Univerzita Karlova v Praze

Filozofická fakulta

Ústav informačních studií a knihovnictví

Studijní program: informační studia a knihovnictví

Studijní obor: informační studia a knihovnictví

Diplomová práce

Bc. Eliška Žáčková

Bezpečnost práce s elektronickými daty v průmyslových podnicích

Security of Work with Electronic Data in Industrial Enterprises

Praha 2013 **Vedoucí práce: Mgr. Vít Šisler, Ph.D.**

Oponent bakalářské práce:

Datum obhajoby:

Hodnocení:

Prohlášení:

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

V Praze, dne 4. ledna 2013

……..
podpis studenta

Identifikační záznam:

ŽÁČKOVÁ, Eliška. *Bezpečnost práce s elektronickými daty v průmyslových podnicích*. Praha, 2013. 96 s. 3 přílohy. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce Mgr. Vít Šisler, Ph.D.

Abstrakt

Diplomová práce „Bezpečnost práce s elektronickými datyv průmyslových podnicích“ si klade za cíl charakterizovat základní termíny vztahující se k této oblasti a s jejich pomocí pak dále analyzovatmožnost řešení dané problematiky ve vybraném průmyslovém podniku v Českérepublice skrze metodu kvalitativního výzkumu, kterou je případová studie.

V teoretické části jsou nastíněny pojmy, kterými jsou informace,data, znalosti, kyberprostor, podnikové informační systémy, počítačová kriminalita a kyberterorismus. Z tohoto oddílu vychází část praktická, kterádetailně rozebírá výchozí stav podniku z odvětví potravinářského průmyslua v něm následnou implementaci systému pro řízení a správu digitálníhofiremního obsahu jako možné řešení problematiky bezpečnosti práce s elektronickými daty.

Klíčová slova:

Elektronická data, digitalizace, počítačová kriminalita, informace, znalosti, podnikové informační systémy, potravinářský průmysl, Enterprise Content Management, ECM, Document Management System, DMS, bezpečnost informačních technologií

Abstract

The aim of this thesis is not only to characterise the key terms related to this field, but also to analyse the possible solutions to the area in a particular industrial enterprise in the Czech Republic by means of a case study which is a reliable method of qualitative research.

The thesis is divided into theoretical and practical part. In the theoretical part the terms such as information, electronic data, know-how, enterprise information systems, cybercrime, and cyberterrorism are defined.

The practical part drawing on the theoretical part gives a thorough analysis of the initial state of an industrial enterprise in food industry. Furthermore, it deals with the implementation of the ECM (Enterprise Content Management) which is considered a possible solution to the security of work with electronic data in industrial enterprise.

Keywords:

Electronic data, information, digitalization, cybercrime, cyberterrorism, know-how, enterprise information systems, food industry, Enterprise Content Management, ECM, Document Management System, DMS, cybersecurity, IT security

Obsah

Předmluva

Tato diplomová práce se bude zabývat bezpečností práce s elektronickými daty v průmyslových podnicích. Úvod je rozdělen na tři části, tedy na úvod pro všeobecnou, teoretickou a praktickou sekci. Všeobecný úvod diplomové práce nastiňuje situaci, ve které se dnes společnost i podniky z pohledu užívání ICT a tedy i elektronických dat nacházejí. V úvodu teoretické části budou definovány pojmy informace, data, znalosti a kyberprostor.

Teoretický úvod dále rozšiřuje kapitola zabývající se podnikovými informačními systémy, který jsou Enterprise Resource Planning, Enterprise Content Management a Document Management System. Tyto systémy jsou schopné monitorovat a řídit oběh podnikových elektronických dat. Skrze tyto systémy se také nastavují práva k jednotlivým dokumentům, a proto mají v této práci významné místo.

Následuje kapitola, která rozebírá otázku počítačové kriminality a to včetně rozboru situace v České republice. Pro úplnost je též zmíněn i termín kyberterorismus jako ve své podstatě specifická forma počítačové kriminality. Tato část pojmenovává a specifikuje hrozby, které se dělí na vnější a vnitřní.

Z vnějších hrozeb je podrobněji zmíněno sociální inženýrství, které obchází bezpečnostní politiku firem, kterou většinou zastává oddělení IT, skrze zaměstnance. A tzv. Advanced Persistent Threts, což jsou sofistikované útoky ze strany hackerů a crackerů, které sice využívají základních penetračních technik, ale v jisté cílené posloupnosti či je vytrvale opakují.

Podkapitola „*Vnitřní hrozby: Zaměstnanci“* se snaží vystihnout specifika mladé generace Y, jejíž počet ve firmách se pomalu zvyšuje a její vztah k informačním technologiím dává vzniknout novým druhům hrozeb skrze jejich touhu používat vlastní zařízení nebo si do služebních počítačů instalovat předem oddělením IT neschválené aplikace. Tento nový směr, kdy zaměstnanec pracuje na svém zařízení nebo s aplikacemi, které nejsou ve služebních zařízeních standardně instalovány, se nazývá BYOD (Bring Your Own Device) a BYOA

(Bring Your Own Application). Toto doplňuje tzv. evergreen v bezpečnostní tématice, kterým jsou statická hesla. Předně jejich složení a jejich délka. A to hlavně z toho důvodu, že se začíná přecházet na metodu, kdy člověk jednou zapíše své heslo a má s tím zároveň přístup do všech databází, což opět případným agresorům poskytuje značnou výhodu.

Poslední kapitola teoretické části se zabývá legislativou. Tato kapitola si nedává za cíl popsat všechna legislativní zákoutí, pouze se snaží vysvětlit tu část, která je zmiňována zejména v souvislosti s prací s elektronickými dokumenty.

Praktická část, která vychází z poznatků načerpaných v teoretické části, se snaží popsat jedno z možných řešení problematiky bezpečnosti práce s elektronickými dokumenty. V úvodní části charakterizuje vybranou metodu kvalitativního výzkumu, kterou je případová studie, a vybraný podnik z oblasti potravinářského průmyslu, kterým je Budějovický Budvar, n.p.

Posléze je za pomoci interview s vybranými zaměstnanci a vedoucími oddělení popsán výchozí stav k otázce bezpečnosti práce s elektronickými dokumenty, který plynule přechází v deskripci řešení problematiky oběhu elektronických dat v podniku na základě implementace ECM/DMS systému.

V závěru případové studie jsem se nastínila možné otázky, ze kterých by se daly stanovit hypotézy pro kvantitativní výzkum.

Při výběru literatury jsem se dbala na její aktuálnost a na problematiku, kterou zkoumá. Nejvýznamnějším zdrojem pro mě byly specializované časopisy, které novým trendům přizpůsobovaly témata svých článků. Problém byl pouze v tom, že čím dál tím více do těchto periodik přispívají zainteresované firmy a je tedy důležité podrobovat tyto články, které jsou ne vždy přehledně odděleny od textů psaných redakcí, kritičtějšímu čtení. U bakalářských a diplomových prací jsem také sledovala, jak byly hodnoceny vedoucími a oponenty včetně výsledku obhajoby, abych tak mohla určit jejich relevanci a případně si informace ověřovala v jimi citované literatuře.

V kvalifikačních pracích zaměřených na bezpečnost dat, informací nebo počítače byla velmi často přejata teorie bezpečnosti od Josefa Požára (2005), a proto, abych obohatila práci o nové myšlenky a úhly pohledu, jsem jej nezařadila mezi primární zdroje této práce. Ze stejného důvodu jsem nerozebírala ani Janouškovo členění kyberteroristů (2006) a zaměřila se spíše na kategorizaci, jaké uvádí společnosti, které se zabývají bezpečností, a odborné články v anglickém jazyce. Vynechala jsem také detailní popis rodiny norem ČSN ISO/IEC 27 00X, neboť o nich byla přímo napsána kvalifikační práce a BBNP zatím o jejím zavedení neuvažuje, tudíž by ji nebylo možné propojit s praktickou částí.

Z hlediska legislativního rámce jsem se u definic a výkladu trestního zákoníku zaměřila především na literaturu vydávanou od roku 2010, u které jsem předpokládala, že má v sobě již zahrnuty přelomové změny, které nastaly v roce 2009. Při pročítání materiálů, které se legislativy týkaly i samotných zákonů, jsem dospěla k názoru, že je velmi pravděpodobně tvořena lidmi ze starších generací, pro které informační technologie nejsou tak výraznou součástí života, ale pouhým podpůrným prostředkem, který je možné nahradit či úplně vypustit. Chápu, že vzhledem ke komplikovanosti schvalovacího procesu zákonů, nemůže přesně kopírovat aktuální situaci, ale tím více by se měla zaměřit, dle mého názoru, na jistou predikci budoucího vývoje.

Jelikož jsem se orientovala na situaci v České republice, kterou jsem ještě podpořila případovou studií podniku, který klade velký důraz na svou příslušnost k České republice skrze chráněné zeměpisné označení, odpovídá tomu i poměr zastoupení českých a cizojazyčných zdrojů. Také je evidentní, že firmy zabývající se bezpečnostními otázkami, své produkty i dokumentaci k nim mají přirozeně alokovánu do českého jazyka.

Ve své práci jsem využívala i poznatky a poznámky především z přednášek a seminářů Internetová kriminalita (dříve IT právo), Informační a komunikační technologie, Podnikové informační systémy, Projektování podnikových informačních systémů, Rešerší strategie pro vědu a výzkum, Zpravodajské služby, Reprezentace znalostí a Teorie argumentace.

Text diplomové práce splňuje všechny požadavky a náležitosti dané *Studijním a zkušebním řádem FF UK* a na konci obsahuje 3 nečíslované přílohy. Všechny záznamy práce jsou vytvořeny na základě českého překladu mezinárodní normy ISO 690.

ČSN ISO 690 (01 0197). *Informace a dokumentace: pravidla pro bibliografické odkazy a citace informačních zdrojů*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Dostupné z: http://csnonline.unmz.cz/

Citace v samotném textu práce jsou uzavřeny do kulatých závorek a obsahují příjmení autora a rok.

1 Úvod

Během několika posledních let se informační a komunikační technologie (dále jen ICT) rozšířily do většiny, možná všech, odvětví lidské činnosti ve vyspělých částech světa. Staly se nezbytným a nedílným nástrojem pro vzdělávání, práci i volný čas. Zároveň s tím se také zvýšila rychlost osvojení si těchto technologií mainstreamovou populací. Tato skutečnost postupně začala obracet zažitý pořádek v podnicích a institucích, kdy samy organizace ztratily svou jedinečnost v podobě inovačního prvku při své cestě za ziskem, protože s novinkami přicházejí sami zaměstnanci, kteří si ve svém osobním životě adoptovali novou technologii natolik, že ta v práci jim nyní znenadání připadá nevyhovující nebo dokonce zastaralá.

Ovšem toto nelze dle mého názoru jednoduše vztáhnout na celou populaci v produktivním věku, která je v současnosti rozdělována do třech hlavních skupin. První jsou tzv. Baby boomers, kteří si zvykli používat především televizi, rádio, telefon a mobilní telefon (nikoliv však tzv. chytrý telefon). Druhou skupinou jsou lidé, tzv. generace X, která většinu života prožila bez Internetu, ale hlavně kvůli práci se s ním naučila relativně dobře pracovat. Třetí skupinou je generace Y (též Net Generation, Millennials, Děti sítě), datuje se různě, ale většinou se zdroje shodují, že se od ní začínají řadit narození okolo roku 1980. Jedná se o první generaci, která od dětství užívá informační technologie, a proto se dokáže rychleji naučit s nimi i pracovat. V současné době začíná stoupat počet Dětí sítě v produktivním věku. Tím pádem i ve firmách narůstá počet zaměstnanců z této generace a domnívám se, že to zcela jistě bude zásadní vliv na chod podniků. Čtvrtá generace, generace Googlu, která je jich od útlého dětství pevně spjata s informačními technologiemi, zatím ještě sedá ve školních lavicích.

Neustálá tendence zkracovat časové prodlevy mezi našimi jednotlivými činnostmi se vrývá hluboko do každodenního života. Nechceme ztrácet čas čekáním. Pro výplň nebo zkrácení tohoto času nabízejí firmy a instituce mobilní hry, knihy, vyšší pokrytí signálem, rychlejší dopravní prostředky apod. Efektivně reagovat na potřeby spotřebitelů je samozřejmě třeba v mezích legislativy a získat výhodu na trhu lze přinejmenším dvěma způsoby. Buď komplexně zkvalitnit sebe sama, nebo pomocí konkurenčního zpravodajství získat informace o konkurenci a na jejich základě se nastalé situaci přizpůsobit. Každý podnik je pouze jedním spojem v pavučině trhu, tudíž nelze zůstat izolovaným.

Současně s tím se firmy se mohou dostávat také do jakéhosi vnitřního rozkolu, kdy jsou předchozí generace pozvolna nahrazovány, nebo spíše omlazovány, generacemi následujícími. Toto období se vyznačuje například tím, že podnik přechází na elektronickou podobu dokumentů, avšak stále si udržuje zvyky starších generací, mezi které patří tištění si materiálů v elektronické podobě. Čím více podob ale dokument má, tím více se, bohužel, rozšiřuje paleta možností pro případné „agresory".

Tato práce si dává za úkol zmapovat problematiku bezpečnosti práce s elektronickými daty v průmyslovém podniku. Chtěla bych se pokusit o moderní pohled na oběh dokumentů a jeho slabá místa s přihlédnutím k různým přístupům k ICT, které se objevují na základě postupné obměny poměrného zastoupení jednotlivých generací ve firmě. Také bych chtěla pro větší ucelenost práce zmínit základní legislativní požadavky k otázce digitalizace a bezpečnosti elektronických dokumentů. Pro co nejvyšší objektivitu práce bych se chtěla pokusit zmínit klady digitalizace dat i její zápory v podobě vnějších a vnitřních hrozeb podniku včetně pohledu skrze trestní zákoník.

K bližšímu popsání tohoto tématu jsem se rozhodla přistoupit ke kvalitativní analýze, přesněji řečeno k případové studii, ve které jsem popsala současný a nastínila budoucí vývoj podniku z odvětví potravinářského průmyslu vyrábějící tzv. rychloobrátkové zboží, Budějovického Budvaru, n.p.. Administrativa, stejně jako ICT, je podle mého názoru v tomto typu podniku vnímána spíše jako podpůrná složka výroby a na základě toho musí být schopná se plně přizpůsobit a podřídit jejím požadavkům a potřebám.

Od doby zadání mé práce do Studentského informačního systému, se objevilo několik vysokoškolských kvalifikačních prací na dílčí témata této práce, ale byly vždy poněkud úzce zaměřené (i z důvodu, že se v některých případech jednalo o práce bakalářské), aniž by byl brán v potaz širší kontext této problematiky, který dle mého názoru přidává jednotlivým úkazům originální úhel pohledu. Myslím si, že je to především proto, že obory, které rozebíraly otázky spojené s bezpečností práce s elektronickými daty, jsou spjaté s konkrétní specializací. Například s ekonomií, aplikovanou logikou, legislativou nebo psychologií. Já se v této práci nechci přímo zaměřovat na osoby, ukazatele či faktory ovlivňující zisk vybraného podniku, ale na jedno z nejpodstatnějších nehmotných aktiv firem, kterým jsou informace, konkrétně informace v elektronické podobě. Chtěla bych využít jedné z předností našeho

oboru, kterou shledávám v nalézání propojení souvislostí jednotlivých řešení, komunikačních dovednostech a vytváření ucelených rešerší.

TEORETICKÁ ČÁST

2 Úvod k teoretické části

„Cesta, jak přimět společnosti přemýšlet o počítačové kriminalitě, vede přes diskuzi nad riziky, ne přes technické debaty o šifrování, penetračním testování nebo o nastavení firewallů. Nechme společnosti zamyslet se nad tím, co se může stát s jejich dobrým jménem, pokud ke ztrátě důležitých dat dojde.“

Filip Volavka
senior manažer, Oddělení forenzních technologií
(PWC, 2011)

V úvodu teoretické části diplomové práce budou definovány základní termíny vztahující se k bezpečnosti práce s elektronickými dokumenty. Jedná se o syntézu a vymezení poznatků, ze kterých budou čerpat na ni navazující kapitoly.

2.1 Informace, data a znalosti

„Část překážek má společného jmenovatele – data a informace. Nejde o to je umět efektivně získávat a využívat, ale musíme je mít k dispozici tehdy, kdy potřebujeme, ve stavu, kdy se na ně můžeme spolehnout, a chráněné tak, aby se nedostaly k někomu, kdo je nemá vidět.“

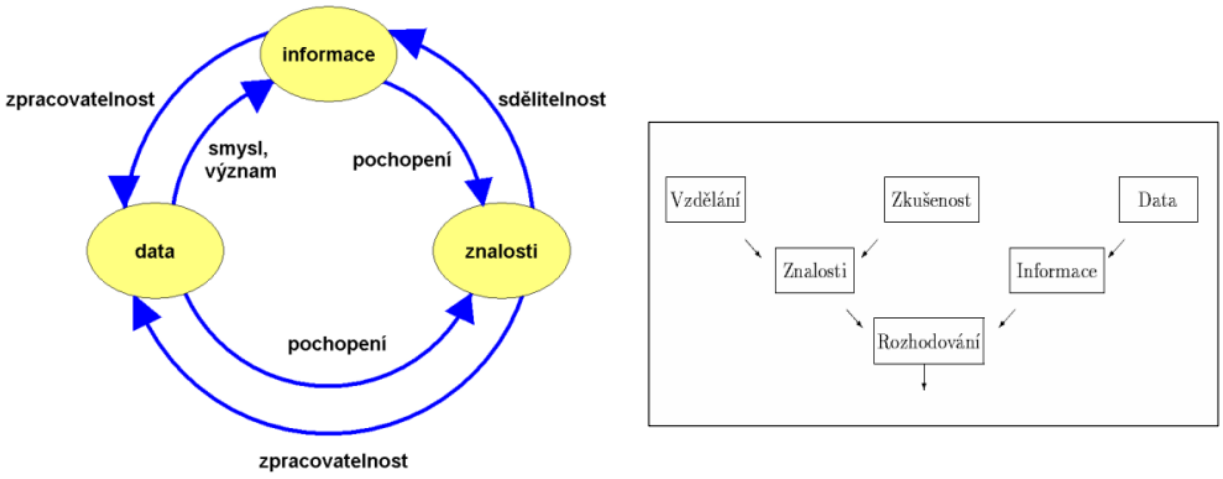
(SEIGE, 2002)

Informace představují ve vzájemně propojeném světě kritické **aktivum podniku**. Podle normy o informačních technologiích jsou informace na roveň **se softwarem**, **hardwarem**, **službami**, **lidmi** (s jejich klasifikací, dovednostmi a praxí) **a nehmotnými aktivy**, mezi které patří např. pověst nebo image tzv. goodwill. (ČSN ISO/IEC 27 000). Je však ještě potřeba brát v úvahu skutečnost, že se jejich hodnota na základě okolností (času, dostupnosti a jejich potřebnosti) výrazně mění.

Informace jsou definovány jako *„**poznatek týkající se** jakýchkoliv **objektů**, např. fakt, událostí, **procesů**, **věcí** nebo **myšlenek**, včetně pojmů, **který má** v daném kontextu **specifický význam**“* (ČSN ISO/IEC 2382-1). Jedná se také o **poznatek**, který **snižuje nebo odstraňuje entropii**. (ČSN ISO/IEC 2382-16; KUČEROVÁ, 2012). *„Jinak též můžeme informaci definovat jako **sdělení**, které vede k jednoznačnější volbě z více možností, nebo jako signál či skupinu signálů, **které umožňují rozhodování** systému.“* (VYMĚTAL, 2010)

Bezpečnost informací zahrnuje dle normy ČSN ISO/IEC 27 000 tři aspekty, kterými jsou **dostupnost**, **integrita** a **důvěrnost**.

Data (zastarale a často užívané též údaje) **jsou** s informacemi úzce spjata, jelikož se jedná o *„**opakovaně interpretovatelnou** formalizovanou podobu **informace** vhodnou pro komunikaci, vyhodnocování nebo zpracování.“* (ČSN ISO/IEC 2382-1) Zjednodušeně tedy můžeme říci, že **ICT zpracovává informace ve formě dat**. (POŽÁR, 2005) **Znalosti jsou** normou ČSN ISO/IEC 27 000 definovány jako **nevyjádřené informace** např. ve formě know-how, vědění pravdy, přesvědčení, úsudku. Webster sděluje, že **znalosti jsou** fakta či ideje **získané pozorování, studiem, zkoumáním nebo zkušeností.** Znalosti představují poznání určité části reality a díky tomu jsou na rozdíl od dat zobrazujících realitu na úrovni rychle se měnících detailů, stálejší. (VYMĚTAL, 2010) **A jsou** také zároveň **tím**, **co** nám **dovoluje odvodit či pochopit novou informaci**. Tento pohled ještě můžeme rozšířit o to, jak s danými pojmy „informace, data a znalosti“ pracují znalostní/expertní systémy (viz obrázek č. 1).



Obrázek č. 1 – Vzájemné propojení informací, dat a znalostí (KUČEROVÁ, 2012;

WIEDERHOLD, 1986)

Ačkoliv byly dříve **informace ve firmách** uchovávány pouze v materiální formě (listinná podoba), kdy pro jejich ochranu postačilo fyzické zabezpečení objektu, dnes **jsou** ukládány i **v digitální podobě**. V té jsou **ukládány a sdíleny prostřednictvím intranetu či internetu**. Spolu s firmami expandují a prostřednictvím podnikatelské činnosti se globálně propojují (mateřské firmy sdílejí ERP systémy (viz níže) s dceřinými společnostmi nezávisle na zemi, ve které se vyskytují, atd. Vzhledem k této skutečnosti přibývá i počet hrozeb, zvyšuje se zranitelnost systémů a toto se projevuje v nárůstu nároků na jejich ochranu. (VESELÝ, 2011; ČSN ISO/IEC 27 000)

2.2 Kyberprostor

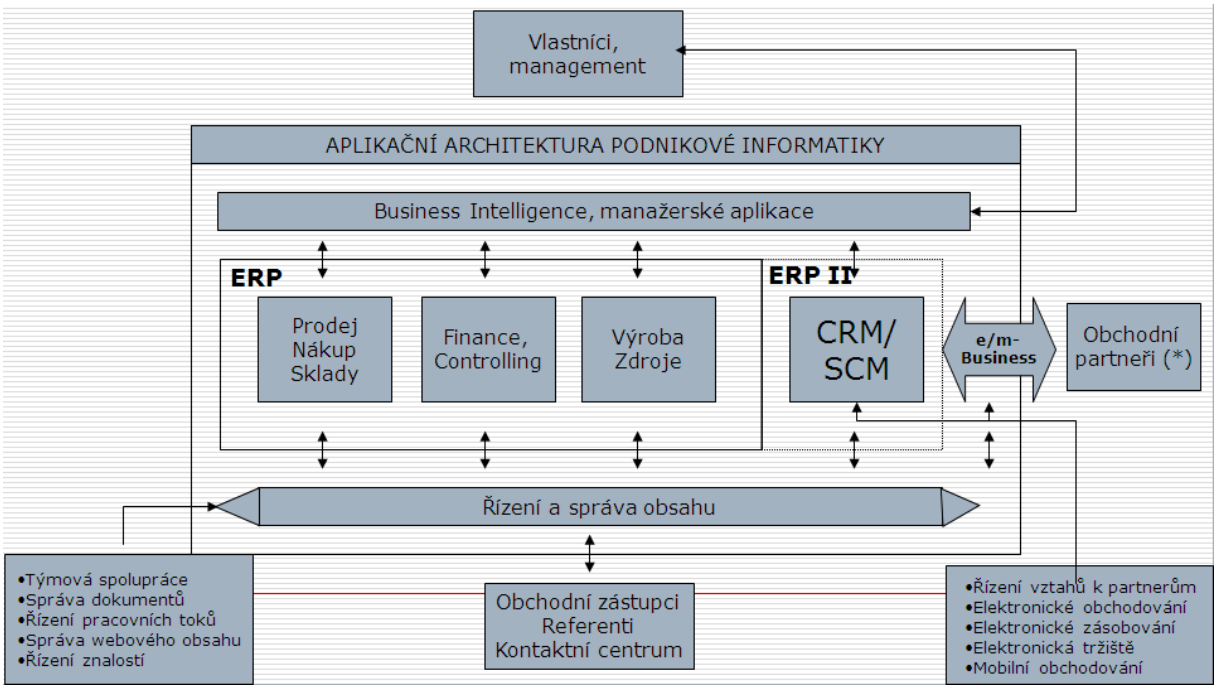
Definice kyberprostoru je klíčová z hlediska pojetí počítačové nebo též internetové kriminality. Rostoucí popularita užívání ICT technologií uměle vytváří mezi uživateli jakýsi **druh společného prostoru**, který je možné pojmenovat jako „kyberporostor“. (TÁBOROVÁ, 2010) Na rozdíl od reálného světa **nemá žádnou konkrétní hranici**, což koliduje s trestním zákoníkem, který se řídí zásadou teritoriality (§4 trestního zákoníku)

Kyberprostor je zajímavý hned z několika hledisek. Nelze popřít fakt, že na něj již vzniká závislost a to přímo v globálním měřítku. Je decentralizovaný, otevřený, řízený uživateli, interaktivní a závislý na informační infrastruktuře. Obsahuje množství informací, (BENEŠOVSKÁ, 2011) ale ty je potřeba filtrovat, protože v současnosti dochází k tzv. informačnímu přetížení, kdy je těžší relevantní informace nacházet.

3 Podnikový informační systém

„Rozhodovat se podle aktuálních dat, nikoli podle odhadů, je snem každého řídícího pracovníka. Obrovské množství dat, která dnes počítačové systémy produkují, umožňují detailní pohledy do dění uvnitř světa.“

Podnikový informační systém (dále jen PIS) **je nástrojem** podniku **pro zpřehlednění a urychlení procesů** (zjednodušení, snížení pracovní a technické náročnosti, vyloučení duplicitních operací, aj.). PIS je poskládán z několika modulů**, které jsou schopné pokrýt** všechny **podnikové procesy**. **Podporují** evidenční, analytické, plánovací, rozhodovací a kontrolní **činnosti i** transakční **operace**. A tím **napomáhají zvýšení bezpečnosti**, **spolehlivosti**, **výkonu** a **zkrácení doby odezvy**. (LIPKOVÁ, 2011)



Obrázek č.2 – Obecná aplikační architektura podnikové informatiky (LIPKOVÁ, 2011)

3.1 Enterprise Resource Planning (ERP)

ERP systém je srdcem PIS, **je považován za aplikaci** používanou k **řízení podnikových dat**, **koordinaci aktivit** a **disponibilních zdrojů**. Mezi hlavní vlastnosti ERP patří schopnost automatizovat a integrovat klíčové podnikové procesy a funkce, sdílet společná podniková data a umožnit jejich dostupnost v reálném čase v rámci celé firmy. (BASL, 2008; LIPKOVÁ, 2011)

3.2 Enterprise Content Management

Enterprise Content Management (dále jen **ECM) je systém, který by měl** komplexně **pokrývat životní cyklus podnikového obsahu** (od jeho zachycení až po jeho skartaci) v elektronické podobě. Jeho základní funkcionalitou jsou data v elektronické podobě zachycovat, spravovat, ukládat, uchovávat a v případě potřeby předávat dále (viz příloha č. 1). (KUČEROVÁ-ZRÁLÍKOVÁ, 2011) Jedná se o nástroj, který ve své podstatě obsahuje definici DLP (viz kapitola Advanced Persistent Threts (ATP) a obrana skrze Data Loss Prevention (DLP))

Vzhledem k jeho postavení v rámci obecné aplikační architektury podnikové architektury (viz obrázek č. 2) je stěžejní jeho správné napojení na ostatní informační systémy podniku, především na ERP systém. Jestliže se firma rozhodne, že bude mít data pouze v elektronické podobě, je nutné, aby ECM systém splňoval také veškeré legislativní požadavky (viz kapitola Úprava bezpečnosti a práce s elektronickými daty v legislativě).

Níže popíši jednotlivé fáze, kterými musí projít dokument předtím, než se s ním začne dále pracovat. Popíši strukturu dat a také cest, kterými se dokument do firemního oběhu dostává. Dle mého názoru je důležité vědět, co všechno je součástí firemního obsahu, nikoliv majetkem zaměstnance, a jak je možné tento objem nejednotných dat indexovat a spravovat.

3.2.1 Proces přijetí dokumentu

Jelikož **ECM** systém **pracuje pouze s daty v elektronické podobě** s možností propojení s jejich listinnou podobou**, je třeba** potřebné **listinné dokumenty digitalizovat**. Při digitalizaci je vhodné dokument uložit **do formátu** určeného pro dlouhodobou archivaci, kterým je **PDF/A**. Při skenování je také možno opatřit dokument elektronickým podpisem či značkou.

Proces přijetí dokumentu do databáze ECM systému může být rozdělen do těchto etap (JAKEŠ, 2008; KUČEROVÁ-ZRÁLÍKOVÁ, 2011):

1. Příprava dokumentu
2. Zachycení elektronického dokumentu
   - Skenování, mail, FAX, datová schránka
3. Rozpoznávání dat
4. Klasifikace
5. Validace
6. Verifikace
7. Export do databáze a začátek workflow

3.2.2 Příprava dokumentu

Před vlastní **digitalizací je potřeba dokumenty** manuálně **roztřídit** např. oddělit faktury a jejich přílohy, tzv. rozsponkovat sešité části a určit jakému oddělení příslušný dokument nebo sada dokumentů náleží. **Pro oddělení** jednotlivých dílčích **částí se** zpravidla **užívá BAR kód**, který zároveň propojuje listinnou podobu s elektronickou. To následně usnadňuje vyhledávání listinné podoby pro vlastní potřeby firem nebo pro potřeby státních kontrolních orgánů, soudních řízení či skartaci apod.

3.2.3 Zachycení dokumentů

Dokumenty, se kterými podnik pracuje, **se do** firemního **oběhu dostávají** několika cestami. Buď **v listinné podobě** přes podatelnu, **v elektronické podobě** např. přes email (DOC, EDI[1], apod.), **datové schránky** (PDF, PDF/A) **nebo si je podnik tvoří sám** jako např. vnitropodnikové směrnice, propagační materiály nebo zápisy z porad atd.

Stuchlík člení listinné a elektronické dokumenty do kategorií (STUCHLÍK, 2008):

[1] *„EDI (Electronic Data Interchange) – výměna strukturovaných zpráv mezi počítačovými aplikacemi“* (WIKIPEDIE, 2012) je možné dle §24 odst. 4 zákoně č. 235/2004 Sb., o DPH využívat ji pro elektronickou podobu daňového dokladu, kde *„je zaručena věrohodnost původu a neporušitelnost obsahu daňového dokladu elektronickou výměnou informací (EDI).“*

- Externí dokumenty (vystupující z jiných PIS např. objednávky, dodací listy)
- Interní dokumenty (dokumentace k výrobku, aj.)
- Dokumenty vzniklé z komunikace s partnery nebo okolím podniku

Další dělení je dle typu dat (JAKEŠ, 2008):

- Strukturovaná (databázové tabulky, faktury, dodací listy)
    - Jedná se o ta data, která mají pevně danou strukturu s proměnlivým obsahem
- Semi-strukturovaná (smlouvy, projektová dokumentace, vnitropodnikové směrnice, pokyny a nařízení)
- Nestrukturovaná (emailová komunikace)

Toto také ovlivňuje další fáze, především náročnost jejich digitalizace a indexace. Je nutné hledět, zda dokument nepřichází již s nějakým označením např. citlivých dat či určitého stupně utajení.

3.2.4 Rozpoznání dat

Rozpoznání dat a jejich **indexace probíhá** na základě rozhodnutí podniku buďto **ručně, poloautomaticky či automaticky**. Většinou se přistupuje k poloautomatické indexaci za použití některé z technologií ICR[2], OCR[3], BCR[4] a OMR[5]. Každá z metod vyžaduje vlastní speciální software. V komerční sféře v ČR, zdá se, se nevyužívá metoda ICR, neboť spolehlivost správného přečtení údajů ručně psaných dokumentů je nízká a SW s touto technologií jsou poměrně drahé. V praxi jsem se setkala se dvěma způsoby pojetí výkladu systému OCR. OCR je vrstva vytvořená nad vlastním dokumentem, která umožňuje fulltextové prohledávání dokumentu (je to stejné jako když vyhledáváme např. v DOC, XLS, HTML či některých PDF) a nad touto vrstvou je další vrstva, která je pro potřeby tzv. „vytěžování dat“ (viz níže). Tato technologie umožňuje vybraným slovním či numerickým

[2] *„ICR (Inteligent Character Recognition) – rozlišování a rozpoznávání ručně psaného písma*
[3] *OCR (Optical Character Recognition) – rozpoznávání tištěného a strojem psaného písma*
[4] *BCR (Bar Code Reading) – systém pro převod čárových kódů do podoby řetězců číslic a písmen*
[5] *OMR (Optical Mark Reading) – převod značky v podobě zaškrtaných nebo zakřížkovaných okének na formuláři“*
(STUCHLÍK, 2008)

spojením přiřadit konkrétní význam. Je tedy schopna rozpoznat např. IČO, DIČ, název firmy, celkovou sumu na faktuře apod. Pro některé firmy jsou tyto dvě části chápány pod názvem OCR, jiné firmy toto rozdělují na OCR technologii a technologii tzv. vytěžování dat.

3.2.5 Validace dat

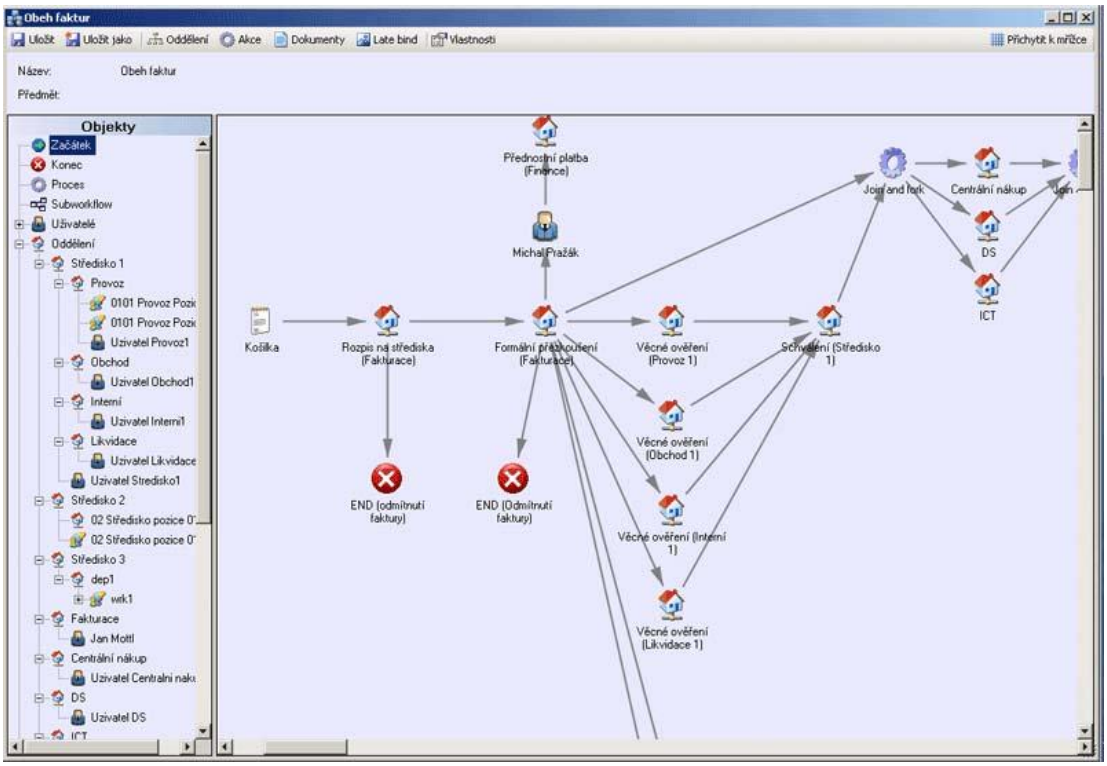
Validace je obvykle prováděna s ERP systémem. Jedná se o propojení např. IČO, DIČ s číselníky dodavatelů, provázání objednávky (je-li vystavena přes informační systém) s fakturou (faktura musí obsahovat číslo objednávky), apod.

3.2.6 Verifikace dat

Systém pro vytěžování dat je možno označit za tzv. expertní systém, neboť **je schopen** „**se učit**“ tj. zdokonalovat. Zpočátku se uvádí úspěšnost vytěžení dat 60% na jednu položku či údaj (nikoliv na jednu fakturu a všechna z ní vytěžovaná data), a posléze je možné dosáhnout až 80-90%. **Systém** u jednotlivých vytěžených údajů **ukazuje, nakolik** si je jistý, že **data vytěžil správně** (stupně jsou tři: je si jistý zcela, zčásti nebo vůbec). Políčka jsou zpravidla barevně rozlišena, spolu s vytěžovanou částí textu, ze kterého software data čerpal (viz příloha č. 2). Je možné systém nastavit tak, že pokud si je 100% jistý, uvolňuje data do databáze a startuje tzv. workflow bez čekání na provedení následné manuální kontroly. Na základě toho mluvíme o tří fázovém nebo dvou fázovém systému verifikace dat (verifikace samotným systémem pro vytěžování dat, porovnání s dalšími informačními systémy, manuální kontrola).

3.2.7 Export dat do databáze

Je část, kdy **systém dokument** se všemi řádně doplněnými náležitostmi **ukládá do** své **databáze** a je možné nastartovat workflow dokumentu (viz obrázek č. 3). Samotný **dokument** po celou dobu manipulace s ním **zůstává nepozměněný**, **mění se** pouze **metadata** k dokumentu. WF je klíčové z hlediska možnosti nastavení kompetencí a zpřehlednění procesu putování digitálního dokumentu po podniku. V jeho vrstvách je možno provést anonymizaci vybraných údajů pro určité uživatele či oddělení.



Obrázek č. 3 – Ukázka workflow faktury (zdroj: web společnosti Way Up)

3.3 Document Management System (DMS)

Document Management System **je**, jak již ze samotného názvu vyplývá, **systém pro správu elektronických dokumentů.** Mapuje a zaznamenává životní cyklus dokumentů od jejich exportu do databáze (včetně metadat, která sdělují, kdy byl dokument přijat a digitalizován) až po jejich elektronickou skartaci. **Organizuje** digitální dokumenty do přehledných struktur **a vytváří** mezi nimi tzv. **provazby** (logická organizační propojení). **Jsou** tedy jasně **odlišené** jednotlivé **verze dokumentů** (systémy je buďto řadí chronologicky nebo uživatelé vybírají majoritní tedy v té chvíli aktuální verzi a minoritní verze), **stav** dokumentů (schválené, zamítnuté, zpracovávají se) včetně toho u koho se v současné době nacházejí nebo jak dlouho s ním který uživatel pracoval (**historie manipulace** s dokumentem včetně údaje, **kdo jej ukládal** jinam než do DMS) **s možností psaní komentářů** k jednotlivým akcím. Systém umí pružně operovat s jednoduchým, pokročilým nebo fulltextovým vyhledáváním. Dále se přes DMS nastavuje **i tzv. konkurenční přístup**, kdy s dokumentem může pracovat více uživatelů najednou.

DMS dokáže zpracovávat **statistiky a reporty** dle předem nebo ad hoc definovaných parametrů (př. upozorňovat na blížící se konce doby splatnosti faktur, hlídá tedy i termíny zpracování dokumentů). **DMS bývá využíván i pro zadávání úkolů** jednotlivým pracovníkům či **zasílání zprávy** „na vědomí“ všem, kteří jsou do workfolow (viz níže) zařazení. DMS má velmi široké uplatnění ve všech organizacích s výrobním či nevýrobním programem.

Výstupy z DMS **je** samozřejmě **možné exportovat do** různých **formátů**, podoby **dle firemních šablon** (př. objednávky), publikovat **na intranet** (př. směrnic) či přesunout **do elektronického uložiště** a následně provádět skartaci elektronických dokumentů s provazbou na jejich listinnou podobu (některé systémy nabízejí skartaci jednotlivých dokumentů – faktura, objednávka, dodací list; jiné skartují soubory dokumentů jako celek). (JAKEŠ, 2008; KUČEROVÁ-ZRÁLÍKOVÁ, 2011)

DMS je nutné chápat jako **dočasné** nikoliv trvalé **uložiště** (KUČEROVÁ-ZRÁLÍKOVÁ, 2011), čím více dat v sobě obsahuje, tím více zaměstnává operační systém.

3.3.1 Workflow

Workflow (dále jen WF) je možné označit za základní „řídící“ jednotku DMS, **dělíme** jej **do dvou skupin**. **Ad-hoc** WF **a standardní**, předem definovaná, WF.

Ad-hoc WF je nastaveno tak, že si **každý uživatel volí svého následovníka** (dalšího v pořadí) nebo tak, že se jedná o velmi jednoduchý řetězec úkolů, jehož základní linii je předem nadefinovaná a uživatel pouze doplní jména následovníků (např. schválení zápisu z porady). Toto je schopen provádět i běžný uživatel.

Standardní WF je obvykle spravováno klíčovým uživatelem. **Jedná se o sadu složitých přednastavených definic**, podle nichž probíhá schvalovací proces určité agendy. (STUCHLÍK, 2008)

WF tak **obsahuje přístupová práva**, která se mohou vztahovat nejen na celý dokument, ale i jen na jeho části (samozřejmě existuje možnost zakrytí předem specifikovaných dat vybraným uživatelům)[6].

Ve WF jsou uživatelé většinou rozdělováni do tří základních skupin:

- Administrátoři
- Klíčoví uživatelé
- Běžní/koncoví uživatelé

Výše uvedené dělení je v praxi běžně používáno dodavateli DMS řešení.

3.3.1.1 Administrátoři

Jedná se o skupinu, která je zevrubně proškolena ohledně administrace celého systému. Z této skupiny mohou být ještě vyjmuti tzv. operátoři, kteří umí pracovat pouze se základními administrativními operacemi systému.

3.3.1.2 Klíčoví uživatelé

Jedná se o skupinu kvalifikovaných uživatelů, správců/vlastníků aplikací. Tito uživatelé by měli být komplexně seznámeni s implementovaným řešením po praktické stránce, aby mohli spravovat konkrétní nadefinované WF.

3.3.1.3 Běžní/koncoví uživatelé

Jedná se o skupinu, která je seznámena se základní funkcionalitou systému, která je důležitá pro jejich práci.

[6] Informace byly přebrány z rozhovorů, materiálů a prezentací firem, které BBNP oslovil v rámci průzkumu

Jednotlivá **práva přístupů** těmto skupinám **jsou sestavována na** základě **Active Directory** (dále jen AD), které odráží organizační strukturu společnosti obvykle definovanou ve vnitropodnikových směrnicích. Možností je i konfigurace na konkrétní účty konkrétních zaměstnanců nebo na skupinu pracovníků (př. účetní oddělení). Při nastavení WF na konkrétní zaměstnance ale hrozí ztráta dat například při jejich odchodu z firmy.

Ve WF se také **nastavují podmínky**, které mají vliv na to, jakým způsobem budou data procházet nadefinovaným schvalovacím procesem. Většinou jsou tyto podmínky (např. u faktur) nastaveny dle výše částky. V jiných případech **jsou kompetence jednotlivých pracovníků** zařazených do WF obvykle definovány organizačními řády firem, jejich postavením v organizačním systému řízení té které firmy.

3.3.2 Delegování

Delegování může probíhat ve WF hned několika způsoby. Systém může být nastaven tak, že **pokud uživatel nezareaguje** do určité doby, **systém jej přeskočí** a pošle dokument následujícímu v pořadí, další možností je, že **uživatel nastaví delegování** určitého (nebo všech) WF, ve kterých figuruje, na někoho jiného, **popřípadě** se **může být provedeno automaticky** za pomoci funkce tzv. „out of office“, který může být předem nakonfigurován nebo může být automaticky spuštěn přes napojení na informační systém pro řízení lidských zdrojů[7].

Toto je důležitá funkce zejména proto, že je někdy nutné zpětně dohledávat, kdo daný dokument schválil, přijal nebo na něj odpověděl. Některé urgentní záležitosti je nutné řešit rychle a je tedy potřeba mít jistotu, že budou řešeny. Ve firmách se narychlo shánějí hesla k účtům lidí, kteří jsou např. na dovolené nebo se myslí, že to někdo vyřídí, a to je, dle mého, hazard, kdy odpovědnost za případnou škodu jde na člověka, který tou dobou ani nebyl v práci (a měl př. dovolenou oficiálně schválenou a zanesenou v HRM)

[7] Tomuto systému se též říká Human and Resources Management a je spravován personálním oddělením. Obsahuje údaje o zaměstnancích, monitoruje dovolené nebo např. spravuje docházkový systém.

4 Počítačová kriminalita

„S rostoucí popularizací internetu a rozšiřováním uživatelské základny však došlo k pozvolné degradaci ideálu kybernetického světa a jeho postupnému ztotožňování se světem reálným. Virtuální povaha kyberprostoru nemohla zabránit převzetí některých záporných společenských jevů, mezi nimiž na předním místě figuruje i kriminalita.“

Alice Táborová

S **nárůstem** počtu uživatelů ICT narůstá i **počet útoků**, **které se týkají** nejenom **firem či různých institucí**, ale **i domácností**. **Počítačová kriminalita** by se dala charakterizovat jako *„hospodářský **trestný čin spáchaný pomocí počítače či internetu**. Typickými příklady počítačové kriminality jsou šíření virů, nelegální stahování médií, phishing, pharming a krádeže osobních informací. Nespadají sem běžné podvody, kdy je počítač používán jako vedlejší nástroj s cílem spáchat podvod. **Zahrnujeme** zde pouze takové **hospodářské zločiny**, kde jsou počítač, internet nebo **užití elektronických médií a zařízení hlavním**, nikoliv nahodilým, **prvkem**.“* (PRICEWATERHOUSECOOPERS, 2011) Norma ČSN ISO/IEC 2382-8 užívá pojem počítačový zločin a krátce jej definuje jako *„**zločin spáchaný pomocí systému zpracování dat nebo počítačové sítě** nebo s nimi přímo spojený.“* (ČSN ISO/IEC 2382-8, 2001). Toto ještě Požár ve své definici počítačové kriminality upřesňuje na „***trestný čin namířený proti integritě, dostupnosti** nebo **utajení** počítačových systémů nebo trestný čin, při kterém bylo použito informačních či telekomunikačních technologií. (…) Počítačovou kriminalitou jsou chápány **aktivity**, **které vedou k neautorizovanému čtení, manipulaci, vymazání nebo zneužití dat**.“* (POŽÁR, 2005)

„Oblíbenost“ útoků skrze kyberprostor je jistě ovlivněn také tím, že *„naučit se postup pro spáchání takových trestných činů je v zásadě snadné a v porovnání se škodami, které tyto trestné činy mohou způsobit, vyžadují nemnoho zdrojů a jsou zdánlivě levné. Také mohou být spáchány v rámci určité jurisdikce, aniž by jí byl pachatel podroben fyzicky. Počítačová data jsou snadno přenosná a není snadné jejich tok sledovat.“* (TÁBOROVÁ, 2010) Myšlenku o jurisdikci bych ještě rozvedla tak, že kyberprostor je globální prostředí, tudíž se útočník může připojit odkudkoliv na světě, kde je přítomna síť. (ZEMKO, 2011)

Podle společnosti Symantec[8] množství útoků vzrostlo mezi rokem 2010 a 2011 (letošní rok ještě vyhodnocen není) o 81%. (KUŽEL, 2012) **Útoky se** ve firmách **dělí na** ty, které jsou **prováděny zevnitř** (zaměstnanci – stávající, bývalí, infiltrovaní) **a** na ty, které jsou **vedeny z vnějšku** organizace (dodavatelé, zprostředkovatelé, odběratelé, apod.). (PRICEWATERHOUSECOOPERS, 2011; MEJCHAROVÁ, 2008) **U útočníků** lze vysledovat zejména **dva** primární **cíle**, kterými je přímý **finanční prospěch** a **úmyslné poškození** někoho, kdo se jim znelíbil. Nelze ovšem opomenout i **další možnosti**, mezi které se řadí prostý **vandalismus**, snaha o **zvýraznění** sebe sama (ego) nebo **ukázaní** vlastní **technické zdatnosti** (výzva, prestiž). (HOUSER, 2011; ČSN ISO/IEC 27 005)

Ovšem při přehodnocování rizik a zhodnocením adekvátnosti podnikového bezpečnostního řešení nebo strategie, bychom měli mít na zřeteli fakt, že **některé podniky jsou ohroženy více a jiné méně**. **Ohroženější jsou** především ty, které mají **zakázky z** oblasti **obrany**, **finančních služeb**, **zdravotnictví a** společnosti **s významným duševním vlastnictvím** (např. převratné výrobní procesy). (FITZGERALD, 2012; VELECKÝ, 2012; STACHNÍK, 2012) A na základě toho také realisticky přistupovat k **bezpečnostním opatřením**, která **by neměla překážet** uživatelům při rutinní práci, jak říká Požár *„velmi účinná bývají často i ta nejjednodušší bezpečnostní opatření“*. (POŽÁR, 2005)

Jak jsem již zmínila výše, do popředí zájmu se dostávají informace, protože čím dál tím **více firem má rozhodující podíl** svého **majetku** právě **v nehmotných aktivech** (HOUSER, 2011). **Mezi**, pro útočníky, zajímavá **data patří citlivá** nebo **osobní** (rodné číslo, adresa trvalého bydliště, biometrické údaje, apod.)**, krádeže údajů z platební karty** (ty ale, dle novějšího průzkumu od Symantec, už dnes nejsou tak časté) **a seriózní dokumenty** (smlouvy, plány, technická dokumentace, marketingové plány, výsledky výzkumu a vývoje, zdrojové kódy v případě softwarového byznysu). (OBLUK, 2011; KUŽEL, 2012, HOUSER, 2011) Mezi **nepřímé útoky** se řadí **zneužití počítače** k dalším útokům a jiné nelegální činnosti. (OBLUK, 2011)

[8]Společnost zabývající se poskytováním řešení pro zabezpečení, správu systémů a uložišť. Jedním z jejích produktů je antivirus Norton

4.1 Kyberterorismus

Jako podkategorii počítačové kriminality vnímám tzv. **kyberterorismus**. Kyberterorismus **je konvergencí terorismu a kyberprostoru** obecně chápaný jako **nezákonný útok** nebo **nebezpečí útoku proti počítačům, počítačovým sítím a informacím v nich skladovaným** v případě, že **útok je realizován substátními skupinami**, **tajnými agenty** (zasvěcené osoby, interní pracovníci) **či jednotlivci** (crackeři, hackeři). Jeho **účelem je zastrašit nebo donutit vládu**, **nebo obyvatele k podporování sociálních nebo politických cílů** a **výsledkem je násilí**. (DENNING, 2000; POLLITT, 2001; JANCZEWSKI, COLARIK, 2005; ABERLE, 2010) Kyberterorismus je velkou hrozbou zejména proto, že výrobní procesy jsou v podnicích řízeny přístroji – počítačovými systémy, stačí tedy pouze upravit jejich nastavení, aby došlo k hmotné škodě. Pozměněné dávkování by např. ve farmaceutickém průmyslu mohlo mít až fatální následky. Nemluvě o propojení celé informační infrastruktury ať už organizací či státu, kde i nejmenší zásah může způsobit velký rozsah škod.

4.2 Počítačová kriminalita v České republice

Studie PriceWaterhouseCoopers (dále jen PWC) za rok 2011 ukázala, že počítačová kriminalita se v ČR nachází s 13% na čtvrté pozici. České společnosti se nejvíce obávají krádeže duševního vlastnictví (včetně krádeže dat), poškození dobrého jména společnosti a krádeže osobních údajů. Jako nejpravděpodobnější pachatelé uvnitř společnosti se jeví zaměstnanci z oddělení IT (51%). Konkrétně se jedná o ty zaměstnance, kteří mají administrátorská práva pro přístup do systémů s možností editovat či mazat data, a tím pádem i možnost za sebou zahlazovat stopy. Respondenti vidí další riziko v oddělení obchodu a marketingu (31%), financí (22%) a oddělení provozu (20%).

Po odhalení vnitřního pachatele došlo v 81% případů k rozvázání pracovního poměru, a k tomu u každého druhého případu byla ještě informována i policie. V případě externího pachatele byla policie informována v 86% případech a v 71% společnost ukončila vztah s obchodním partnerem. Ačkoliv PWC zmiňuje, že tato cesta vypořádání se s pachateli, je správná, doporučuje klást větší pozornost na samotnou prevenci.

(PRICEWATERHOUSECOOPERS, 2011) Ne všechny společnosti chtějí vyrozumět policii, protože nechtějí poukazovat na chyby v bezpečnostní politice např. banky.

4.3 Vnější hrozby

Útoky na počítače či jejich uživatele **autoři** zpravidla **rozdělují do čtyř kategorií**. Veselý člení útoky na **hackerské nástroje**, **síťové útoky**, **útoky na webové aplikace a sociální inženýrství**. Hájiček se shoduje v obsahu s tímto členěním, ale útoky nejprve rozlišuje na automatizované a manuální, a teprve poté je dále dělí do podskupin. Ty se skládají z malware (automatizovaný útok), zachycení/podvržení komunikace (manuální útok), exploit (manuální útok) a předstírání identity (automatizované/manuální útoky). Benešovská se ve své práci soustředí na hrozby, které štěpí na základní a aktivační. (VESELÝ, 2011; HÁJIČEK, 2012; BENEŠOVSKÁ, 2011) Poukazuje tak na jejich provázanost, kdy počítačové viry mohou v počítačích zanechávat Backdoors apod. Jelikož první tři druhy útoků studentské kvalifikační práce a další materiály velmi dobře a skutečně podrobně rozebírají, vyjmenuji pouze pojmy, které se pod jednotlivými kategoriemi skrývají a budu se více věnovat čtvrtému typu, kterým je sociální inženýrství:

- Hackerské útoky/malware
    - Promalovače hesel (viz kapitola Hesla), Backdoors, Skenery, Rootkity, Trojské koně, Počítačové viry, Počítačoví červi, Spyware, Keylogger, Adware
- Síťové útoky/zachycení nebo podvržení komunikace
    - Sniffing, Man-In-the-Middle, DoS, DDoS
- Útoky na webové aplikace/Exploit
    - Cross-Site Scripting, SQL Injection, HTTP Response Splitting
- Sociální inženýrství/Předstírání identity

4.3.1 Sociální inženýrství

Rostoucím **typem útoků je** právě tzv. **sociální inženýrství** nebo také **sociotechnika**, které se zaměřuje na lidský faktor a zdá se, že to je zatím relativně podceňovaným aspektem hackingu. **Cílem je**, skrze manipulaci na základě důvěry, soucitu, sympatie, stresu, aj., **získat**

informace důvěrného charakteru, **anebo** je přinutit k **vykonání požadovaného úkolu**. (FITZGERALD, 2012; NETOLICKÁ, 2012) Toto vyzrazení by se mohlo označit za porušení zákona č. 148/1998 Sb., o ochraně utajovaných skutečností. *„Zachováním mlčenlivosti je povinnost nesdělovat utajovanou skutečnost osobě, která není oprávněna se s takovou skutečností seznamovat.“* (§2 odst. 3 zákona č. 148/1998)

Způsoby vyzrazení vyjadřuje Požár tabulkou č. 1, která, pokud bychom na případy hleděli jako na nedbalost nebo nedostatečnou informovanost zaměstnanců, koresponduje s rozdělením sociálního inženýrství, které se dělí do těchto kategorií: phishing, vishing, trashing a pharming. (HORNÍČEK, 2009) Pharming se týká především internetového bankovnictví, které pro potřeby diplomové práce není považováno za relevantní.

Způsob	**Nosič**
Bezprostředně (ústně)	Mluvené slovo
Vypracování a předání dokumentu grafického, písemného, zvukového na materiálním nosiči papírovém nebo elektronickém	Písemnost, obraz, foto, film, video záznam, magnetofonová nahrávka, disketa
Elektronické předání pomocí počítačové sítě, drátovými nebo bezdrátovými pojítky	Elektronické zařízení a příslušná média jako disky, CD a DVD

Tabulka č. 1 – Způsoby vyzrazování informací mezi osobami (POŽÁR, 2005)

4.3.1.1 Pishing

Phishing, v češtině též „rybaření“ nebo „rhybaření“, je podvodné jednání, které **se snaží získat** od uživatelů **osobní data** např. čísla kreditních karet, přihlašovacího jména a hesla, apod. Setkat se s ním můžeme **v emailové komunikaci**, **na webových** stránkách sociálních sítí, na falešných webových stránkách (např. banka nebo vybírání darů pro charitativní účely - webové stránky se snaží tvářit a vypadat důvěryhodně, ale liší se od té pravé URL adresou), při instant messagingu (ICQ) nebo jako zprávy na mobilních telefonech**. Phishing přes** Voice over Internet Protocol (**VoIP**) se nazývá **vishing** (HORNÍČEK, 2009; BEZPECNYINTERNET.CZ, 2012)

4.3.1.2 Trashing

Trashing je mnohými společnostmi i lidmi často podceňovanou technikou. Jedná se doslova o **fyzické prohledávání odpadků firmy**. (HORNÍČEK, 2009) V dnešní době i firmy přistupují k odpadu ekologicky, tudíž je snazší prohledávání pouze papírového odpadu. Tato technika se soustřeďuje na podceňování užitečnosti staré listinné dokumentace a také na zvyk některých zaměstnanců si vše elektronické tisknout.

4.3.1.3 Prevence sociálního inženýrství

Z pohledu bezpečnosti informací je zde napadán aspekt důvěrnosti. Dle mého názoru jedinou možnou prevencí je to, že zaměstnanci vědí, co je důvěrné a na co nemá někdo nepovolený nárok. Norma ČSN ISO/IEC 27 001 doporučuje zajistit informacím odpovídající úroveň ochrany na základě jejich kategorizace, která by měla být provedena s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost. To je třeba chápat ne v soupisu citlivých informací, ale jako součást každého digitálního dokumentu, nejlépe jasně viditelné již na první stránce.

Toto se odráží i v možném řešení hrozby trashingu, kterou je práce buďto pouze s elektronickými dokumenty nebo řádné dodržování skartace veškeré listinné podoby. Ovšem i samotná skartace má několik stupňů, např. dle typu dokumentu dle NBÚ (neklasifikované, vyhrazené, důvěrné, tajné, přísně tajné) od skartace na proužky až po křížový řez (viz příloha č. 3).

4.3.1.4 Testování sociálního inženýrství

Ačkoliv si např. společnost ESET zařazujeme jako společnost, jejímž produktem je antivirová ochrana, není to docela přesné. Zaujalo mě, že dnes již tyto firmy nabízejí i testování skrze sociální inženýrství.

Testy fungují na základě definice znalosti prostředí útočníkem:

- Bez znalosti interního prostředí (neznámý útočník)
- S částečnými poznatky (bývalý zaměstnanec, pracovník dodavatele)
- Disponující jistou úrovní fyzického a logického přístupu k aktivům organizace (současný zaměstnanec)

Dále nabízejí užití těchto metod:

- Phishingový test
- Vishingový test (telefonický test)
- Test s přenosnými médii
- Pokus o průnik do prostoru organizace
- Trashing

Metody lze pro jejich vyšší důvěryhodnost kombinovat. Např. zaslání phishingového e-mailu může být podpořeno telefonickou žádostí o prověření doručení nebo může být zdůrazněna jeho důležitost. (NETOLICKÁ, 2012)

4.3.2 Advanced Persistent Threts (ATP) a obrana skrze Data Loss Prevention (DLP)

Všechny výše zmíněné **útoky** jsou stále častěji **cílené a** čím dál tím více sofistikované, a proto již mají svůj vlastní termín. **Označují** se jako **Advanced Persistent Threts** (ATP). Přesná definice, kterou přináší Národní institut standardů a technologií (NIST), zní takto *„Nepřítel má rozsáhlé odborné znalosti a značné zdroje, které mu umožňují vytvářet příležitosti k dosažení jeho cílů pomocí více vektorů útoku (např. počítačového, fyzického a pomocí podvodu). Tyto cíle obvykle zahrnují vytvoření a rozšíření opěrných bodů v rámci infrastruktury informačních technologií napadené organizace za účelem extrahování (tj. přenosu z vnitřní sítě na externí servery) informací, podkopávání či blokace důležitých záměrů mise či programu samotné organizace nebo jen získání pozice pro dosažení těchto cílů v budoucnosti. Útok APT usiluje o své cíle opakovaně po delší dobu, přizpůsobí se úsilí*

obránců odolat a je určený k zajištění úrovně interakce potřebné k dosažení jeho cílů.“ (FITZGERALD, 2012) **Možnou obranou je** změna přístupu v ochraně. Tedy **přesun pozornosti** ze zabezpečení počítačů a firemních sítí **na** samotná **data** skrz **nástroje Data Loss Prevention** (DLP), které **monitorují** data v celém jejich životním cyklu. Sledují jejich kopírování, modifikaci, tisk, jejich přeposílání e-mailem, změna formátu, vytváření PrintScreenu, nahrávání na přenosná média (př. USB flashdisk), apod. **a mohou** tyto činnosti **i blokovat**. (HOUSER, 2011; JAVORA, 2012) Bohužel DLP zatím neexistuje pro mobilní zařízení, (JAVORA, 2012) kde se dle společnosti Eset očekává v roce 2013 zvýšení útoků prostřednictvím malware.

4.4 Vnitřní hrozba: Zaměstnanci

Směrnice ČSN ISO/IEC 27 005 uvádí, že motivace ke spáchání bezpečnostního incidentu interních pracovníků mohou být zvědavost, ego, vyzvědačství, finanční prospěch, odplata, ale nesmíme opomenout ani neúmyslné chyby a opomenutí (př. instalace programů, chybné manipulace s daty, atd. Na vině může být špatné zaškolení pracovníků, nespokojenost, škodolibost, nedbalost, nečestnost nebo se může jednat o pracovníky s ukončenými poměrem. Možné důsledky se dle směrnice mohou projevit formou napadení zaměstnance, vydírání, prohlížení chráněných informací, zneužití počítačů, podvod a krádež, získání informace za úplatu, vložení falešných nebo upravených dat, instalace škodlivého softwaru (př. počítačový vir, trojský kůň) apod. Bohužel, studie provedená společností Cisco toto doplňuje, že stále u některých zaměstnanců převládá pocit, že nedělají nic špatného, když občas poruší bezpečnostní pravidla (RYVOLA, 2012).

Směrnice, ale také mnohé jiné práce hovoří o zaměstnancích nebo celkově o lidském faktoru ve firmě, jako kdyby se jednalo o ucelenou skupinu. **Já se přikláním k teorii informačních generací** podle Davida Bawdena, která **rozděluje generace do** několika **skupin**. **Generace veteránů** (rok narození 1915-1945), **Baby boomers** (někdy též poválečné děti; 1945-1964), **generace X** (1965-79), **generace Y** (1980-1994) a **generace Googlu** (někdy též Digital natives 1995-2010) (IKAROS REDAKCE, 2009). **Personalisté generaci Y rozdělují** do let 1975-1995 a zároveň dodávají, že narození mezi rokem 1975 a 1984 mají ještě stále blíže ke generaci předchozí. Generaci Googlu označují také jako generaci Z. Dále

rovněž upozorňují na fakt, že *„do roku 2025 bude generace Y tvořit převážnou část populace v produktivním věku.“* (REZLEROVÁ, 2009)

Vzhledem k tomu, že nejstarším z této generace je 32 let, a i ke slovům personalistů, nemusí mít tato generace zatím projevovat ani výrazně a ani nemusí mít významný hlas v organizaci, přesto je očividné, že se tato skutečnost bude postupně vyvíjet s poměrem počtu zaměstnanců zastupujících tuto generaci ve firmě či v instituci. Co tedy s sebou výměna generací přinese? Jak se to bude projevovat na informační politice firmy? Snažila jsem se popsat pouze dle mého názoru reálné prognózy do budoucnosti na základě důvěryhodných studií prováděných společností Gartner (viz níže).

4.4.1 Generace Y

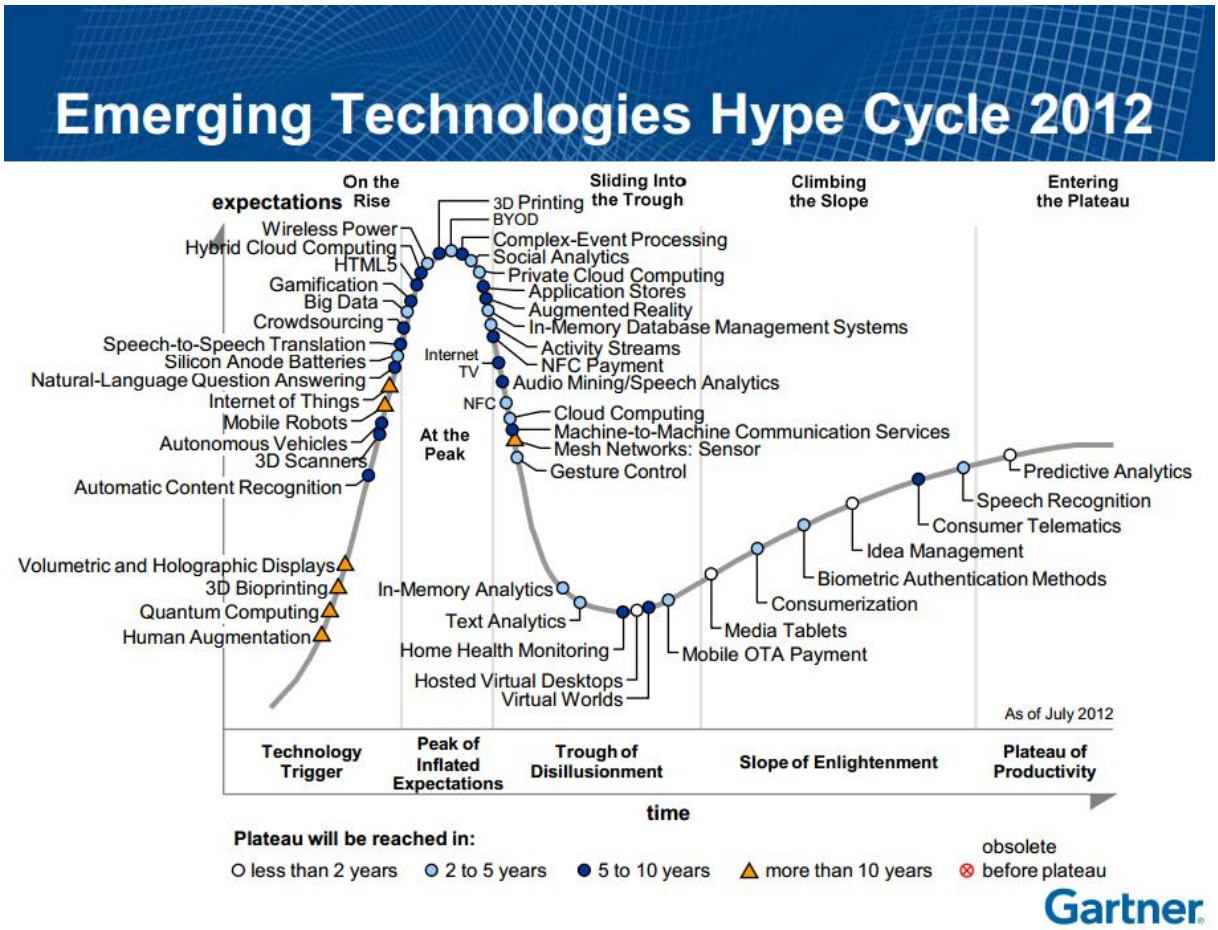
Mezi faktory, které **na tuto generaci působí**, ať už přímo či nepřímo, se řadí **digitalizace světa**, **konec studené války**, **nové politické a ekonomické struktury** a **teroristický útok 11. září 2001**, který byl v podstatě jedinou významnou tragickou událostí, kterou generace prožila. I když má tato generace **přístup ke všem druhům médií**, **začíná** u ní **dominovat** používání **webu** a **mobilních telefonů** (ty jsou nahrazovány tzv. chytrými telefony). (KOUDELOVÁ, 2012; REZLEROVÁ, 2009).

Další charakteristikou je **užívání sociálních sítí** (Twitter, Facebook, Linked-in, Google +, aj.), které se postupně přerodilo z užívání instant messaging (ICQ, Messanger, aj.). Socializace prostřednictvím internetu může následně vykrystalizovat v spojení ve fyzickém světě. A proto je tedy i z hlediska bezpečnosti elektronických dat více zaměřená z pohledu bezpečnosti na útoky spojené s technologií peer-to-peer při sdílení souborů v rámci výměnných síti. (KOUDELOVÁ, 2012; DIMENSIONAL RESEARCH, 2012; ČERMÁK, 2003)

Na základě tohoto krátkého profilu jsou poté pochopitelné výsledky výzkumu, který poukazuje na to, že 75% zástupců generace Y usuzuje, že právě **skrz technologii je možné dosáhnout vyšší efektivnosti** jednotlivých činností. Mnoho pracovníků z řad této generace se cítí *„být omezováno zastaralými pracovními postupy,“* (KOUDELOVÁ, 2012), které souvisí i

s výběrem podnikového SW. Ten totiž většinou postrádá flexibilitu a efektivitu sociálních sítí. (VITÁSKOVÁ, 2012)

Pojďme se nyní podívat na Gartnerův **Emerging Technologies Hype Cycle diagram**[9] (který bývá překládán jako Křivka nastupujících technologií) (graf č. 1), který byl společností sestaven v červenci roku 2012.



Graf č. 1 – Emerging Technologies Hype Cycle Diagram 2012 (GARTNER, 2012)

Křivka *„znázorňuje vyspělost nových technologií, jejich připravenost na implementaci i úroveň jejich viditelnosti na veřejnosti.“* (BARTOLŠIC, 2012) Jackie Fen[10] říká: *„Na křivce*

[9] Vysvětlení jednotlivých částí Hype Cycle diagramu je možno nalézt přímo na stránkách společnosti Gartner www.gartner.com

[10] Viceprezidentka společnosti Gartner, její projev k diagramu je možné nalézt na tomto odkaze: http://www.gartner.com/technology/research/hype-cycles/

najdete řešení, která se těší pozornosti veřejnosti a médií, ale i ta méně populární, jež však mají velký význam.“

Z křivky je patrné, že společnost již nechce být nezávislá nejenom z pohledu času a místa, ale také z hlediska možností zařízení. To zahrnuje **BYOD**, **hostované virtuální deskostopy**, **HTML5**, **Cloud computing**, **silikonové baterie** a **tablety**. Dalšími ucelenými kategoriemi jsou **Chytřejší přístroje**, **Big data** a **Global Scale Computing** (překládaný jako globální výpočetní výkon za nízké ceny) a Lidská komunikace s technologiemi. (LAUSCHMANN, 2012; BARTOLŠIC, 2012; GARTNER, 2012) Pro tuto práci je nejzajímavější z pohledu provázanost generace Y jako zaměstnanců s trendem BYOD a cloud computingem (privátním i veřejným), jejichž nástup se očekává mezi 2-5 lety. Přesto se o této problematice začínají objevovat čím dál tím víc články ve specializovaných časopisech.

4.4.2 BYOD a BYOA

„Podnikoví CIO[11] už nechodí a neříkají: „Chtěli bychom pořídit notebook všem ve firmě, ale prohlašují: Rádi bychom spravovali každý notebook každého ve firmě. Takto vypadá nástup konzumerizace.“

Dave Asprey,
Viceprezident pro zabezpečení cloudu společnosti Trend Micro

BYOD je zkratkou pro **Bring Your Own Device**, tedy přines si „do práce“ své vlastní zařízení, a BYOA (**Bring Your Own Application**), tedy přines si svou vlastní aplikaci. Oba tyto trendy **jsou úzce spojeny s** tzv. **konzumerismem**, kdy se lidé setkávají s novými ICT ve svém soukromém životě a zvyknou si je používat. V této chvíli přichází BYOD nebo BYOA, kdy si své zařízení či aplikaci, které z pohledu SW i HW mohou být lepší než ty, které nabízí pracovní zázemí, chtějí přinést i do práce. Průzkum společnosti Fortinet[12] dokonce ukázal, že respondenti (více jak polovina z nich) považují možnost BYOD spíše jako své právo než jako výsadu. (BROŽ, 2012)

[11] Chief Information Officer, vedoucí oddělení IT
[12] Společnost zabývající se bezpečností informačních technologií (http://www.fortinet.com)

To ovšem znamená **poměrně velký objem úložné kapacity**, která se z firemního pohledu **může označit za nespravovanou**. (ZAJÍC, 2012) Nemluvě o faktu, že mnoho lidí si ve svých smartphonech užívají cloudové služby jako např. Gmail, iCloud nebo služby sociálních sítí. Díky tomu vpuštění takového zařízení do sítě LAN znamená přinést do firmy všechna nebezpečí, cloudu i tradičních bezpečnostních problémů (BRAUE, 2012; GARTNER, 2012)

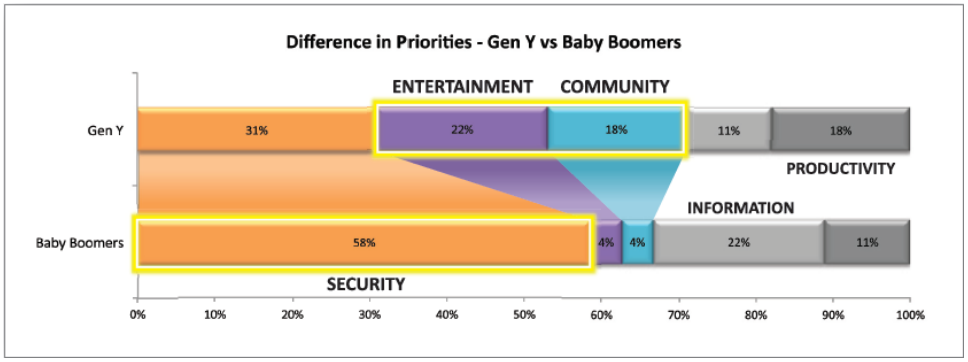
„Chcete-li zabezpečit cloudové služby, musíte především chránit svá mobilní zařízení.“

Dave Asprey

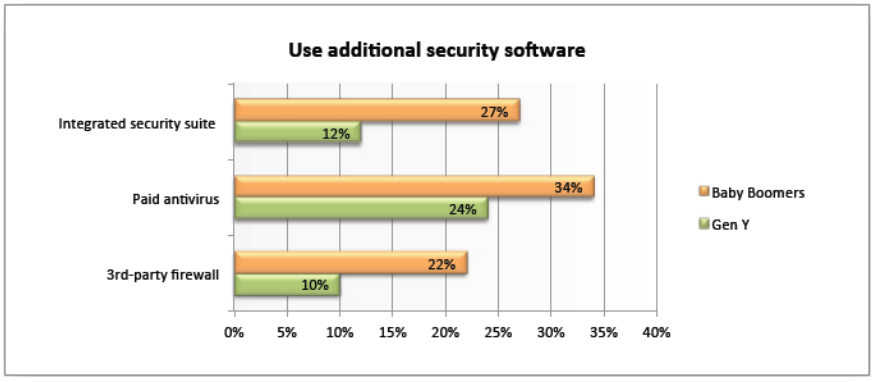
Gartner varuje, že je snazší tyto přístroje ztratit nebo napadnout skrze **slabé heslo** či **slabou ochranu operačního systému**, na druhou stranu se zde objevují i názory, že **zaměstnanec si na své** vlastní zařízení naopak **dává větší pozor** (KUNEŠ, 2012). Narušena ovšem může být touha zajistit data tak, aby byla ve správnou chvíli na správném místě (GARTNER, 2012), vzhledem k tomu, že **oddělení IT** nad tím nemůže mít 100% kontrolu.

Jako možné řešení BYOD je přispění určitou sumou zaměstnancům na nákup oddělením IT vybraného zařízení a definovat požadavky na SW vybavení včetně specifikace antivirového řešení. (KUNEŠ, 2012)

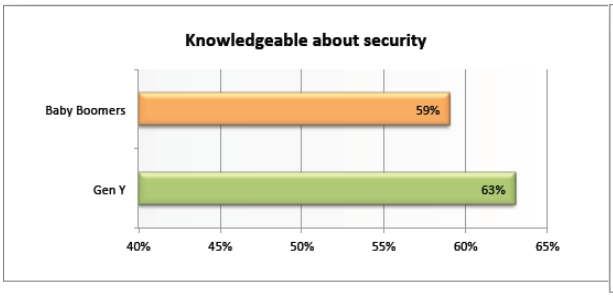
S touto problematikou souvisí i studie Dimensional Research, která poukazuje na rozdílné přístupy generací k bezpečnostní otázce. Poukazuje, že bezpečnost (graf č. 2), stejně jako **užívání placeného SW** pro ochranu počítače (graf č. 3), **generace Y** nevnímá jako prioritu. A to i přesto, že **je informovanější** a touto problematikou více dotčena, **než generace předchozí** (graf č. 4 a č. 5) (DIMENSION RESEARCH, 2012).

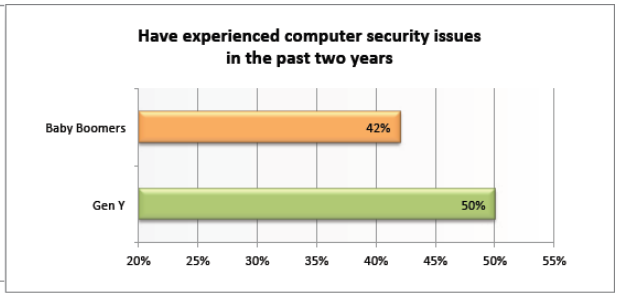


Graf č. 2 – Rozdíly v prioritách generace Y a Babyboomers (DIMENSIONAL RESEARCH, 2012)



Graf č. 3 – Užívání SW pro ochranu zařízení (DIMENSIONAL RESEARCH, 2012)





Graf č. 4 – Znalosti týkající se bezpečnosti

Graf č. 5 – zkušenosti s bezpečnostním problémem za poslední dva roky (DIMENSIONAL RESEARCH, 2012)

4.4.3 Hesla

Použití hesla je jednou z možností procesu **autentizace**[13] do systému. Hesla je možné rozdělit na dva druhy a to na **hesla statická a dynamická**. **Dynamická hesla se mění** dle předem stanovených algoritmů a příkladem může být jednorázové heslo generované přes lokální zařízení nebo vzdáleně přes mobilní přístroj (př. SMS). (ŽÁČKOVÁ, 2011) Pro nás jsou ale z firemního pohledu zajímavější hesla statická.

Statické heslo je i dnes stále ještě nejčastější autentizací. Jeho neprolomitelnost určují především čtyři faktory: četnost jeho obměny, délka (řetězec 8-12 znaků), složení a obsah znaků. Za **bezpečné heslo je** označováno to, **jehož prolomení** obvyklými technikami **je** jednoduše **příliš časově náročné** (viz tabulka č. 2). Toto se dá ještě prodloužit na základě opatření, které po určitém počtů neúspěšných pokusů počítač na několik minut uzamkne (HOUSER, 2011). Hesla by neměla mít žádný sémantický význam (fráze, data, ID uživatelů, jména, slova), měla by obsahovat nahodilost, chaotičnost (informační entropii) (SCHULTZOVÁ, 2012; MATYÁŠ, 2008; GRYGAR, 2007). Grygar velmi přehledně shrnuje několik zásad pro silné heslo:

- Heslo by mělo být alespoň osm znaků dlouhé
- Heslo b sobě nesmí obsahovat smysluplné slovo (např. narozeniny, jana2009 apod.)
- Heslo nesmí být spojeno s informacemi o uživateli (např. rodné číslo, telefonní číslo, datum narození, apod.)
- Heslo obsahuje malá i velká písmena standardní abecedy
- Heslo obsahuje číslice a speciální znaky (např. !,§,#, apod.)
- Heslo by se mělo v určité periodě měnit (GRYGAR, 2007)

Ovšem u speciálních znaků se může vyskytnout problém při zadávání hesla v zahraničí. (POKORNÝ, 2011) Stejně jako u dlouhého hesla je výskyt vyšší pravděpodobnosti překlepu.

[13] *„Proces, ve kterém informační systém ověřuje identitu uživatele nebo služby.“* (POKORNÝ, 2011)

Dnes je moderní integrovat mnoho služeb do jedné a tím pádem mít ke všemu přístup skrze stejný login. Případným útočníkům stačí získat pouze jedno heslo, přes které se dostanou k celé digitální identitě oběti. (BESTUZHEV, 2012) Bohužel sduie Zhanga a McDowella ukázala, že i v případě, kdy mají uživatelé na internetu průměrně 25 účtů a denně píší zhruba 8 hesel denně, střídá uživatel pouze okolo 6 typů hesel. (ZHANG, MCDOWELL, 2009).

Dalším zlozvykem je si hesla poznamenávat. Výjimkou není heslo zapsané v předmětu emailu nebo na papírku nalepeném na monitoru. (ŽÁČKOVÁ, 2011) Je tedy možné, že právě proto Požár ve své publikaci píše, že *„vnitřním útočníkem je většinou zaměstnanec organizace, který je připojený do vnitřní počítačové sítě.“* (POŽÁR, 2005)

Kombinace použitá pro heslo	Odhad doby práce prolamovače
4 velká nebo malá písmena	několik sekund
4 velká a malá písmena, libovolně kombinovaná	několik sekund
4 velká a malá písmena a číslice v libovolné kombinaci	několik sekund
5 velkých a malých písmen	méně než jedna minuta
5 velkých a malých písmen v libovolné kombinaci	cca 6 minut
5 velkých a malých písmen a číslic v libovolné kombinaci	cca 15 minut
8 velkých a malých písmen	cca 58 hodin
8 velkých a malých písmen v libovolné kombinaci	cca 21 měsíců
8 velkých a malých písmen a číslic v libovolné kombinaci	cca 7 let
10 velkých a malých písmen	cca 5 let
10 velkých a malých písmen v libovolné kombinaci	cca 4648 let
10 velkých a malých písmen a číslic v libovolné kombinaci	cca 26984 let

Tabulka č. 2 – Odhad doby práce prolamovače hesel podle typu hesla (VESELÝ, 2011)

5 Úprava bezpečnosti a práce s elektronickými daty v legislativě

V úvodu této části bych chtěla ještě jednou zdůraznit, že si tato část neklade nároky na provedení vyčerpávajícího přehledu legislativní úpravy problematiky řešené v ostatních částech. Shledala jsem ovšem za vhodné tuto část zařadit pro celkovou celistvost řešeného tématu, ale pouze v následujícím rozsahu bez ambicí na naplnění odbornosti z hlediska právního pojetí.

5.1 Úprava digitalizace dat a jejich dlouhodobé uložení v zákoně o archivnictví a spisové službě

Legislativní rámec je významným faktorem, který obzvláště ovlivňuje proces digitalizace dat v podniku.

Na konferenci DOCURIDE, která se konala v Jihlavě 10. – 11. října 2012, Vladimír Smejkal definoval šest hlavních problémů digitalizace takto:

1. *„Chybné chápání pojmů: písemnost, listina, dokument*
2. *Technologicky závislá legislativa, která se sestává z konkrétních pojmů, které nelze ani výkladem rozšířit*
3. *Prováděcí předpisy, které zužují univerzální dikci zákonů*
4. *Přílohy, které nelze mít v elektronické podobě*
5. *Démonizace zákona o archivnictví a spisové službě*
6. *Obecná touha mít papír v ruce a tedy „mít kontrolu“ nad procesem“* (SMEJKAL, 2012)

5.1.1 Písemnost

Písemnost v tom nejobecnějším smyslu slova **nemusí být vyhotovena pouze na papíře**, může být zaznamenána např. na kameni, zvířecí kůži nebo být ve formě elektronického dokumentu.

Charakteristiku písemnosti lze shrnout do čtyř bodů:

1. *„Jde o **hmotný nosič (substrát)**, obsahující určitou informaci*
2. *tato **informace je** na onen hmotný substrát **někým zapsána** a souvisí s ním,*
3. *a to tak, **aby mohla být následně** informace **přečtena** libovolnou osobou,*
4. ***Přičemž bude zřejmé, kdo tuto informaci** na nosič **zaznamenal, nejde-li o anonym**.“*

Definice nezmiňuje technologickou realizaci zápisu, fyzikální podstatu hmotného substrátu, ani způsob, jakým se může libovolná osoba ujistit o obsahu písemnosti. (SMEJKAL, 2010)

Podle ustanovení § 2 písm. e) zákona č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, ***dokumentem je** každá **písemná, obrazová, zvuková nebo jiná zaznamenaná informace**, ať již **v podobě analogové či digitální**, **která byla vytvořena původce nebo byla původci doručena**.*

5.1.2 Digitální dokument

V rámci digitalizace je pohlíženo na **elektronický dokument** podle toho, jakým způsobem vzniknul. První možnost je, že *„dokument vznikl jako listina, dochází tedy k digitalizaci a vzniklý dokument bude **digitální faksimilií**.“* Druhý případem je, že *„dokument již vznikl v digitální podobě, a proto bude posuzován jako **digitální originální dokument**.“* (SMEJKAL, 2012)

V obou případech je ovšem **stěžejní zachovat** základní právní požadavky, kterými jsou **trvalost, formální určitost a autenticita**. (HÝBLOVÁ, 2012) Je tedy potřeba, aby původce digitálního dokumentu dbal na postup, který zaručuje *„věrohodnost původu dokumentu, neporušitelnost jeho obsahu, čitelnost dokumentu, a to včetně údajů prokazujících existenci dokumentu v digitální podobě v čase.“* (SMEJKAL, 2012)

K tomuto zákon o archivnictví a spisové službě upravuje v §69a odst. 5 tuto vyvratitelnou domněnku: „*Neprokáže-li se opak, dokument v digitální podobě se považuje za pravý, byl-li podepsán uznávaným elektronickým podpisem*[14] *nebo označen uznávanou elektronickou značkou osoby, která k tomu byla v okamžiku podepsání nebo označení oprávněna, a následně za doby platnosti uznávaného elektronického podpisu a kvalifikovaného certifikátu, na kterém je uznávaný elektronický podpis založen, nebo uznávané elektronické značky a kvalifikovaného systémového certifikátu, na kterém je uznávaná elektronická značka založena, opatřen kvalifikovaným časovým razítkem. To platí i pro dokumenty vzniklé z činnosti původců, kteří nejsou určenými původci.“*

Odbor archivnictví a spisové služby toto ještě upřesňuje ve svém stanovisku k užívání časového razítka v souvislosti s odesíláním a ukládáním dokumentů v digitální podobě z 6. dubna 2010. *„Skutečnost, že dokument obsažený v datové zprávě*[15] *není opatřen náležitostmi stanovenými § 69a odst. 5, neznamená, že takový dokument není pravý, pouze na něj nelze aplikovat vyvratitelnou domněnku pravosti ve výše uvedeném smyslu, tj. je nutno prokazovat jeho pravost, nikoliv jeho nepravost.“* (MINISTERSTVO VNITRA, 2010)

Zde je ale potřeba připomenout následující skutečnost: *Je-li ale vyžadováno vlastnoruční sepsání dokumentu či pořízení dokumentu opatřeného úředně ověřenými podpisy, pak není jejich pořízení v elektronické podobě možné ani v případě, že by tyto dokumenty byly opatřeny zaručeným elektronickým podpisem.* ***Současná právní úprava neumožňuje nahrazení úředně ověřeného podpisu podpisem elektronickým****.“* (HÝBLOVÁ, 2012)

---

[14] Jedná se o *„zaručený podpis založený na kvalifikovaném certifikátu vydaném akreditovaným poskytovatelem certifikačních služeb a obsahující údaje, které umožňují jednoznačnou identifikaci podepisující osoby.“* (Zákon č. 227/2000 Sb., SMEJKAL, 2012)

[15] *„Datové schránky nejsou e-mailem, ale zaručenou službou přístupu k informacím (datům, datovým zprávám, dokumentům apod.) s důvěryhodnou třetí stranou (provozovatel systému) a registrovanými (a autentizovanými) uživateli.“* (SMEJKAL, 2012)

Radim Polčák v diskuzi na konferenci DOCURIDE se k problematice dlouhodobého uchovávání dokumentů vyjádřil tak, že v **současné době** prakticky **neexistuje judikatura týkající se dlouhodobého uchovávání digitálních dokumentů v důvěryhodném uložišti**, které splňuje požadavky důvěryhodnosti, prokazatelnosti neměnnosti informací a nepopiratelnosti existence záznamů a dále garanci čitelnosti a bezpečnosti. Ve veřejné správě jsou digitální dokumenty považované za důvěryhodné, pokud by byly námitky proti pravosti, musel by být zároveň zpochybněn celý systém veřejné správy. Odpovídající právní úprava v soukromoprávní oblasti je však nedostačující. V závěru diskuze proto vyplynulo, že je pro tuto chvíli nejvhodnější mít např. fakturu podepsanou konkrétní osobou, orazítkovanou a mít ji zaslanou doporučeně s doručenkou. **Pro firmu je** tedy z právního pohledu **lepší pracovat s elektronickou verzí písemnosti, ale** pro kontrolní orgány **uchovávat** i **verzi listinnou**, což se v praxi obvykle tak děje.

K tomu je vhodné uvést, že zákon o archivnictví a spisové službě upravuje převádění dokumentu v analogové podobě na dokument v digitální podobě a naopak, a to právě v ustanovení § 69a. Jistou analogii lze zřejmě proto aplikovat i v oblasti soukromoprávní.

5.2 Zákon č. 500/2004 Sb., správní řád, ve znění pozdější předpisů

V souvislosti s činností v oblasti veřejné správy je v návaznosti na uvedené třeba upozornit také na zákon č. 500/2004 Sb., správní řád, ve znění pozdějších předpisů.

Dle § 19 odst. 1 správního řádu, věty *první a druhé, písemnost doručuje správní orgán, který ji vyhotovil. Správní orgán doručí písemnost prostřednictvím veřejné datové sítě do datové schránky.*

Dle § 37 odst. 4 správního řádu *podání je možno učinit písemně nebo ústně do protokolu anebo v elektronické podobě podepsané uznávaným elektronickým podpisem. Za podmínky, že podání je do 5 dnů potvrzeno, popřípadě doplněno způsobem uvedeným ve větě první, je možno je učinit pomocí jiných technických prostředků, zejména prostřednictvím dálnopisu, telefaxu nebo veřejné datové sítě bez použití uznávaného elektronického podpisu*.

Dle § 37 odst. 5 správního řádu *ten, kdo činí podání v elektronické podobě podle odstavce 4 věty první, uvede současně poskytovatele certifikačních služeb, který jeho certifikát vydal a vede jeho evidenci, nebo certifikát připojí k podání.*

5.3 Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů

„Oddělení virtuální identity od fyzického základu a geografický dosah, který mohou aktivity v kyberprostoru mít, utvoření platných vzorců prakticky znemožňují“

Alena Táborová

Kyberzločin se dle Táborové může dělit na tři základní oblasti:

1. Cílem je počítač nebo síť jako taková, jedná se o narušení jejich zabezpečení, integrity a fungování (hackerské útoky, šíření virů, aj.)
2. Zahrnuje „klasické“ trestné činy, jako jsou podvod či krádež, spáchané za pomoci nebo prostřednictvím počítače
3. Počítač je pouze okrajovým prostředkem při páchání „klasické“ trestné činnosti (napsání dopisu vyděračem, komunikace přes Skype mezi dvěma pachateli). (TÁBOROVÁ, 2010)

Třetí kategorie je pro potřeby této práce nerelevantní, a proto s ní nebude dále pracováno. K trestnímu zákoníku bylo přistupováno s ohledem na téma diplomové práce. Z hlediska vnitřních hrozeb, tedy běžných zaměstnanců, je vhodné se zaměřit na především na nedbalost a opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat.

Nedbalost je definována v § 16 takto:

„(1) Trestný čin je spáchán z nedbalosti, jestliže pachatel

a) věděl, že může způsobem uvedeným v trestním zákoně porušit nebo ohrozit zájem chráněný takovým zákonem, ale bez přiměřených důvodů spoléhal, že takové porušení nebo ohrožení nezpůsobí, nebo

b) nevěděl, že svým jednáním může takové porušení nebo ohrožení způsobit, ač o tom vzhledem k okolnostem a k svým osobním poměrům vědět měl a mohl.

(2) Trestný čin je spáchán z hrubé nedbalosti, jestliže přístup pachatele k požadavku náležité opatrnosti svědčí o zřejmé bezohlednosti pachatele k zájmům chráněným trestním zákonem.“

Konkrétní skutkové podstaty jsou pak následně upraveny zejména v ustanovení § 231 a § 232 trestního zákoníku.

§ 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat

„(1) Kdo v úmyslu spáchat trestný čin porušení tajemství dopravovaných zpráv podle § 182 odst. 1 písm. b), c) nebo trestný čin neoprávněného přístupu k počítačovému systému a nosiči informací podle § 230 odst. 1, 2 vyrobí, uvede do oběhu, doveze, vyveze, proveze, nabízí, zprostředkuje, prodá nebo jinak zpřístupní, sobě nebo jinému opatří nebo přechovává

a) zařízení nebo jeho součást, postup, nástroj nebo jakýkoli jiný prostředek, včetně počítačového programu, vytvořený nebo přizpůsobený k neoprávněnému přístupu do sítě elektronických komunikací, k počítačovému systému nebo k jeho části, nebo

b) počítačové heslo, přístupový kód, data, postup nebo jakýkoli jiný podobný prostředek, pomocí něhož lze získat přístup k počítačovému systému nebo jeho části.“

Ustanovení § 232 trestního zákoníku vymezuje skutkovou podstatu **poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti**.

Dle tohoto ustanovení:

„(1) Kdo z hrubé nedbalosti porušením povinnosti vyplývající ze zaměstnání, povolání, postavení nebo funkce nebo uložené podle zákona nebo smluvně převzaté

a) data uložená v počítačovém systému nebo na nosiči informací zničí, poškodí, pozmění nebo učiní neupotřebitelnými, nebo

b) učiní zásah do technického nebo programového vybavení počítače nebo jiného technického zařízení pro zpracování dat,

a tím způsobí na cizím majetku značnou škodu, bude potrestán odnětím svobody až na šest měsíců, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“

Z výše zmíněného „přechovává“ vyplývá, že trestné je ukradnout heslo, i když s ním pak není dále manipulováno.

Z pohledu vnějších i vnitřních hrozeb zkušených uživatelů ICT, je důležité zmínit přípravu trestného činu, poškození cizí věci a neoprávněný přístup k počítačovému systému a nosiči informací.

Hacking se postihuje zejména podle § 228 trestního zákoníku, který vymezuje skutkovou podstatu poškození cizí věci. Toto ustanovení stanovuje: *„Kdo zničí, poškodí nebo učiní neupotřebitelnou cizí věc, a způsobí tak na cizím majetku škodu nikoli nepatrnou, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.“* **Na útoky počítačovými viry**, červi apod. **se** zejména **vztahuje §230**, který definuje neoprávněný přístup k počítačovému systému a nosiči informací.

„(1) Kdo překoná bezpečnostní opatření, a tím neoprávněně získá přístup k počítačovému systému nebo k jeho části, bude potrestán odnětím svobody až na jeden rok, zákazem činnosti nebo propadnutím věci nebo jiné majetkové hodnoty.

(2) Kdo získá přístup k počítačovému systému nebo k nosiči informací a

a) neoprávněně užije data uložená v počítačovém systému nebo na nosiči informací,

b) data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými,

c) padělá nebo pozmění data uložená v počítačovém systému nebo na nosiči informací tak, aby byla považována za pravá nebo podle nich bylo jednáno tak, jako by to byla data pravá, bez ohledu na to, zda jsou tato data přímo čitelná a srozumitelná, nebo

d) neoprávněně vloží data do počítačového systému nebo na nosič informací nebo učiní jiný zásah do programového nebo technického vybavení počítače nebo jiného technického zařízení pro zpracování dat.“

5.4 Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim

Trestní zákoník dále **rozšiřuje zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob** a řízení proti nim s platností od 1.1. 2012.

„Tento zákon upravuje podmínky trestní odpovědnosti právnických osob, tresty a ochranná opatření, které lze za spáchání stanovených trestných činů právnickým osobám uložit, a postup v řízení proti právnickým osobám.“ (§1 odst. 1 zákona o trestní odpovědnosti právnických osob a řízení proti nim)

Pro potřeby této **práce je zajímavý** zejména **§8 tohoto zákona**, který ustanovuje **trestní odpovědnost právnické osoby**, a to takto:

„(1) Trestným činem spáchaným právnickou osobou je protiprávní čin spáchaný jejím jménem nebo v jejím zájmu nebo v rámci její činnosti, jednal-li tak

a) statutární orgán nebo člen statutárního orgánu, anebo jiná osoba, která je oprávněna jménem nebo za právnickou osobu jednat,

b) ten, kdo u této právnické osoby vykonává řídící nebo kontrolní činnost, i když není osobou uvedenou v písmenu a),

c) ten, kdo vykonává rozhodující vliv na řízení této právnické osoby, jestliže jeho jednání bylo alespoň jednou z podmínek vzniku následku zakládajícího trestní odpovědnost právnické osoby, nebo

d) zaměstnanec nebo osoba v obdobném postavení (dále jen „zaměstnanec“) při plnění pracovních úkolů, i když není osobou uvedenou v písmenech a) až c),

jestliže jí ho lze přičítat podle odstavce 2.

(2) Právnické osobě lze přičítat spáchání trestného činu uvedeného v § 7, jestliže byl spáchán

a) jednáním orgánů právnické osoby nebo osob uvedených v odstavci 1 písm. a) až c), nebo

b) zaměstnancem uvedeným v odstavci 1 písm. d) na podkladě rozhodnutí, schválení nebo pokynu orgánů právnické osoby nebo osob uvedených v odstavci 1 písm. a) až c) anebo proto, že orgány právnické osoby nebo osoby uvedené v odstavci 1 písm. a) až c) neprovedly taková opatření, která měly provést podle jiného právního předpisu nebo která po nich lze

spravedlivě požadovat, zejména neprovedly povinnou nebo potřebnou kontrolu nad činností zaměstnanců nebo jiných osob, jimž jsou nadřízeny, anebo neučinily nezbytná opatření k zamezení nebo odvrácení následků spáchaného trestného činu.“

PRAKTICKÁ ČÁST

6 Úvod do praktické části

Pro praktickou část jsem si zvolila vzhledem k zvolenému tématu kvalitativní výzkum. Při získávání teoretických znalostí jsem zjišťovala, o jak rozsáhlý okruh zkoumání se jedná a také o to, jak je možné přistupovat k řešení bezpečnosti a nakládání s elektronickými daty na základě mnoha faktorů různě. Proto jsem se pokusila o všestranné, intenzivní a podrobné zkoumání podstaty práce s elektronickými daty v podniku z oblasti potravinářského průmyslu zaměřeným na výrobu tzv. rychloobrátkového zboží.

6.1 Kvalitativní výzkum

Hendl **kvalitativní výzkum** definuje za pomoci citace Creswella takto: *„Kvalitativní výzkum **je proces hledání porozumění** založený na různých metodologických tradicích zkoumání daného **sociálního nebo lidského problému**. Výzkumník vytváří komplexní, holistický obraz, analyzuje různé typy textů, informuje o názorech účastníků výzkumu a provádí zkoumání **v přirozených podmínkách**"* (HENDL, 2005)

Ve svém díle **dále vymezuje čtyři metody** včetně jejich vlastností a výhod. První metodou je **pozorování**, které vyžaduje delší období kontaktu, a napomáhá k pochopení subkultury. Druhou metodou je **analýza autentických textů a dokumentů**, skládající se z rozboru významu, organizace a jejich využití, a přispívá k teoretickému porozumění dané problematiky. Třetí metoda je relativně nestrukturované **interview**, které se v průběhu rozhovoru vyvíjí, tato metoda pomáhá k porozumění zkušenosti a znalostí. Poslední, čtvrtá, metoda je vytváření a následný **rozbor audio a videozáznamů**, který je přesnou transkripcí přirozených interakcí, který je pro porozumění průběhu interakcí. (HENDL, 2005; RABUŠIČ, 2010)

Hendl jmenuje tyto **základní přístupy** ke kvalitativnímu výzkumu. **Případová studie**, **etnografický výzkum**, **zakotvená teorie**, **fenomenologické zkoumání**, **biografický výzkum**, **zkoumání dokumentů**, **akční výzkum a kritický výzkum**. Já jsem si pro potřeby mé diplomové práce z nich zvolila případovou studii.

6.2 Případová studie

Případová studie je dělena dle sledovaných případů ještě **na osobní případovou studii**, **studii komunity**, **studium sociálních skupin**, **studium organizací a institucí a na zkoumání událostí, rolí a vztahů**. (HENDL, 2005)

Zde jsem z pochopitelných důvodů vybrala studium organizací a institucí, které je doslovně definováno takto: *„Zkoumají se firmy, školy, odborové organizace, implementace programů a intervencí, kultura organizací, procesy změn a adaptací. Cíle jsou různorodé – hledání nejlepšího vzorce chování, zavedení určitého typu řízení, evaluace, zkoumání procesů změn a adaptace.“* (HENDL, 2005)

6.2.1 Určení výzkumné otázky

Účelem této studie je zjistit, jak podnik nakládá s elektronickými daty se zaměřením na jejich bezpečnost a jak toto nakládání s daty vnímá. Toto jsem rozdělila do tří otázek:

- Jak průmyslový podnik přistupuje k elektronickým datům?
- Jak průmyslový podnik řeší otázku bezpečnosti práce s elektronickými daty?
- Jak k této problematice přistupují samotní zaměstnanci?

6.2.2 Výběr případu, určení metod sběru a analýzy dat

Pro tvorbu případové studie jsem si zvolila podnik z oblasti potravinářského průmyslu a to Budějovický Budvar, n.p. především z toho důvodu, že jsem dostala příležitost zde pracovat na pozici praktikanta spisové služby s možností zapojit se do projektu pro impelementaci informačního systému pro správu a obsah podnikového obsahu.

Tím se rozšířily možnosti metod sběru dat, které jsem zvolila tři – tj. pozorování, interview a analýzu textů a dat.

6.2.3 Pozorování

Pozorování bylo otevřené a zúčastněné (participantní), neboť jsem byla součástí projektového týmu jako pomocník koordinátora. Ten byl seznámen s tím, kdo jsem a s tím, že pracuji na diplomové práci na téma bezpečnost práce s elektronickými daty v průmyslových podnicích. Pozorování bylo prováděno v přirozené situaci, tady v prostoru podniku nebo v areálu referenční firmy.

6.2.4 Analýza textů a dat

Jednalo se o průběžnou analýzu dat , kterému předcházelo nastudování současné situace podniku. To se skládalo především ze seznámení se s vnitropodnikovými směrnicemi, kde jsem vyhledala ty, které se se zabývaly v současné době podnikem užívanými informačními systémy a politikou užívání/archivace emailové komunikace, internetu a intranetu.

Následně jsem vycházela z analýzy dokumentů, které postupně vznikaly na základě jednání projektového týmu (zápisy z porad, soupisy potenciálních dodavatalů, seznamy otázek na dodavatele, cestovní zprávy, apod.), které byly vytvořeny oslovenými potenciálními dodavateli (souhrnné nabídky, prezentace) a které byly podpůrné (manuály k informačním systémům např. systém pro tvorbu výběrových řízení, webové stránky společností, apod.). Bohužel ne ke všem dokumentům jsem během své práce měla přístup, např. k záznamům bezpečnostních incidentů nebo seznamu zaměstnanců s neomezeným přístupem k Internetu.

6.2.5 Interview

Rozhovory probíhaly v neformálním i formálním duchu, poznávala jsem základní skutečnosti vzhledem k výše položeným výzkumným otázkám. Zajímala jsem se o to, jak klíčoví i běžní uživatelé přistupují k informačním systémům, nakolik využívají jejich funkcionalitu. Zajímalo mě také, jak uživatelé informační systémy vnímají, zda se s nimi pracuje dobře či ne, a pokud ne, jak si práci usnadňují ve smyslu např. záložek či hledání jiných možností.

Teprve poté jsem si připravila otázky pro rozhovor, který byl upraven na základě již zodpovězených otázek, pomocí návodu, abych se tak snáze dozvěděla přímé odpovědi na otázky, které vyplynuly z teoretické části. Tento rozhovor, který je zaznamenán níže, byl veden s vedoucím oddělení informačních technologií, vedoucí personálního oddělení, vedoucí referátu organizace řízení a vnitropodnikové kontroly a ekonomickým ředitelem. Poté jsem vedla ještě strukturovaný rozhovor s vybranými zaměstnanci, kteří mají přístup k neomezenému Internetu a jsou z různých generací, abych jimi dokreslila některé odpovědi z výše zmiňovaného rozhovoru.

6.3 Případová studie řešení bezpečnosti práce s elektronickými daty v Budějovickém Budvaru, n.p.

6.3.1 Stručná historie a popis společnosti

6.3.1.1 Pivovarnictví v Čechách

„Nápad byl jednoduchý – vyrábět pivo stejné kvality, barvy a chuti jakou má pivo vyráběné v Budějovicích nebo v Čechách.“

Adolphus Busch, zakladatel amerického pivního gigantu Anheuser-Busch, se kterým Budějovický Budvar, n.p. (dále BBNP) vedl a stále vede v celém světě řadu soudních sporů ve věci originality ochranných známek
(BBNP, 2012)

Na úvod bych pro úplnost ráda zmínila několik důležitých historických okamžiků pro pivovarnictví ve světě i v Čechách.

Pivo jako nápoj znali již staří Sumerové, jedná se tedy o nápoj starý přes 7 000 let. Na území České republiky jej okolo 3. století začali vařit Keltové, později Germáni, ale nakonec až Slované do něj poprvé přidali chmel. První historická zmínka pochází z roku 922 n. l. od mnichů z Břevnovského kláštera v Praze.

Pivo ve středověku mohl vařit každý, proto je dalším důležitým momentem vznik tzv. práva várečného, které bylo ustanoveno ve 13. století a zpočátku jej uděloval pouze panovník. Po 15. století se začínají objevovat první specializované pivovary a v polovině 19. století se začíná vyrábět spodně kvašený ležák českého (bavorského) typu.

Dnes Česká republika patří mezi 10 největších exportérů piva na světě, možná je to dané tím, že Češi vypijí na hlavu nejvíce piva. V ČR funguje přibližně 45 průmyslových pivovarů a asi 150 mikropivovarů, proto je možné nalézt na českém trhu přes 700 pivních značek a tento počet se každoročně ještě zvyšuje.

Z výše uvedeného je tedy patrné, že pivovarnictví je významným pilířem české ekonomiky. To potvrzují i statistiky, neboť přímo či nepřímo vytváří 55 tisíc pracovních míst a jeho příspěvek činí okolo 10,8 mld. Kč formou přímých daňových odvodů. (BBNP, 2012)

6.3.2 Pivovar Budějovický Budvar, n.p.

„Nezapomínejme, že v hlavní roli je vždy produkt. Objektivní pravda o nás se ukrývá právě v produktu samém… Když pivo nestojí za nic, komunikace značku nezachrání.“

„Naše originalita dává slovu pivo nový, lepší význam, který rezonuje s těmi, kteří hledají trvalé hodnoty.“

(BBNP, 2012)

Historie tohoto podniku se začíná psát rokem 1895, kdy byla uvařena první várka piva. Tehdy byl součástí Akciového pivovaru České Budějovice. První ochrannou známku si nechal zaregistrovat 31. 8. 1911. Jednalo se o obrázek dívky sklepnice v blatenském kroji. V roce 1930 bylo zaregistrováno označení Budvar, které vzniklo spojením slov „**Bud**ějovický“ a „pivo**var**“. A v roce 1934 název Budbräu. Mezi další zajímavosti patří fakt, že v roce 1945 byl Budějovický Budvar spolu s Plzeňským Prazdrojem jediný, kdo mohl vyvážet do zahraničí a díky tomu mu byl zvýšen v té době značně omezený příděl chmele. V roce 1973 začal podnik stáčet pivo do plechovek. Jméno podniku prošlo řadou změn a zatím konečné ustálení jeho názvu Budějovický Budvar, n.p. je z 1. 3. 1991. (HAJN, 1995 a 2001)

Podnik Budějovický Budvar, n.p. (dále jen BBNP) je 4. největším vývozcem piva v České republice. Jako národní podnik z odvětví potravinářského průmyslu spadá pod Ministerstvo zemědělství České Republiky. V současnosti, vzhledem k obtížnosti známkoprávních sporů, je možné Budvar najít pod více jmény: Budweiser Budvar, Budějovický Budvar, Czechvar (pro Kanadu a USA) a Bud (speciální pivo).

Ačkoliv je od roku 2008 označení „české pivo“ v rámci EU uznáváno jako „Chráněné zeměpisné označení“, označení „Českobudějovické pivo“ a „Budějovické pivo“ jej má již od roku 2004.

„Cenné duševní vlastnictví Budějovického Budvaru dnes tvoří ochranné známky, ochranná označení původu, zeměpisná označení a obchodní jméno jako jsou Budweiser Budvar, Budweiser, Budvar, Bud a Budějovický Budvar. Tento fond je tedy výlučně vázán na místo původu. Pivovar jich má celkem registrováno na 380 ve více než 100 zemích celého světa.“ (BUDEJOVICKYBUDVAR.CZ, 2012)

6.3.2.1 Vize a mise BBNP

*„**Tradice** - Při výrobě originálního budějovického ležáku Budweiser Budvar používáme tradiční postupy a stavíme na znalostech a vědomostech, které nám zanechaly generace sládků.*

***Kvalita** - Naše pivo vaříme z nejkvalitnějších surovin, žateckého chmelu, moravského sladu a vody z našich vlastních artéských studní.*

***Jedinečnost** - Díky lahodné chuti, jedinečnému složení a charakteru vyhledávají náš ležák tisíce milovníků kvalitních piv prakticky po celém světě.*

***Originalita** - Kdekoli na světě si koupíte Budweiser Budvar, můžete si být jisti, že byl vyroben v místě svého původu Českých Budějovicích (dříve Budweis). Proto se můžeme v rámci přístupu České republiky do Evropské unie pyšnit "ochranou podle místa původu" pro naše výrobky.“* (BUDEJOVICKYBUDVAR.CZ, 2012)

BBNP nabízí kromě piva také gastronomické služby v podobě Pivnice Budvar a restaurace Masné krámy, prohlídky Budvaru, multimediální expozici Příběh budějovického piva a prodej suvenýrů v návštěvnickém centru nebo prostřednictvím e-shopu.

V České republice vlastní 8 distribučních center (obchodní střediska), která se nacházejí v Českých Budějovicích, Pardubicích, Praze, Ostravě, Plzni, Mladé Boleslavi, Brně a v Teplicích. Jeho součástí jsou také tři dceřiné společnosti v Německu (BBI GmbH, Erfurt), Velké Británii (BBUK Ltd., London) a ve Slovenské republice (BB SK, s.r.o., Senec).

V roce 2011 vystavil 1 318 849 hektolitrů piva a mezi jeho výrobky patří: Světlý ležák (12%), Světlé výčepní pivo (10%), Tmavý ležák, Nealkoholické pivo, Kroužkovaný ležák (12%), Bud Premier Select (16%), Pardál Echt (11%), Pardál (10%) a je rovněž výhradním dovozcem do ČR dánského piva Carlsberg a Somersby (jablečný cider). Světlý a tmavý ležák je do USA a Kanady exportován pod obchodním názvem Czechvar. Také BBNP pro rok 2013 vyvíjí a připravuje nové výrobky na bázi pivních ovocných mixů, které se zvláště v poslední době těší rostoucí popularitě zejména u mladé generace.

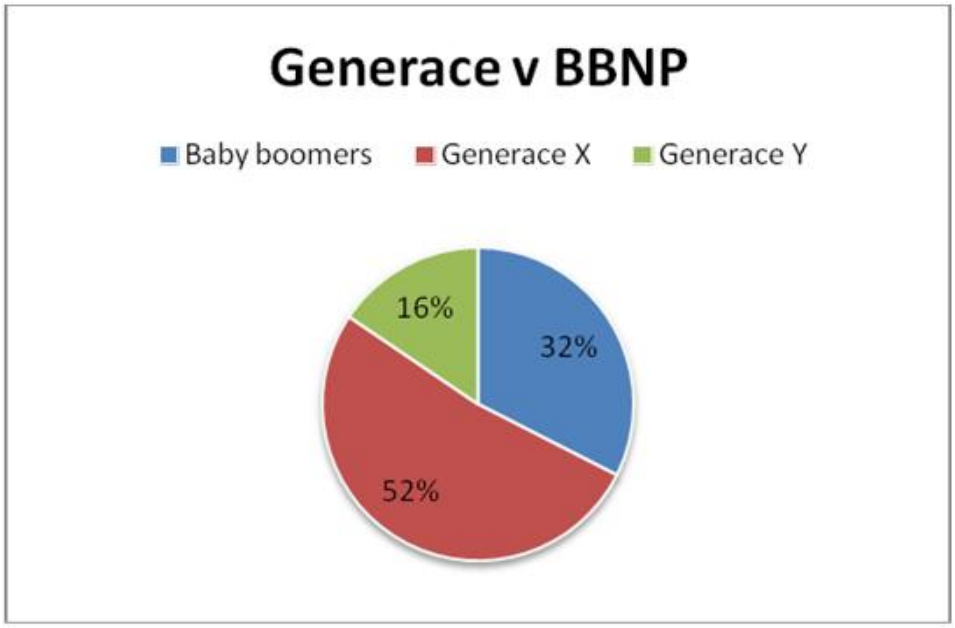
Zajímavá je i statistika soudních sporů a známkoprávních řízení, které od roku 1970 dosud vedl Budějovický Budvar se společností Anheuser-Busch 213 celkem ukončených sporů z toho:

- 86 soudních sporů: 6x smír; 6x remíza; 52x ve prospěch Budvaru
- 127 správních řízení: 94 ve prospěch Budvaru

6.4 Výchozí stav

V současné době pracuje v BBNP přibližně 600 zaměstnanců (včetně obchodních středisek), z toho zhruba 300 z nich má přístup k počítači. A z nich má pouze cca 100 neomezený přistup k Internetu. Ostatní mohou otevřít jediněs vybrané tj. předdefinované webové stránky, mezi které patří např. registr živnostenského podnikání, swift kódy bank, celní správa ČR apod. Internet v BBNP není z důvodu zajištění bezpečnosti řešen přes wifi spojení.

V BBNP pracují lidé z generace Baby boomers, generace X a Generace Y, jejichž procentuální rozložení je možné shlédnout na grafu č. 6.



Graf č. 6 – Procentuální zastoupení generací zaměstnanců v BBNP

(Zdroj: autorka DP)

Podnik nemá žádný systém pro komplexní správu digitálního obsahu v podniku v podobě ECM nebo DMS systému, ale již má zkušenosti s informačními systémy např. v podobě ERP, HRM[16], MIS[17], systém pro řízení logistiky, speciálních SW pro řízení kvality aj.

6.4.1 Současný stav popsaný na základě rozhovoru vybranými odděleními

Tyto rozhovory byly následně obohaceny ještě o odpovědi a názory, které jsem získala ze strukturovaných rozhovorů s otevřenou odpovědí. Otázky byly pokládány dle následujícího soupisu, otázky v závorce jsou doplněním na bázi škálovatelnosti odpovědi):

1. Jaký jste ročník?
   a. 1945-1964
   b. 1965-1979
   c. 1980-1995

[16] Systém pro správu a řízení lidských zdrojů
[17] Manažerský informační systém

2. Jak vnímáte informační a komunikační technologie? (Spíše jako pomocníka nebo spíše jako součást života?)

3. Máte účet na sociálních sítích?

4. V případě, že ano, na jakých? V případě ne, proč?

5. Vlastníte osobní notebook, netbook, iPad, tablet, smartphone?

6. Chtěl/a byste je používat i v práci?

7. Používáte doma nějakou aplikaci, která by se Vám hodila i v práci, ale na služebním přístroji ji nemáte?

8. Volal Vám někdy v pracovní době někdo, kdo po Vás chtěl nějaká citlivá data, na které neměl právo?

9. Měníte si v pravidelných intervalech heslo?

10. Kolik mívá znaků a z čeho se skládá? (alfabetické znaky – velká a malá písmena; numerické znaky, speciální znaky)

6.4.1.1 Bezpečnost elektronických dat v BBNP z pohledu oddělení IT

Jak se v BBNP pracuje s daty?

Data jsou uložena v podnikových informačních systémech, intranetu nebo v osobní složce jednotlivého zaměstnance. Intranet je rozdělen do adresářů na základě jednotlivých útvarů (útvar ředitele, výrobní, ekonomický a obchodní), které se dále dělí na oddělení, která pod tyto útvary spadají. Každé oddělení má ve vymezeném diskovém prostoru k dispozici tzv. interní složku a sdílenou složku. Interní složka je adresář správy pro užší skupinu pracovníků – obvykle daného oddělení. Záleží pak na správcích složek[18], zda jsou soubory poté ještě dodatečně zašifrovány nebo zaheslovány.

Jaká data jsou považována za citlivá?

Data týkající se duševního vlastnictví pivovaru. Receptury, ceníky (kalkulace), personální data, smlouvy, ochranné známky a data týkající se vývoje nových výrobků.

[18] Správci složek nejsou totožní s tzv. klíčovými uživateli

Odkud hrozí BBNP, dle Vás, největší riziko?

Zevnitř přes zaměstnanecký účet, který je nejvíce ohrožen přes vzdálený přístup.

Jaké bezpečnostní incidenty[19] se v BBNP objevují?

Jedná se o porušení směrnic, většinou se jedná o instalaci freewaru, kdy se do počítače dostávají viry (př. „trojský kůň") či backdoors[20]. Při odhalení takového jednání oddělení IT jedná buď přímo s viníkem, nebo s jeho přímým nadřízeným. Postihy mohou vést až k rozvázání pracovního poměru, to však během posledních let nebylo nutné. Nicméně některým pracovníkům byla krácena pohyblivá složka mzdy.

Existuje rozdíl mezi mladými a staršími pracovníky, co se týče té instalace freewaru?

Ano, mladší jsou zvyklí freeware používat a zdají se být více informovaní o hrozbách, a proto používající bezpečnější aplikace. U starších by se dalo říci, že je instalují tak, jak potřebují bez ohledu na bezpečnost zdroje.

Jaké jsou způsoby odhalení bezpečnostních incidentů?

Způsoby existují tři. První skenování firemních počítačů speciálním SW, zda je tam nainstalovaný oficiální SW. Druhý je přes hlášení antivirové kontroly, na jejímž základě se poté dohledává příčina a poslední je monitoring zvýšeného pohybu na Internetu např. vyvolaném stahováním větších objemů dat. I internet z tuzemských obchodních středisek jde a je řízen přes BBNP. Skenování je prováděno jednou ročně, antivirová hlášení a monitoring Internetu je však sledováno denně.

[19] *„Jedna nebo více nechtěných nebo neočekávaných bezpečnostních událostí, u kterých existuje vysoká pravděpodobnost kompromitace činností organizace a ohrožení bezpečnosti informací"* (ČSN ISO/IEC 27 001)
[20] Backdoors neboli zadní vrátka jsou velmi výstižným názvem pro kódy, které po instalaci na cílový počítač umožňují jeho vzdálené řízení. (DOBEŠ, 2012)

Dalším prvkem monitoringu na způsob DLP bude chystaný ECM/DMS systém, systém je momentálně ve fázi výběrového řízení a jeho instalace by měla být dokončena do poloviny roku 2013.

Jaké jsou způsoby ochrany dat?

Jelikož vnímáme vzdálený přístup jako nejvíce rizikový, je nejvíce chráněný. Je samozřejmě použito heslo a připojení probíhá přes VPN[21] klienty - *přes certifikáty.*

Jsou dvě hlavní hesla. Jedno je do ERP[22] *a druhé do zařízení. Zavádí se nová politika hesel dle Windows 8, kdy heslo musí obsahovat minimálně 8 znaků a musí být složené s alfabetických (malá a velká písmena), numerických a speciálních znaků. Je tak ztíženo prolamování hesla skrze slovníkové tvary. K lámání hesel dochází, pokud se někdo zmocní zařízení. Každý uživatel má za povinnost změnit si prvotní heslo, to zda si jej bude měnit pravidelně, je ponecháno na něm – jde o jeho přímou odpovědnost. V praxi se totiž opakované výzvy ke změně hesla ukázaly jako nepříliš účinné. Zvláštní opatrnost při volbě hesla je zaměřena na ty pracovníky, kteří se připojují přes VPN.*

Uživatel, který není registrován v AD, se do sítě nepřihlásí. AD má jasně stanovený rámec, a proto je jakýmsi podpůrným prostředkem pro další aplikace, které si z něj přebírají informace o tom, kdo má jaké pravomoce a přístupy. Podobá se LDAP Provideru[23]*.*

Pro bezpečnost připojení se dá využít služeb externí firmy nebo webový portál, kde je rozhraní vystavené přes firewally směrem ven. Takto komplexně je například řešena pošta.

---

[21] *„Virtuální privátní síť (zkratka VPN, anglicky virtual private network) je v informatice prostředek k propojení několika počítačů prostřednictvím (veřejné) nedůvěryhodné počítačové sítě. Lze tak snadno dosáhnout stavu, kdy spojené počítače budou mezi sebou moci komunikovat, jako kdyby byly propojeny v rámci jediné uzavřené privátní (a tedy důvěryhodné) sítě. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dojde k autentizaci, veškerá komunikace je šifrována, a proto můžeme takové propojení považovat za bezpečné.“* (WIKIPEDIE, 2012)

[22] Enterprise Resource Planning – *„typ aplikace, umožňující řízení a koordinaci všech disponibilních podnikových zdrojů a aktivit. Mezi hlavní vlastnosti ERP patří schopnost automatizovat a integrovat klíčové podnikové procesy, funkce a data v rámci celé firmy.“* (LIPKOVÁ, 2011)

[23] *„Lightweight Directory Access Protocol je definovaný protokol pro ukládání a přístup k datům na adresářovém serveru.“* (WIKIPEDIE, 2012)

Dotazování zaměstnanci měli z velké části heslo alespoň 8 znaků dlouhé, jako problematičtější se ukázalo jeho složení, kdy u některých heslo obsahovalo pouze malá písmena. Také valná většina potvrdila slova expertů z oddělení IT, když přiznala, že si heslo pravidelných intervalech nebo alespoň občas nemění.

Jak se BBNP staví k BYOD[24] nebo BYOA[25]?

Zatím o BYOD neuvažujeme. Je to dáno i tím, že ERP se na tabletu vůbec nedá spustit. ERP funguje na určité verzi prohlížeče apod. Také máme sestavený standard, ve kterém je prověřený SW i HW. Kdybychom chtěli na politiku BYOD, musel by na to být připravený dodavatel, který by v tuto chvíli musel systém dodatečně uzpůsobit.

Všichni dotazovaní se shodli na tom, že nemají potřebu vlastní zařízení používat v práci. Hlavním důvodem byl fakt, že většinou disponují vlastním i pracovním notebookem. Na otázku týkající se BYOA, dotazovaní z generace X a Y odpovídali, že pokud by nějakou aplikaci chtěli, byl by to Skype. Jeden z dotazovaných z generace Y ale překvapivě odpověděl, že Skype si již po dohodě a pod dohledem oddělení IT z důvodu zkvalitnění a zlevnění služební komunikace nainstaloval.

Jak jsou uživatelé vzděláváni?

O pravidelných školeních se neuvažuje, každý uživatel ale na začátku prochází školením, kde je zdůrazněn význam délky a složení hesla a další důležité body z vnitropodnikové směrnice, která tuto problematiku také zmiňuje. Například aby uživatelé zavírali nebo se odhlásili z počítače, pokud někam odchází, nebo aby dovolili systému provádět pravidelnou antivirovou kontrolu.

„Zaměstnancům je zejména zakázáno

- *vyvíjet jakoukoliv činnost, jež by mohla vést ke zjištění hesla k uživatelskému účtu jiného uživatele*

[24] Používání osobního zařízení v práci
[25] Používání jiné než podnikem definované aplikace

- *přihlašovat se k podnikové informační síti pomocí cizího uživatelského účtu*
- *přebírání souborů z internetové sítě, které nesouvisejí s jejich pracovní náplní nebo s jejich pracovní náplní souvisejí, ale jedná se o programy, k nimž nebyla zakoupena potřebná licenční práva, příp. by byla porušena práva autorská*
- *provádět bez vědomí a souhlasu zaměstnanců oddělení IT (dále OIT) jakéhokoliv instalace a úpravy softwaru, včetně instalací tzv. freeware a shareware produktů. Tento zákaz se vztahuje i na software přikládaný k různým odborným časopisům, knižním publikacím a propagačním materiálům*
- *bez souhlasu odborného ředitele a vědomí zaměstnanců OIT vytvářet a využívat v rámci podniku jakéhokoliv vlastní programy*
- *vypalování dat na CD a DVD pro jiné než archivační případně propagační účely, zejména došlo-li by touto činností k porušování autorských práv"*

Úryvek ze směrnice Správa podnikových informačních a řídicích systémů a ochrana dat.

Co BBNP a Cloud computing?

Cloud v zásadě funguje tak, že více serverů dělá jednu službu, takže na požadavek odpovídá ten nejméně zatížený. Je to chytré řešení, které umožňuje redundantní rozložení dat. Vyplatí se to ovšem až od určité velikosti.

BBNP není tak velký podnik, abychom museli cloudové uložiště z pohledu objemu dat řešit. Také z pohledu historie nám narůstal počet serverů a jejich kapacit na základě HW požadavků jednotlivých systémů a zatím není důvod pro radikální změnu.

Naše antispamové řešení napojené na poštovní služby, je skrz cloud. Nechová se pořád stejně, utahuje nebo povoluje přísnost, takže někdy propustí více spamu a někdy méně. Je však vidět, že nové spamy analyzují a procházejí i nejasné případy, díky čemuž se snížil počet spamů na přibližně na 1/20 a méně. Toto skóre se neustále zlepšuje. Dříve spamy narůstaly hlavně o dovolených, kdy lidé měli na svých emailech omluvnou zprávu, že si email vyzvednou

tehdy a tehdy, dávali tím tedy najevo, že účty jsou aktivní, takže tyto účty byly více atakovány. Teď je nejvíce spamu na veřejných adresách např. budvar@budvar.cz.

Řešili jste někdy útok v podobě sociálního inženýrství?

Občas se lidé dotazují na některé emaily, u kterých si nejsou jistí, zda jde o spam nebo ne. My se poté na to nedíváme z hlediska obsahu, ale z technického úhlu. Zjišťujeme např. kredibilitu zdroje, odkud email přišel.

Jelikož IT oddělení zmínilo útoky skrze emailovou komunikaci, dotazovala jsem se na sociální inženýrství prováděné přes telefon, přesněji přes budvarskou telefonní linku. Dotazovaní se na mne většinou poněkud udiveně podívali a až poté jich většina odpověděla, že ne. Ti, kteří odpověděli kladně, řekli, že se jednalo o volajícího, který se obvykle představil jako zaměstnanec banky.

Jak se data uchovávají?

Záloha dat, stavů serverů a operačních systémů je prováděna 5x týdně s ním, že minimálně 2x se jedná o tzv. full backup, tedy kompletní zálohu, ostatní mohou být zaměřeny jenom na nějaká data. Záloha je prováděna na interní disky, externí disky a magnetické pásky, které slouží především jako krátkodobý archiv a jen občas jako archiv dlouhodobý. Nahrávání na magnetické pásky ale trvá nějakou dobu, takže přesahuje tzv. noční okna (noční provoz jednotlivých SW v rámci informačního systému podniku) a za dne to systém zpomaluje. Provádí se to tedy tak, že jsou data nahrána nejprve na externí disk, a poté z něj kopírována na magnetickou pásku.

Elektronická data v BBNP z pohledu ROŘVK (Referát organizace řízení a vnitropodnikové kontroly)

Jak BBNP vnímá z hlediska směrnic elektronická data?

Postupy, které platí pro listinnou podobu, nemohou být zcela totožné s postupy pro elektronické dokumenty, protože cesta, kterou k nám oba druhy dokumentů přichází, je

odlišná, a proto se zpracovávají různě. V rámci vnitropodnikových předpisů tedy pamatujeme na oba typy listin.

Jak do BBNP dokumenty přicházejí?

Dokumenty v listinné podobě přicházejí přes podatelnu anebo si je generujeme sami. Elektronické dokumenty přicházejí přes datovou schránku, emaily nebo si je sami generujeme. V momentě, kdy se dostanou do režimu nastaveného procesu, zachází se s nimi podle předdefinovaného postupu (př. Spisový a skartační řád).

Na vstupu je na dokumenty pohlíženo rozlišně a poté?

Poté jsou už stejné např. stejnou dobou skartace.

Jak často se provádí aktualizace směrnic, na základě čeho?

Aktualizace směrnic probíhá tak, že každý předpis tj. směrnice, příkaz nebo metodický pokyn má tzv. majitele problému, který zodpovídá za to, že předpis bude trvale aktuální nebo aktualizován. Když zjistí, že tomu tak není, navrhuje aktualizaci či změnu předpisu, přičemž součástí tohoto procesu je i připomínkové řízení. Nová verze musí být opět v souladu s legislativou a ostatními našimi vnitropodnikovými předpisy a postupy. Majitelé problému toto mají uloženo ve směrnici Systém tvorby a kontroly organizačních a řídících aktů.

- *1. stupeň kontroly aktuálnosti předpisů (viz výše popsané), kdy tato odpovědnost se promítá do zápisů z kontrol, které mají za úkol provádět 1x ročně v prvním čtvrtletí kalendářního roku.*
- *2. stupeň je kontrola referátem organizace řízení a vnitropodnikové kontroly. A při této kontrole se postupuje buď podle plánu kontrol, který je vydáván v posledním čtvrtletí kalendářního roku na celý další rok. Jsou tam určeny předpisy, které se budou kontrolovat. Jejich výběr vyplývá z důležitosti předpisu a z doby, která uplynula od předchozí kontroly. Anebo jsou prováděny kontroly namátkové. Z obou*

těchto kontrol konaných ROŘVK se pořizuje zápis, kde se definuje zjištění, nedostatky a nápravná opatření včetně termínů a konkrétních odpovědností jednotlivých zaměstnanců. Kontrola vnitropodnikové dokumentace i uložená nápravná opatření se v podniku provádí velmi důsledně.

6.4.1.2 Elektronická data z pohledu personálního oddělení

Jaká data vnímáte v podniku jako citlivá?

Z personálního hlediska se striktně řídíme zákonem o osobních údajích. Nejcitlivějším údajem je rodné číslo, takže to např. na pracovní smlouvu netiskneme. Data jsou uložena v elektronické podobě v HRM systému.

Stává se, že kontaktuje personální oddělení někdo a chce některé z osobních údajů?

Ano, státní orgány, zejména policie, která potřebuje některá data ověřit. My tyto informace dle zákona sdělit musíme. Totožnost si však pečlivě ověřujeme.

6.4.1.3 Implementace ECM/DMS systému z pohledu ekonomického ředitele BBNP

Proč se BBNP rozhodl pro implementaci ECM/DMS systému?

Potřebovali jsme řešení, které by zpřehlednilo firemní dokumentaci. Jedná se o vytváření dynamických přehledů o tom, kdo s jakým dokumentem právě pracuje, kde se nachází, kdo a kdy je pozměnil a kdo za daný dokument nese zodpovědnost. Tedy BBNP očekává od DMS vytváření reportů a jasnou definici odpovědností za termíny a plnění uložených úkolů. Neočekáváme však pouze zlepšení organizace a řízení ve firmě, DMS bude mít důležitou roli i v řízení nákladů, kde dojde k jasnému provázání a kontrole mezi vystavenými objednávkami a došlými fakturami za materiál, služby apod. DMS bude univerzálním nástrojem s poměrně rozsáhlým využitím v průřezu přes celý podnik.

Co bylo hlavním impulzem?

Zjistili jsme, že dokumenty jsou sice k dispozici, ale jejich verifikace (např. určení, zda daná verze je platná, zda není ve změnovém režimu) a vyhledávání je časově náročné. Šlo tedy především o rychlost dohledávání dokumentů a jejich provázanosti na ostatní vnitropodnikovou dokumentaci. Vnitropodnikové směrnice a normy na sebe vzájemně navazují a správa celého systému vnitropodnikové dokumentace je časově náročná.

Byly nějaké předchozí pokusy o implementaci ECM/DMS systému?

Ne, před tím nebyl oficiálně vypsán žádný projekt. BBNP předtím prováděl pouze průzkum SW trhu, zda existuje něco pro řízení dokumentace. Postupem doby tak kompetentní pracovníci získali velmi solidní znalosti o nabízených možnostech a to posléze mohlo být využito při samotném zadání projektu pro zavedení DMS.

Jak se staví vedení k implementaci?

Velmi pozitivně. Podporuje ji, vnímá ji jako budoucí nedílnou součást řízení firmy. Otázka pořízení a následné implementace DMS do systému řízení podniku byla projednána ve vrcholovém vedení podniku i s pracovníky zařazenými do středního článku řízení. DMS byl schválen a pro jeho pořízení byly uvolněny i finanční zdroje z investičního programu podniku.

Kolik procent z investic tvoří položky ICT?

Zhruba 3%, každoroční objem investic celkem však činí cca 10% z celkové bilanční sumy podniku.

Prošel jste někdy bezpečnostním kurzem?

Ano, absolvoval jsem na dané téma interní školení a také školení u externí bezpečnostní firmy. Pracovníci podniku mají k disposici celou řadu odborné literatury z oblasti IT, kde se velmi často bezpečnost nakládání s elektronickými daty řeší.

6.5 Řešení problematiky oběhu elektronických dat v podniku na základě implementace ECM/DMS systému

Pro popis přístupu BBNP k implementaci ECM/DMS systému jsem se rozhodla použít chronologickou strukturu, protože samotný projekt je založený na časové návaznosti jednotlivých etap. Jak jsem se již výše zmínila, jsem členkou projektového týmu, a proto jsem měla přístup k veškeré dokumentaci, která s projektem souvisí.

Na začátku září roku 2012 byl sestaven projektový tým pro implementaci informačního systému pro řízení a správu digitálního obsahu ve firmě. Tým se skládal z 6 zaměstnanců zastupující oddělení IT, ROŘVK, referát spisové služby a ekonomický úsek. Já jsem byla přiřazena ke koordinátorce projektu, která pracuje na referátu OŘVK. Později byli přidáni ještě 2 zástupci z obchodního oddělení a oddělení informační soustavy a na prezentace některých společností se dostavil i ředitel podniku a zástupcí z controllingu.

Na začátku projektu bylo vedoucím projektu jen velmi neurčitě naznačeno, co se od týmu vyžaduje a bylo tedy jasné, že bude potřeba bližší specifikace. Ta měla probíhat na základě průzkumu a analýzy trhu a také na bázi rozhovoru s potenciálními dodavateli. Pro konkrétní vyjádření použiji tzv. metodu SMART, která obsahuje pět základních otázek, na které je nutné znát odpověď, dříve, než se zahájí kroky pro realizaci projektu v podobě výběrového řízení. (DOLEŽAL, 2009; LIPKOVÁ, 2012)

S (Specific) – Co se bude dělat?
M (Measurable) – Jak budou měřeny výsledky?
A (Agreed) – Souhlasí všechny dotčené strany?
R (Realistic) – Jsou cíle realistické?
T (Timed) – Je čas realistický?

Co se bude dělat?

V BBNP bude implementován systém pro řízení firemního obsahu, vytváření reportů, s jasně definovanou odpovědností za termíny, plnění uložených úkolů a možností komunikace mezi jednotlivými pracovníky, kteří s konkrétním obsahem pracují. Pro tento projekt bylo

v první etapě řešení rozhodnuto, že se zaměří na agendu objednávek a faktur pro přibližně 150 uživatelů (včetně digitalizace faktur a k nim přidaných dokumentů př. dodacích listů a dalších příloh, které mohou být součástí do podniku došlých faktur. S výhledem na rozšíření o vnitropodnikové směrnice, porady/úkoly, smlouvy, aj.

Jak budou měřeny výsledky?

Projekt byl rozdělen do několika jednotlivých fází:

1. Průzkum a analýza trhu
2. Pozvání vybraných firem a prezentace jimi nabízeného řešení, návštěva referenčního podniku nebo rozhovor se zástupcem referenčního podniku
3. Odstartování 1. kola výběrového řízení
4. Odstartování 2. kolo výběrového řízení (zúžení potenciálních dodavatelů na 2)
5. Předimplementační analýza
6. Implementace
7. Akceptační řízení, školení a testovací provoz
8. Spuštění ostrého provozu

Souhlasí všechny dotčené strany? Ano.

Jsou cíle realistické?

O cíli implementovat kompletní ECM/DMS systém, který byl na začátku naznačen, se vědělo, že by byl nerealistický, a proto byla nutné zúžení požadované funkcionality na to, jak trefně poznamenal jeden z možných dodavatelů, *„co Budvar nejvíce pálí.“* S následným přidáváním dalších agend. Zúžením implementace na agendu objednávek a faktur se cíl zdál být realistický a stal se první etapou řešení. Nicméně se do budoucna počítá s rozšiřováním systému o další agendy, které se prostřednictvím DMS mohou řešit.

Je čas realistický?

Časové rozložení celého projektu přesně stanoveno nebylo především proto, že bylo ponecháno na firmách, aby v rámci výběrového řízení navrhly termíny realizace samy. Vycházelo se z toho, že tyto firmy budou mít bohaté zkušenosti se zaváděním systému v celé řadě firem, kde pomáhaly s jeho implementací.

6.5.1 Popis jednotlivých dílčích částí projektu

6.5.1.1 Průzkum, analýza trhu a specifikace projektu

V této fázi byl prováděn průzkum a analýza trhu dodavatelů ECM systémů v České republice. První orientační soupis mělo za úkol sepsat oddělení IT, který se skládal z firem, se kterými již v minulosti na tuto či podobnou problematiku BBNP jednal. Poté byl seznam obohacen ještě o firmy, které nabízely platformu společností s vůdčím postavením dle Gartnerova magického ECM kvadrantu, přesněji jeho pravé horní části (viz graf č.X).

Graf č. 7 – Gartnerův magický ECM kvadrant

Hodnocena byla také webová prezentace firmy, reference, a pokud byly k dispozici, tak i případové studie k implementacím v konkrétních podnicích, které se podobaly BBNP. Tedy jednalo-li se o firmy z odvětví potravinářského průmyslu či průmyslové výroby obecně.

Typy referencích zmiňovaných společnostmi by se na základě podrobnosti a tedy i jisté transparentnosti daly rozdělit do tří skupin:

- Ty, které obsahovaly pouze logo nebo název firmy
    - Tento druh se mi zdál velmi zavádějící, protože velké společnosti jako např. Tatra nebo Telefónica se vyskytovaly v referencích vícero společností
- Ty, které obsahovaly nejen název, ale také stručnou anotaci
- Ty, kde byla přiložena i případová studie

Naneštěstí případových studií nebylo mnoho, a proto jsme přistoupili k tomu, že u zajímavě vypadajících referencí požádáme o upřesnění. To probíhalo přes telefonické dotazy. Firmy se k nim stavěly obecně negativně a bylo nutné opakovat požadavek přes firemní email (jmeno@budvar.cz). Bylo jasné, že firmy se obávají sociálního inženýrství např. ze strany konkurence, a proto žádají alespoň takovéto ověření totožnosti či příslušnosti k avizované firmě, než začnou posílat a sdělovat bližší informace.

Během průzkumu se taktéž dalo vypozorovat, že firmy nabízející ECM systém, jsou v podstatě trojího typu:

- Tvůrci platforem (Microsoft, OpenText, IBM, apod.)
- Business partneři tvůrců (mohou být rozděleni ještě např. na zlaté partnery, platinové partnery atd.; nabízí jednu platformu v rámci konkrétního řešení např. ECM, HRM)
- Tzv. integrátoři (vybírají řešení pro zákazníka z více platforem)

Integrátoři potřebovali zpočátku nejvíce informací ohledně toho, co BBNP bude potřebovat, aby věděli, jaké řešení prezentovat. Zda upřednostnit robustní variantu či levnější.

V průběhu analýz se ukázalo, že samotný pojem DMS je vnímán a používán firmami odlišně. Některé firmy byly více zaměřeny na bezpečnost dlouhodobého uchovávání dat

(listinných dokumentů ve speciálních certifikovaných uložištích) či na integraci datových schránek do informačního systému (ty se v současné době ale příliš nepoužívají na komunikaci Business-to-Business). V BBNP byly upřednostněny firmy, které se zabývaly komplexním oběhem elektronických dokumentů se zaměřením na komerční sféru. Certifikované dlouhodobé uložiště se v současné době nejevilo v souvislosti s platnou legislativou, požadavky státních orgánů a politikou elektronických podpisů (ověřených, uznávaných, zaručených) a značek jako prospěšné. BBNP se rozhodl současně s elektronickou podobou dat uchovávat také jejich listinnou podobu. Listinná podoba úschovy celé řady dokumentů je vcelku pochopitelná v kontextu s vedením řady soudních sporů ve věci ochrany doševního vlastnictví podniku.

Na základě průzkumu byla aktualizována předešlá tabulka. Ta obsahovala název společnosti, kontakt, zdroj, ze kterého se vycházelo při analýze (web, prezentace, youtube), relevantní reference a platforma, kterou nabízí. A z té poté byly vybráni možní kandidáti pro první kolo výběrového řízení a ti byli pozváni k osobní prezentaci jimi nabízeného řešení.

6.5.1.2 Prezentace firem a referenční návštěvy s rozhovory s otevřenými odpověď mi

Na základě poznatků z této fáze byl počet firem ještě zúžen, protože některé z nich nabízely pouze řešení ERP, jehož součástí byl ECM systém (BBNP nepoptával systém ERP). Při jednotlivých prezentacích si obě strany (projetkový tým i dodavatelé) specifikovaly a definovaly obsah jednotlivých pojmů či co je chápáno jako standartní součást a funkcionalita systému. Zjišťováno bylo i to, zda je systém kompletně alokován do českého jazyka, protože v současné době reference z firem na území ČR nemusí znamenat práci se systémem v českém jazyce. Velmi často jsme se setkávali s tím, že mateřská firma měla sídlo v zahraničí, a tak dceřiné společnosti pracovaly pouze v anglickém jazyce.

Firmy naopak kladly značný důraz na součinnost zadavatele s dodavatelem (předně jeho konzultanty) a toto se později projevilo i v návrzích termínů projektů, které byly součástí výběrového řízení, kde bylo zmíněno, že termíny počítají s plnou součinností zadavatele. Součinností je myšlena spolupráce klíčových uživatelů s konzultatny dodavatelské firmy, to je hlavně z toho důvodu, že zavedené postupy a procesy nemusejí být tolik efektní a je potřeba je pozměnit, což může v rámci konkrétní agendy jedině klíčový uživatel. Jako další důležitou

složku vnímali existenci a aktuálnost vnitropodnikových směrnic, které by měly jistým způsobem postupy a procesy jednotlivých agend zrcadlit.

Během těchto dvou fází jsem pozorovala pozvolnou proměnu pohledu projektového týmu na zadaný úkol. Na začátku o ECM/DMS systému vědělo nejvíce oddělení IT, proto také vypracovávalo první seznam. Postupem času na základě sdílení zkušeností, nových poznatků a teoretických znalostí, stával tým informovanějším a tím pádem v daném tématu „zběhlejším“, což se posléze projevovalo především na větší složitostí a detailností otázek směřovaných na zástupce firem.

6.5.1.3 1. kolo výběrového řízení

Požadavky na 1. kolo výběrového řízení byly rozčleněny do několika kritérií, z nichž některá byla blíže specifikovaná v příloze. Výběrové kolo bylo vypsáno v online elektronickém systému Softrade, kde jsou jednotlivá kritéria vyhodnocována na základě bodového ohodnocení. Seznam jednotlivých kritérií byl vytvořen na základě předchozích zkušeností, jednání z možnými dodavateli a porady projektového týmu. Bylo kritické se přesně shodnout na vnímání a pochopení jednotlivých pojmů a také na tom, zda je pokyny pro VŘ obsahují všechny důležité body.

Body byly za nabídku ceny, splnění požadavků zadavatele (ty byly složené ze specifikace předimplementační analýzy, procesu přijetí dokumentu, zpracování dokumentu a na funkcionalitu systému, výstup dokumentu, technickou specifikaci a popis možností rozšíření systému), uživatelská přívětivost systému (hodnocena na základě prezentací systémů, firem a referencí) a nabízených OCR technologií. OCR technologie většinou nabízejí jako službu třetí strany, a protože těch kvalitních není na trhu tolik, tak její název opakoval. Proto bylo rozhodnuto ponechat ji pro 1. kolo VŘ stranou od zbylé cenové nabídky.

Každý z projektového týmu dostal po společné diskuzi a specifikaci jednotlivých bodů a podbodů soupis hlavních částí, aby bodově ohodnotil jejich důležitost. Součet musel dávat dohromady 100 bodů. Poté byly výsledky vyhodnoceny koordinátorem a zprůměrovány, zapsány a podány ke schválení vedoucímu projektu.

V průběhu celého výběrového řízení byly koordinátorem zodpovídány upřesňující dotazy uchazečů týkající se pokynů k VŘ.

6.5.1.4 Vyhodnocení 1. kola výběrového řízení

Dokumentace, která přišla od uchazečů, v rámci výběrového řízení (dále jen VŘ), byla ve své struktuře velmi odlišná. Společným znakem většiny bylo zřetelné označení toho, že dokument je součástí obchodního tajemství a podmínky případného šíření jeho obsahu. Toto vnímám jako základní bezpečnostní opatření, které je zmíněno v rodině norem ČSN ISO/IEC 27 000 a já si myslím, že je důležité toto nepodceňovat. Zpracování dokumentace bylo provedeno koordinátorem projektu s mou pomocí na základě jejího porovnání s pokyny VŘ daných BBNP. Pokud popis nebyl jasný, ne zcela odpovídal pokynům VŘ nebo text z pokynu přeformulovával a dával mu tím odlišný význam, byl tento bod chápán jako splněný napůl nebo jako nesplněný.

V této fázi bylo poutavé pozorovat, jak jednotliví členové projektového týmu přitupovali k hodnocení. Na co kladli důraz v jednotlivých částech kritérií v části „splnění pokynů zadavatele“ a s jakou pečlivostí nyní přistupovali k hodnocení uživatelské přívětivosti. Dalším poměrně podstatným faktorem se ukázala být maintenance[26], která se za software platí v pravidelných smlouvou stanovených intervalech a pohybuje se většinou okolo 20% z ceny SW. Otázka následných nákladů (nákladů spojených s provozováním systému) se stala důležitým kritériem pro výběr systému. Dále bylo potřeba si všímat, jak firmy řešily zadaný počet 150 uživatelů, protože v licencích se k nim může přistupovat ze dvou různých pohledů. Uživatelé byli členěni na aktivní a tzv. „reading only“ nebo na ty, kteří potřebují sofistikovnější systém (klíčoví uživatelé, administrátoři) a ty, kterým stačí základní funkcionalita.

Při konečném vyhodnocení postupujících firem bylo cítit napětí v očekávání stížností firem, které do dalšího kola nepostoupily. Ty na sebe dlouho nenechaly čekat, ale naštěstí většina z těchto firem chtěla znát pouze v jakém kritériu neprošla.

[26] Údržba softwaru včetně jeho aktualizace, řešení jeho technických poruch v rámci předem definovaného času na základě kritičnosti poruchy

V současné době (v době, kdy je psána tato DP) je vypsáno 2. kolo výběrového řízení, které bude ukončeno do konce ledna 2013.

Na tomto projektu si všímám, že čím více stoupá zainteresovanost jednotlivých aktérů, tím více stoupá informační gramotnost ohledně celé problematiky DMS. To se projevuje používáním zkratek, odborné terminologie, konkrétnějšími dotazy a jasnou představou, co se od dané věci očekává. Zpočátku šlo především o to, co má daný systém umět, načež se postupně přešlo na řešení toho, jak má daný systém vypadat. Tyto dvě etapy se projevily i ve VŘ, kdy 1. kolo bylo především o funkcionalitě a 2. kolo je primárně zaměřeno hlavně na způsob práce se systémem. Tedy bude hodnoceno, jak pochopitelný a intuitivní systém je.

Firmy byly také ochotné nejen akceptovat fixní cenu projektu, ale také fixní dobu trvání, tedy tzv. full scope, která by měla bude ustanovena na základě předimplementační analýzy.

6.5.2 Závěr případové studie

Otázky položené na začátku této případové studie byly zodpovězeny spolu s těmi, které se objevily v průběhu samotného výzkumu. Na otázku „Jak průmyslový podnik přistupuje k elektronickým datům?“ Mohu odpovědět, že elektronická data jsou výrazným pomocníkem, ale v současné chvíli, ať už z hlediska legislativního rámce, nedostatku judikatury nebo kvůli zažitým zvyklostem podniku, nejsou schopna fungovat sama o sobě bez podpory své listinné podoby. Ta ovšem již není tak kvalitní, jako bývala dříve, kdy se psalo na kvalitní veltlíny či papíry. Účtenky tištěné na termopapíru z benzínových pump jsou nejpozději do dvou let zcela nečitelné, ale i tak, pokud je na nich razítko, mají pro kontrolní orgány, dle slov jejich zástupců na konferenci DOCURIDE, větší hodnotu, než čitelná naskenovaná digitální faksmilie. Touto problematikou se v českém prostředí aktuálně zabývá mnoho profesionálů jako J. Peterka vyučující na MFF UK, V. Smejkal působící jako soudní znalec nebo R. Polčák přednášející na PF MU.

V tomto ohledu by byl jistě zajímavý výzkum o trvanlivosti a čitelnosti jednotlivých listinných dokumentů nebo o poměru toho, kolik metrů listin podnik ročně vyprodukuje a kolik jich skartuje v závislosti na způsobu uchovávání, rozloze úložných prostor a metody

řazení a ukládání na regály (vlastními silami nebo přes outsourcovanou službu). Po této stránce by měl jistě zejména obor knihovnictví v komerční sféře hodně co nabídnout, např. v podobě metodické příručky vypracované ze zjištění takového výzkumu, pokud by dokázala ošetřit odlišnost skartačních lhůt u jednotlivých dokumentů, které v knihovnách u fondu dané nejsou.

Další otázkou bylo „Jak průmyslový podnik řeší otázku bezpečnosti práce s elektronickými daty?“. Hlavní odpovědnost za bezpečnostní politiku nese v BBNP IT oddělení, které toto poslání naplňuje skrze technologická zabezpečení. Lidé z IT jsou informování o různých hrozbách a orientují se i v trendech jako je BYOD, BYOA nebo cloud computing a kromě trendu BYOD se k nim nestaví odmítavě. Oddělení IT chce mít ale o stahování aplikací, zastoupených hlavně těmi freewarovými, přehled.

Zároveň s odpovědí na tuto otázku byla zodpovídána i otázka následující a to „Jak k této problematice přistupují samotní zaměstnanci?“ Ostatní zaměstnanci (ať už z pozice klíčových nebo běžných uživatelů) dostávají školení na začátku, kdy obdrží firemní zařízení a přístupy do náležitých informačních systémů, ale poté již nejsou průběžně vzděláváni ohledně práce s elektronickými daty.

Po prvním přihlášení jsou všichni zaměstnanci povinni změnit si heslo, které dostanou od oddělení IT, a jsou poučení před tvorbou vlastního hesla o jeho minimální délce a doporučeném složení znaků. To ovšem ne všichni dodržují, stejně jako si většina z dotázaných pravidelně nebo alespoň občas své heslo neobměňuje. Aby neutrpěla důvěra dotazovaných osob, vyhnula jsem se citlivé otázce, zda jsou hesla složená z celých slov nebo z náhodně poskládaného shluku písmen. Tyto otázky by bylo obecně vhodnější pokládat metodou kvantitativního výzkumu například přes elektronický dotazník v Google Drive, aby byla zaručena co největší anonymita zaměstnanců a jejich příslušnosti ke konkrétní průmyslové firmě. Bohužel, návratnost kvantitativních dotazníků je bez vidiny např. finanční odměny u respondentů velmi nízká a je tedy otázkou, zda by toto riziko dokázal autor vysokoškolské kvalifikační práce nějak zmírnit či odstranit.

Zaměstnanci, se kterými jsem měla možnost hovořit, jsou nejvíce obezřetní při otevírání emailů, což je vidět i v rozhovoru s oddělením IT, mají i zkušenosti s telefonickou verzí phishingu, vishingem, kdy se volající např. představuje jako zaměstnanec banky a žádá informace, na které dle dotazovaných nemá právo.

S ohledem na to, jak já osobně přistupuji k ICT, mně po nějakém čase stráveném v BBNP a při pročítání studií zmíněných v teoretické části, především Gartnerova Hype Cycle diagramu (2012) a výsledků Dimensional Research (2012), začalo zajímat, nakolik současný stav v BBNP ovlivňuje zastoupení jednotlivých generací.

V BBNP je zatím relativně nízké zastoupení generace Y, ale zdá se, že tato mladá generace zaměstnanců ani výrazně netouží po změně zažitých postupů např. v podobě BYOD. V otázce BYOA by nejčastěji volila Skype, z nichž někteří jej na svých firemních zařízení nainstalovaný mají. Ve většině případů dotázaní odpověděli, že nepoužívají chytré telefony a nedisponují tabletem/iPadem. Nikdo z dotázaných aktivně, pokud měl, neužíval svůj účet na sociálních sítích. Ti, kteří měli účet na sociálních sítích, zmiňovali Facebook. Ti, kteří jej neměli, jej vnímali jako ztrátu času, obávali se o ztrátu svého soukromí nebo neměli důvod si jej zakládat kvůli tomu, že lidé v jejich okolí jej také nevlastní.

Hledání odpovědi na otázku, jak se liší touha po BYOD a BYOA nebo celkově vnímání ICT mladé generace v závislosti na odvětví, ve kterém pracují, by mohlo být další cestou pro stanovování hypotéz kvantitativního výzkumu. Nebo např. porovnat zaměstnance z firem z jednoho odvětví, které se liší svými vizemi a misemi (tradice versus nové přístupy), ale jsou si v podstatě podobné délkou působení na trhu. Je velmi pravděpodobné, že výrobní program - zaměření firem ovlivňuje počítačovou gramotnost zaměstnanců a řízení interních IT procesů.

Jedním z možných řešení bezpečnosti práce s elektronickými daty se jeví právě implementace ECM/DMS systému. Jedná se v zásadě o jednoduché řešení, které by svými procedurami tolik nemělo zdržovat lidi od práce, proto by zde mohla být nižší tendence systém obcházet přes emaily, intranet, internet nebo nahrávání si dokumentů na přenosný disk. Na základě tohoto tvrzení věřím, že v budoucnu by mohl sloužit jako spojovací článek

všech informačních systémů, hlavně co se týká dodatkových informací, které většinou chodí přes emaily, nikoliv přes vlastní informační systémy. Pokud by vedení té které firmy striktně dbalo a požadovalo komunikaci a dodržování WF, potom by to zcela jistě mělo svůj pozitivní dopad do řízení celé firmy.

Podstata ECM/DMS systému mi připadala velmi známá, neboť jsem v něm shledala jistou podobnost s knihovnickým systémem a studentský informační systém (dále jen SIS), se kterými jsem v minulosti pracovala. Co ovšem vysokoškolská knihovna oproti ECM řešení z mého pohledu nemá, je nejen možnost customizace nejen vzhledu, ale také možnost osobního nastavení jednotlivých agend dle požadavků klíčových uživatelů a dokonce i běžných uživatelů. Na druhou stranu v knihovnictví je hlubší povědomí o problémech digitalizace, tvorbě metadat a otázce dlouhodobého uchovávání dat, ačkoliv obě sféry narážejí na problematiku omezení ze strany legislativy. V této části jsem také měla možnost vyzkoušet si demo verzi ECM systému a podívat se na manažerský informační systém, systém pro řízení lidských zdrojů a na ERP systém. Zjistila jsem, že znalosti ohledně možností jednotlivých systémů se zmenšují a logicky bývají omezeny pouze na rutinní provoz spojený s prací a odpovědností toho kterého pracovníka.

Dále DMS napomáhá strukturovat data tak, aby byla stále snadno dohledatelná a tedy i k dispozici. Oceňuji možnost propojení jednotlivých částí do uceleného celku (např. objednávky, smlouvy, faktury, dodací listy, apod. provázané např. na jednoho dodavatele atd.). S tím, že dokument je uložen pouze jednou na jednom místě, předchází to tvorbě duplicit a z hlediska bezpečnosti se lépe monitoruje, co se s ním děje. V tomto případě shledávám dosud používaný systém adresářů v intranetu sice jako logicky uspořádaný, ale také zbytečně komplikovaný. Jako člověk, který sice zná organizační řád, ale nemá povědomí o tom, který dokument spadá pod jaké oddělení, jsem postrádala možnost pokročilého fulltextového vyhledávání a při vlastní práci možnost verzování dokumentů.

7 Závěr

V této práci jsem se pokusila nastínit problematiku bezpečnosti práce s elektronickými daty v průmyslových podnicích a porovnat teoretické poznatky s praxí, kterou jsem se rozhodla reprezentovat ve formě kvalitativního výzkumu v podobě případové studie Budějovického Budvaru, n.p.

Chápání pojmu bezpečnosti práce s elektronickými daty se od doby zadání tématu do SISu, což bylo před rokem a půl, velmi změnilo. Prvním důležitým okamžikem bylo vyhotovení seminární práce *„Kyberterorismus: zaměření se na nedbalost zaměstnanců při tvorbě statických hesel“* na seminář Zpravodajské služby. Chtěla jsem se zaměřit především na prevenci např. v duchu rodiny norem ČSN ISO/IEC 27 00X a ČSN ISO 2382. Následně jsem probírala v předmětu PIS certifikaci systému managementu jakosti dle ČSN EN ISO 9001, a začala se více zajímat, co pro firmu takový krok znamená. Výsledkem bylo zjištění, že certifikace je relativně drahou záležitostí, která obvykle vyžaduje rozsáhlé změny v organizačním řádu a dle obsáhlosti bezpečnostního managementu velmi pravděpodobně i přijetí nových zaměstnanců. Zjištění z tohoto plynoucí mě přivedlo na myšlenku zabývat se hledáním jednoduššího řešení, které by však splňovalo základní požadavky na bezpečnost.

V letním semestru jsem si následně při předmětu Projektování PIS začala uvědomovat přitažlivost řešení v podobě systému, který místo toho, aby práci s daty sešněrovával přísnými pravidly, zahrnuje již ve svém základu všechny myslitelné způsoby práce s elektronickými daty a tím pádem je má plně pod kontrolou. Následná možnost účasti v roli praktikanta v BBNP na implementaci takového PIS mě přivedla k řešení otázek dlouhodobé archivace. Problematika dlouhodobé archivace elektronických dat a složitost elektronických podpisů a značek mě přiměla zaobírat se rovností listinných a elektronických dokumentů z pohledu legislativy a zavedených zvyklostí zaměstnanců.

Na základě rozhovorů s různými zaměstnanci jsem dospěla k názoru, že se některé názory výrazně odlišují od těch mých a to mě přivedlo k otázce, zda je to konkrétně mnou nebo mým věkem. Díky tomu jsem se dostala ke studiím o generaci Y a jejich přístupu k ICT a bezpečnosti, abych při rozhovorech zjistila, že v BBNP věk z hlediska trendů ICT zas až

takovou roli, možná i díky absenci wifi nebo nemožnosti spuštění ERP na čemkoliv jiném než počítači, nehraje. Kde jsme se ale lišily, byla tvorba statického hesla, což mě opět přivedlo k počáteční úvaze vnitřních hrozeb a systému, který by je mohl zredukovat.

Vzhledem k dedukci, která mě přivedla k tomuto tématu, jsem se více zaměřila na hrozby, které Josef Požár (2005) definuje jako tzv. subjektivní, a řadí k nim hrozby plynoucí z lidského faktoru ať již úmyslné či neúmyslné. Mezi objektivní následně započítává hrozby přírodní, fyzikální, technické nebo logické. Ve své práci jsem se jen zlehka dotkla logických hrozeb při vyjmenovávání nástrojů hackerů či crackerů. U subjektivních hrozeb jsem se snažila postihnout všechny potenciální faktory a činitele, které mohou mít vliv na oběh elektronických dat. Zjistila jsem, že je možné na bezpečnost hledět ze tří hledisek a to z pohledu elektronických dat jako takových, z pohledu těch, kteří s daty manipulují anebo z pohledu zařízení, přes která jsou data zobrazována.

Proto je nutné nespoléhat se pouze jeden systém ochrany. V obou částech bylo zřetelně naznačeno, že mnoho firem i jejích zaměstnanců se spoléhá na oddělení IT, které je ale, jak vyplynulo z interview, pouze technickou podporou a zároveň studie PWC (2011) to také označuje za možnou vnitřní hrozbu. Dle mého názoru by jistě měli zůstat první linií ve zdokonalování firemního SW i HW, ale ne jedinou.

Druhou linií by mělo být vyznačení dokumentů tak, aby nikdo, kdo s nimi manipuluje, neměl pochybnosti o jejich důvěrném charakteru, např. skrze DMS systém citlivé části dokumentů zakrýt. Klasifikace by též mohla být součástí metadat a při pokusu o nahrání dokumentu jinam, by se mohl pro jistý psychologický efekt ukázat kontrolní dotaz ve smyslu „Jste si opravdu jistý/á, že chcete tato citlivá data uložit jinam?“. Tento způsob mi připadá vhodnější, než kdyby se tato otázka měla zobrazovat při otevírání dokumentu.

A třetí linií by mělo být pravidelné vzdělávání zaměstnanců. Při pozorování rostoucího povědomí o ECM/DMS systému u členů projektového týmu, jsem si všimla, jak se mění i jejich postoj vůči tomuto systému, k jeho důležitosti, k jeho možnostem i potenciálním rizikům. Nelze tedy říci, že zaměstnancům, ačkoliv to svým způsobem naznačoval článek v časopise Security Word (2011), nejde o bezpečnost podniku. Sama studie PWC (2011) říká,

že při zjištění kyberzločinu spáchaného ve firmě klesá jejich morálka. Osobně se spíše domnívám, že si nedokáží dovodit důsledky svého jednání a ani si nedokáží odvodit závažnost svého pochybení či nedbalosti.

K praktické části považuji za důležité ještě podotknout, že jsem se předtím v praxi setkávala především s vysokoškolskými knihovnami, a tak jsem se při nástupu do BBNP, který byl co do počtu pracovníků i pravidel nejméně desetinásobně větší, trvala prvotní analýza prostředí delší dobu. Do tohoto období započítávám i studium vnitropodnikových směrnic a v BBNP užívaných informačních systémů.

Sepisování této diplomové práce mi mírně zkomplikoval fakt, že citlivost jednotlivých dokumentů v podniku není v některých případech zcela jednoznačně vyznačena. V příloze pracovního řádu je sice seznam dat, která jsou považována za součást obchodního tajemství podniku BBNP, ale je definován velmi obecně, tudíž jsem si pod některými pojmy nedokázala představit, co přesně jimi bylo myšleno. Tím pádem jsem ne u všech dokumentů či jejich částí dokázala s jistotou určit, zda se zde na ně vztahuje obchodní tajemství či ne. Z toho důvodu jsme se rozhodla v těchto sporných případech postupovat obezřetněji a v této práci z nich přímo necitovat.

8 Seznam zkratek

ERP – Enterpriser Resource Planning

PIS – Podnikový informační systém

ECM – Enterprise Content Management

EDI - Electronic Data Interchange

ICR - Inteligent Character Recognition

OCR - Optical Character Recognition

BCR - Bar Code Reading

OMR - Optical Mark Reading

WF – Wokrflow

AD – Active Directory

ČR – Česká republika

ATP - Advanced Persistent Threts

DLP - Data Loss Prevention

BYOD - Bring Your Own Device

BYOA - Bring Your Own Aplication

BBNP – Budějovický Budvar, n.p.

DP – diplomová práce

HRM – Human and Resources Management

MIS - Management Information Systém

SW – software

IT – informační technologie

ROŘVK – Referát organizace řízení a vnitropodnikové kontroly

VŘ – výběrové řízení

MFF UK – Matematickofyzikální fakulta Univerzity Karlovy

PF MU – Právnická fakulta Masarykovy univerzity

NBÚ – Národní úřad pro bezpečnost

SIS – Studentský informační systém

9 Bibliografie

1. ABERLE, Pavel. *Budoucnost kybernetického terorismu: analýza současné podoby kybernetického terorismu a prognóza jeho budoucího uplatnění*. Brno, 2010. Dostupné z: http://bit.ly/VA4991. Diplomová práce. Masarykova Univerzita, Fakulta sociálních studií, Katedra politologie. Vedoucí práce Mgr. Martin Bastl, Ph.D.
2. BARTOLŠIČ, Martin. Křivka nastupujících technologií. *Computerworld: Ucelený informační zdroj pro IT profesionály*. Praha: IDG Czech, a.s, 2012, č. 18, s. 12. ISSN 1210-9924.
3. BARTONĚK, Martin. *Kybernetická kriminalita: zkáza přichází z webu*. Brno, 2010. Dostupné z: http://dspace.k.utb.cz/handle/10563/13922. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta humanitních studií, Institut mezioborových studií Brno. Vedoucí práce PhDr. Mgr. Zdeňka Vaňková.
4. BBNP. *Budějovický Budvar, národní podnik: prezentace pivovaru*. České Budějovice, 2012.
5. BENEŠOVSKÁ, Tereza. *Kyberterorismus jako hrozba v průmyslu komerční bezpečnosti*. Zlín, 2011. Dostupné z: http://dspace.k.utb.cz/handle/10563/18243?show=full. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce JUDr. Vladimír Lacký.
6. BIČIANOVÁ, Anna. *Kybernetický terorizmus a počítačová kriminalita*. Zlín, 2008. Dostupné z: http://dspace.k.utb.cz/handle/10563/5482. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce Ing. Radek Šilhavý, Ph.D.
7. BRANČÍK, Ctibor. *Internetová jurisdikce: působnost práva na Internetu*. Brno, 2012. Dostupné z: http://bit.ly/UjLqhG. Diplomová práce. Masarykova Univerzita, Právnická fakulta, Právo a právní věda, Ústav práva a technologií. Vedoucí práce JUDr. Radim Polčák, Ph.D.
8. BRAUE, David. BYOD: klíčem je zabezpečení. *Computerworld: Ucelený informační zdroj pro IT profesionály*. Praha: IDG Czech, a.s, 2012, č. 18, s.46 ISSN 1210-9924.
9. BROŽ, Vladimír. Chovejme se k datům stejně jako ke klíčům od bytu. *IT Systems: www.SystemOnline.cz s přehledem ve světě podnikové informatiky*. Brno: CCB s.r.o, 2012, č. 9, s. 48. ISSN 1802-002x.
10. BROŽ, Vladimír. Soukromá zařízení na pracovišti: očekávání vs. zabezpečení firemních dat. *IT Systems*. Brno: CCB s.r.o, 2012, 7-8, s. 50-51. ISSN 1802-002x.
11. BUDĚJOVICKÝ BUDVAR, n.p. *Budějovický Budvar 1895-1995*. 1. vyd. České Budějovice: Ages, 1995, 102 s. Text Ivo Hajn
12. BUDĚJOVICKÝ BUDVAR, n.p. *Budějovický Budvar, národní podnik* [online]. 2011 [cit. 2013-01-03]. Dostupné z: http://www.budejovickybudvar.cz
13. *Communications of the ACM*. 2012-06-01, roč. 55, č. 6. ISSN 00010782. Dostupné z: http://dl.acm.org/citation.cfm?doid=2184319.2184330
14. ČERMÁK, Jiří. *Internet a autorské právo*. 2. aktualizované a rozšířené vyd. Praha: Linde Praha, 2003, 251 p. ISBN 80-720-1423-4.
15. ČESKÁ REPUBLIKA, ministerstvo vnitra. *Stanovisko odboru archivní správy a spisové služby k užívání časového razítka v souvislosti s odesíláním a ukládáním dokumentů v digitální podobě*. Praha, 6.4.2010. Dostupné z: http://www.mvcr.cz. č. j. MV-36491-1/AS-2010.

16. Česká republika. Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. In:*http://business.center.cz/business/pravo/zakony/trestni-zakonik/*. 2011.
17. Česká republika. Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim. In: *http://portal.gov.cz/app/zakony/*. 2011.
18. Česká republika. Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů. In: *http://portal.gov.cz/app/zakony/*. 2004.
19. Česká republika. Zákon č. 500/2004 Sb., správní řád. In:*http://business.center.cz/business/pravo/zakony/spravni_rad/*. 2004.
20. Česká republika. Zákon č. 513/1991 Sb., obchodní zákoník. In:*http://business.center.cz/business/pravo/zakony/obchzak/*. 2012
21. ČSN ISO 2382-1. *Informační technologie - Slovník: část 1:Základní termíny*. 3. vyd. s.l.: Český normalizační institut, 1997. Dostupné z: http://csnonline.unmz.cz/.
22. ČSN ISO 2382-16. *Informační technologie - Slovník: část 16: Teorie informace*. 2. vyd. s.l.: Český normalizační institut, 1998. Dostupné z: http://csnonline.unmz.cz/
23. ČSN ISO 2382-2. *Informační technologie - Slovník: část 8: Bezpečnost*. 2. vyd. s.l.: Český normalizační institut, 2001. Dostupné z: http://csnonline.unmz.cz/
24. ČSN ISO/IEC 2382-8. *Informační technologie - Slovník - Část 8: Bezpečnost*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2001. Dostupné z: http://csnonline.unmz.cz/
25. ČSN ISO/IEC 27 000. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Přehled a slovník (36 9790)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2010. Dostupné z: http://csnonline.unmz.cz
26. ČSN ISO/IEC 27 001. *Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky (36 9790)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006. Dostupné z: http://csnonline.unmz.cz
27. ČSN ISO/IEC 27 003. *Informační technologie - Bezpečnostní techniky - Směrnice pro implementaci systému řízení bezpečnosti (36 9790)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Dostupné z: http://csnonline.unmz.cz
28. ČSN ISO/IEC 27 004. *Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací - Měření (36 9790)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011. Dostupné z: http://csnonline.unmz.cz
29. ČSN ISO/IEC 27 005. *Informační technologie - Bezpečnostní techniky - Řízení bezpečnosti informací (36 9790)*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2009. Dostupné z: http://csnonline.unmz.cz
30. DIMENSIONAL RESEARCH. *The Generation Gap in Computer Security: A Security Use Survey from Gen Y to Baby Boomers*. s.l., 2012. Dostupné z: http://www.zonealarm.com/products/downloads/whitepapers/generation_gap_research_2012.pdf
31. DISMAN, Miroslav. *Jak se vyrábí sociologická znalost: Příručka pro uživatele*. 3.vyd. Praha: Karolinum, 2000, 374 s. ISBN 80-246-0139-7.

32. DOBEŠ, Jakub. *Prostředky řízení bezpečnosti informací*. Brno, 2012. Dostupné z: http://is.muni.cz/th/325453/fi_b/?lang=en. Bakalářská práce. Masarykova univerzita, Fakulta informatiky. Vedoucí práce Ing. Mgr. Zdeněk Říha, Ph.D.
33. DOLEŽAL, Jan, Pavel MÁCHAL a Branislav LACKO. *Projektový management podle IPMA*. 1. vyd. Praha: Grada, 2009, 507 s. Expert (Grada). ISBN 978-80-247-2848-3.
34. DOUCEK, Petr. Bezpečnost IS/ICT a proces globální integrace: proč bezpečnost?. *AT&P journal*. 2005, č. 1, s. 65-68. ISSN 1335-2237. Dostupné z: http://www.atpjournal.sk/buxus/docs/atp-2005-01-65.pdf
35. DVOŘÁK, Drahoslav, Martin RÉPAL a Martin MAREČEK. *Řízení portfolia projektů: nejlepší praktiky portfolio managementu*. Vyd. 1. Brno: Computer Press, 2011, 198 s. ISBN 978-80-251-3075-9.
36. EDI. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 3.7.2012 [cit. 2013-01-03]. Dostupné z: http://cs.wikipedia.org/wiki/EDI
37. FOLTZ, C. Bryan. Cyberterrorism, Computer Crime and Reality. *Information Management and Computer Security*. 2004, vol. 2, 12, s. 154-166. Dostupný komerčně také z WWW:. DOI 10.1108/09685220410530799. ISSN 0968-5227.
38. GOODCHILDOVÁ, Joan. Čtyři pravidla, která zaměstnanci rádi porušují. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2011, č. 1, s. 17. ISSN 1802-4505.
39. GRYGAR, Josef. *Detekce a prevence počítačového útoku*. Zlín, 2007. Dostupné z: http://dspace.k.utb.cz/handle/10563/2511. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky, Ústav aplikované informatiky. Vedoucí práce doc. Mgr. Roman Jašek, Ph.D.
40. HÁJIČEK, David C. Svoboda "v síti". *Revue pro právo a technologie*. 2012, roč. 3, č. 5, s. 12-17. ISSN 1804-5383.
41. HEJTMAN, Jan. *Získávání dat z cizího počítače a možnosti aktivní obrany*. Zlín, 2010. Dostupné z: http://dspace.k.utb.cz/handle/10563/14307?show=full. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce doc. Mgr. Roman Jašek, Ph.D.
42. HENDL, Jan. *Kvalitativní výzkum: základní metody a aplikace*. Vyd. 1. Praha: Portál, 2005, 407 s. ISBN 80-736-7040-2.
43. HODULÁK, Petr. *Ochrana informací v organizaci*. Praha, 2010. Dostupné z: https://www.vse.cz/vskp/show_evskp.php?print=yes&evskp_id=23064. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií. Vedoucí práce prof. Ing. Zdeněk Molnár, CSc.
44. HORNÍČEK, Jan. *Sociální inženýrství*. Zlín, 2009. Dostupné z: http://dspace.k.utb.cz/handle/10563/9113. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce Ing. Jaroslava Gregušová.
45. HOUSER, Pavel. Útočníci přerůstají přes hlavu i největším firmám. *HN Hospodářské noviny: Deník pro ekonomiku a politiku*. Praha: Economia, a.s, 2011, č. 10, s. 22-23. ISSN 0862-9587. Vyšlo jako příloha v ICTrevue.

46. HOUSER, Robert. Desatero uživatele IT: v roce 2011 budu žít opět nebezpečně!. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2011, č. 1, s. 18-19 ISSN 1802-4505.
47. HÝBLOVÁ, Kateřina. *Elektronické dokumenty v právní praxi*. Brno, 2012. Dostupné z: http://bit.ly/WZJk9a. Diplomová práce. Masarykova Univerzita, Právnická fakulta, Právo a právní věda, Ústav práva a technologií. Vedoucí práce JUDr. Radim Polčák, Ph.D.
48. CHRBOLKOVÁ, Markéta. *Správa dat a informací v malé firmě* [online]. Praha, 2012 [cit. 2012-11-08]. Dostupné z: http://www.vse.cz/vskp/eid/33879. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ing. Miroslav Lorenc, Ph.D.
49. IKAROS, Redakce. Informační generace: změna nebo kontinuita? (David Bawden). *Ikaros Elektronický Časopis o Informačni Společnosti / Ústav Informačních Studií a Knihovnictví Praha* [online]. 2009, roč. 13, 5/2 [cit. 2013-01-02]. ISSN 1212-5075. DOI: URN-NBN:cz-ik5462. Dostupné z: http://ikaros.cz/informacni-generace-zmena-nebo-kontinuita-david-bawden
50. JAKEŠ, Jiří. *DMS systémy a workflow*. Praha, 2008. Dostupné z: http://theses.cz//id/4ipnt9/. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra systémové analýzy. Vedoucí práce doc. Ing. Stanislav Horný CSc.
51. JELÍNEK, David. *Rozšíření informačního systému výrobní společnosti o správu dokumentů*. Praha, 2011. Dostupné z: http://www.vse.cz/vskp/eid/29328. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií. Vedoucí práce Ing. Renáta Kunstová, Ph.D.
52. JELÍNKOVÁ, Lenka. *Význam informačních technologií v průmyslu komerční bezpečnosti*. Zlín, 2006. Dostupné z: http://dspace.k.utb.cz/handle/10563/2231?show=full. Bakalářská práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky, Ústav elektrotechniky a měření. Vedoucí práce Mgr. Roman Jašek, Ph.D.
53. KALVODA, Ondřej. *Kyberkriminalita*. Brno, 2011. Bakalářská práce. Masarykova Univerzita, Fakulta sociálních studií, Katedra politologie. Vedoucí práce Mgr. Martin Bastl, Ph.D.
54. KALVODA, Ondřej. *Kyberkriminalita*. Brno, 2011. Dostupné z: http://is.muni.cz/th/333077/fss_b/Ondrej_Kalvoda_bak._prace.pdf. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií, Katedra politologie.
55. KOČÍ, Martin. *Bezpečnost a nakládání s daty a elektronickými dokumenty v podniku* [online]. Praha, 2012 [cit. 2012-11-08]. Dostupné z: http://theses.cz/id/a3zubj/93084_bpdp_final.pdf. Bakalářská práce. Vysoká škola ekonomie a managementu. Vedoucí práce Ing. Miroslav Lorenc.
56. KOHOUTEK, Michal a QURESHI. PWC BUSINESSCOMMUNITYCENTER. *Počítačová kriminalita pod lupou: celosvětový průzkum hospodářské kriminality - Česká republika*. 2011. Dostupné z: http://www.pwc.cz/crimesurvey
57. KRÁL, Roman. *Management informační bezpečnosti*. Praha, 2007. Dostupné z: https://www.vse.cz/vskp/show_evskp.php?evskp_id=2575. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky, Katedra informačních technologií. Vedoucí práce RNDr. Igor Čermák CSc.

58. KRAUSOVÁ, Alžběta. Identification in Cyberspace: 83-95. *Masaryk University journal of law and technology*. 2008, vol. 2, no. 1, s. 13. ISSN 1802-5951.
59. KUČEROVÁ ZRÁLÍKOVÁ, Václava. *Současné možnosti řešení správy a oběhu dokumentů ve firmě*. Praha, 2011. Dostupné z: http://digitool.is.cuni.cz/R/-?func=dbin-jump-full&object_id=698859&silo_library=GEN01. Diplomová práce. Univerzita Karlova v Praze, Filozofická fakulta, Ústav informačních studií a knihovnictví. Vedoucí práce PhDr. Jan Pokorný, Ph.D.
60. KUČEROVÁ, Helena. Definice informace: data - informace - znalosti. VYŠŠÍ ODBORNÁ ŠKOLA INFORMAČNÍCH SLUŽEB. *Zpracování informací a znalostí - ZIZ 2009/2010* [online]. 2010, 27. 12. 2012 [cit. 2013-01-03]. Dostupné z: http://info.sks.cz/users/ku/ZIZ/inform1.htm
61. KUKELKOVÁ, Adéla. *Nastupující generace talentovaných pracovníků: kulturní rozdíly motivace k práci generací Y a Z*. Olomouc, 2012. Dostupné z: http://theses.cz//id/xs0sgz/. Bakalářská práce. Univerzita Palackého v Olomouci, Filozofická fakulta. Vedoucí práce doc. Ing. Jaroslava Kubátová Ph.D.
62. KUŽEL, Stanislav. Podceňování investic do bezpečnosti může mít fatální následky. *HN Hospodářské noviny: Deník pro ekonomiku a politiku*. Praha: Economia, a.s, 2012, č. 12, s. 12-13. ISSN 0862-9587. Vyšlo jako příloha v ICTrevue.
63. *Kyberkriminalita a právo*. Vyd. 1. Editor Tomáš Gřivna, Radim Polčák. Praha: Auditorium, 2008, 220 s. ISBN 978-809-0378-674.
64. LAUSCHMANN, Jindřich. Gartner Hype Cycle 2012: jak si vedou nové technologie?.*Tyinternety.cz* [online]. 2012 [cit. 2013-01-03]. Dostupné z: http://www.tyinternety.cz/2012/08/22/clanek/gartner-hype-cycle-2012-jak-si-vedou-nove-technologie/
65. LDAP. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2.9.2012 [cit. 2013-01-03]. Dostupné z: http://cs.wikipedia.org/wiki/LDAP
66. LIPKOVÁ, Helena. *Materiály k přednáškám Podnikové informační systémy*. Praha, 2011.
67. LIPKOVÁ, Helena. *Materiály k přednáškám Projektování podnikových informačních systémů*. Praha, 2012.
68. LORENC, Miroslav. *Rozhodování o pořízení informačního systému pro podnik*. Praha, 2012. Dostupné z: http://theses.cz//id/epp5nb/. Disertační práce. Vysoká škola ekonomická v Praze, Fakulta hospodářská. Vedoucí práce prof. Ing. Jiří Fotr, CSc.
69. MELICHAR, Jan. *Bezpečnost a ochrana dat a informací v bankovnictví pro manažery* [online]. Jindřichův Hradec, 2009 [cit. 2012-11-08]. Dostupné z: http://www.vse.cz/vskp/eid/14183. Diplomová práce. Vysoká škola ekonomická v Praze. Vedoucí práce Ing. Pavel Pokorný.
70. NĚMEČEK, Ivo. Objem spamu klesá, zločinci objevují nová teritoria. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2011, č. 1, s. 30-31. ISSN 1802-4505.
71. PETERKA, Jiří. Elektronické podpisy: z bláta do louže?. *Lupa.cz* [online]. 2012 [cit. 2013-01-02]. ISSN 1213-0702. Dostupné z: http://www.lupa.cz/clanky/elektronicke-podpisy-z-blata-do-louze/

72. POKORNÝ, Jan. *ICT pro provoz informačních zdrojů : autentikace a autorizace v IS*. Praha, 2011. 24 slidů. Materiál z přednášek. Univerzita Karlova, Filozofická fakulta, Ústav informačních studií a knihovnictví.
73. POŽÁR, Josef. *Informační bezpečnost*. Plzeň: Aleš Čeněk, 2005, 309 s. Vysokoškolská učebnice (Vydavatelství a nakladatelství Aleš Čeněk). ISBN 80-868-9838-5.
74. PŘIKRYL, Lukáš. Blokování nežádoucích aktivit a prevence úniku dat. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2012, č. 3, s. 40-41. ISSN 1802-4505.
75. RABUŠIC, Ladislav. *Kvalitativní výzkum*. Praha, 2010. Prezentováno v rámci předmětu Metody výzkumu v sociologii.
76. REICH, Jan. *Lidský faktor v bezpečnosti IS/ICT* [online]. Praha, 2012 [cit. 2012-11-08]. Dostupné z: http://www.vse.cz/vskp/eid/32304. Bakalářská práce. Vysoká škole ekonomická v Praze. Vedoucí práce prof. Ing. Petr Doucek, CSc.
77. RINGER, Allison C. a Romana GARMA. Does the Motivation to Help Differ Between Generation X and Y?. In: *ANZMAC 2007: Reputation, Responsibility, Relevance*. Dunedin: University of Otago, 2007, s. 1067-1073. ISBN 978-1-877156-29-9. Dostupné z: http://anzmac.info/conference/2007/papers/RRinger_1.pdf
78. RYVOLA, Petr, Jaroslav TÍK a Jakub HYNEK. BYOD: koncept, který mění způsob, jakým pracujeme. BUNNELL, David a Adam BRAT. CISCO SYSTEMS, Inc. *Cisco* [online]. 2012 [cit. 2013-01-02]. Dostupné z: http://www.cisco.com/web/CZ/about/news/2012/20120430.html
79. RYVOLA, Petr, Jaroslav TÍK a Jakub HYNEK. Studie Cisco: Pravidla pro bezpečnou práci s IT je potřeba uzpůsobit současným potřebám. BUNNELL, David a Adam BRAT. CISCO SYSTEMS, Inc. *Cisco*[online]. 2012 [cit. 2013-01-02]. Dostupné z: http://www.cisco.com/web/CZ/about/news/2012/20120105.html
80. ŘEHÁČEK, David. Nová tvář kyberzločinu. *Security World: magazín o bezpečnosti v kybernetickém světě*. Praha: IDG Czech, 2012, č. 3, s. 32. ISSN 1802-4505.
81. SEIGE, Viktor. Informační bezpečnost? Proč ne!. *IT Systems*. Brno: CCB s.r.o, 2002, 7-8. ISSN 1802-002x. Dostupné z: http://bit.ly/Qg0nFg
82. SÍPAL, Luboš. *Dokument management Systém*. České Budějovice, 2009. Dostupné z: http://theses.cz/id//id/2x7mab/. Bakalářská práce. Jihočeská univerzita v Českých Budějovicích, Pedagogická fakulta, Katedra fyziky. Vedoucí práce Ing. Václav Novák, CSc.
83. SKÁLA, Zbyněk. Nástrahy implementace BYOD politiky. *IT Systems*. Brno: CCB s.r.o, 2012, 7-8, s. 52-53. ISSN 1802-002x.
84. SMEJKAL, Vladimír. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada, c2006, 296 s. ISBN 80-247-1667-4.
85. SMEJKAL, Vladimír. *Řízení rizik ve firmách a jiných organizacích*. 3., rozš. a aktualiz. vyd. Praha: Grada, 2010, 354 s. Expert (Grada). ISBN 978-80-247-3051-6.
86. STOHL, Michael. Networks, Terrorists and Criminals : the Implications for CommunityPolicing. *Crime, Law & Social Change*. 2008, vol. 50, issue 1/2, s. 59-72. DOI 10.1007/s10611-008-9120-x. ISSN 0925-4994.

87. STUCHLÍK, Pavel. *Systémy pro správu dokumentů*. Jindřichův Hradec, 2008. Dostupné z: http://www.vse.cz/vskp/eid/5061. Bakalářská práce. Vysoká škola ekonomická v Praze, Fakulta managementu v Jindřichově Hradci. Vedoucí práce Ing. Pavel Pokorný.
88. ŠUSTR, Josef. (Ne)bezpečná hesla. *IT Systems*. Brno: CCB s.r.o, 2002, 7-8. ISSN 1802-002x. Dostupné z: http://bit.ly/W9mxpq
89. TÁBOROVÁ, Alice. Veřejnoprávní ochrana informační společnosti a místní působnost práva. *Revue pro právo a technologie*. 2010, č. 1, s. 29-60. ISSN 1805-2797. Dostupné z: http://www.law.muni.cz/dokumenty/10467
90. Trendy vývoje autentizačních metod. MATYÁŠ, Vašek a Jan KRHOVJÁK. *Autorizace elektronických transakcí a autentizace dat i uživatelů*. Brno: Masarykova univerzita, 2008, s. 15-55. ISBN 978-80-2104556-9.
91. VAŘEČKA, Martin. *Bezpečnost a nakládání s elektronickými dokumenty v podniku* [online]. Praha, 2011 [cit. 2012-11-08]. Dostupné z: http://bit.ly/YP2SPB. Bakalářská práce. Vysoká škola ekonomie a managementu. Vedoucí práce Ing. Miroslav Lorenc.
92. VELECKÝ, Petr. Důležité uzly firemní bezpečnosti. *HN Hospodářské noviny: Deník pro ekonomiku a politiku*. Praha: Economia, a.s, 2012, č. 10, s. 14-16. ISSN 0862-9587. Vyšlo jako příloha v ICTrevue.
93. VESELÝ, Jakub. *Etický hacking: učební pomůcka pro předmět Bezpečnost informačních systémů*. Zlín, 2011. Dostupné z: http://dspace.k.utb.cz/handle/10563/17030. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce doc. Mgr. Roman Jašek, Ph.D.
94. VI. Cybercrime and Cybersecurity. KOŠČÍK, Michal, Libor KYNCL, Matěj MYŠKA, Radim POLČÁK, Václav STUPKA a Jaromír ŠAVELKA. *European ICT Law 2012: Texts, Cases, Materials*. 1. vyd. Brno: Tribun EU, 2012, s. 108-163. ISBN 978-80-263-0258-2.
95. VPN. In: *Wikipedia: the free encyclopedia* [online]. San Francisco (CA): Wikimedia Foundation, 2001-, 2.12.2012 [cit. 2013-01-03]. Dostupné z: http://bit.ly/ZeMU3m
96. VYMĚTAL, Jan. *Informační zdroje v odborné literatuře*. Vyd. 1. Praha: Wolters Kluwer Česká republika, 2010, 433 s. ISBN 978-80-7357-520-5.
97. ZAJÍC, David. Trendy v podnikové infrastruktuře v příštích třech letech. *HN Hospodářské noviny: Deník pro ekonomiku a politiku*. Praha: Economia, a.s, 2012, č. 10, s. 18-19. ISSN 0862-9587. Vyšlo jako příloha v ICTrevue.
98. ZEMKO, Jan. *Bezpečnostní rizika v prostředí internetu*. Zlín, 2011. Dostupné z: http://dspace.k.utb.cz/handle/10563/18505. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované logiky. Vedoucí práce PhDr. Mgr. Stanislav Zelinka.
99. ZHANG, Lixuan; MCDOWELL, William C. Am I Really at Risk? Determinants of Online Users' Intentions to Use Strong Passwords. *Journal of Interntet Commerce*. 2009, no. 8, s. 180-197. DOI 10.1080/15332860903467508. ISSN 1533-2861.
100. ŽÁČKOVÁ, Eliška. *Kyberterorismus: zaměření se na nedbalost zaměstnanců při tvorbě statických hesel*. Praha, 2011, 11 s. Pro potřeby semináře Zpravodajské služby.

10 Seznam obrázků, grafů a tabulek

Obrázky

Grafy

Tabulky

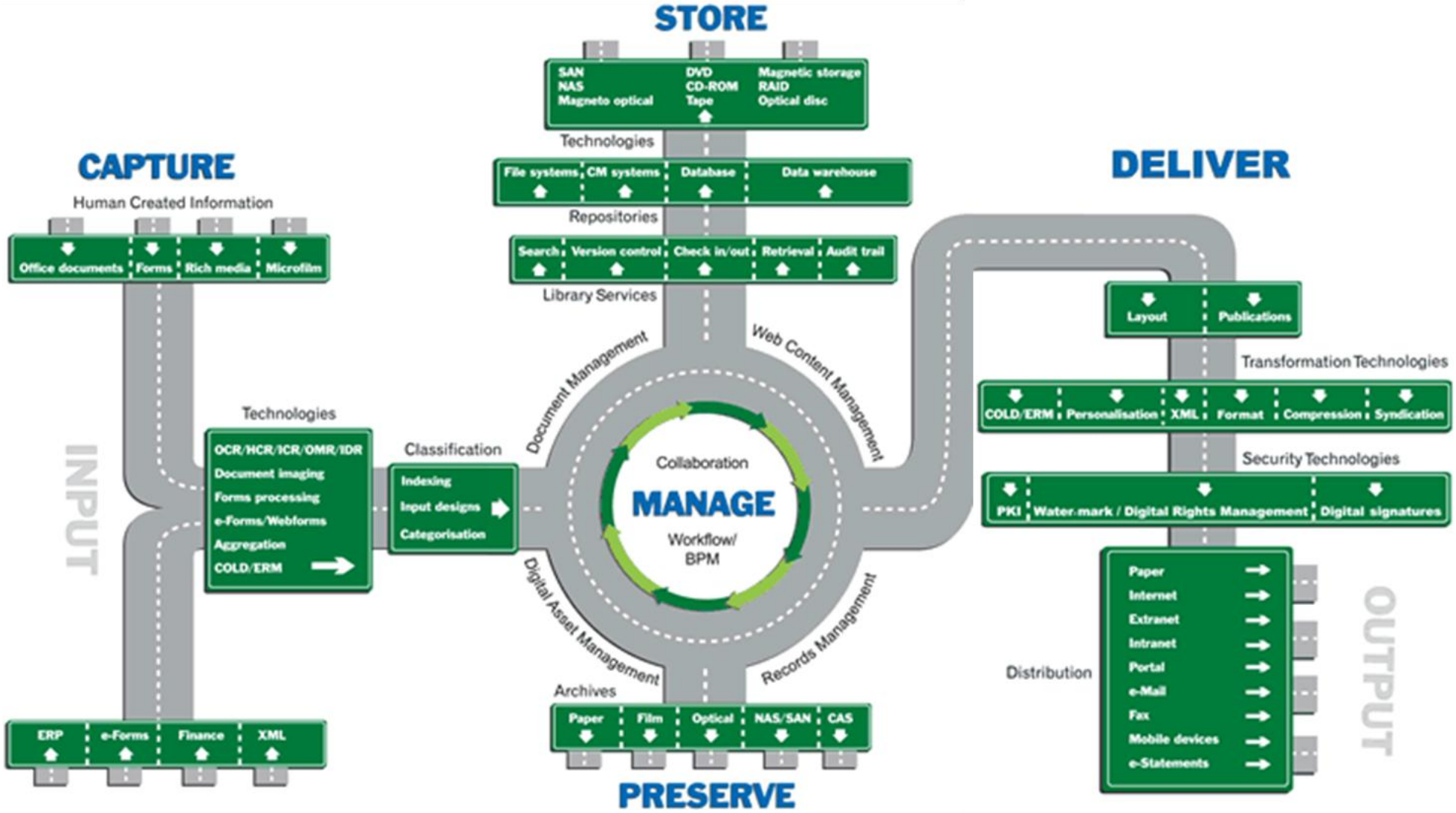
11 Seznam příloh

Příloha č. 1 - Schéma ECM Systému

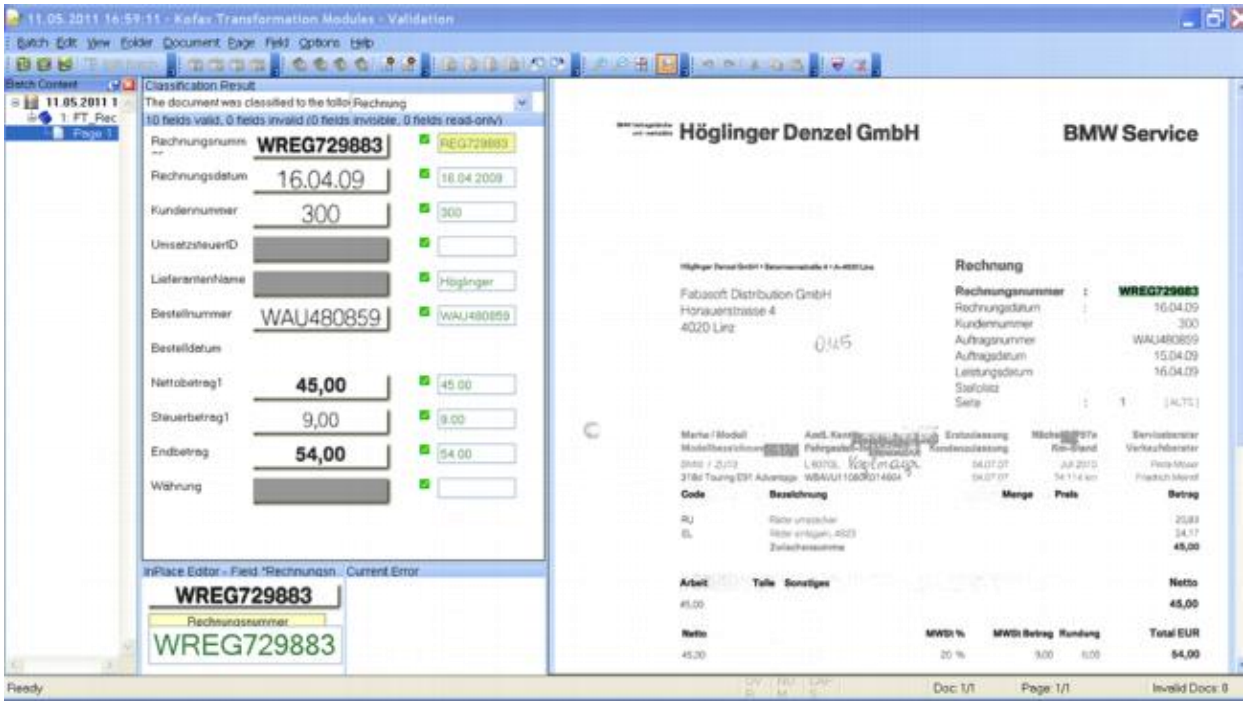
Příloha č. 2 - Validace a verifikace digitalizovaných dat

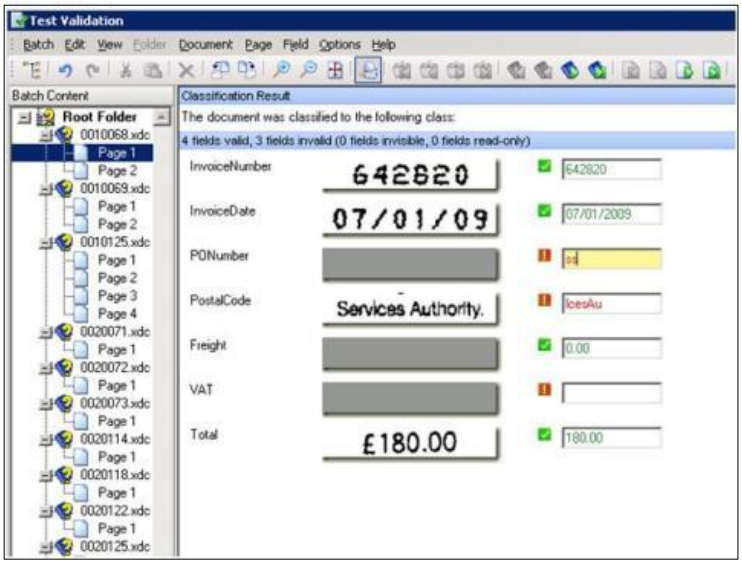
Příloha č. 3 - Ukázka možných typů skartace

Příloha č. 1 – Schéma ECM systému (Zdroj: AIIM – The Global Community of Information Professionals)



Příloha č. 2 – Validace a verifikace digitalizovaných dat (Zdroj: Internet)





Příloha č. 3 – Ukázka možných typů skartace (Zdroj: Internet)

Stupně bezpečnosti

NBÚ neklasifikován - DIN 1:

Pásek užší než 12 mm.

NBÚ Typ 1 vyhrazené - DIN 2: Vhodné pro skartaci běžných firemních dokumentů.

Pásek užší než 6 mm.

NBÚ Typ 2 důverné - DIN 3: Vhodné pro skartaci důvěrných firemních dokumentů nebo dokumentů s osobními údaji.

Pásek užší než 2 mm nebo

Křížový řez menší než 4 ×80 mm.

NBÚ Typ 3 tajné - DIN 4: Vhodné pro skartaci strategických dokumentů.

Křížový řez menší než 2 ×15 mm.

NBÚ typ 4 přísně tajné - DIN 5: Vhodné pro skartaci dokumentů vedených v režimu přísně tajné.

Křížový řez menší než 0,8 ×13 mm.