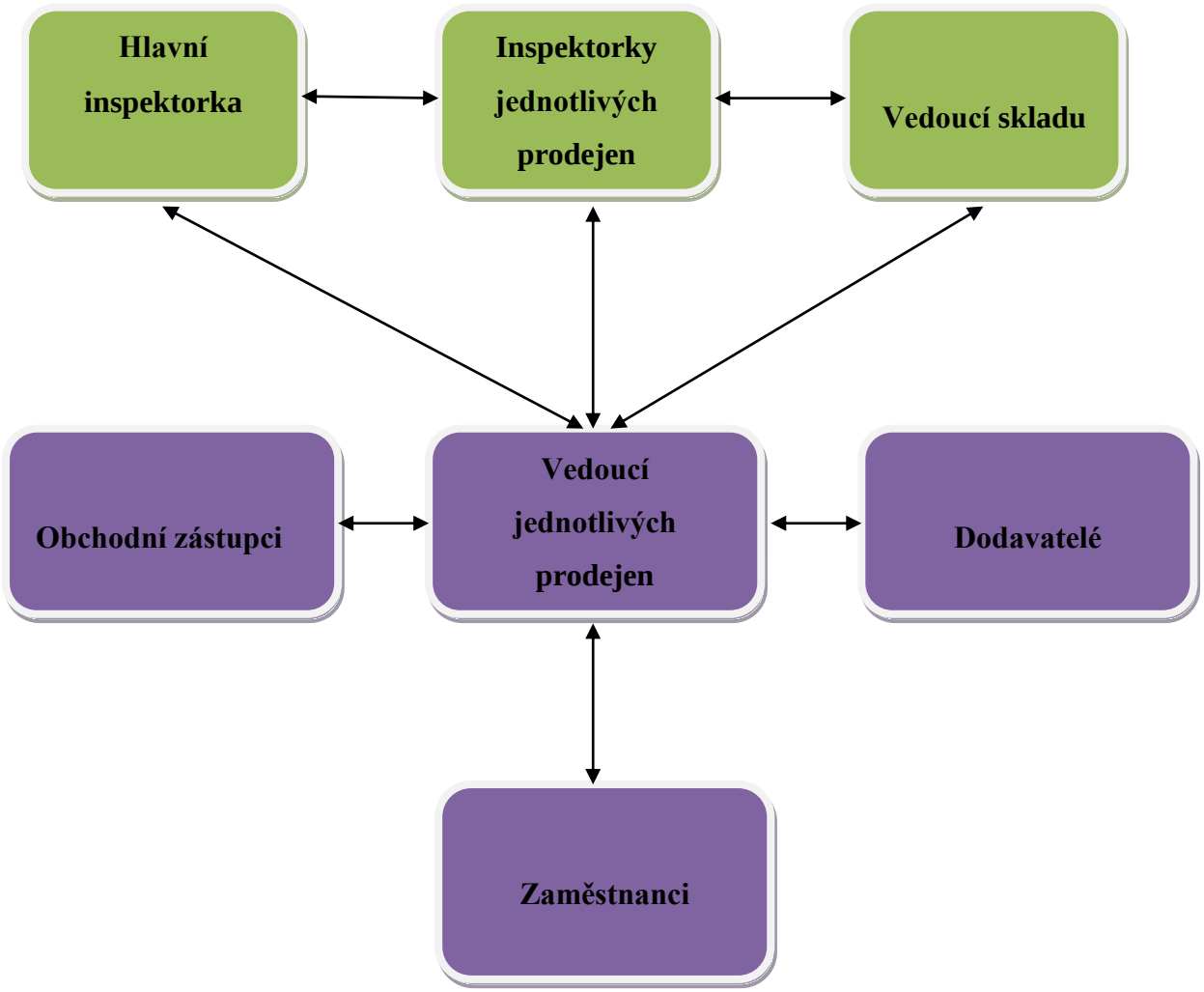
Obr. 5 Informační tok středního managementu [zdroj: vlastní]

5.2.3 Operativní management

Nejnižší úroveň řízení je zde zastoupena zejména jednotlivými vedoucími prodejen, kteří mají za úkol řídit management svých prodejen, který zahrnuje především řízení zaměstnanců, objednávání zboží, zajištění a kontrolu bezpečnosti práce, kontrola jakosti a kvality zboží, jednání se zástupci jednotlivých firem, jejichž zboží je v rámci tohoto

obchodního řetězce nabízeno a také vedení účetnictví. Vedoucí jednotlivých prodejen poskytují informace zejména své nadřízené inspektorce, která je jim přidělena, popř. s hlavní vedoucí inspektorkou. Dále zde probíhá informační tok také mezi prodejnou a skladem v daném regionu. Tato komunikace je zaměřena především na výměnu informací týkající se kvality zboží, reklamace a objednávání zboží. Jistá informační vazba je zde také s ředitelem firmy, ale nutno říci, že tato komunikace probíhá velmi zřídka. Jedná se spíše o výjimečné případy.

Vedoucí jednotlivých prodej tak komunikují především se svými vlastními zaměstnanci a s dodavateli a jejich zástupci, se kterými jsou v přímém obchodním styku a kteří navštěvují v pravidelných intervalech jednotlivé prodejny.



Obr. 6 Informační tok operativního managementu [zdroj: vlastní]

5.3 Popis vnějších informačních toků vůči organizaci

Z pohledu vnějších informačních toků, které směřují vně nebo dovnitř organizace, jsou zde zahrnuty převážně subjekty, které jsou v přímém kontaktu s firmou v rámci plnění svých pohledávek a závazků vůči organizaci a mezi které lze zahrnout:

5.3.1 Dodavatelé

Skupina dodavatelů je velmi široká a představuje nejrůznější činnosti od dodávky materiálů a surovin až po hotové zboží, výrobky a služby. Mezi materiál, který je dodáván firmě lze zahrnout například technické vybavení pro skladování (regály, paletizační vozíky, vysokozdvižné vozíky, chladící zařízení, police, apod.), které slouží nejen pro hlavní sklady firmy, ale také pro jednotlivé prodejny, pokud je třeba nahradit staré vybavení novým. Dále zde patří dodávání surovin, které slouží pro výrobu vlastních firemních výrobků a polotovarů (těsto, pomazánky apod.) a také samozřejmě dodávání samotných potravinářských a nepotravinářských výrobků.

V rámci dodavatelsko – odběratelských vztahů, je pro zachování stability informačních a komunikačních toků, kladen důraz především na včasné uhrazení pohledávek, které jsou evidovány v systému firmy. Pro tento účel je zde navrhnut speciální program, který eviduje všechny závazky vůči dodavatelům, splatnosti faktur, odchozí bankovní transakce apod. Tento program také přímo umožňuje koordinovanou spolupráci s programem na vedení účetnictví, ve kterém se evidují všechny účetní případy firmy vůči dodavatelům.

Zatím zde byly popsány pouze vztahy dodavatele vůči organizaci, nicméně tento vztah je realizován i v opačném směru, ve kterém vystupuje organizace jako dodavatel vůči jiným subjektům. V tomto případě zde neprobíhá takové množství operací, jako v předchozím. Zde je možné zahrnout například dodávání výrobků jiným soukromým firmami, se kterými má organizace smlouvu o prodeji jejího zboží, čili tzv. franšízing.

5.3.2 Odběratelé

Ve skupině odběratelů neprobíhá tolik informačních komunikačních a finančních toků, jako v předchozí skupině. V tomto případě je možné zde zahrnout již zmíněný franšízing, kde firma, které daná organizace dodává zboží v rámci smluvního ujednání, vystupuje jako odběratel. V případě této konkrétní organizace zde ale nejsou realizovány jiné odběratelské vztahy, jako v případě jiných subjektů.

5.3.3 Banka

Banka patří mezi subjekt, který má v rámci vnějších informačních toků jednu z nejvýznamnějších funkcí a to především z důvodu finančních transakcí, které jsou v rámci platebního styku realizovány. Banka je důležitým článkem, jak ve vztazích týkající se dodavatelů a odběratelů, tak ve financování vnitřních záležitostí organizace, jako je vyplácení mezd apod.

Finanční transakce spojené vyplácením mezd zaměstnancům jsou prováděny samotnou bankou a to prostřednictvím předem nastavených odchozích plateb z účtu firmy. Firma podá částku, kterou je třeba vyplatit pro každého zaměstnance a banka tuto platbu uskuteční.

Zadávání částek je prováděno v rámci integrace dvou systémů a to účetního systému firmy a bankovního systému. Tato integrace je velmi přínosná, protože firma uskutečňuje velké množství plateb a v rámci propojení těchto dvou prků je tato činnost mnohem rychlejší a efektivnější. Nutno zmínit, že tato integrace je placenou službou banky, u které má organizace zřízený účet.

5.3.4 Veřejná správa

Komunikace s veřejnou správou probíhá zejména v případě přiznávání DPH za každé čtvrtletí. Tato komunikace již od roku 2014 probíhá pouze elektronicky. V tomto případě se podává v elektronické podobě daňové přiznání, dodatečné daňové přiznání, přílohy k daňovému přiznání a hlášení.

Tato instituce samozřejmě není jedinou ve veřejné správě, se kterou firma komunikuje. Dále zde probíhá pravidelná výměna informací s úřadem práce a to v případě nabídky nových pracovních míst, dále pak se Státním úřadem bezpečnosti práce a se Státní zemědělskou a potravinářskou inspekcí, ale to pouze v případech zjištění nevyhovujících podmínek, které náleží do působnosti těchto dvou institucí.

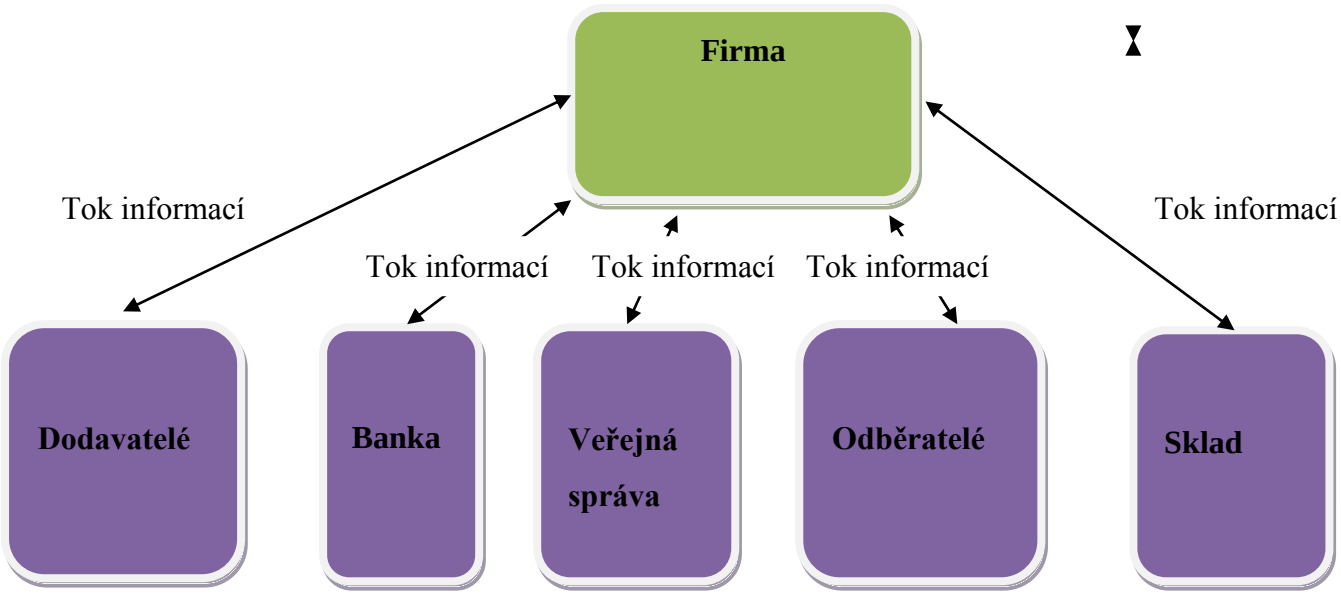
Další subjekty veřejné správy jsou Česká správa sociálního zabezpečení, kde se odvádí sociální pojištění a samozřejmě také zdravotní pojišťovny, kde je odváděno zdravotní pojištění.

5.3.5 Sklad

Sklad, jako samostatný subjekt svou existencí sice náleží spíše do vnitřní struktury firmy, nicméně plní jisté důležité funkce v rámci dodavatelsko – odběratelských vztahů. Skladová agenda a hospodářství zaujímá v rámci informačního systému jakési místo „prostředníka“, tedy toho, kdo zprostředkovává dodávání zboží nejen mateřským prodejnám firmy, ale také jiným obchodníkům, se kterými má organizace uzavřenou smlouvu.

Další funkcí skladu, je jeho odběratelská pozice, protože v tomto případě opět zaujímá místo „prostředníka“ a to v případě, kdy firma nakupuje materiál, popř. suroviny, které chce dále zpracovávat. Suroviny a materiál jsou zde uskladňovány pro jejich další využití nebo pro další distribuční cestu, která vede až ke konečnému spotřebiteli.

Na skladové hospodářství, je třeba pohlížet v tomto případě jako na vnější subjekt, protože skladové prostory jsou v rámci této organizace realizovány externí formou a proto plní také specifické funkce, které nelze zařadit pod jeden firemní subjekt.



Obr. 7 Vnější informační toky vůči organizaci [zdroj: vlastní]

6 BEZPEČNOSTNÍ SITUACE V ORGANIZACI

6.1 Informační systém firmy

Pro výměnu informací a dat je v rámci organizace navržen speciální systém, který by vyvinut výhradně pro tento účel. Cílem tohoto systému je poskytnout kvalitní a rychlé nástroje pro komunikaci, která má zajistit efektivní spolupráci jednotlivých maloobchodních jednotek s hlavní centrální organizací.

Tento systém je také určen pro správu objednávek, které jsou realizovány prostřednictvím kódů zboží, které jsou zadávány do objednávek a následně odesílány do skladu firmy. Systém má také vlastní databázi výrobků, které jsou do ní vkládány a registrovány prostřednictvím šestimístných číselných kombinací. U každého výrobku je uveden jeho název, gramáž, cena, marže, DPH a EAN. Prostřednictvím této databáze jsou poté tyto výrobky importovány do objednávkového listu.

Systém také umožňuje zboží vyhledávat prostřednictvím vyhledávacího pole, do kterého stačí zadat část názvu výrobku nebo také pomocí kódu EAN. V rámci editace dat systém umožňuje úpravu, popř. odstranění některých informací. Některé z těchto úkonů může ovšem provádět pouze administrátor systému. Běžný uživatel má k dispozici pouze omezený počet funkcí, týkající se trvalé změny nebo odstranění dat.

V rámci komunikace mezi firemními subjekty, je zde využíván Windows Live Mail, což je bezplatný e-mail klient, který je součástí operačního systému Windows Vista. Prostřednictvím tohoto programu je realizována komunikace jednotlivých MO prodejen s centrální organizací.

Mezi další funkce systému patří vedení tzv. pokladního deníku, který slouží pro vypisování a zaznamenávání tržeb a platebních karet za určité časové období. Pokladní deník je předem naformátovaný soubor, který je vytvořen v programu MS EXCEL. Jedná se o jednoduchou, avšak důležitou evidenci finančních údajů organizace.

6.2 Analýza rizik informačního systému firmy

Pro analýzu rizik souvisejících s informačním systémem firmy jsem zvolil nejprve standardní postup analýzy rizik, skládající se z identifikace rizik jednotlivých částí systému a poté identifikace hrozeb a zranitelností. Dále jsou tyto údaje rozpracovány pro detailnější přehled v matici rizik.

1) **Identifikace a ocenění aktiv**

   Pro označení důležitosti aktiv, která vyplývají z předchozího popisu IS, jsem zvolil číselnou škálu od 1 do 5, přičemž číslo 5, je označení pro nejdůležitější aktivum. Identifikace je znázorněna v následující tabulce.

Tab. 1 Identifikace aktiv v informačním systému firmy

Aktivum	Identifikovaná aktiva	Hodnota aktiva
Hardware	PC, tiskárna, scanner	4
	Server	3
Software	Databázové systémy	3
	Operační systémy	4
Informace	Databáze serveru	5
	Databáze skladu	5
	E-mail	5
Služby	Připojení PC k internetu	4
	Připojení k serveru	5

2) **Identifikace hrozeb a zranitelností**

   Dalším krokem je identifikace hrozeb a zranitelností. Pro aktiva, která byla identifikována výše, jsou zde přiřazeny různé druhy zranitelností. V tabulce jsou uvedeny pravděpodobnosti hrozeb spolu s příklady zranitelností. Pro určení pravděpodobnosti, je zde opět použita číselná škála od 1 do 5, kdy číslem 5 je označena nejpravděpodobnější hrozba. I zde je dobré připomenout, že jedna hrozba

může mít více druhů zranitelností a jedna zranitelnost může být využita například více druhy hrozeb.

Tab. 2 Identifikované hrozby a související zranitelnosti

Hrozba	Pravděpodobnost hrozby	Příklad zranitelností
Selhání software	3	Neefektivní nastavení a naprogramování aplikací
Selhání hardware	3	Náchylnost zařízení na prach a vlhkost
Odcizení aktiv	2	Nedostatečná fyzická ochrana dveří, oken a budov
Selhání komunikačních služeb	4	Nechráněná veřejná síťová připojení
Požár, Povodeň	1	Umístění v místech náchylných k požárům a povodním
Neúmyslná modifikace	5	Nedostatečný bezpečnostní výcvik
Kybernetický útok	5	Nedostatek aktualizací software na ochranu před kybernetickými útoky

3) **Analýza rizik využívající matici aktiv, zranitelností a hrozeb**

Při tomto postupu zde bude využíváno dvou tabulek. První z nich zobrazuje aktiva a identifikované hrozby s jejich hodnotami. V dalším kroku je posouzena zranitelnost jednotlivými hrozbami. Tuto matici zranitelnosti můžeme vidět v tabulce č. 3. V případě, kdy nedochází k interakci zranitelnosti s příslušnou hrozbou, zůstává toto pole prázdné. Opět je zde použita stupnice od 1 do 5, kdy číslem 5 je označena nejpravděpodobnější hrozba.

Tab. 3 Matice zranitelnosti

Matice zranitelnosti	Popis aktiva	PC, tiskárna, scanner	Server	Databázové systémy	Operační systémy	Databáze serveru	Databáze skladu	E-mail	Připojení PC k internetu	Připojení k serveru
	Hodnota aktiva (H)	4	3	3	4	5	5	5	4	5
Popis hrozby	**Pravděpodobnost hrozby (T)**									
Selhání software	3			2	2					
Selhání hardware	3	3	2							
Odcizení aktiv	2	3	2							
Selhání komunikačních služeb	4							4	4	3
Požár, Povodeň	1	2	1							
Neúmyslná modifikace	5					3	4			
Kybernetický útok	5			3	4					

Dalším a také posledním krokem je výpočet míry rizika. Tato hodnota je vypočítána pomocí vzorce **R = T * H * V**, kde **R** je míra rizika, **T** je pravděpodobnost hrozby, **H** je hodnota aktiva a **V** je zranitelnost aktiva. Prostřednictvím tohoto vzorce je vypočítána matice rizik, která je uvedena v tabulce č. 5. Pro upřesnění a přehlednost výsledků rizik je níže vytvořena stupnice, kde jsou hodnoty rozděleny do tří kategorii, podle jejich závažnosti a dopadu na daná aktiva. Tyto kategorie jsou také pro lepší přehlednost barevně rozlišeny.

Tab. 4 Stupnice závažnosti rizik

Riziko	**Rozmezí hodnot**	**Barva**
Nízké riziko	1 až 30	
Střední riziko	30 až 65	
Vysoké riziko	65 a více	

Tab. 5 Matice rizik

Matice zranitelnosti	Popis aktiva	PC, tiskárna, scanner	Server	Databázové systémy	Operační systémy	Databáze serveru	Databáze skladu	E-mail	Připojení PC k internetu	Připojení k serveru
	Hodnota aktiva (H)	4	3	3	4	5	5	5	4	5
Popis hrozby	**Pravděpodobnost hrozby (T)**									
Selhání software	3			18	24					
Selhání hardware	3	36	18							
Odcizení aktiv	2	24	12							
Selhání komunikačních služeb	4							80	64	60
Požár, Povodeň	1	8	3							
Neúmyslná modifikace	5					75	100			
Kybernetický útok	5			45	80					

Z matice rizik vyplývá, že největšími riziky pro firmu jsou kategorie selhání komunikačních služeb, konkrétně e-mailu. Dále zde hrozí vysoké riziko neúmyslné modifikace, která je v organizaci častým jevem a jejíž následky bývají velmi obtížně odstranitelné. Posledním vysokým rizikem je kybernetický útok na operační systémy, který by mohl být zaměřen například na získání utajených informací firmy, někdy také nazývané. „know-how“.

Mezi střední rizika lze zařadit selhání hardware, připojení PC k internetu a k serveru a také kybernetický útok na databázové systémy. Mezi nízká rizika pak lze zařadit selhání software, což se děje velmi zřídka, selhání hardware u serveru, odcizení aktiv a také požár nebo povodeň. Většina těchto aktiv nebyla nikdy přímo v organizaci ohrožena.

4) **Analýza rizik vyhodnocující pravděpodobnost incidentu a jeho dopad**

   Tento postup je dalším možným způsobem, jak vyhodnotit riziko dopadu nežádoucí situace, která by mohla mít velký vliv na fungování celé organizace. Tato metoda ovšem prezentuje ovšem zcela odlišný přístup k analýze rizik, než metoda předchozí. V tomto případě je využíváno pouze dvou parametrů a to pravděpodobnost incidentu a jeho dopad. Stejně jako při běžném postupu analýzy rizik je potřeba určit nejprve aktiva a jejich hodnotu. Dále je třeba k jednotlivým aktivům identifikovat hrozby, zranitelnosti a stávající opatření.

   Dopad je v tomto případě zvolen podle hodnoty aktiva, nicméně v některých případech je hodnota nižší a to z důvodu možnosti částečného poškození aktiva, nikoliv úplného poškození nebo zničení. Tato metoda analýzy rizik je mnohem přesnější a detailněji zpracována a proto poskytuje více holistický přístup k dané problematice. Stupnice analýzy rizik je zde stejná, jako v předchozím případě. Míra rizika je vypočítána pomocí vzorce: **R = PI x D**.

Tab. 6 Analýza rizik

Aktivum	Druh aktiva	Hodnota	Hrozba	Zranitelnosti	Pravděpodobnost incidentu	Dopad	Riziko	Opatření
Hardware	PC, tiskárna, scanner	4	Selhání hardware, Požár, Povodeň	Náchylnost zařízení na prach a vlhkost. Umístění objektu v rizikovém prostředí	11	(3 + 1) = 4	(36 + 8) = 44	Pravidelná údržba a čištění. Umístění hardware ve vyšším patře budovy
	Server	3	Selhání hardware, Požár, Povodeň	Náchylnost zařízení na prach a vlhkost. Umístění objektu v rizikovém prostředí	5,25	(3 + 1) = 4	(18 + 3) = 21	Pravidelná údržba a čištění. Umístění hardware ve vyšším patře budovy
Software	Databázové systémy	3	Selhání software, Kybernetický útok	Neefektivní nastavení a naprogramová ní aplikací. Nedostatek aktualizací softwarena ochranu před kybernetickými útoky	7,88	(3 + 5) = 8	(18 + 45) = 63	Pravidelné aktualizace a ochrana prostřednic tvím kvalitního antiviru
	Operační systémy	4	Selhání software, Kybernetický útok	Neefektivní nastavení a naprogramová ní aplikací. Nedostatek aktualizací software na ochranu před kybernetickými útoky	13	(3 + 5) = 8	(24 + 80) = 104	Pravidelné aktualizace a ochrana prostřednic tvím kvalitního antiviru
Informace	Databáze serveru	5	Neúmyslná modifikace	Nedostatečný bezpečností výcvik	15	5	75	Pravidelné zálohování
	Databáze skladu	5	Neúmyslná modifikace	Nedostatečný bezpečnostní výcvik	20	5	100	Pravidelné zálohování
	E-mail	5	Selhání komunikačních služeb	Nekvalitní síťové připojení	16	5	80	Pravidelné kontroly síťového propojení
Služby	Připojení PC k internetu	4	Selhání komunikačních služeb	Nechráněná veřejná síťová připojení	16	4	64	Pravidelné kontroly síťového propojení
	Připojení k serveru	5	Selhání komunikačních služeb	Nechráněná veřejná síťová připojení	12	5	60	Pravidelné kontroly síťového propojení

6.2.1 Závěr a návrh možných opatření

Cílem provedené analýzy rizik byla identifikace aktiv, která jsou důležitá pro zachování bezpečného fungování celé organizace na všech úrovních od technického zabezpečení jednotlivých systémů až po vzájemnou komunikaci mezi jednotlivými subjekty. Výstupem této analýzy jsou pak pravděpodobnosti hrozeb rozdělených podle jejich závažnosti. K těmto hrozbám jsou také přiřazeny jednotlivé hodnoty, které umožňují jejich klasifikaci dle stanovené číselné stupnice.

Závěrem k této kapitole lze říci, že zde bylo použito několik postupů analýzy rizik, které na sebe navzájem navazují a jejichž výsledky poskytují ucelenější přehled o dané situaci v organizaci, o jejich aktivech, pravděpodobných hrozbách a také možných opatřeních, která by měla sloužit potenciálnímu manažerovi rizik k efektivnímu rozhodování a přijímají opatření, která budou mít pro firmu a její budoucí vývoj zásadní vliv.

Co se týká jednotlivých opatření, považuji za nutné zde zmínit lepší výstavbu programového vybavení. Systém pro správu informací, dodavatelů, odběratelů apod., je vytvořen a naprogramován soukromou firmou, u které byla zadán požadavek na vytvoření informačního systému, který by měl být vhodně implementován na řízení a informační podporu organizace. Vzhledem k nízkým požadavkům na náklady ze strany odběratele (tedy firmy), byl vytvořen systém, který sice splňuje zadané požadavky, ovšem jeho přehlednost a struktura je mnohdy zbytečně komplikovaná. Rozvržení systému je v některých případech nelogické a potřebné ovládací nebo informační prostředky se nacházejí v částech systému, kde by je běžný uživatel nehledal. Některé úkony jsou zde také zakázány administrátorem, což je v pořádku z pohledu bezpečnosti, ovšem týká se to i přístupu k operacím, které by uživatel mohl provádět pro zlepšení svého komfortu ovládání a efektivity a nemá k nim umožněn přístup. Zde bych tedy navrhl přehodnocení uživatelských práv a úrovní, protože některé z možných operací jsou uživatelům zbytečně znepřístupněny. Tudíž po této stránce systém nedostatečně splňuje jeden ze základních požadavků na IS firmy, totiž logické a intuitivní ovládání.

Dalším úskalím informačního systému firmy je jeho softwarové vybavení. Pro správu aplikací a systému je zde využíván výhradně software, který je bezplatný, tzv. free. Tato okolnost není sama o sobě rizikem, ale jsou zde použity starší verze těchto programů a tudíž je zde opět problém ovládání, popř. rychlosti ovládání. Některé aplikace nabízejí pouze základní úkony, které může uživatel provádět a efektivnější možnosti nejsou

k dispozici (z pohledu programového vybavení). Tato okolnost sice může být brána jako jisté bezpečnostní opatření, které brání neúmyslné modifikaci nastavených parametrů systému, ale také neumožňuje uživateli plné využití software.

Pro používání hardware a software IS firmy je využíváno osobních PC, které jsou nainstalovány na jednotlivých prodejnách. Tyto PC jsou starších typů, tudíž je zde opět problém nižší rychlosti spuštěných aplikací, popř. provozu celého systému. Často tak dochází k „zamrznutí“ počítače, což je řešitelné pouze restartem PC. Tento problém často nastává během spuštěných aplikací nebo prováděných úkonů a celý proces bývá nenávratně přerušen a ukončen. Tento problém může být samozřejmě způsoben více vlivy, jako například stavem hard disku, teplotou, viry apod. To se dá samozřejmě zjistit pomocí záznamu o chybách, kde lze přesně diagnostikovat příčinu. Vzhledem k tomu, že počet PC je velký (má ho 455 prodejen), tak jejich pravidelná údržba musí být zajištěna jednotlivými vedoucími prodejen, což ovšem klade nároky na jisté technické znalosti, kterými ne všichni disponují. Zde by bylo také dobré, provádět pravidelná školení (stačilo by jednou za dva roky například ve spojení s BOZP a PO), kde by se vedoucí zaměstnanci dozvěděli základní pravidla o správném využívání jejich počítačů a daných příslušenství.

V rámci poradenství, co se týká řešení problémů IS a provozních podmínek, je zde možnost kontaktovat firemního technika, který může po telefonu poskytnout rady, jak postupovat při řešení daného problému. Jedná se většinou ale o řešení problémů, kterým lze snadno předejít právě správnou informovaností a znalostmi, které většinou u zaměstnanců chybí. Protože řešení problémů, které vznikají ze zbytečných příčin, dochází ke ztrátě času, který může být využit pro smysluplnější činnosti, týkající se provozu MO jednotky. Čas je dnes velmi drahocenný, tudíž by nemělo docházet k jeho zbytečnému plýtvání.

Níže přikládám tři možná řešení, kterými by bylo možné nedostatky odstranit. Jedná se o varianty s využitím různých zdrojů a pohledů na danou problematiku, které mohou přispět k řešení a zlepšení stavu IS firmy a k efektivnějšímu využívání hardware a software.

ŘEŠENÍ 1 - ZLEPŠENÍ FUNGOVÁNÍ INFORMAČNÍHO SYSTÉMU Z HLEDISKA NÁKLADOVOSTI

Pro zlepšení dané situace je třeba využívat náklady efektivně, tedy tak, aby byla pokryta co největší oblast nákladovosti a zároveň aby bylo zajištěno efektivní fungování všech těchto sektorů v co největší rovnováze. K tomuto řešení samozřejmě slouží různé finanční nástroje a analýzy, jako například analýza stavových ukazatelů, analýza rozdílových ukazatelů, analýza tokových ukazatelů, analýza zisku apod.

Mělo by se zde investovat především do zlepšení hardwaru, protože ten se jeví jako největší překážkou pro úspěšnější fungování organizace a její bezpečnosti. Problém zde není v tom, že by firma neměla finanční prostředky na zlepšení provozuschopnosti zařízení, ale tyto prostředky jsou ve zvýšené míře vkládány do jiných oblastí firmy, ve kterých není potřeba takových rozsáhlých investic. Vedení firmy by si tedy mělo, kromě svých vlastních finančních analýz, nechat vypracovat také jiné posudky pro zlepšení jejich nákladových investic a to od nezávislých subjektů, které tyto služby poskytují. I pohled zvenčí od nezávislého pozorovatele, může přinést inspiraci pro určení dalšího směru, kterým by se organizace mohla vydat, za účelem neustálého zlepšování své finanční situace.

Dalším aspektem nákladovosti, který by přispěl k lepší efektivitě celého informačního systému je cílený outsourcing. V tomto případě by šlo zejména o přesunutí správy účetnictví a IT služeb na jiné, specializované subjekty. Firma platí některé zaměstnance zbytečně, protože jejich služeb nevyužívá pravidelně, ale pouze v některých případech. Tím vzniká nárok na pravidelné placení mzdy, ačkoliv náplň zaměstnance není pro firmu v každodenní činnosti potřeba.

V outsourcingu se využijí služby specialistů pouze tehdy, je-li to potřebné a tím nevznikají zbytečné mzdové náklady. U specializovaných firem jsou také pracovníci, kteří danou problematiku řeší každý den a tím jsou také mnohem zkušenější a mají větší portfolio znalostí. Vlastního zaměstnance je třeba pravidelně školit, což obsahuje opět zbytečné výdaje navíc.

V případě jednorázového outsourcingu týkajícího se oblasti IT, se může jednat o tyto činnosti:

- návrh a implementace počítačové sítě,
- pravidelné zálohování informací,

- vytvoření webové prezentace firmy,
- zvýšení bezpečnosti firemního intranetu pomocí firewallu a antivirového programu,
- výběr vhodného poskytovatele internetu,
- nastavení a zabezpečení vnitřní bezdrátové sítě (Wi-Fi).

V případě pravidelného outsourcingu, využívajícího se na delší časové období, se může v oblasti IT jednat o tyto služby:

- rychlé řešení drobných softwarových problémů dálkově, přes internet,
- kontrola legálnosti instalovaných programů a následné proškolení zaměstnanců,
- zaškolení zaměstnanců v základní obsluze IT včetně bezpečnosti práce s ní,
- optimalizace nákupu licencí za účelem snížení nákladů,
- optimalizace výkonu počítače,
- pravidelná aktualizace webové prezentace,
- zastupování nebo součinnost při jednání v problematice IT techniky.

Výše zmíněné body jsou zde prezentovány jako možný způsob zlepšení podnikových procesů, protože většina z nich je realizována vlastními zaměstnanci firmy, jejichž počet, je dle mého názoru, zbytečně velký a tudíž také nákladný. Tyto služby může zajistit jedna osoba v rámci outsourcingu, která bude pro firmu představovat menší finanční zatížení a tím také rozšíření možností vynaložení finančních prostředků na potřebnější výdaje. Tyto výdaje mohou být například uplatněny ve zlepšení podmínek bezpečnosti a ochrany zdraví apod.

Využívání nákladů na provoz IS organizace není v tomto případě příliš efektivní. Z celkového rozpočtu, který má firma k dispozici pro své hospodaření, využívá pouze určitou část na financování provozu informačních technologií a bezpečnosti. Tato část nepokrývá všechny náklady, které by měly sloužit pro výhodné investice při nákupu potřebného vybavení. Proto se také tento problém promítá do kvality hardwaru a softwaru.

Není samozřejmě potřeba nakupovat vybavení, pokud k tomu nejsou relevantní důvody (například selhání počítače s následným elektrickým zkratem), ale je nutné vynakládat alespoň minimální částku na včasnou prevenci těchto incidentů a to prostřednictvím pravidelných technických prohlídek a kontroly programového vybavení.

Přístup řešení je navrhnut z pohledu nákladovosti jako priority a bezpečnost je v tomto případě pouze důsledkem. Tento způsob je možné aplikovat za předpokladu, že pro

organizaci jsou prioritní náklady, které jsou významně upřednostňovány před jinými oblastmi zajištění bezpečnosti.

ŘEŠENÍ 2 – ZLEPŠENÍ FUNGOVÁNÍ INFORMAČNÍHO SYSTÉMU Z HLEDISKA BEZPEČNOSTI

Z pohledu bezpečnosti jsou zde dva významné problémy. Jedním z nich, je možný útok na IS z vnějšího prostředí a druhým je zneužití informací z IS prostřednictvím interního zaměstnance. Útok zvenčí je především záležitostí firewallu. Dnešní firewally často detekují i neoprávněné aktivity útočného charakteru. Jejich úspěšnost odhalení těchto útoků je nicméně značně omezená.

Potenciální útok z vnějšího prostředí za účelem získání citlivých informací, popř. s cílem vyřadit některý z komponentů, je sice pravděpodobný, nicméně u firmy tohoto typu, spíše ojedinělý. Nicméně je potřeba alespoň základní zabezpečení před tímto potenciálním napadením. K funkci firewallu, který sám o sobě pro detekování těchto útoků není dostačující, je dobré jej doplnit systémem pro detekci neoprávněného průniku (IDS). Tyto prostředky v kombinaci s firewallem vytváří vhodný prostředek k ochraně, který ve firmě chybí. Proto by případný zkušenější útočník neměl žádný problém s překonáním stávajících překážek. Systém IDS pracuje tak, že lze jeho používáním zachytit včas útoky jak vnějšího (internet), tak i z vnitřního prostředí (vnitřní síť).

Pro zabránění těchto útoků, které mohou být vedeny, jak z vnitřního, tak z vnějšího prostředí, je třeba mít zpracovanou bezpečnostní politiku, která v tomto případě spíše chybí. Je zde sice k dispozici určitý dokument, který zahrnuje jistá bezpečnostní pravidla, ale ten je určen výhradně správci IT systému, který je dle svých vlastních potřeb neustále doplňuje. Forma zpracování tohoto dokumentu, ale není na dostačující profesionální a odborné úrovni a tudíž jej nelze aplikovat na organizaci, jako celek.

Bezpečnostní politika by měla být souhrnem bezpečnostních zásad, směrnic, doporučení, potřeb a předpisů, který pokrývá problematiku bezpečnosti jako celku ve všech jeho oblastech, ať už se jedná o fyzickou bezpečnost, tak i elektrický zabezpečovací systém. V tomto případě bych doporučil si nechat bezpečností politiku zpracovat jiným subjektem, protože firma nedisponuje zaměstnanci, kteří by byli dostatečně vzdělání v této oblasti. Tento nezávislý subjekt také může nabídnout pohled zvenčí, což může být pro organizaci velmi přínosné, protože může zpracovat komplexní analýzu, která bude zahrnovat i rizika, kterých si zaměstnanci firmy nejsou ani vědomi. Vrcholový management zde spíše spoléhá

na práci jednotlivce, ve snaze ušetřit výdaje za zpracování důkladnější analýzy, což se ale vzhledem k budoucímu vývoji nemusí ve svých důsledcích vyplatit.

Řešení č. 2 je zde předkládáno z pohledu bezpečnosti, jako základního pilíře fungování firmy. Finanční prostředky nejsou zásadním kritériem pro rozhodování řešení, protože největší důraz je zde kladen na bezpečnostní politiku.

ŘEŠENÍ 3 - ZLEPŠENÍ FUNGOVÁNÍ INFORMAČNÍHO SYSTÉMU Z HLEDISKA INFORMAČNÍCH TOKŮ

Tento způsob řešení je spíše pod-bodem předchozího řešení, který je zaměřen důkladněji na informační politiku. Informační politika je koncepce neustálého rozvoje informačních vazeb jak mezi technickými prostředky IS, tak i mezi lidským faktorem. Tato koncepce zde chybí úplně, na rozdíl od bezpečnostní politiky, která zde má alespoň jistý základ.

O způsobu uplatňování a implementaci informačních toků, je zde rozhodováno během pracovních briefingů, během kterých je navrhován další postup předávání a rozvoje informací v organizaci. Tato forma je spíše brainstormingového charakteru, což je možná dostačující na určité úrovni řízení (zejména na vrcholovém stupni managementu), ale pro firmu jako celek, to není příliš vhodný způsob, protože zaměstnanci na nižším stupni řízení tyto informace nezachytí včas anebo jsou jim předávány, v již částečně pozměněné formě.

V rámci IS firmy jsou zde využívány informační kanály, které tento systém nabízí a tak je zde jistý druh spojení od nejnižšího stupně vedení až po vrcholový management. V elektronické podobě probíhá komunikace prostřednictvím e-mail klienta mezi různými subjekty organizace. Jediným problémem, který tento druh předávání informací představuje, je jejich dostupnost. Zde se opět dostávám k problematice hardware a software, protože pokud má probíhat komunikace rychle a smysluplně, pak to často není v některých případech možné, jako například při aktualizacích. Pokud si operační systém stahuje aktualizace, tak používání komunikačních služeb je značně ztíženo, protože dochází ke zpomalení počítače a to až na takovou úroveň, že jeho praktické používání je úplně znemožněno. Zakázat aktualizace nelze a to z důvodu bezpečnosti, ale je dobré aktualizovat pouze používané aplikace a software a ne zbytečné programy, které nejsou využívány. Tudíž by bylo vhodné provést občas revizi počítačů a zbytečný software odinstalovat, aby nedocházelo ke snižování výkonnosti počítače prostřednictvím zbytečných aktualizací, které nemají v případě nepoužívaného softwaru význam.

Uvedená statistika vychází ze záznamu chybovosti, který je veden u administrátora systému. IS firmy se začal požívat v roce 2012, a proto je zde tento rok uveden jako počáteční. Počet chyb a kolapsů, které jsou zde uvedeny, vychází z konkrétní MO jednotky, která se nachází ve Zlínském kraji.

Tab. 7 Statistika chybovosti

	Chyby	**Co bylo příčinou?**	**Počet**
2012	Zamrznutí PC	Příliš velký počet aktualizací.	156
	Snížená rychlost		120
2013	Zamrznutí PC	Příliš velký počet aktualizací. Složité naprogramování internetových stránek.	169
	Zkrat	Havárie potrubí.	1
	Snížená rychlost	Příliš velký počet aktualizací. Nepravidelná defragmentace disku.	128
2014	Zamrznutí PC	Příliš velký počet aktualizací. Složité naprogramování internetových stránek.	175
	Snížená rychlost	Příliš velký počet aktualizací. Nepravidelná defragmentace disku	135
	Výpadek připojení k Wi-Fi	Poškození routeru	2

Informační politika by tudíž měla v tomto případě mít alespoň základní koncepci a nastínění jejího rozvoje v rámci informačního prostředí firmy, což v tomto případě není vůbec zavedeno a předávání informací tak není plnohodnotnou záležitostí pro všechny zainteresované subjekty.

Poslední návrh řešení je předložen z pohledu dostupnosti řízení, které je prioritní pro funkci celé firmy a bezpečnostní politika ani nákladovost zde nezastupují významnější roli. Předávání informací, je v tomto případě nejdůležitějším kritériem pro správnou efektivitu podnikového systému.

7 SOUČASNÉ TRENDY A VÝVOJ V OBLASTI BEZPEČNOSTI A INFROMAČNÍCH A KOMUNIKAČNÍCH SYSTÉMŮ

V této kapitole se zaměřuji na výběr vhodného řešení, popř. kombinace řešení, která byla navrhnuta v předchozí kapitole. Pro výběr nejvhodnější varianty byly zvoleny metoda známková a metoda párového hodnocení. Aby bylo rozhodování co nejpřesnější, byly zde navrhnuty kritéria, které slouží k hodnocení a výběru nejvhodnější varianty řešení.

7.1 Metoda známkování

Pro aplikaci této metody je zde použita stupnice 1 až 5, kde nejvhodnější a nejdůležitější kritérium dostává nejvyšší počet bodů a nejméně důležitému kritériu je naopak přidělen nejmenší počet bodů.

Tab. 8 Numerická stupnice

Numerická stupnice	Verbální hodnocení
5	výborné hodnocení, rizika minimální, relativní aspekt velmi pozitivní, absolutní aspekt zanedbatelný
2	hodnocení velmi dobré, míra rizika velmi nízká, relativní dílčí aspekt pozitivní, absolutní aspekt nízký
3	hodnocení dobré, rizika jsou nízká, relativní aspekt indiferentní nebo zanedbatelný, absolutní aspekt střední
2	hodnocení vyhovující, míra rizika střední, relativní aspekt dílčím způsobem negativní s možností realizace kompenzačních nebo eliminačních opatření, absolutní aspekt vysoký,
1	hodnocení nejméně vyhovující, míra rizika vysoká, relativní aspekt negativní se značně omezenou možnosti kompenzačních a eliminačních opatření, vliv je v absolutním aspektu velmi vysoký

Tab. 9 Hodnocení variant a kritérií

	Řešení 1	**Řešení 2**	**Řešení 3**
Vliv na chod celé organice	1	4	5
Vliv na bezpečnost	1	5	4
Vliv na pracovní prostředí	2	4	4
Vliv na komunikaci v organizaci	2	4	5
Vliv na informační systémy organizace	1	5	5
Celkem	**7**	**22**	**23**

7.2 Metoda párového hodnocení

Tato metoda spočívá ve výběru a porovnaní dvojce kritérií mezi sebou. K tomu slouží tzv. **Fullerův trojúhelník**, který je tvořen dvojřádky jednotlivých kritérií, které se mezi sebou porovnávají a z nichž to důležitější je vždy zvýrazněno.

Tab. 10 Fullerův trojúhelník

ch. organizace	**ch. organizace**	**ch. organizace**	ch. organizace
bezpečnost	prac. prostředí	komunikace	**inf. systémy**
bezpečnost	**bezpečnost**	bezpečnost	
prac. prostředí	komunikace	**inf. systémy**	
prac. prostředí	prac. prostředí		
komunikace	**inf. systémy**		
komunikace			
inf. systémy			

Tab. 11 Metody párového hodnocení

Kritérium	Preference	Preference / 10	Váhový koeficient
Vliv na chod celé organizace	2	0,2	20
Vliv na bezpečnost	3	0,3	30
Vliv na pracovní prostředí	0	0	0
Vliv na komunikaci v organizaci	1	0,1	10
Vliv na informační systém organizace	4	0,4	40
Celkem	10	1	100

Za pomocí aplikace těchto matematických metod, lze vyvodit následující závěry. Vzhledem k navrhnutým řešením, které byly porovnávány s danými kritérii, je nejvíce vhodné implementovat řešení 3, popř. vzhledem k podobným výsledkům, pak kombinace řešení 2 a řešení 3. Problematika bezpečnosti a zejména informačních systémů, je zde prioritní záležitostí a nákladovost není v tomto případě tím nejdůležitějším faktorem.

Vzhledem k sortimentu, se kterým firma obchoduje a který uskladňuje, je kladen důraz spíše na použití řešení 3, protože se nejedná o nebezpečné látky, které by podléhaly zvláštním předpisům, co se týká jejich převozu a uskladnění. V tomto případě tedy nemusí být brána oblast bezpečnosti jako nejdůležitější faktor.

Pro organizaci a její budoucí fungování, tedy bude vhodné, pokud využije výše navrhnutého řešení, protože oblast, které se dané problémy týkají, zde není zcela uspokojivě řešena, a tudíž by v následujících letech mohly nastat větší komplikace, které

by měly vliv, jak na chod celé organizace, tak také na pracovní podmínky a zaměstnance firmy.

ZÁVĚR

Cílem mé diplomové práce, bylo posouzení bezpečnostní politiky a informačního systému s následným návrhem možných řešení, které by přispělo ke zlepšení situace v organizaci. Vhledem k tomu, že tyto dvě oblasti spolu úzce souvisí, tak je nutné znát postupy a metodiky, které se vzájemně doplňují a přispívají tak k vytvoření holistického pohledu na firmu.

Bezpečnostní politika a s ní související informační bezpečnost, jsou v současné době nejdůležitějšími trendy, které zastávají významnou roli v podnikovém řízení. Jelikož se jedná o oblasti, které mají vliv na organizaci na všech jejich řídících úrovních, je třeba, aby pro jejich správnou implementaci byly neustále aktualizovány a kriticky hodnoceny, což pro praktické využití znamená neustále zlepšování a vývoj, který bude pro podnik velkou výhodou, přispívající k jeho stabilitě. V celosvětovém měřítku je oblast bezpečnosti a informačních technologií předmětem neustálého vývoje, který přináší nové poznatky z této vědy a umožňuje tak vývoj bezpečnostního a informačního prostředí směrem k lepší a bezpečnější budoucnosti.

Bezpečnostní incidenty a konflikty, které jsou již bez nadsázky, součástí dnešního světa, nelze podceňovat a je třeba se co nejlépe připravit nejen na jejich řešení, ale také především, na prevenci, v podobě bezpečnostních opatření a sofistikovaných bezpečnostních systémů, které budou zvyšovat komfort a úroveň zabezpečení různých subjektů.

Vzhledem k podstatě firmy, jejichž analýza byla předmětem mé diplomové práce, jsem zvolil přístup, který se soustředil na posouzení a vzájemné srovnání bezpečnosti a informační politiky s následnou integrací těchto dvou oblastí do třech možných řešení, které jsou koncipovány s ohledem na povahu a zaměření organizace a které nabízejí tři různé pohledy na danou problematiku.

Doufám, že tato práce pomohla čtenáři vytvořit si kvalitní a odborný pohled na bezpečnostní politiku a informační systémy, které jsou součástí každodenního života a s nimiž se ve své podstatě každý setkává, ať už si to plně uvědomuje nebo ne. Mým přáním také je, že tato práce bude taktéž prakticky využita a to nejen pro danou firmu, která byla předmětem zkoumání, ale i pro jiné organizace podobného charakteru, pro které může být velkým přínosem.

CONCLUSION

The aim of my thesis, was to assess the security policy and information system with consequent possible solutions that would help to improve the situation in the organization. Bearing in mind that these two issues are closely related, it is necessary to know the procedures and methodologies that complement each other and contribute to creating a holistic view of the company.

Security policy and related information security, are currently the most important trends which play a significant role in the corporate governance. Since these are areas that have an impact on their organizations at all levels of management, it is necessary to make sure that their implementation has been updated constantly as well as evaluated critically. In practice, such continuous improvement and development will be of great advantage to the company, contributing to it‘s stability. On the global scale, security and information technology is a subject to continuous development that brings new knowledge of this science and enables the development of security information environment towards better and safer future.

Security incidents and conflicts that are already without exaggeration, part of today's world can not be underestimated and it is necessary to best prepare not only for their solutions, but also and above all, prevention, in terms of security measures and sophisticated security systems which will increase the comfort and the level of security of various entities.

Due to the nature of the company, whose analysis was the subject of my thesis, I chose an approach that focused on the assessment and comparison between security information and policies and the integration of these two areas into three possible solutions that are designed with regard to the nature and direction of the organization and offering three different views of the issue.

I hope that this work has helped readers to create high quality and expert view of the safety policy and information systems that are part of everyday life and which is, in essence, every encounter, whether it is fully aware of it or not. My wish is also that this work will also be practically used not only for the company which has been the subject of research but also for other organizations of similar nature which can greatly benefit from it as well.

SEZNAM POUŽITÉ LITERATURY

[1] BÍLÁ, Jiří ŠMÍD, František KRÁL a Vladimír HLAVÁČ. Informační technologie: Databázové a znalostní systémy. Praha: České vysoké učení technické, 2009, 126 s. ISBN 80-01-02790-2.

[2] JAŠEK, Roman a Martin LUKÁŠ. Informatika ve veřejné správě. Zlín: Univerzita Tomáše Bati ve Zlíně, 2003, 215 s. ISBN 80-7318-147-9.

[3] JAŠEK, Roman. Informační a datová bezpečnost. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-7318-456-7.

[4] ČANDÍK, Marek. Základy informační bezpečnosti. Zlín: Univerzita Tomáše Bati ve Zlíně, 2004, 107 s. ISBN 80-7318-218-1.

[5] MOLNÁR, Zdeněk, Bohumil JUŘENČÁK, Petr REIESSLER a Petr SODOMKA. Informační systém podniku. Zlín: Univerzita Tomáše Bati ve Zlíně, 2001, 184 s. ISBN 80-238-6525-0.

[6] GÁLA Libor, Jan POUR a Zuzana ŠEDIVÁ. Podniková informatika. 2. vyd. Praha: Grada Publishing, a. s., 2009, 496 s. ISBN 978-80-247-2615-1.

[7] VALOUCH, Jan. Projektování integrovaných systémů. Zlín: Univerzita Tomáše Bati ve Zlíně, 2013, 152 s. ISBN 978-80-7454-296-1. Dostupné z: https://dspace.k.utb.cz/handle/10563/25814

[8] POŹÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-8689-838-5.

[9] LUDVÍK, Miroslav. Teorie bezpečnosti počítačových sítí. Praha: Computer Media, 2008, 98 s. ISBN 80-86686-35-3.

[10] POLČÁK, Radim. Právo na internetu: Spam a odpovědnost ISP. Vyd. 1. Brno: Computer Press, 2007, 150 s. ISBN 978-80-251-1777-4.

[11] AEC SECURITY. Bezpečnostní politika organizace [online]. [cit. 2014-10-14]. Dostupné z: http://www.aec.cz/cz/download

[12] AEC SECURITY. Procesy a dokumentace bezpečnosti. [online]. [cit. 2014-10-14]. Dostupné z: www.aec.cz/cz/download

[13] ROZÍNKOVÁ, Eva. Obecné základy práce s portálem Czech Point [online]. Havlíčkův Brod: eGon Centrum, 2013 [cit. 2014-10-14]. Dostupné z: http://www.muhb.cz/czp-obecne-zaklady-pdf/s-829834

[14] Vyhláška č. 523 / 2011 Sb.: Národní bezpečnostní úřad [online]. 2011 [cit. 2014-10-16]. Dostupné z: http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005/

[15] CHAUDHARI, Nilesh. Pharming on the Net. In: Palizine Magazine: Applicati on Security Intelligence [online]. 2006 [cit. 2014-09-21]. Dostupné z: http://palizine.plynt.com/issues/2006Mar/pharming/

[16] MENDELOVA UNIVERZITA V BRNĚ. Globální architektura IS / IT [online]. 2012 [cit. 2014-10-16]. Dostupné z: http://is.mendelu.cz/eknihovna/opory/zobraz_cast.pl?cast=5115

[17] SULEK, Martin. Organizační a režimové opatření: Slezská univerzita v Opavě [online]. 2013 [cit. 2014-10-16]. Dostupné z: http://www.slu.cz/math/cz/knihovna/ucebni-texty/Ochrana-osob-a-majetku/Organizacni-a-rezimove-opatreni-a-fyzicka-ochrana.pdf

[18] NĚMEČEK, Milan. Co je to phishing [online]. 2014 [cit. 2014-10-20]. Dostupné z: http://www.hoax.cz/phishing/co-je-to-phishing

[19] VAŇKOVÁ, Jana a Michal ČERNÝ. Hoax jako problém [online]. 2014 [cit. 2014-10-20]. Dostupné z: http://clanky.rvp.cz/clanek/c/G/13977/hoax-jako-problem.html/

[20] POŽÁR, Josef. *Manažerská informatika*. Plzeň: Aleš Čeněk, 2010, 360 s. ISBN 978-80-7380-276-9.

[21] Červ: Počítačové viry [online]. 2014 [cit. 2015-04-04]. Dostupné z: http://www.viry.estranky.cz/clanky/cerv.html

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

BI	Bezpečnost informací
BOZP	Bezpečnost a ochrana zdraví při práci
BS	Jedná se o standard publikovaný BSI group (British Standard Institution)
COM	Generická doména nejvyššího řádu
DES	Data Encryption Standard – Označení v kryptografii pro symetrickou šifru
DNS	Je systém doménových jmen, který je realizován servery DNS a protokoly se stejným jménem, kterým si vyměňují informace
EIS	Executive IS, podpora vrcholového řízení, strategické řízení
EXE	Executable – Spustitelný
ICT	Informační a komunikační technologie
IDS	Systém pro detekci neoprávněného průniku
IEC	International Electrotechnical Commission – Mezinárodní elektrotechnická komise
IM	Instant messaging – internetová služba informující uživatele o připojení jeho přátel do sítě
IP	Je v informatice označení pro adresu, které identifikuje rozhraní v počítačové síti, která využívá IP (internetový protokol)
IS	Informační systém
ISO	International Organization for Standardization – Mezinárodní organizace zabývající se tvorbou norem
IS/IT	Jedná se o zkratku pro „informační systém“ a „informační technologie“
IT	Informační technologie
IRC	Otevřený protokol, který používá TCP a SSL pro komunikaci v reálném čase na internetu
MBR	Master Boot Record, jedná se o hlavní spouštěcí záznam, který je umístěn v prvním sektoru pevného disku

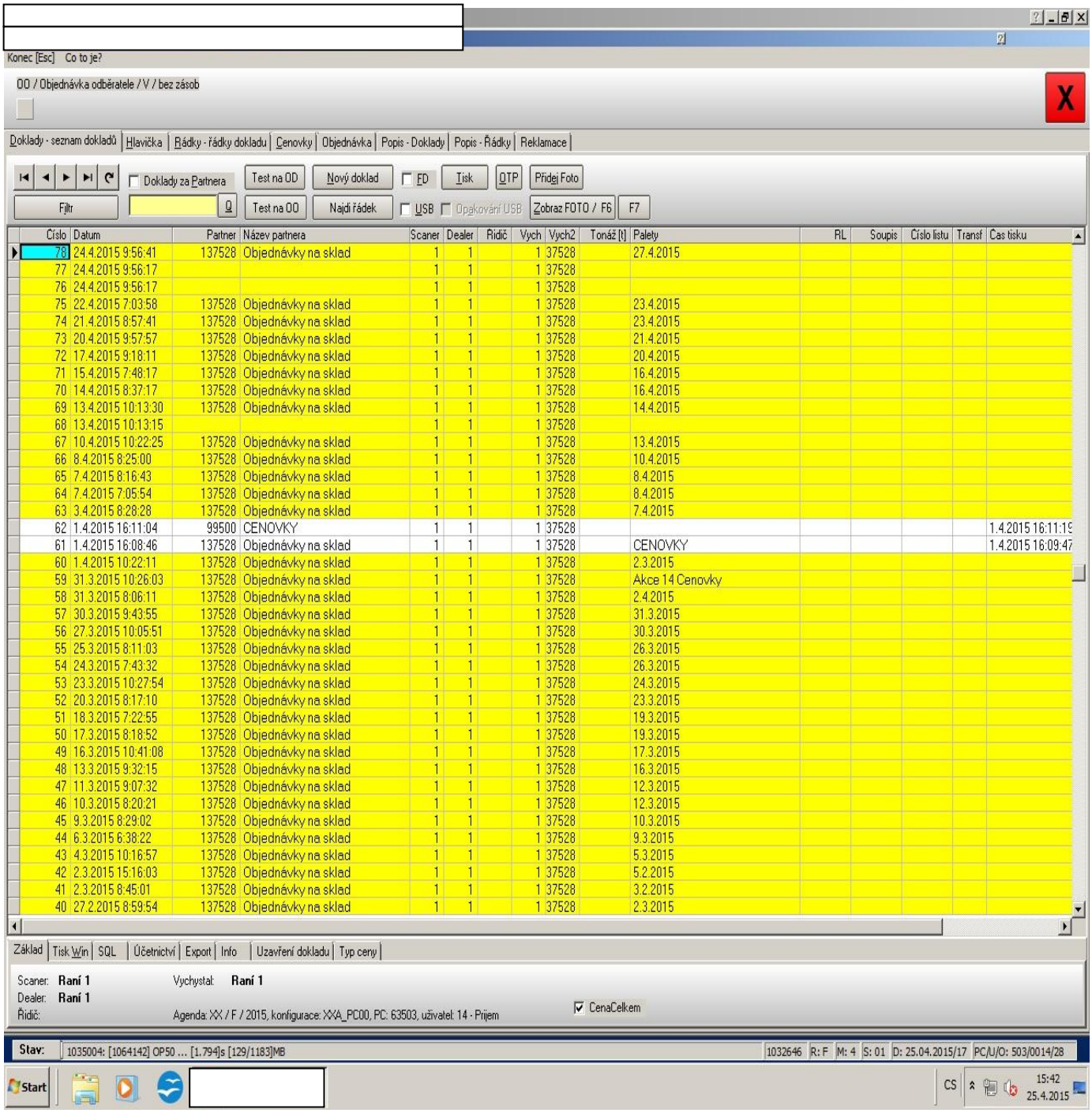
MIS	Management IS, podpora taktické úrovně řízení
MO	Zkratka označující pojem „maloobchod“
MV	Ministerstvo vnitra ČR
NBÚ	Národní bezpečnostní úřad
NV	Nařízení vlády
OS	Operační systém
OVL	E-Sword v8 Overlay Data – Překryvový soubor
PO	Požární ochrana
PRG	Jedná se o zvukové soubory a primárně je jim přiřazen program OzWin CompuServe E-mail/Forum Access Purged Message File
SYS	Formát, který byl vyvinut pro ukládání systémových prostředků, jako je například konfigurace proměnných ve Windows
TPS	Transaction Processing Systém, podpora operativní úrovně řízení
TR	Technical Report – Technická zpráva
ÚOOÚ	Úřad pro ochranu osobních údajů
Wi-Fi	Bezdrátová veřejná síť

SEZNAM OBRÁZKŮ

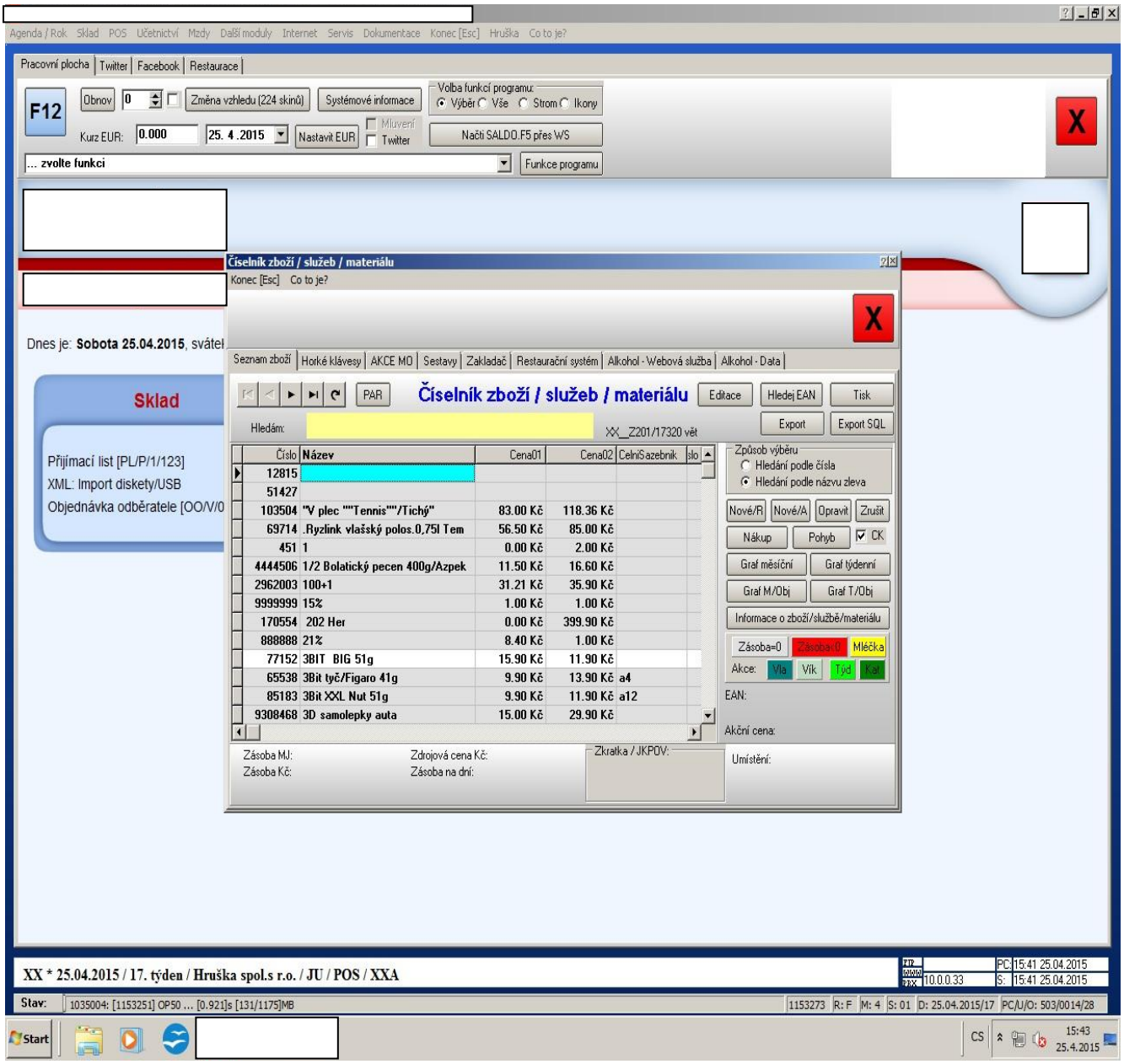
SEZNAM TABULEK

SEZNAM PŘÍLOH

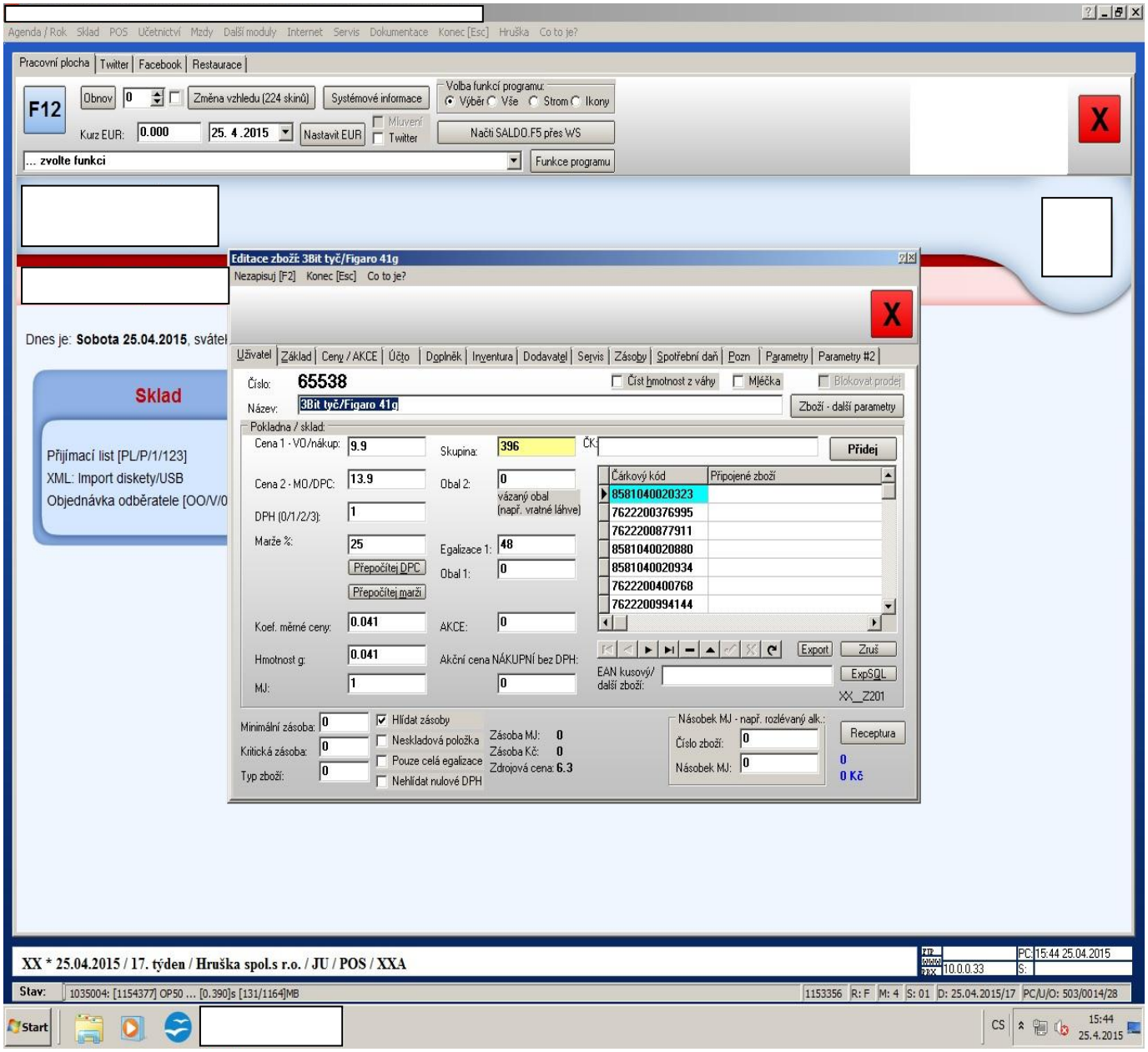
PŘÍLOHA P I: DATABÁZE OBJEDNÁVEK



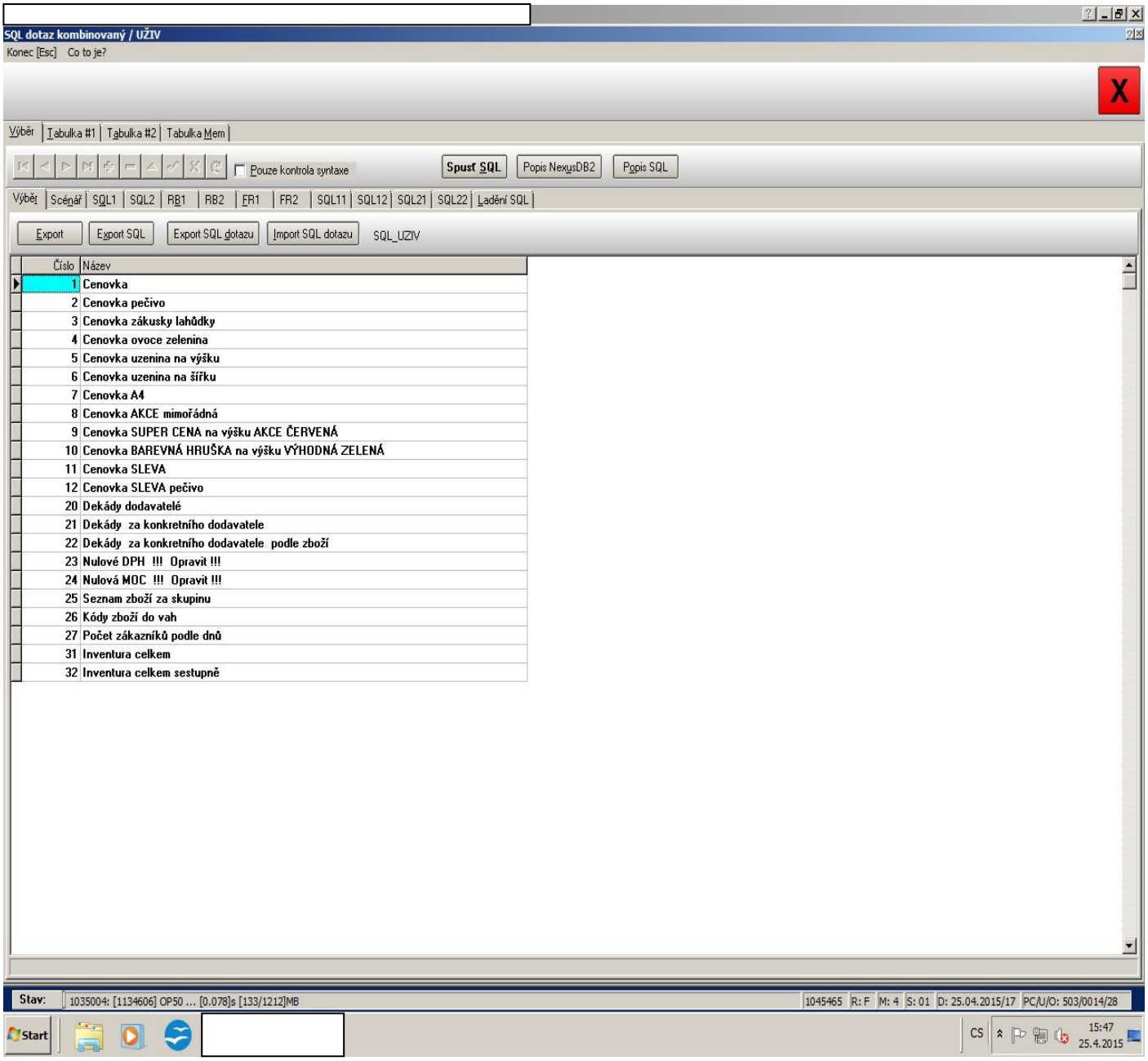
PŘÍLOHA P II: DATABÁZE VÝROBKŮ



PŘÍLOHA P III: INFORMAČNÍ KARTA VÝROBKU



PŘÍLOHA P IV: INFORMAČNÍ KARTA TISKU CEN



PŘÍLOHA P V: INFORMAČNÍ KARTA OBRATU