Bezpečnost dat a informací ve veřejné správě

Mgr. Jiří Čihák

Diplomová práce 2013

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky

Univerzita Tomáše Bati ve Zlíně
Fakulta managementu a ekonomiky
Ústav regionálního rozvoje, veřejné správy a práva
akademický rok: 2012/2013

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

Jméno a příjmení:	**Mgr. Jiří Čihák**
Osobní číslo:	**M11726**
Studijní program:	**N6202 Hospodářská politika a správa**
Studijní obor:	**Veřejná správa a regionální rozvoj**
Forma studia:	**prezenční**
Téma práce:	**Bezpečnost dat a informací ve veřejné správě**

Zásady pro vypracování:

Úvod

I. Teoretická část

- **Vysvětlete základní pojmy a principy spojené se správou dat a informací.**
- **Charakterizujte rizika spojená se zneužitím dat a informací, se kterými operují orgány veřejné správy.**

II. Praktická část

- **Na podkladech teoretické části zhodnoťte reálná a nejvýznamnější rizika.**
- **Navrhněte projekt pro instituci veřejné správy, jehož cílem bude dlouhodobé udržení a další navyšování bezpečnosti správy dat a informací z personálního hlediska.**

Závěr

Rozsah diplomové práce: **cca 70**

Rozsah příloh:

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

Seznam odborné literatury:

JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN. Informační technologie ve veřejné správě. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 183 s. ISBN 978-8-07318-607-4.
LIDINSKÝ, Vít. EGovernment bezpečně. Praha: Grada, 2008, 145 s. ISBN 978-80-247-2462-1.
POŽÁR, Josef. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005, 309 s. ISBN 80-86898-38-5.
TIPTON, Harold a Micki KRAUSE. Information security management handbook. 6. vyd. Boca Raton: Auerbach, 2007, 3231 s. ISBN 0-8493-7495-2.

Vedoucí diplomové práce: **Ing. Miroslava Komínková, Ph.D.**
Ústav statistiky a kvantitativních metod

Datum zadání diplomové práce: **3. února 2013**

Termín odevzdání diplomové práce: **2. května 2013**

Ve Zlíně dne 3. února 2013

L.S.

prof. Dr. Ing. Drahomíra Pavelková
děkanka

RNDr. Oldřich Hájek, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že:

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1];
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému,
- na mou diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2];
- podle § 60[3] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;

---

[1] *zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:*

(1) Vysoká škola nevýdělečně zveřejňuje disertační, diplomové, bakalářské a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy.

(2) Disertační, diplomové, bakalářské a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

[2] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:*

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

[3] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

- podle § 60[4] odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);

- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům.

Prohlašuji, že:

- jsem diplomovou práci zpracoval samostatně a použité informační zdroje jsem citoval;

- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně 29.4.2013 ..... Jiří Čihák .....

[4] *zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:*

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Práce Bezpečnost dat a informací ve veřejné správě se zabývá problematikou bezpečnosti dat a informací ve veřejné správě, speciálně z pohledu personálního pojetí bezpečnosti dat a informací. Ústředním tématem jsou lidé, zaměstnanci a rizika, která mohou tyto subjekty představovat pro veřejnou správu.

Cílem práce je důsledně poukázat na aspekty digitalizace veřejné správy a společnosti a identifikovat související rizika spojená s personální stránkou bezpečnosti ve vztahu k významnému rozsahu dat a informací, se kterými operuje veřejná správa, a vytvoření konceptu, který umožní zajištění dlouhodobé udržitelnosti a dalšího navyšování bezpečnosti správy dat a informací ve veřejné správě z personálního hlediska.

Předkládaný text v úvodu definuje pojmy a principy, na jejichž základě práce dále pátrá a definuje nová, příliš nepodchycená a aktuálně se objevující rizika vzrůstající z personálního prostředí, spojeného s postupující penetrací využívání elektronických informačních systémů a ohrožujících bezpečnost dat a informací nejen ve veřejné správě.

Na základě představených poznatků práce prezentuje efektivní a udržitelný koncept bezpečnostního vzdělávání pracovníků veřejné správy, který reaguje na zjištěná rizika a je aplikovatelný do současného prostředí veřejné správy.

Práce vychází z kontextu přelomu let 2012 a 2013.

Klíčová slova: bezpečnost dat a informací, digitalizace veřejné správy, kultura organizace, personální bezpečnost, veřejná správa, vzdělávání zaměstnanců

ABSTRACT

This work is about Data and Information Security in Public Administration, focused on employees role in providing data and information security. People, staff and the risks that these entities pose to public administration are key themes of this work. The aim is to point out aspects of digitalization of public administration and society and to identify risks, associated with the personal aspects of providing safety – in the context of a significant range of data and information, which public administration operates – and design a concept that will ensure sustainability and further increasing of data and information safety in public administration, especially from the personnel point of view of providing security.

This work is based on the context of the years 2012 and 2013.

Keywords: Data and Information Security, Digitalization of Public Administration, Employees Education, Organization Culture, Personnel Security, Public Administration

OBSAH

ÚVOD

Práce se jmenuje Bezpečnost dat a informací ve veřejné správě. Vzhledem k tomu, že se jedná o velice široké téma zahrnující rozsáhlý soubor vztahů, je práce zaměřena na užší oblast, a to především na zajištění bezpečnosti dat a informací ve veřejné správě z personálního hlediska pojetí bezpečnosti. Ústředním tématem jsou lidé, zaměstnanci a rizika, která mohou představovat pro veřejnou správu.

Cílem práce je důsledně poukázat na aspekty digitalizace veřejné správy a společnosti a identifikovat související rizika spojená s personální stránkou bezpečnosti, především ve vztahu k významnému rozsahu dat a informací, se kterými veřejná správa operuje, a dále vytvoření konceptu, který umožní zajištění dlouhodobé udržitelnosti a dalšího navyšování bezpečnosti správy dat a informací ve veřejné správě z personálního hlediska.

Práce v počáteční teoretické části definuje nezbytný teoretický základ, aby na těchto podkladech mohla diskutovat a poukázat na aspekty digitalizace veřejné správy a související rozsáhlá rizika spojená s personální stránkou bezpečnosti, ve vztahu k významnému rozsahu dat a informací, se kterými veřejná správa nakládá. Na těchto teoretických podkladech práce dále rozvíjí svojí analytickou část, ve které vymezuje reálná a pro veřejnou správu nejvýznamnější rizika současné doby. Práce pátrá po nových, dosud příliš nepodchycených a také aktuálně se objevujících rizicích vzrůstajících z personálního prostředí, spojeného s postupující penetrací využívání elektronických informačních systémů napříč společností.

V návaznosti na analytickou část a zjištěná a diskutovaná rizika práce zhodnocuje definovaná rizika a na tomto analytickém základě práce v řešící části představuje vlastní efektivní, dostupné a udržitelné řešení, aplikovatelné do prostředí české veřejné správy. Řešící část představuje udržitelný koncept bezpečnostního vzdělávání pracovníků veřejné správy, aplikovatelný do jejího současného prostředí. Práce také vysvětluje, proč je právě personální přístup k zajištění bezpečnosti dat a informací prostorem s velkým potenciálem k navyšování bezpečnosti dat a informací ve veřejné správě a ilustruje rizika a možnosti, kterých může veřejná správa, při tomto pojetí zajištění bezpečnosti, dosáhnout. Práce zároveň reflektuje možná rizika a překážky implementace navrhovaného projektového řešení a nabízí drobný výhled budoucího možného vývoje bezpečnostní problematiky ve veřejné správě.

I. TEORETICKÁ ČÁST

1 ZÁKLADNÍ POJMY A PRINCIPY SPOJENÉ SE SPRÁVOU DAT A INFORMACÍ

1.1 Informační společnost

Žijeme v informační společnosti. Společnosti, ve které je trendem digitalizace většiny dostupných dat, tvorba informačních databází a další nárůst využívání počítačových systémů, za neustálého snižování cen výpočetní techniky, při souběžném nárůstu výkonu. (Rosman, 2002, s. 15; Lukáš, Hrůza a Kný, 2008, s. 7)

Je těžké exaktně pojmenovat právě tuto etapu, ve které se současná společnosti nachází. Je možné narazit na pojmy informační společnost, společnost znalostí, vědomostní společnost, společnost informací, technokratická společnost, učící se společnost a tak jak někteří autoři některé pojmy spojují, někteří je opět ostře odlišují. Je však zřetelné, že „klíčovou roli ve všech oblastech lidského konání přitom zaujímají informační a komunikační technologie“ a i z tohoto hlediska pojmenování informační společnost se jeví jako nejvýstižnější. (Rosman, 2002, s. 15, 17)

V dnešní době je potřeba umět s daty především zacházet, neboť dnes je již produkováno takové množství dat, že není v lidských schopnostech tato data obsáhnout. Problematika dat je rozsáhlá. Množství poznatků, které má lidstvo k dispozici, roste obrovskou rychlostí. A právě tak čím více informací mají lidé k dispozici, tím důležitější je umět tyto informace efektivněji třídit, zpracovávat a umět je efektivně sdělovat dalším lidem (Rosman, 2002, s. 17). Je tedy potřeba, aby ruku v ruce s rozvojem informační společnosti, která nabízí možnosti správy větších a větších objemů dat, šlo i uvědomění si potřeby vnitřní hygieny, datové očisty. Zda jsou všechna data opravdu relevantní k nějakému účelu a potřeba. Je důležité, aby lidé zvládali schopnosti vybírat si pouze ta data, pro ně relevantní a o ostatní se nezajímali. Neboť by mohlo dojít po čase například k nervovému zhroucení jedince. Právě takového jedince, který by chtěl obsáhnout všechna data, být neustále online. Je potřeba umět zacílit svoji pozornost na zájmová data a nesnažit se obsáhnout všechny dostupné zdroje. Toto je však úkol pro informační management.

Informace nabývají rostoucího významu ve společnosti a právě informace, respektive znalosti, se staly v současném světě jedním z nejcennějších zdrojů. Informační společnost s sebou nese však ale i negativní jevy. Mezi ně patří permanentní informační zahlcení, redundance ale také dezinformace (Rosman, 2002, s. 18).

Informační společnost přináší výrazné změny do společnosti, změny týkající se využití zdrojů a času, ale také přináší změny struktur, informačních struktur a procesů, které s informacemi a daty operují a je potřeba, aby veřejná správa, pokud chce být efektivní, štíhlá a účinná, aby pružně reagovala na tyto změny a trendy (Rosman, 2002, s. 18). Pro naplnění těchto cílů, je potřeba tomuto dění kvalitně porozumět.

Proto v této době obzvlášť nabývá na významu otázka vzdělávání. Dnešní trendy směřují k digitalizaci většiny dostupných dat a k jejich skladování po takřka neomezenou dobu. Dochází tak k hromadění osobních dat, jejich výměnám, kombinování a lze tak po nějakém čase, i ze zdánlivě kusých informací, získat až překvapivě, či znepokojivě, realitě věrně odpovídající informace o cílových osobách. A tím, jak jsou tato data globálně dostupná, navyšuje se riziko jejich zneužití nebývalým způsobem. Způsobem, který výrazně narušuje soukromí a vystavuje jedince tlaku sociální manipulace a komerčním zájmům. (Rosman, 2002, s. 19, 20) Důležité je tedy důkladně rozmyslet, co uveřejnit do virtuálního prostoru a jak se v tomto prostoru chovat. Toto je právě velké téma, o kterém je důležité diskutovat, a to především ve vztahu k zaměstnancům veřejné správy. Vzdělávání je tohoto vhodným nástrojem. Ona sama informační společnost podporuje vzdělávání. Tím, jak umožňuje shromažďovat množství informací a usnadňuje a urychluje k nim přístup, je právě informační společnost vhodnou dobou a podpůrným nástrojem k jakýmkoli formám vzdělávání.

1.1.1 Globalizace a informační trendy

Jak bylo řečeno, žijeme v informační společnosti, která podporuje vzdělávání. Informační společnost je charakterizována využíváním digitálního zpracování k uchování a přenosu informací (Rosman a Buřita, 2011, s. 17) a tento přenos se děje v globálním měřítku. Takzvaná globální informační společnost s sebou nese své klady, ale i zápory. Mezi její klady patří možnosti a prostory pro rychlé šíření informací, pokroku, vědeckého výzkumu a spolupráce a možnosti dostupného skladování takto nabytých znalostí. Mezi negativa patří s tímto spojená kriminalita, anonymita a zranitelnost tohoto prostoru.

Globalizace usnadňuje pozici útočníkům. Jednak jsou citlivé systémy stále více a více navzájem propojovány, kdy jakoby stále otevírají nová propojení, okna k možným útokům, ale také dochází i ke stále se zvětšující unifikaci systémů, certifikaci a standardizaci a globálnímu uplatňování nejrůznějších norem a standardů. Tento trend snižuje unikátnost a varietu jednotlivých systémů a nabízí rizika, kdy pokud se ve standardizovaném systému, návrhu objeví bezpečnostní nedostatek, tento nedostatek již neohrožuje pouze jednu dílčí

organizaci, ale globálně všechny organizace, které dané řešení implementovaly. (Brabec, 2001, s. 9; Doucek, 2011, s. 14)

Globalizace sama o sobě nevyžaduje žádná zvláštní opatření, ale je potřeba, aby základní články globálního systému, tedy jednotlivé organizace, zastupované lidmi, pevně dbaly na svá opatření. Neboť jak zní jedno z všeobecně známých mott bezpečnostního konání, „systém je tak silný, jak silný je jeho nejslabší článek“. A v globalizovaném světě se toto jen násobí.

Současně s informační explozí (Požár, 2005, s. 19) či, místy se setkáváme s pojmem totální digitalizace (Rosman, 2002, s. 17), jež provází informační společnost, dochází zároveň k vytrácení soukromí. Soukromí lze dle Čandíka (2004, s. 6) v této sféře chápat jako svou možnost kontrolovat vlastní osobní údaje, kontrolu informací o sobě a své činnosti. Dochází v současnosti k nebrzděnému hromadění informací (Laucký, 2009, s. 111), jež se bude do budoucna jen zvětšovat. Již dnes denně za sebou dobrovolně i nedobrovolně necháváme mnohé vyhodnotitelné stopy. Těch dobrovolných je mnohdy ještě více než oněch nedobrovolných a leckdy, i díky sociálním sítím, větší hodnoty.

Toto vše je potřeba, aby si speciálně zaměstnanci veřejné správy uvědomili. Neboť veřejná správa spravuje nesmírné množství dat a informací o každém z nás a tyto spravované údaje mohou být pro nejrůznější subjekty velmi zajímavé. A právě například i další publikování osobních údajů vlastních zaměstnanců, může tyto zaměstnance udělat i dále ještě velmi zranitelné, pro případné kriminální aktivity cizích subjektů. Cílem vzdělávání je tedy nabídnout koncept bezpečného jednání a práce s informačními systémy tak, aby byla zajištěna bezpečnost dat a informací ve veřejné správě a zajištěn tak bezpečný chod a výkon veřejné správy za dodržení podmínek 3E a výkonu dobré správy.

1.1.2 Množství informací ve společnosti

Problematika množství informací ve společnosti má několik aspektů, se kterými se musí veřejná správa vypořádávat. Na straně jedné může docházet k hromadění informací například neetickým způsobem, protispolečenských informací a na straně druhé může docházet ne k jejich hromadění, ale k jejich nezdravému zadržování, filtraci a selekci. Obojí nevede k dobré kultuře ve společnosti jako celku, ale ani dílčích částí společnosti, například na pracovišti. Zaměstnanci mohou hromadit informace nebo své kompetence s cílem vyrovnat se vedoucím pracovníkům, přisoudit si jistou dávku důležitosti a obdobně mohou zadržovat informace před ostatními. Obojí je pro společnost a její organizace nezdravé.

Zaměstnanci mohou mít zájem dovědět se více, dovědět se ono zakázané a mohou začít pátrat po informacích a v průběhu tohoto pátrání narazit i na jiné informace, o které může mít zájem někdo jiný. Tvrdí se také, že „mnoho úniků dat a informací není vůbec cílených, ale jsou prováděny prostě pouze proto, že mohou být provedeny“. (Požár, 2005, s. 67)

Informace jsou vnímány jako hodnota a jako taková se spolu s penězi stávají hybnou silou společnosti. Onen nadbytek informací se stává stresorem moderní informační doby (Lukáš, Hrůza a Kný, 2008, s. 9) a jak k tomuto dodává Brabec (2001, s. 264) který uvádí, že agentura Reuters zjistila, že informace mohou být i rizikové, neboť narůstá ve společnosti právě nezdravá závislost na informacích. Lidé, kteří propadnou konzumaci informací, mohou trpět neurózou při pobytu mimo jejich zdroj, nejčastěji počítač nebo mobilní telefon, a tyto osoby mohou mít problémy v určitých částech svého života. Což ve svém důsledku vede k tomu, že získané informace nejsou schopni účelně použít ve prospěch svůj ani své organizace. Stanou se tedy namísto určité hodnoty zbytečnými a pouhými původci problémů. Jak k tomuto dodává výše uvedený zdroj (Lukáš, Hrůza a Kný, 2008, s. 9) doplněný o (Brabec, 2009, s. 143), problémem je také dále rostoucí stres lidí zaplavených informacemi. Dle Brabce (2009, s. 143) až třetina manažerů trpí zdravotními obtížemi souvisejícími s množstvím informací zatěžujících jejich mozek a 43 % respondentů se někdy nemohlo rozhodnout, protože měli příliš mnoho informací. Jak již bylo v úvodu uvedeno, nastavení správné míry přístupu k informacím, a správným informacím, je úkolem informačního managementu. To je také důležitý úkol, neboť lidé, kteří jsou vystaveni proti své vůli množství informací, trpí depresemi, jsou náchylní ke zdravotním potížím v podobě srdečních chorob, poruch spánku a sexuálních problémů, jejich pracovní výkonnost dále klesá a to vše přináší následné problémy v soukromém životě, které se zpětně promítají do pracovního výkonu. Ponížený pracovní výkon, nedostatečné znalosti správných zásad, postupů, rizik a trendů nebo neopatrnost, to vše vede k oslabování pozice bezpečnosti dat a informací v organizaci.

Jak je zde důkladně ilustrováno, data a informace nejsou jen jakási čísla a fakta, ale hodnoty, mající výrazné vlivy a dopady nejen na fungování celé společnosti, ale každého jejího jedince. Je proto důležité dobře zvládat informační management, který by měl nastavit správnou míru a regulaci informací, a na těchto základech může být později vystavěn kvalitní bezpečnostní management. Bezpečnostní management zajistí, že dané a potřebné údaje a informace nebudou užívány neoprávněnými způsoby a bude zajištěno jejich bezpečí, důvěrnost a integrita.

1.2 Vymezení základních pojmů a principů

1.2.1 Data

Je možné se setkat s častou záměnou či slučováním pojmů data a informace. Nutno dodat, že v průměrné většině textů díky této záměně nedojde ke zkreslení obsahu a je tedy prakticky možno tyto pojmy přiměřeně zaměňovat. Nicméně pro odstranění nepřesností je potřeba tyto pojmy definovat a jemně rozlišit jejich detaily.

Data mohou být chápána různými způsoby, například dle Požára (2005, s. 21) jako „statická fakta, časově nezávislá, kdy v praxi se také používá pojem údaj, jako obecný výraz pro data i informace. Informace je význam, přisouzený datům. Je to to, co vyplývá z analýz, zpracování a prezentace dat v takové formě, která je potřeba“. Dle jiných definic (Benda, Sodomka a Rosman, 2000, s. 13) jsou data spíše „odrazem jevů, procesů a vlastností, které existují v reálném světě“, a proto jsou „data ve své podstatě abstraktními pojmy“, kdy vlastní „pojem data je chápán spíše ve smyslu technického záznamu skutečnosti“.

Možná nejčistší definici pro rozlišení rozdílu mezi daty a informacemi nabízí Doucek (2011, s. 38), který uvádí, že „data jsou základním zdrojem informací. Data sama o sobě jsou však nepoužitelná, pokud se neorganizují nebo se s nimi nezachází tak, aby se stala informacemi. Informace se definují jako data s významem, relevantním účelem. Informace je pak dále základem pro znalost“. Data tedy dle jeho (Doucek, 2011, s. 37) vnímání jsou „údaje skutečnosti, které bezprostředně odrážejí zkoumanou skutečnost a představují nejnižší prvek informačního systému. Procházejí dalším zpracováním a vytvářejí se z nich tak sekundární data a po jejich následné analýze se stávají dalším podkladem formulace empirických tvrzení, tedy faktů. Jedná se o obraz skutečnosti“.

Výše uvedený autor (Doucek, 2011, s. 37) dále dodává, že data se uchovávají na nosičích dat, zpracovávají se různými typy prostředků, dnes především výpočetní technikou. Tím nepřímo potvrzuje v úvodu zmiňované, že dnes informační systémy, tedy systémy pro práci s daty, jsou v podstatě synonymem pro elektronické informační systémy. Dochází k digitalizaci původních informačních zdrojů (Benda, Sodomka a Rosman, 2000, s. 13) a nová data jsou prakticky obsluhována výhradně v digitální podobě. S tím souvisí, jak dodávají dále Benda, Sodomka a Rosman (2000, s. 13) změna „tradičního pohledu na data, kdy postupně mizí problémy spojené s daty a s otázkami typu jak a kde data uchovat a nastupuje nový fenomén. Fenomén spojený s otázkou: Jak se má člověk v takovém množství

dat orientovat a nejrychleji najít tu, kterou právě potřebuje?“ Problematika zahlcení daty a informacemi byla diskutována v předchozích kapitolách, netřeba ji proto znovu opakovat. Lze jen dodat, že právě s touto otázkou hledání nového orientování a zacházení s daty a informacemi v novém formátu, souvisí ještě o něco palčivější otázka, kterou je otázka dostatečného zajištění právě bezpečnosti dat a informací při těchto činnostech. Tato problematika bude rozebírána v následujících kapitolách.

1.2.2 Informace

Jak bylo uvedeno u dat, obdobně mnohé vnímání je také u pojmu informace. Záleží na oboru, ze kterého se na tento pojem díváme, ale také velmi na autorovi, který daný pojem definuje, neboť možnosti jsou tu opravdu široké. Bude proto nejvhodnější si pojem informace u tohoto bodu ilustrovat dle vnímání jednotlivých autorů.

Shodu lze nalézt v pojednání o hodnotě a charakteru informací. V podstatě většina autorů se shoduje na hodnotě informací jako na výrazné, i když leckdy obtížně až nevyčíslitelné hodnoty pro současnou společnost, kdy „informace se stávají nejcennějšími zdroji“ (Rosman a Buřita, 2011, s. 14), které mají „klíčovou roli ve všech oblastech“ (Brabec, 2009, s. 5) současného lidského konání. Dále se mnozí autoři shodují na vnímání informací jako na druhu zboží (Jašek, Dolejšová a Rosman, 2007, s. 16; Požár, 2005, s. 24; Brabec, 2001, s. 211), kdy právě toto vnímání informací jako zboží, spolu s rozšiřováním technologií, „mění roli informací na zdroj svým významem rovnocenný tradičním ekonomickým zdrojům jako jsou půda, práce a kapitál“ (Doucek, 2011, s. 28). Informace jsou také vedle materiálních, energetických a finančních zdrojů jedním z hlavních faktorů pokroku vývoje lidské společnosti (Požár, 2005, s. 19).

K samotné definici pojmu informace dodávají Jašek, Dolejšová a Rosman (2007, s. 13), že pojem informace pochází z latinského informo – information – informare a znamená sdělení, jeho přenos ale také poučení či popis něčeho. Mates a Smejkal (2012, s. 18) vykládají pojem informace původem z latiny a spíše ve smyslu dnešního instruovat či poskytovat znalosti.

Brabec (2001, s. 211) definuje informace o nějakém jevu „jako jisté veličiny, které nám snižují dosavadní neurčitost, neznalost právě o onom jevu“. Tedy informací není podle této definice jakékoli sdělení, to by byl spíše údaj, ale takové sdělení, které nám poskytuje něco nového, něco ze kterého se něco nového dovídáme. Něco, co jsme předtím nevěděli. Tedy informace může být chápána jako snížení či zmenšení neurčitosti.

Co se vztahu data – informace týče, Brabec (2001, s. 216) a posléze i Požár (2005, s. 25) k tomuto naprosto shodně dodávají, že „každá informace je tedy údajem, ale každý údaj se nutně nemusí stát informací. Informací se tedy stane v okamžiku, kdy příjemci přinese něco nového“, respektive „každá informace je tedy údajem, datem, ale jakákoli uložená data se nemusejí stát nutně informací“.

Nositelem informace je signál (Jašek, Dolejšová a Rosman, 2007, s. 14) a protože je informace nehmotná, musí být uložena na nějakém nosiči (Brabec, 2001, s. 211). Tím je buď hmotné paměťové médium, ale také paměťové stopy obsažené v hmotném nosiči, kterým je například i lidský mozek. S tímto souvisí prapůvod častého neuvědomění si hodnoty informace. Hodnota informace není reprezentována hodnotou nosiče, ale její skutečnou, často nevyčíslitelnou ale někdy i nulovou, hodnotou.

Jak bylo názorně podloženo, „pojem informace tedy není jednoznačný“ (Požár, 2005, s. 22) a jeho význam vždy vychází z kontextu, v jakém je používán. Je jinak chápán v žurnalistice, jinak ve filosofii nebo politologii a obdobně jinak také v informatice nebo managementu (Lukáš, Hrůza a Kný, 2008, s. 12). Stejní autoři Lukáš, Hrůza a Kný (2008, s. 16) dále zmiňují i vlastnosti informace, mezi které řadí její včasnost, dostupnost, spolehlivost přístupu k informacím a dále zmiňují, že pro informace, jejich hodnocení a zhodnocení jsou důležitými faktory také jejich obsah, jeho aktuálnost, relevantnost, pravdivost, objektivnost, přiměřenost, dále formát informace, jejich cena a užitná hodnota, jde-li vyčíslit, legálnost a takto pokračují dále, včetně aspektů relevantnosti, správnosti, včasnosti, aktuálnosti a úplnosti. V tomto bodě, k problematice aktuálnosti informací, Lukáš, Hrůza a Kný (2008, s. 16) vhodně parafrázují Einsteina, kdy uvádějí jeho větu, že „Odpovědi na loňské otázky jsou letos jiné než loni“. Dále Lukáš, Hrůza a Kný (2008, s. 6) dodávají, že informace umožňují vzdělávat, sdělovat, rozhodovat a díky tomu jsou rozhodně fenoménem současnosti. Zde je vidět shoda s definicí informační společnosti. A právě současná informační společnost, její organizace a dnes i jedinci, ač si to možná neuvědomují, jsou na informacích závislí více než kdykoli v minulosti.

Co se legislativního zakotvení pojmu informace týká, Mates a Smejkal (2012, s. 19) zmiňují § 3 odst. 3 zákona 106/1999 Sb. o svobodném přístupu k informacím. Dle tohoto zákona se informací rozumí jakýkoli obsah nebo jeho část v jakékoli podobě, zaznamenaný na jakémkoli nosiči, zejména obsah písemného záznamu na listině (klasické dokumenty) záznamu uloženého v elektronické podobě (elektronické dokumenty) nebo záznamy zvu-

kového, obrazového nebo audiovizuálního charakteru. I lidská komunikace může být informací.

Dále dodávají (Mates a Smejkal, 2012, s. 19), že informace představuje míru uspořádanosti systémů, na rozdíl od entropie. Tj. jak bylo zmíněno, snižuje míru neuspořádanosti. Její nejmenší jednotkou pro počítačovou sféru je bit, kdy 1 bit zjednodušeně reprezentuje informaci, či respektive údaj, získanou odpovědí na otázku ano nebo ne.

Co se vztahu k veřejné správě týká, lze najít i zmínku, kdy Brabec (2001, s. 210) komentuje, že tak jak jsou informace podstatné, tak právě bez informací nelze vykonávat veřejnou správu. Bez informací a také pravidel. Požár (2005, s. 23) k legislativním definicím pojmu informace ještě doplňuje několik dalších zákonů, ze kterých lze zmínit zákon číslo 101/2000 Sb. o ochraně osobních údajů, kde „informace (či vhodněji spíše data), které se vztahují k určité osobě, jsou osobními údaji“ a dále zákon číslo 148/1998 Sb. o ochraně utajovaných skutečností, kde je definováno, co je utajovanou skutečností. Také soukromoprávní sféra práva definuje informace, konkrétně obchodní zákoník, tedy zákon číslo 513/1991 Sb. vymezuje obchodní tajemství (Požár, 2005, s. 23).

Pro úplnost k tématu lze zmínit zajímavý příspěvek Bendy, Sodomky a Rosmana (2000, s. 11), kteří nalezli několik starších vnímání pojmu informace. Citujme některé tyto starší vnímání.

„Informace:

- je název pro obsah toho, co se vymění s vnějším světem, když se mu přizpůsobujeme a působíme na něj svým přizpůsobováním (N. Wiener 1954)
- je to, co vyplývá z pečlivých analýz, zpracování a prezentace dat v takové formě, která bude vhodná pro rozhodovací proces (L. Long 1989)
- je poznatek o určité skutečnosti, předmětu nebo jevu zachyceném ve zpřístupnitelné formě (Cigánik 1964)
- je objektivní obsah komunikace vzájemně na sebe působících materiálních objektů, který se projevuje změnou stavu těchto objektů (Brillouin 1958)
- je každý znakový projev (sdělení, zpráva, věta) který má smysl pro komunikátora i příjemce. Je objektivním obsahem komunikace. Tento výklad zahrnuje tři složky: znakový projev, sémantickou ekvivalenci a sdělitelnost (Merta 1970)“

Hodnotu informací je všeobecně složité exaktně vyčíslit (Norman, 2010, s. 347). Jak bylo zmíněno v kapitole pojednávající o pojmu informace, její hodnota rozhodně není definována hodnotou nosiče a pro dnešní společnost, informační společnost, mohu mít některé informace až nevyčíslitelnou hodnotu. Takovou hodnotu by měla dozajista informace o tom, jaká bude budoucnost. Nicméně existují i informace s nulovou hodnotou. Všeobecně se dá říci, že „hodnotu informace může představovat především její výlučnost, například to, že vím něco, co jiný neví, ale také přesnost a vypovídací hodnota," (Jašek, 2006, s. 9) a dále že „cena a hodnota informací je dána vynaloženými náklady na jejich pořízení, uchování a údržbu a zároveň cenou danou informačním obsahem a užitnou hodnotou informace" (Požár, 2005, s. 35). Podstatné je, i kde se informace nachází a jak je dostupná. To je důležité zmínit, neboť i cenná informace, uložená v nepřístupné databázi nebo napsaná nerozluštitelným jazykem či šifrou, bude mít sice velkou cenu, ale její užitná hodnota bude téměř nulová. Samotné informace jsou předpokladem k tvorbě znalostí.

A jak trefně glosuje Požár (2005, s. 53), „hodnotu něčeho zpravidla oceníme až tehdy, když tuto hodnotu ztratíme".

1.2.3 Znalosti

Znalosti jsou dalším stupněm zpracování informace. Pouze člověk je schopen přeměnit informace ve znalosti a takto je také zhodnotit. Znalosti jsou ve své podstatě informace, u kterých jejich držitel, vlastník ví, jak je využít a je schopen je takto použít. (Brabec, 2009, s. 35; Jašek, Dolejšová a Rosman, 2007, s. 15) Právě tato znalost a schopnost použití, reálné aplikace je to, co odlišuje informaci od znalosti. Informace je tedy základem pro znalost a znalost je vyšším stupněm použití informace. Pro účely této práce není podstatné hlouběji se zaobírat pojmem znalosti. O mnoho podstatnější je vztah, který mezi sebou pojmy data, informace a právě znalosti mají.

1.2.4 Vztah data – informace – znalosti

Data, informace a znalosti jsou tři neoddělitelné pojmy a tato kapitola osvětlí vztahy mezi nimi. Pravděpodobně nejlépe podávají výklad a shrnutí vztahu mezi daty, informacemi a znalostmi Brabec (2001, s. 267) s Lukášem, Hrůzou a Kným (2008, s. 202, 203, 208) a to následovně. Data jsou ve shrnutí dle jejich vnímání v podstatě interpretací nebo popisy skutečnosti, určité vyjádření souborů fakt. Data jsou předmětem zpracování a jsou základní

součástí informačních systémů. Informace jsou data relevantní k nějakému konkrétnímu problému, jevu, věci, osobě a jsou to ta data, která přinášení nějaké nové poznatky o jeho skutečnosti, snižují onu neurčitost a tím dávají význam svému držiteli. V procesu komunikace informaci obsahuje sdělení, zpráva. Znalost je dle Lukáše, Hrůzy a Knýho (2008, s. 202, 203, 208) doslova „osvojená, zaregistrovaná zásoba poznatků o objektivní realitě, jež jsou důležité pro výkon určité činnosti. Vzniká odvozováním z informací, jejich porovnáváním, tříděním, vyhodnocováním, ověřováním, zasazováním do kontextu ostatních informací, znalostí a zkušeností. Jedná se o vědomé i nevědomé potenciály, již oproti datům a informacím obtížně přenositelné bez výcviku a zkušeností“.

Jak je představeno, data, informace a znalosti tvoří jakousi posloupnost, pyramidu, kdy směrem nahoru, ke znalostem, přibývá jakási přidaná hodnota (Marek, 2013, s. 8). Klíčovým pojmem je zde ještě čtvrtý pojem a tím je rozhodování. Rozhodování je spojení znalostí s dalšími informacemi. (Lukáš, Hrůza a Kný, 2008, s. 14) Zde je právě vidět důležitost informací, neboť nebylo by rozhodování bez informací a zároveň by nebylo znalostí, také potřebných pro rozhodování, bez informací. Rozhodování je jednou ze základních manažerských aktivit a jako takové, je postavené právě na informacích.

Samotné informace však ještě nejsou klíčem ke znalostem, což je jeden z přetrvávajících omylů, možná právě přiživující takový hlad po informacích současné společnosti. Pravděpodobně všichni by chtěli znalosti a zabývat se znalostním managementem, znalostní ekonomikou a domnívají se, že když seženou dostatečné množství informací, nabydou znalosti. Ale to je omyl, tak tomu není. Lze dodat k tomuto vhodný příklad původem od Milana Zeleného (Marek, 2013, s. 8), který zmiňuje dva kuchaře. Oba dostali shodné suroviny (data), přečetli si recept (informace) a jeden uvařil výborné jídlo, druhý nikoli. Tomu druhému totiž scházely znalosti. Samotné informace, v podobě přečtení kuchařky, totiž ke znalostem nevedou. Samotným účelem, dalo by se říci informací, jsou znalosti, kdy „informace jsou nutné, ale ne postačující“. Obdobně tak, co se týká vzdělávání, „účelem vzdělávání nejsou informace, ale znalosti“. V dnešní době jsou informace takřka všude, ale to co není, jsou právě znalosti. Proto je vzdělávání, dle Milana Zeleného, v moderním světě nadmíru důležité. A nejde o vzdělávání se informací (biflování z učebnic a příruček), ale vzdělávání se ve znalostech, tedy umění vymyslet, navrhnout, vyrobit a hlavně prodat nový výrobek či službu nebo myšlenku. (Marek, 2013, s. 8)

Pro kompletnost lze ještě doplnit, že obsahem informačních systémů jsou především data, oproti tomuto lidé většinou obsahují informace. Člověk těžko bude sdělovat pouze data,

většinou ví, proč je ví, tedy zná kontext, tedy zná informace, je obvykle zvědavý. Pokud tedy dojde k úniku z informačního systému, unikají obvykle data, oproti tomuto dojde-li k úniku přes lidský faktor, unikají zpravidla informace. Nicméně toto je již výrazné rozlišení a v praxi není potřeba takto přísně rozlišovat.

1.2.5 Aktiva

Pojem, se kterým se lze také setkat a se kterým bude místy dále operováno, je pojem aktiva. Jednotné číslo aktivum. Aktiva jsou dle Dobdy (1998, s. 13), Doucka (2011, s. 38), Jaška (2006, s. 10) a Požára (2005, s. 37) všechny hmotné a nehmotné statky, vše, co má pro majitele informačního systému hodnotu. Za jedny z nejcennějších se považují právě data a informace. Obzvláště cenná jsou ta aktiva, jejichž zneužití, ztráta nebo modifikace by organizaci samotné nebo navázaným subjektům způsobily určitou škodu. Ta jsou velmi významná a vyžadují adekvátní ochranu. Nicméně aktivy jsou i samotná výpočetní zařízení nebo pracovní postupy a další.

1.3 Bezpečnost

Bezpečnost je dnes mnohdy vnímána jako jakási notorieta (Mates a Smejkal, 2006, s. 64) – tedy něco, co všichni znají – ale je tomu tak opravdu? Chápou tvůrci a uživatelé pojem bezpečnosti stejně?

Samotných definic bezpečnosti je opět mnoho. Ivanka (2009, s. 15) uvádí definici bezpečnosti jako „ochranu života a zdraví osob, ochranu majetku všeho druhu před ztrátami vzniklými v důsledku nehody, krádeže, podvodu nebo plenění a zahrnující všechny aspekty prevence ztrát“. Nejvíce komplexní definici však podává zřejmě Lidinský (2008, s. 104), který uvádí, že „obecně bezpečnost definujeme jako souhrn opatření (administrativních, fyzických, personálních a opatření z oblasti informačních a komunikačních technologií), která mají zajistit bezpečnost informací. Bezpečnost informace pak charakterizujeme jako zajištění integrity, důvěrnosti a dostupnosti. V praxi to znamená, že informace zůstávají přístupné, správné, ucelené a původní“. Toto je pravděpodobně nejkomplexnější výklad pojmu bezpečnosti, zároveň zodpovídající pojem bezpečnosti informace a prvků, které musejí být zajištěny, aby mohla být informace či jiný subjekt považován za zabezpečený.

Někdejší spolupracovníci Požár (2005, s. 37) s Čandíkem (2004, s. 6) se shodují, že bezpečnost je „vlastnost nějakého prvku, který je na určité úrovni chráněn proti ztrátám nebo také stav ochrany na určité úrovni proti případným ztrátám“. Je potřeba ale také uznat,

že pod pojmem bezpečnosti si každý může představit něco jiného. Shodneme se však na tom, že bezpečnost znamená v nejobecnějším vnímání určitou míru jistoty, která snižuje pocit ohrožení (Jašek, 2006, s. 7).

Předmětem zabezpečení jsou tři hlavní skupiny: zdraví a život, majetek, informace a znalosti, což, jak bylo definováno dříve, jsou dnes také formy majetku.

Zažitým omylem bývá, že bezpečnost, datová a informační, je často chápána pouze jako pojem výlučně pro oblast informatiky. To je však výrazný omyl. Jak dodává Lidinský (2008, s. 98), toto je zcestné, neboť tam není „základ bezpečnosti". „Ten se," dle něj, „nachází uvnitř organizace", v podobě vlastních zaměstnanců a na toto dále navazuje zajištění vnější bezpečnosti. Uživatelé a obsluha se podílejí na 80 % chyb a úniků a informatika je pouze dílčí částí, zajišťující aspekty bezpečnosti, včetně datové a informační.

Je potřeba, jak uvádí Jašek (2006, s. 8), aby si subjekt mající zájem na zajištění bezpečnosti, odpověděl na několik základních otázek. Zda a co má být chráněno, před čím má být předmět ochrany chráněn, jakým způsobem a jakými prostředky má být ochrana prováděna. Jen takto je možné zajistit dostatečné nastavení bezpečnosti. Toto se týká bez výjimky i veřejné správy. V dalších kapitolách bude toto důkladně rozebíráno, především z aspektů vnějších okolností, které ovlivňují bezpečnost, zejména existence hrozeb a míry rizika, s jakou se hrozby mohou uskutečnit a také z aspektů vnitřních okolností, mezi které patří například ekonomické možnosti subjektu, realizovat nutná protiopatření a opatření k zajištění bezpečnosti.

Koch a Ondrák (2008, s. 158) ještě k problematice bezpečnosti dodávají, že „bezpečnost je proces, ne produkt". Za bezpečnost musí někdo odpovídat, obdobně tak za vyvážené nastavení odpovídajícího poměru mezi požadavky na bezpečnost a uživatelskou provozuschopnost. V neposlední řadě podtrhují, že bezpečnost *může být sice drahá*, ale škody ještě dražší.

Zde, u pojmu bezpečnosti, více než kde jinde, jak také zdůrazňuje Přibyl (2004, s. 219), platí, že bezpečnost celého systému je tak silná, jak silný je jeho nejslabší článek. Je proto podstatné postihnout všechny aspekty bezpečnosti, včetně personálního pohledu na zajištění bezpečnosti dat a informací a žádný detail nevynechat. Zároveň, není potřeba aplikovat žádná drahá řešení, leckdy jednoduchá opatření bývají nejefektivnější. Oproti tomuto, jak dodává Paleček (2006, s. 32), „bezpečnost v žádném případě nesmí trpět na úkor zisku" a i když nebudou vidět výsledky přijatých opatření bezprostředně, je potřeba mít na pamě-

ti, že, jak podtrhuje Paleček (2006, s. 31), „bezpečnost se vyplácí především z dlouhodobého hlediska“.

1.3.1 Informační bezpečnost

Informační bezpečnost je ve své podstatě rozšířením či podmnožinou základního vnímání pojmu bezpečnosti. Informační bezpečnost je obor zabývající se zabezpečením informací v počítačových technologiích, informačních systémech (Jašek, 2006, s. 9). Nicméně, jak dodává Lidinský (2008, s. 104) „ochrana informací je mnohem složitějším problémem než fyzická ochrana majetku“. Jde především o to, že informace jsou umístěny v informačním systému jako neviditelné a nehmatatelné objekty a tento systém, má také tak, například od domu nebo trezoru, určitý počet na první pohled ne zcela vždy viditelných přístupů. Tento systém může být dále napojen na další systémy a tyto na další, a možná i dále k internetu a to jen rozšiřuje počet potenciálních, oprávněných i neoprávněných uživatelů. Ti opět nemusejí být vždy spatřitelní a především, ne všichni musejí notně sdílet zájem na udržení bezpečnost systému svěřených dat. Nehledě na to, že do role zde vstupuje kromě jejich vůle, také jejich informační gramotnost.

Informační bezpečnost je nejen o vnějších nebezpečích, například klientech veřejné správy, ale i o vlastních zaměstnancích. Oboje vnější i vnitřní subjekty mohou narušit spolehlivost faktorů bezpečnosti nejen úmyslnými jednáními, ale i neúmyslným působením. Týká se to jiných osob i zmiňovaného vlastního personálu. Obě dvě strany jsou schopné způsobit svým jednáním „přímé i nepřímé ztráty“. (Laucký, 2004, s. 15) Informační bezpečnost, lze ji tedy chápat jako „zodpovědnost za ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace, prostřednictvím dostupných (technických, fyzických a organizačních opatření) opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti těchto dat“ (Jašek, Dolejšová a Rosman, 2007, s. 78; Jašek, 2006, s. 9) oproti všem rizikům, která hrozí.

Čandík (2004, s. 8) ještě dodává, že bezpečností rozumíme „takovou ochranu informací, systémů a služeb proti chybám, nehodám manipulaci a zneužití, která minimalizuje pravděpodobnost a účinek těchto skutečností“. Zde stojí za podtrhnutí, že tato definice o něco lépe vystihuje bezpečnostní působení ve smyslu nikoli jako odstraňování rizika, ale jeho minimalizace. Toto věrněji odpovídá postavení bezpečnosti, která je vždy o krok pozadu za riziky, proti kterým působí.

Cílem informační bezpečnosti je tedy bezpečný informační systém, který chrání data jemu svěřená ve všech jejich fázích a zároveň nikterak neomezuje výkon veřejné správy.

Podle Brabce (2001, s. 203) by se měla informační bezpečnost odehrávat v rovinách metodologické a koncepční, bezpečnostně organizační, která by měla zahrnovat prvky bezpečnosti režimové a technologické. Dále v rovině prosazování a uplatňování informační bezpečnosti, tedy uplatňování bezpečnostních postupů a opatření, dále v rovině bezpečnostních informačních auditů, což je složkou kontroly a v neposlední řadě také v rovině personální a v rovině technických řešení.

Mezi hlavní požadavky na bezpečnost patří: důvěrnost, či, řízení přístupu, integrita dat a autentizace (Rosman a Buřita, 2011, s. 191). Čandík (2004, s. 9) pojmenovává důvěrnost utajením a přidává dostupnost. Definici informační bezpečnosti lze nalézt i v zahraničním právu, například podle amerického práva, jak zmiňují Andress a Rogers (2011, s. 2) je informační bezpečnost definována jako ochrana informací a informačních systémů před neoprávněným přístupem, použitím, sdělováním, narušením, změnou a zničením. Definice bezpečnosti dle CIA, jak zmiňuje Čandík (2004, s. 6), uvádí na prvním místě především potřebu zajištění důvěrnosti informace. Důvěrnost je v chápání výše citovaného textu definována doslovně jako „vlastnost, kdy informace nemůže být odhalena nebo zneužita neautorizovanou osobou“. Setkáváme se tedy i mezinárodně s obdobným vnímáním těchto pojmů a pojmu informační bezpečnosti celkově.

Doucek (2011, s. 38) uvádí, že aby „organizace dosáhla udržitelného rozvoje, musí stanovit odpovědnost za bezpečnost informací jako samostatnou část řízení a nikoli jako součást jiných rolí“. Jen tak bude prý možno přisoudit řízení této problematiky dostatečné pravomoci, odpovědnost a zdroje k jejímu prosazování. A dodává (Doucek, 2011, s. 35), že je nedílnou součástí bezpečnosti organizace a připojuje vlastní definici, kdy uvádí, že „cílem a úkolem řízení bezpečnosti informací je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů – tedy nejen s informacemi v digitální podobě“. Ano, je tomu přesně tak a právě tato definice naráží na to, že informace v digitální podobě jsou dnes majoritní částí informační bezpečnosti. Ale nebývalo tomu tak vždy a jedná se spíše o fenomén posledních desetiletí. Ten postihuje i veřejnou správu, která prochází svým procesem digitalizace a již dnes spravuje výrazný objem digitálních dat, který bude i nadále do budoucna ještě více převažovat a růst. Doucek (2011, s. 38) toto ještě zpodrobňuje, kdy uvádí, že „informační bezpečnost v sobě zahrnuje podsložku bezpečnosti IS/ICT a také způsoby zpracování dat, jejich uložení a také správu archivů nedigitálních dat, dále

zásady skartace materiálů, nakládání s informacemi během jejich transportu na jiná místa, zásady pro poskytování informací novinářům a jiným subjektům“. Toto je pravděpodobně nejvíce komplexní definice systému informační bezpečnosti. Zmiňuje, že právě bezpečnost informačních systémů je tedy nejužším prvkem v informační bezpečnosti, která je podmnožinou bezpečnosti jako takové.

Je tedy podstatné, že nelze chápat informační bezpečnost jako pouze bezpečnost informačních systémů. Bezpečnost informačních systémů je součástí informační bezpečnosti, která dále zahrnuje například fyzické nebo právě personální aspekty bezpečnosti. A obdobně tak informační bezpečnost je součástí celkového bezpečnostního vnímání a jednání organizace, které se nezaobírá pouze informační bezpečností, ale celou bezpečnostní problematikou jako celkem.

A ač je informační bezpečnost, respektive její část bezpečnosti informačních systémů, zmiňována jen jako dílčí část, co se týká objemu a hodnoty spravovaných dat, jedná se o dozajista nejmohutnější prvek bezpečnosti, především s velmi výrazným trendem pro budoucí růst.

Informační bezpečnost je náročným tématem a oborem zajištění. Vyžaduje pozornost k detailu a kontinuální bdělost, neboť jde o stále se formující a vyvíjející proces (Tipton a Krause, 2007, s. 623), a k jejímu kvalitnímu řešení se vyžaduje trvalý zájem a nasazení a proto management organizace musí věnovat tomuto tématu neustálou pozornost (Požár, 2005, s. 72). To je významné i proto, protože jednou z významných vlastností bezpečnosti je její „časová závislost, kdy například bezpečnost v informačních technologiích v závislosti na čase klesá“ (Čandík, 2004, s. 8), neboť „některé důvěrné informace o systémových částech se stávají známými a můžou způsobit ohrožení bezpečnosti celého systému“ (Požár, 2005, s. 12).

Obdobně tak, dlouhodobým používáním každého systému se stávají známými a rozšířenými i jeho chyby a případné nedostatky. Problematika informační bezpečnosti je tak podle něj disciplína, která se velmi rychle rozvíjí a důsledné řízení bezpečnosti by mělo být součástí každého managementu organizace, ať již v podobě soukromého nebo veřejného podniku. Tak by tomu mělo být i v institucích veřejné správy.

1.3.2 Bezpečnost, její pojetí a personální bezpečnost

Požár (2005, s. 72) pojímá bezpečnost na tři oblasti. Informační bezpečnost, majetkovou bezpečnost a personální bezpečnost. Prvá jmenovaná je oblastí, ve které se jedná o bezpečnosti dat a informací v informačním systému při jejich zpracování. Druhá jmenovaná, někdy také nazývaná známějším pojmem fyzická bezpečnost, se zabývá především například neoprávněnými vstupy do budov, k zařízením. Třetí jmenovaná, personální bezpečnost, v té jde o vlastnosti, znalosti a dovednosti potenciálně rizikové pro bezpečnost. Právě o lidský faktor, personální stránku. O nositele informací je potřeba dbát stejně jako o samotné informace. Lidé jsou klíčovým faktorem a nosí v sobě kromě informací leckdy klíčové know how, znalosti. Jejich management je proto objektem řízení lidských zdrojů organizace a na stejné úrovni bezpečnosti by mělo být i zajištění personální bezpečnosti.

Samotná personální bezpečnost je podle Brabce (2001, s. 204, 249) „ochrana v rámci jednání a událostí způsobených pracovníky, a to především z pohledu prevence," a zabývá se primárně otázkou, aby se k informacím dostaly jen povolané a nerizikové osoby a tyto osoby v systému nezpůsobily škody. Vhodným dílčím nástrojem je pak školení, které pokrývá, pracuje na propojení personální bezpečnosti a bezpečnosti informačních systémů. Personální bezpečnost lze dále dle Doucka (2011, s. 140) vnímat jako synonymum bezpečnosti z hlediska lidských zdrojů, i když jak dodává, některé společnosti opouštějí pojem personální bezpečnost, neboť ten začíná být vnímán někdy pouze ve smyslu vnitřních zaměstnanců firmy, a nepostihuje tedy, že cílem bezpečnosti je ošetření i vnějších osob. Tedy z tohoto úhlu pohledu, se dle něj jeví vhodnější používat pojem bezpečnost z hlediska lidských zdrojů. Pro účely této práce, i vzhledem k respektování jiných autorů používajících spíše pojem personální bezpečnost a kteří takto nerozlišují, budou tyto pojmy vnímány jako synonyma. Nicméně je vhodné dodat, že i lze narazit na toto chápání a dále i na vnímání, kdy personální bezpečnost je namísto porozumění jako toho, co zaměstnanci mohou udělat pro ochranu organizace, chápána jako ochrana vlastních zaměstnanců. Pojetí může být tedy rozdílné a záleží na oboru, do kterého spadá.

Pro zájmy bezpečnosti dat a informací ve veřejné správě nejlépe pravděpodobně tuto problematiku definuje Ortmeier (2009, s. 120), který uvádí, že personální bezpečnost zahrnuje ochranu vlastních osob a ochranu před všemi, (tedy těmito i ostatními osobami), které mohou být potenciálními riziky pro jiné zaměstnance nebo hmotná či nehmotná aktiva. Dle Ortmeiera (2009, s. 120) je personální bezpečnosti nejlépe dosahováno především „dů-

raznou etickou orientací organizace a silným vedením, motivováním každého v organizaci“. Toto je klíčová teze, která bude později nosnou součástí praktické části této práce.

Dobda (1998, s. 97) doplňuje tuto problematiku tím, že uvádí, že ve spojitosti rizika a personálního zajištění fungování organizace je především kritické to, že lidské chování se nedá předem nastavit. Nelze s jistotou předvídat, co lidé udělají, jak se zachovají. Zaměstnanci, jejichž zájmy nejsou totožné se zájmy zaměstnavatele, představují vždy určité potenciální riziko. Personální bezpečnost je často opomíjena na úkor jiných složek bezpečnosti. Jsou dávány velké náklady na technická zabezpečení, ale na personální bezpečnost se mnohdy zapomíná. Přitom je všeobecně známo, že okolo tří čtvrtin případů narušení bezpečnosti provedli vlastní zaměstnanci, ať již z úmyslných nebo neúmyslných příčin. Personální problematice je tedy proto potřeba věnovat výraznou, minimálně však stejnou pozornost, jako jiným oblastem bezpečnosti.

1.4 Riziko

Při zhodnocování rizika je potřeba, dle Normana (2010, s. 162) vzít v potaz pravděpodobnost, zranitelnost, následky a dospějeme k celkovému risku, tedy riziku. Pokud se podaří riziko změřit, ocenit, jsme schopni daleko lépe vybrat odpovídající úroveň opatření k jeho minimalizaci (Paleček, 2006, s. 21).

Procházková (2007, s. 19) zmiňuje pojem přijatelnosti rizika, kdy uvádí, že přijatelné riziko je takové riziko, když ti, kteří jsou jím ovlivněni, si ho neuvědomují nebo jej vědomě podstupují. Zde s tímto tvrzením nelze až tak úplně souhlasit, neboť neuvědomování si rizika může plynout i z lajdáctví, nepozornosti a nikoli z jeho vědomého přijetí. Protiargumentační tvrzení jiných autorů budou zmíněna dále v této kapitole. Nejčastěji dosahujeme snížení rizika snížením zranitelnosti. Nejlepší metodou by bylo přímé odstranění hrozeb, které však není vždy reálné. Jednou z metod snížení ztrát v případě rizika je pojištění. Snižuje finanční škodu, ale nikterak nebrání proběhnutí samotné škodné události, například únikům dat. Data uniklá mohou ještě dlouhou dobu po úniku způsobovat ještě další škody. Dobda (1998, s. 17) považuje za projevy vzniku škody ztrátu integrity, zničení nebo změnu, respektive ztrátu dostupnosti, důvěrnosti či autentičnosti subjektu. Tedy v podstatě naplnění rizika a hrozeb.

Doucek (2011, s. 57) hluboce zabývající se tímto tématem dále k hrozbám dodává, že hrozba je „potenciální příčina nechtěného incidentu, jehož výsledkem může být poško-

zení systému nebo organizace. Hrozba je zneužitím zranitelnosti. Alternativní definice definuje hrozbu jako pravděpodobnost útoku odvozenou z atraktivity systému pro útočníka“. Dělí hrozby na přírodní (fyzické), technické (technologické) a lidské (personální). Poslední jmenované mohou být dále klasifikovány na neúmyslné (neznalostní a nedbalostní) a úmyslné, páchané zvenku či zevnitř. Doucek (2011, s. 58) dále doplňuje k problematice personálních rizik, že více než 50 % všech hrozeb, které poškodí informační systémy, jsou z kategorie právě neúmyslných hrozeb. Dodává (Doucek, 2011, s. 58), že ke zvyšování rizika přispívají všechny zranitelnosti, což jsou „slabá místa aktiv nebo opatření, kterých může být využito hrozbou. Slabá místa mohou vést k neautorizovaným přístupům se všemi následky“. Proti tomuto je potřeba přijímat opatření (Doucek, 2011, s. 59), což znamená snažit se řídit rizika včetně dostupných politik, postupů a směrnic nebo organizačních struktur, které mohou být různé povahy. Je tedy potřeba využít všech opatření, která umožňují snížit sílu hrozby, která na informační systém působí nebo může působit a pokusit se zabránit v jejím účinku. Hrozbami mohou být lidé, včetně vlastních zaměstnanců, dále přírodní jevy, záplavy, déšť, požáry a také technické poruchy (Jašek, 2006, s. 18).

K samotné definici Doucek (2011, s. 60) dodává, že riziko je „kombinace pravděpodobnosti události a jejího následku. Společné působení hrozeb působících na aktivum a zranitelnost tohoto aktiva či realizovaných opatření může mít za následek vznik škody na těchto aktivech, tedy má na aktivum určitý dopad, který lze definovat jako nepříznivou změnu dosaženého stupně cílů organizace“. Požár (2005, s. 37) oproti tomuto používá asi nejsrozumitelnější definici, kdy definuje riziko jako „pravděpodobnost, s jakou bude daná hodnota aktiva zničena nebo poškozena působením konkrétní hrozby, která působí na slabou stránku této hodnoty. Je to tedy míra ohrožení konkrétního aktiva“. Toto je, na základě výše uvedeného, zřejmě jedno z nejvhodnějších definování rizika pro potřeby této práce.

1.4.1 Bezpečnostní riziko

Bezpečnostní riziko je drobnou podmnožinou všeobecného rizika a Laucký (2004, s. 11) pojednává o bezpečnostním riziku jako o situaci v zájmovém objektu nebo u zájmové osoby, v jejímž důsledku může vzniknout krizová situace a to v příčinné souvislosti mezi jednáním a následkem. Bezpečnostní riziko lze dělit na bezprostřední, tedy okamžitě viditelné nebo následné či latentní, skryté. Všechny tyto druhy bezpečnostních rizik se týkají bezpečnosti dat a informací ve veřejné správě a jsou právě nebezpečné, neboť například na skryté riziko se nemusí po dlouhou dobu vůbec přijít a může tak přivodit značné škody.

Pro stanovení a ocenění bezpečnostních rizik je dle Lauckého (2004, s. 12) důležitá analýza vstupních poznatků o objektu nebo o osobě resp. chráněném zájmu. To je největší úkol bezpečnostního managementu a kroky k jeho stanovení jsou obdobné jako u obecného rizika. Ale jeho stanovení není snadné, jak dodává výše citovaný autor, neboť „identifikaci bezpečnostních rizik se lze, ale jen velmi těžko, naučit a je potřeba na ni mít spíše jakýsi bezpečnostní čich".

Požár (2005, s. 40) k otázce bezpečnostních rizik opět zmiňuje, že mohou být objektivní a subjektivní. Objektivní jsou rizika požáru, povodně, výpadku proudu, technická selhání aj. a za subjektivní považujeme například již zmíněná neúmyslná působení uživatelů, ale také úmyslné poškození útočníky působícími z vnějšího, ale i vnitřního, prostředí. Dle Požára (2005, s. 40) se odhaduje, že až 80 % útoků na IT je vedeno zevnitř, respektive z řad vlastních zaměstnanců. Bohužel se jeho komentář nezaobírá dalšími podrobnostmi a lze tedy těžko určit, jakému druhu organizace toto patří a zda se toto týká i veřejné správy.

1.4.2 Bezpečnostní politika

Z praktických a ekonomických hledisek není možné chránit všechna data důkladně a stejným způsobem a právě míru důležitosti jednotlivých prvků a závažnosti, se kterou by se měly tyto prvky chránit a jak by se tak mělo v rámci jednotlivých složek bezpečnosti činit, definuje bezpečnostní politika (Čandík, 2004, s. 11). Bezpečnostní politika organizace je dokument, který by měl být uvnitř organizace dobře přístupný, dokument který zahrnuje pravidla, normy a postupy, které je potřeba dodržovat, aby byla zajištěna důvěrnost ale také odpovídající dostupnost dat. Zahrnuje technické, fyzické, administrativní, personální, etické, ekologické, právní a sankční opatření (v rámci přístupu a použití informací.) Představuje soubor norem, pravidel a praktik definujících tvar a formát informací, jejich ochranu, distribuci citlivých informací a jiných aktiv informačního systému. (Čandík, 2004, s. 11, 12) Systém, který splňuje bezpečnostní politiku, nazýváme „důvěryhodný systém". A právě prosazení takovéhoto důvěryhodného či bezpečného systému je účelem bezpečnostní politiky. (Čandík, 2004, s. 12) Bezpečnostní politika si uvědomuje, že nejbezpečnější by byla absolutní izolovanost systému od okolí, včetně izolovanosti od uživatelů. Proto tedy jí stanovená pravidla by měla mít formu doporučených nebo nejlépe povinných zásad, které jsou určitým kompromisem mezi důkladným zabezpečením a uživatelskou použitelností systému.

Bezpečnostní politika definuje, co chceme chránit, proč to chceme chránit, jak to chceme chránit, jak bude ověřeno, zda je toto opravdu chráněno a jak se bude postupovat v případě incidentu (Doseděl, 2004, s. 168). Předmětem bezpečnostní politiky je to, co je potřeba chránit, rizikem a hrozbami je to, proti čemu je potřeba chránit a protiopatřeními je to, jak chráníme. Dále může být politika doplněna finanční částí, kdy se oceňují jednotlivá aktiva a hodnotí se finanční přijatelnost zajištění bezpečnosti. (Čandík, 2004, s. 13)

Je žádoucí, aby dokument bezpečnostní politiky byl stručný, srozumitelný, přehledný a zároveň úplný a řešil všechny možné otázky a konfliktní situace v rámci bezpečnosti dat a informací a zároveň však nesmí kompromitovat. Je tedy vidět rozpor mezi potřebou stručnosti a zároveň potřebou pokrytí všech možných bodů. V dokumentu nemusí být ale všechny body řešeny přímo, je možné používat odkazy na příslušné přílohy, normy ad., čímž lze dosáhnout požadované stručnosti. Čandík (2004, s. 12) také napřímo doporučuje, že je výhodné vytvářet bezpečnostní politiku právě jako „více na sebe hierarchicky provázaných dokumentů, které na své úrovni řeší vždy příslušné oblasti bezpečnosti“. Nejobecnější politika je určená vedení organizace a další dílčí části vždy dopodrobna rozpracovávají dílčí problematiky. Tím je možné dosáhnout již zmíněné stručnosti a doručení vždy jen potřebných informací a pokynů k požadovaným osobám. Cílovými osobami, na které by měl být kladen důraz, by měli být především řadoví zaměstnanci. (Čandík, 2004, s. 12)

Čandík (2004, s. 13) velmi dobře vystihuje princip budování bezpečnosti, kdy uvádí, že bezpečnostní politika se řídí dvěmi základními zásadami. Za prvé cena navrhovaných opatření musí být menší než předpokládaná hodnota ztráty v případě, že by došlo k bezpečnostnímu incidentu. Problémem je, pokud se tato cena nedá exaktně vyjádřit. Například u reputace toto může být těžké. Obdobně tak pokud se jedná o data občanů. Ve veřejné správě především měla by být snaha o ochranu vždy maximální. Nelze zde totiž vždy vyčíslit možnou škodu, vzhledem k charakteru dat spravovaných veřejnou správou. A za druhé, dané bezpečnostní opatření by mělo cenu případného útoku útočníka zvýšit nad jeho předpokládaný zisk v případě, že by uspěl (Čandík, 2004, s. 13). Tím se dosáhne změny v jeho poměru mezi výhodností a nevýhodností jeho skutku a dojde k jeho možnému odrazení od jeho uskutečnění. Zde je vidět, že v rámci bezpečnosti tedy není vždy cílem vytvořit absolutně neprostupný systém. To by leckdy bylo nemožné. Ale systém, do kterého by bylo neoprávněné proniknutí tak složité a pro útočníka nákladné, že se mu v porovnání s očekávaným ziskem nevyplatí. Ovšem, toto se dá těžko vyčíslit, pokud by například byla útočníkem státní rozvědka a chráněným zájmem by byla například státní tajemství.

Bezpečnostní politika může být dlouhodobého nebo krátkodobého charakteru (Jašek, 2006, s. 62) nicméně vždy, jak v kontrastu k tomuto doplňuje Doseděl (2004, s. 169), nikdy by neměla zůstat statickým dokumentem. Rizika se vyvíjejí v čase a i potřebné reakce na ně by se měly vyvíjet odpovídajícím tempem. Bezpečnostní politika by také měla mít garanta, který „zodpovídá za její údržbu, aktualizaci v souladu s pevně definovanými revizními procesy". (Mates a Smejkal, 2006, s. 97)

Podkladem bezpečnostní politiky je analýza rizik. Ta identifikuje, označuje a oceňuje aktiva a hrozby, rizika. Provádí tak spíše intuitivní metodou. (Doseděl, 2004, s. 170) Jejím výsledkem je vyjádření velikosti, míry rizika a jejich upřednostnění, které umožňuje se dále v bezpečnostní politice zaměřit na rizika, která jsou největší a nejzávažnější (Paleček, 2006, s. 44).

Při tvorbě politiky je možné se setkat s problémy, kterým je potřeba se vyhnout. Problémem může být velké množství kompromisů, kdy jsou velmi nekonkrétně nastavená pravidla, nebo i naopak, pravidla jsou velmi přísná a pro běžné fungování až nereálně nastavená, nemožná k dodržování. Dalším možným problémem je nekritické a slepé přebírání vzorců, zde částí nebo celých bezpečnostních politik od jiných institucí. Toto nemůže fungovat ani napříč veřejnou správou, neboť každá vlastní organizace je v detailu jiná, v jiných podmínkách. Na jednom místě funkční koncept nezaručí, že bude funkčním i v jiných podmínkách. Může existovat jakýsi centrální koncept, který usnadní budování vlastní politiky, ale její finální znění se musí vždy detailně naladit a přizpůsobit dle konkrétní organizace veřejné správy. V neposlední řadě, nesmí být podceněna „propagace a dostupnost" dokumentu bezpečnostní politiky v rámci organizace směrem k zaměstnancům, na které je cíleno, protože i jinak kvalitní politika by se tak minula efektem. (Jašek, 2006, s. 63)

Doseděl (2004, s. 169) v tomto smýšlení podporuje předchozího autora, kdy přímo uvádí, že bezpečnostní politika „by měla být vysvětlena celé organizaci, a to nejprve od vedení a posléze k zaměstnancům. Musí se s ní všichni dokonale ztotožnit a pochopit její účel a nutnost a také, proč se právě které věci provádějí takovým způsobem". Jak je vidět, toto je přímá návaznost na v předchozích kapitolách zmiňované potřeby, aby zaměstnanci chápali, že potřebují pochopit, proč které procesy fungují v jejich organizaci právě tak a takovým způsobem. Jen tak je možné efektivněji zajistit navýšení bezpečnosti dat a informací, nejen v orgánech veřejné správy. A právě navrhovaný model vzdělávání, představovaný později v praktické části této práce, vytváří k tomuto velmi vhodný prostor.

2 CHARAKTERISTIKA RIZIK SPOJENÝCH SE ZNEUŽITÍM DAT A INFORMACÍ VEŘEJNÉ SPRÁVY

2.1 Informační systémy, rizika a aspekty digitalizace ve veřejné správě

2.1.1 Informační systémy a veřejná správa

Přerod charakteru informačních systémů

Ještě před několika málo desítkami let, byla situace ochrany dat a informací naprosto odlišná. Data se skladovala převážně v písemné podobě, informační systémy měly charakteristiku papírových archivů. Výrazná změna přišla s rozvojem informačních technologií, kdy došlo k radikálnímu přetransformování klasických režimů skladování, přenosu a také i ochrany dat. Do té doby, dokud se množství údajů uchovávalo v papírových kartotékách, dalo se říci, že byla jejich bezpečnost daleko lépe pod kontrolou. Avšak jak výrazně stoupá rozšířenost digitálních informačních systémů, stoupají i rizika jejich zneužití a dat v nich uložených. Dochází k informačnímu boomu, kdy data mohou být neomezeně propojována z velmi odlehlých zdrojů a z těchto míst i přistupována. (Brabec, 2001, s. 209; Lidinský, 2008, s. 32) Toto je nové a v předchozích rozvojových vlnách lidské společnosti agrární a industriální společnosti, nemusel být kladen takový důraz na bezpečnost jako právě nyní, v době informační společnosti (Lukáš, Hrůza a Kný, 2008, s. 9). Dochází tedy již určitý čas k přerodu chápání informačních systémů a je potřeba k tomuto také tak upravit vnímání jejich bezpečnosti. Ta by měla být zpracovávána nejen právě dle charakteru daného informačního systému, ale především, dle jeho poslání a toho, k čemu slouží. Včetně služby ve veřejné správě.

Specifika veřejné správy

Veřejná správa ve vztahu k datům a informacím je specifická především svým obřím rozsahem jí spravovaných dat. Tento rozsah se dá srovnat pouze s několika soukromými subjekty celosvětové působnosti. Česká veřejná správa samozřejmě spravuje množství dat odpovídající její působnosti, nicméně podléhá všem společným charakteristikám moderních veřejných správ. Jedním z prvků, které ovlivňují charakter ochrany dat a informací je, že veřejná správa není založena na komerční bázi. Tedy úniky v případě špatného zabezpečení nepřichází sama o zisk, který bývá často kvalitním hnacím prvkem k zajištění bezpečnosti, ale může způsobit značné škody jiným subjektům, respektive České republice. Bezpečnost ve veřejné správě by měla být standardně vysoká, i přes to, že ji nelze exaktně vy-

číslit v kontrastu k rizikům, neboť, na rozdíl od většiny komerčních subjektů, veřejná správa nespravuje údaje svoje, ale právě o ostatních subjektech. A těchto subjektů je velmi velké množství. Velký objem citlivých dat se uchovává v systému základních registrů. Můžeme jmenovat Registr obyvatel MVČR, Registr právnických osob, podnikajících fyzických osob a orgánů veřejné moci ČSÚ, Registr územní identifikace, adres a nemovitostí ČÚZaK, Registr agend orgánů veřejné moci a další. Údaje, resp. výpisy z některých registrů jsou veřejně přístupné, některé přístupné přes kontaktní místa veřejné správy, některé jsou veřejnosti nepřístupné. Nicméně ale registry jsou stále jen částí objemu dat a informací, které veřejná správa spravuje. (Doucek, 2011, s. 201; Mates a Smejkal, 2012, s. 41) Veřejná správa spravuje také a především intranet veřejné správy. „Proniknutí do intranetu by nemělo přicházet v úvahu“. Obdobně tak, že informace budou posílány a sdíleny mezi organizacemi veřejné správy, namísto vnitřní intranetové sítě, veřejnými sítěmi. (Mates a Smejkal, 2006, s. 235)

Ochrana dat a informací ve veřejné správě je ve veřejném zájmu. Zvyšuje efektivnost prostředků vynaložených na fungování veřejné správy tím, že zamezuje ztrátám a tím i dalšímu navyšování nákladů a plně tak podporuje zásadu 3E. (Strecková, 2005, s. 9) Veřejná správa má, kromě svých zásad, dle kterých by měla fungovat, obdobně jako každá jiná organizace, také své určité cíle a tím i svoji cílovou funkci. Organizace státní správy a samosprávy plní úkoly v rámci své a přenesené působnosti a mezi její cílové funkce patří i správa věcí veřejných v oblasti bezpečnosti. Mělo by jít o zajištění plynulého fungování společnosti a minimalizaci rizik, která by mohla ohrozit plynulé fungování státu a způsobit jemu, nebo jeho občanů, kteří ho tvoří, újmu. (Lukáš, Hrůza a Kný, 2008, s. 12; Brabec, 2001, s. 12) Tedy důsledné zajištění bezpečnosti dat a informací naplňuje vlastní poslání státu.

Informační systémy a veřejná správa

Informační systémy jsou dnes tedy již nedílnou součástí výkonu veřejné správy a mají i své zákonné upravení v zákoně číslo 365/2000 Sb. o informačních systémech veřejné správy. Dle tohoto zákona se jako informační systém chápe „funkční celek nebo jeho část, zabezpečující cílevědomou a systematickou informační činnost. Každý informační systém zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností“. (Česko, 2000c) Existuje však i více vnímání obdobného a informační systém, to je například i dle jiného vnímání také „soubor prvků, které jsou spojeny vzájemnými vztahy, vazbami a operují s daty

a informacemi“ (Požár, 2005, s. 37). Jak bylo zmíněno, nemusí jít jen o digitální informační systémy, i když dnes se tak již stává takřka synonymem. Onen informační systém je „souborem lidí, (kteří jsou tvůrci, správci a uživatelé), technických prostředků a metod které zabezpečují, přenos, uchovávání a zpracování dat“ (Požár, 2005, s. 26). Z těchto definic je vidět, že informační systém nejsou jen pouhé výpočetní hmotné přístroje, ale také lidé a i metody, které jsou součástí informačního systému a měla by jim být věnována obdobná, a ne-li větší pozornost, jako technickým prostředkům.

Lidé tedy hrají podstatnou roli v informačním systému a procesech s ním spojených. A to nejen v rolích tvůrců, správců a uživatelů, ale také jako pachatelů, útočníků na informační systém. Informační systémy se stávají obětmi útoků různých osob z těchto skupin, s různými cíli.

Informační systém zároveň nebude nikdy naprosto bezpečným, neboť není nikdy naprosto izolovaným. Dokonale zabezpečeným systémem by byl takový systém, který by byl izolován od všech vnějších objektů, i od jeho uživatelů. Takový systém by byl ale nepoužitelný. Právě tedy tím, jak je informační systém umístěn v nějakém prostředí a navázán na nějaké uživatele, vždy existují nějaké hrozby a to, zda budou naplněny, záleží na daném prostředí a slabých místech systému. Cílem provozovatele informačního systému, v tomto případě veřejné správy, státu, není tyto hrozby odstraňovat, ale v maximální možné míře minimalizovat pravděpodobnost, s jakou dojde k jejich uskutečnění. A pokud by již došlo k jejich uskutečnění, tak minimalizovat potenciální škody, které způsobí. Jeho cílem je dosažení co nejvyššího stavu bezpečnosti systému a takovýto stav, nabízející minimální prostor pro úniky a možnosti zneužití dat, udržet po co nejdelší dobu. Proto tvorba školení uživatelů je nedílnou součástí bezpečnostní sféry informačního systému. (Čandík, 2004, s. 12; Doseděl, 2004, s. 169; Jašek, 2006, s. 9, 31)

2.1.2 eGovernment a aspekty digitalizace veřejné správy

eGovernment je vlastně transformací veřejné správy k její větší elektronizaci a tento trend jde ruku v ruce s probíhající informatizací společnosti. Hlavním důvodem zavádění eGovernmentu je úspora času a nákladů při poskytování služeb občanům a výkonu veřejné správy. Čas je šetřen na straně zaměstnanců veřejné správy, neboť je jim umožněno rychleji přistupovat k potřebným informacím a také urychlením komunikace, ať již mezi jednotlivými organizacemi či směrem k adresátům. Čas je šetřen ale i na straně občanů, klientů veřejné správy. Ti již nemusí ve všech případech trávit čas ve frontách, ale potřebné do-

kumenty mohou vyřídit elektronicky, z domova nebo kanceláře. Mohou takto učinit prakticky v neomezených úředních hodinách, dvacet čtyři hodin denně, jakýkoli den v týdnu. Obdobně tak, takřka nonstop, mohou občané přistupovat k určitým informačním systémům, například GIS národních parků, opět nonstop. To je jistě ušlechtilé, neboť tyto instituce jsou taktéž placené z veřejných zdrojů a je tedy vhodné, pokud produkty své práce dávají volně k nahlédnutí občanům. Zároveň, pokud chce občan do daného sytému nahlédnout, může tak učinit, aniž by tím jakkoli zatěžoval státního zaměstnance. Toto usnadnění přístupu občanů k informacím a tato dostupnost podporuje dostupnost a otevřenost veřejné správy ve vztahu k občanům. Dílčími úsporami je také úspora prostoru, který je ušetřen digitalizací vedených archivů a skladování dokumentů. Součástí eGovernmentu je i síť poboček Czech Point. (Jašek, Dolejšová a Rosman, 2007, s. 107; Louda, Grospič a Vostrá 2003, s. 192; Požár, 2005, s. 26)

Vlastní pojem eGovernment se do češtiny nepřekládá, zněl by toporně (Mates a Smejkal, 2012, s. 38). Vlastní úspora času, uspořeného při výhodách eGovernmentu, má výhody pro úřady a jejich zaměstnance i v rovině, že uspořený čas, který by jinak věnovali podpůrné administraci své práce, například rozesílání obálek, mohou namísto toho věnovat vlastnímu výkonu práce. Mates a Smejkal (2012, s. 41) dále zmiňují, že jednou z výhod je i možnost, rozšiřovat okruhy účastníků řízení, aniž by stoupaly náklady na řízení. S tímto nelze úplně souhlasit, neboť potenciální lacinost rozšiřování okruhů účastníků, nebo zasílání určitých druhů dotazů naslepo, které musejí být později někým, v nějakou pracovní dobu zodpovězeny, může zpětně i zatížit určité organizace a využití jejich zdrojů.

Dochází tak, právě díky jednoduchosti a lacinosti komunikace, až k situacím, kdy jsou někteří pracovníci a oddělení určitých institucí až zavalovány elektronickými žádostmi z jiných institucí o určité výkony a vzhledem k tomu, že některými výkony je veřejná správa povinna se zabývat, může výkon vyřizování těchto žádostí u nedostatečně personálně zabezpečených organizací až zmrazit jejich fungování.

V protikladu k výhodám digitalizace veřejné správy a zavádění eGovernmentu, má tento proces i svá výraznější negativa. Mezi ta patří právě zvýšená rizika napadení, úmyslná poškození systému či jeho i neúmyslného poškození. Toto všechno se děje díky provázanosti jednotlivých prvků systému a může být i obtížné vůbec zjistit, že k nějakému poškození nebo napadení došlo – či se tak může stát až po velké době. (Mates a Smejkal, 2006, s. 193)

Výhody ale převažují a proto je chvályhodné, že se česká veřejná správa tímto směrem vydala. Jak k tomuto dodává Mates a Smejkal (2012, s. 42), ono totiž mají-li adresáti veřejné moci lepší přístup k informacím, mohou tak i lépe kontrolovat výkon veřejnosprávních činností. Tím se dále podporuje hospodárnost s nakládáním s veřejným rozpočtem, laická kontrola a sledování korupce. Tím, že jsou určité dokumenty, například smlouvy, zápisy a rozhodnutí snadno dostupné, je podpořeno zdravé otevřené prostředí ve veřejné správě. A i tím, že ke čtení těchto dokumentů není potřeba navštěvovat úřad, ale je možno tak učinit z domova nebo kanceláře, určitě i stoupá množství lidí, kteří takto činí a veřejnosprávní laickou kontrolu provádějí.

Nicméně s rozšiřováním eGovernmentu se objevuje otázka takzvaných „občanů druhé kategorie“, či „občanů vyloučených“ či „uvězněných v digitální propasti“ (Mates a Smejkal, 2012, s. 44). Jedná se o občany, kteří digitální technologie neovládají nebo odmítají. Toto se může týkat v menší míře i zaměstnanců, kde jsou potřebné kompetence vyžadovány a osoby, které je absentují, jsou na trhu práce znevýhodněny. Ale především se jedná o problematiku adresátů veřejné správy. Obce se snaží proti tomuto bojovat poskytováním internetu zadarmo, nejrůznější instituce poskytováním potřebného vzdělání. Děje se tak v mottu zpřístupňování služeb veřejné správy. K diskusi je, nakolik je například právě poskytování veřejného internetu z veřejných peněz výhodné a ekonomické, neboť veřejné sítě wi-fi bývají místy nezabezpečené, tedy jen potenciálně více nebezpečné.

A otázkou také tedy zůstává, zda je, vzhledem k výše uvedenému reálné, a zda bylo by i správné, aby rozšiřování eGovernmentu dosáhlo absolutní penetrace.

2.1.3 Datové schránky

Digitalizaci veřejné správy stát prosazuje také tím, že povinně předepisuje zřízení a používání systému takzvaných datových schránek. Jejich využívání má naplňovat všechny předpoklady eGovernmentu. Jsou povinné pro komunikaci orgánů veřejné moci mezi sebou a dále pro komunikaci mezi orgány veřejné moci a právnickými nebo podnikajícími fyzickými osobami. Těmto subjektům se zřizuje datová schránka ze zákona a veřejná správa má povinnost s kýmkoli komunikovat za upřednostnění datové schránky, má-li ji. (Mates a Smejkal, 2012, s. 174) Datová schránka může být zřízena i na vlastní žádost fyzickým osobám. Datové schránky však nemusejí být používány pouze ke komunikaci s orgány veřejné moci, nýbrž mohou být používány i pro komunikaci mezi fyzickými nebo právnickými osobami navzájem. K 1. 11. 2012 bylo registrováno celkem 496 166 datových schrá-

nek a počet odeslaných datových zpráv byl celkem 103 511 571. (Mates a Smejkal, 2012, s. 167) K číslu o počtu registrovaných datových schránek je však třeba upozornit, že toto číslo neodráží skutečný počet osob, protože dle Matese a Smejkala (2012, s. 179) jedna osoba může mít teoreticky až 5 datových schránek, například pracuje-li jako advokát, daňový poradce, insolvenční správce, tlumočník a jednu může používat i jako občan.

2.1.4 Krizové řízení

Jedním rozhodně ne z posledních, ale důležitých ke zmínění aspektů, spojených s výkonem veřejné správy a potřeby ochrany dat a informací ve veřejné správě, je dozajista problematika spojená s krizovým řízením. Činnost veřejné správy v této oblasti můžeme brát jako součást aktivit směřujících k ochraně obyvatelstva. Informační bezpečnost je díky tomu součástí systému ochrany obyvatelstva. Úřady mají přístupy do kritické infrastruktury a informační systémy pro potřeby krizového řízení nenabízejí pouze přístupy k plánům a databázím, ale také platformy pro krizovou komunikaci. A je potřeba, aby nebyla narušena funkčnost této platformy, například skrz nedostatečné zabezpečení úřadu, neboť při nedostatečném zabezpečení by mohlo dojít k rizikovému selhání, například při krizových situacích, kdy by díky předchozím potížím obce, kraje ad. nemusela být dostupná například komunikace nebo narušená dostupnost plánů na této rovině. Dnes musí veřejná správa přiměřeně počítat také s pojmem terorismu. A právě získání dat může být cestou jednak ke konvenčnímu terorismu ale také i eventuální cestou k jeho finančnímu zajištění či maskování. (Fiala a Vilášek, 2010, s. 16, 103, 153; Navrátil, 2005, s. 51, 83)

2.2 Charakteristika rizik v informačních systémech veřejné správy

Jak již bylo důkladně rozebíráno, bezpečnost ve veřejné správě by měla být standardně vysoká, neboť, na rozdíl od většiny komerčních subjektů, veřejná správa nespravuje údaje jen své, ale především o ostatních subjektech. Těchto subjektů je velmi velké množství. Z tohoto plynou i možná rizika. Jedná se jednak o obecná rizika, uvedená v předchozích kapitolách, především v kapitolách pojednávajících o riziku a informačních systémech, ale pro oblast veřejné správy jsou některé aspekty ještě výraznější a specifičtější.

Všeobecná rizika jsou tedy taková a mohou mít takový dopad, jaký byl zmíněn v předchozích kapitolách. Charakteristika vlastních rizik, spojených se zneužitím dat a informací, se kterými operují orgány veřejné správy, je v základním smyslu nejvýraznější v následujících rovinách (Doseděl, 2004, s. 47; Jašek, Dolejšová a Rosman, 2007, s. 78):

Rizika spojená se zneužitím dat a informací související s jejich zničením.

Zde se jedná o znepřístupnění a možnou likvidaci určitých dat. Cílem může být maskování určitých skutečností, ale také prosté dokázání si možnosti takového aktu. Rizikem pro veřejnou správu je možná nenavratitelnost takto zneužitých dat a jejich absolutní ztráta. Ač se nejedná o zneužití, k obdobnému následku může dojít také při technickém selhání přístrojového vybavení, eventuálně také lidské chybě.

Rizika spojená se zneužitím dat a informací související s jejich změnou.

V tomto bodě je situace a riziko nejvýraznější. Může dojít k použití klamných dat, podstrčení určitých falešných hodnot nebo jejich záměně. A takto změněná data, nemusejí být po dlouhou dobu, ne-li vůbec, odhalena. V tom spočívá velmi výrazná rizikovost právě tohoto bodu zneužití. Dojde-li k zničení dat, obvykle se problém odhalí, neboť data chybí, ale v tomto případě je situace komplikovanější a rizikovější.

Rizika spojená se zneužitím dat a informací související s jejich kompromitací.

V tomto případě je situace obdobná jako u předchozího zmiňovaného bodu. Může dojít ke krádeži, kopii dat a tento akt může být odhalen až za dlouhou dobu, ne-li vůbec. Rozdíl spočívá v tom, že cílená data nejsou pozměněna, ale zcizena, zkopírována. Pokud jsou zcizená data následně použita, šance na odhalení takového činu se zvyšují.

K riziku a ohrožení samotného informačního systému Čandík (2004, s. 9) dodává, že může být realizováno „přerušením, ztrátou, nedostupností nebo nepoužitelností některé systémové části, dále sledováním, přístupem nepovolané nebo neautorizované osoby“. Většina rizik, která hrozí datům, při jejich uskladnění, například jejich výše zmíněná modifikace, zničení, hrozí datům „také v rámci jejich přenosu“ skrz jednotlivé prvky informačního systému (Požár, 2005, s. 175) z čehož vyplývají následné „přímé a nepřímé způsobené ztráty“ (Požár, 2005, s. 58).

Ty mohou v případě výše uvedených rizik spojených se zneužitím dat a informací zahrnovat ztráty způsobené (v případě kompromitace dat) vyzrazením záměrů, náklady potřebné k znovuzískání zničených dat (v případě zničení dat nebo jejich modifikace). Ztráty, způsobené zneužitím dat a informací nejsou jen materiálního charakteru ale i nehmotného, v podobě duševních hodnot. (Brabec, 2001, s. 219) Příkladem může být nefunkčnost informačního systému po nějakou dobu. Hmotnými škodami budou náklady, nutné k vynaložení na pracovní čas zaměstnanců, který bude potřeba k znovu obvolání a pozvání klientů,

jejichž požadavky nemohli být v důsledku nefunkčnosti systému vyřízeny nebo byly ztraceny. Nehmotnými škodami bude utrpění pověsti úřadu u těchto klientů. Konkrétně veřejnou správu toto nezasáhne tak výrazně jako soukromé subjekty, kde funguje aspekt konkurence, nicméně utrpí pověstí celá veřejná správa. Obzvláště bude-li případ medializován.

K problematice rizik spojených se zneužitím dat a informací souvisejících s jejich kompromitací Jašek (2006, s. 18) dodává, že toto je velmi obtížná situace, právě vzhledem k dokazování a zároveň, „provozovatel většinou nemá zájem na publicitě incidentu a tak dochází ke všeobecné představě, že k takovýmto únikům napříč společností nedochází a že ochrana informačních systémů a bezpečnost dat je vlastně zbytečným plýtváním peněz daňových poplatníků“. Většina incidentů možná i právě z takovýchto důvodů zůstává neodhalena, což může zpětně povzbuzovat v útočnících pocity vlastní síly a důvěry ve své schopnosti a podněcovat je v podnikání dalších útoků nejen na veřejnou infrastrukturu s různými cíli.

Mezi další rizika, spojená s poškozováním informačních systémů veřejné správy patří to, že soustavné napadání informačních systémů, získávání informací z nich a jejich neprovozuschopňování může způsobovat státnímu aparátu velmi vážné potíže ve výkonu jeho funkcí a vlastní správě státu. Toto může vést, z dlouhodobého nebo intenzivního hlediska, až k rozpadu fungování státu. Právě toto může být cílem určitých mezistátních operací, vedoucích až na pokraj kybernetické války. (Brabec, 2001, s. 210) Problematika průmyslové špionáže se nebude týkat v takové míře veřejné správy jako soukromých subjektů, nicméně právě informační válka může být velmi výrazným problémem nejen pro veřejnou správu, ale jak bylo uvedeno, pro celou jí spravovanou společnost (Laucký, 2009, s. 111).

Snahy o úsporu ve veřejné správě, mohou vést k různým krokům, mezi kterými mohou být i různé formy outsourcingu některých služeb ze soukromého sektoru pro veřejnou správu. Toto, při nedostatečném výběru partnerů a podpůrně také při nedostatečném právním ošetření ve smlouvách, může být momentem, ze kterého mohou také plynout určité hrozby. Není proto vždy účelné, snažit se dosahovat úspor za každou cenu, především v oblasti bezpečnosti, neboť právě takovéto konání může být zdrojem dalších a nových rizik pro veřejnou správu.

Je také potřeba zmínit, že pokud by veřejná správa umožnila, respektive dostatečně nezajistila bezpečnost proti úniku dat a informací ze svých systémů, a umožnila by například únik dat z obchodního partnerství, mohla by se stát právně žalovatelnou ze strany obchod-

ního partnera a musela by za toto pochybení nést všechny důsledky právního rozhodnutí soudu.

2.3 Právní podklady ochrany informací a vzdělávání v sektoru veřejné správy

Následující kapitola nabízí přehled právních zákonných i podzákonných úprav bezpečnostní problematiky v legislativě České republiky, jakožto právního základu pro výkon a zajišťování bezpečnostních činností ve veřejné správě. Jedním z klíčových zákonů upravujících použití informačních systémů ve veřejné správě je zákon číslo 365/2000 Sb. o informačních systémech veřejné správy a o změně některých dalších zákonů (Česko, 2000c). Ten definuje pojmy správce a provozovatel informačního systému, účel, k němuž bude informační systém sloužit, které informace bude evidovat a zpracovávat a jak budou tyto informace poskytovány. Dále zde je možné například dočíst, že určený správce je plně zodpovědný za informační systém, ale může pověřit i jiné subjekty provozem informačního systému veřejné správy (aniž by se však zbavil své vlastní odpovědnosti), pokud to nevylučuje jiný právní předpis. Zde se dostáváme k nové a důležité otázce z tohoto plynoucí, kterou je potenciální výhodnost a nevýhodnost ve vztahu k bezpečnosti dat a informací ve veřejné správě, spojená s možností outsourcingu některých služeb. (Jašek, Dolejšová a Rosman, 2007, s. 36) Tato otázka bude diskutována v pozdějších kapitolách.

Veřejná správa dále používá systém klasifikace a utajování některých informací, obzvláště těch, které jsou důležité pro fungování státu a na jejichž ochraně má stát zájem. Klíčovými předpisy jsou zákon číslo 148/1998 Sb. o ochraně utajovaných skutečností a o změně některých zákonů (Česko, 1998), kterým se mj. stanovují pravidla ochrany utajovaných skutečností a definují pojmy objektová, technická, administrativní a personální bezpečnost. Za naplňování tohoto zákona je primárně zodpovědný Národní bezpečnostní úřad. Zákon vychází ze dvou principů, kterými jsou 1) snažit se utajovat jen to nejnutnější, a to utajovat co nejkvalifikovaněji a 2) poskytovat utajovaná data jen těm osobám, které je nezbytně potřebují pro výkon svého povolání, které je v zájmu státu. Jedná se o to, aby přístup k informacím spadajícím do kategorie například T, měly jednak pouze osoby držící bezpečnostní prověrku na příslušný stupeň a zároveň ale skutečnost, že to, že osoba má oprávnění seznamovat se se skutečnostmi kategorie T by ještě nemělo znamenat, že by jí měly být přístupné všechny dokumenty takto klasifikované. Důležité je, jak bylo uvedeno, aby její seznámení s těmito skutečnostmi bylo v zájmu státu. (Požár, 2005, s. 264, 265,

267) Nedodržení této obecné v bodě dva uvedené zásady, například v případě americké armády a případu vojáka Manninga, bylo právě aspektem, který umožnil tomuto vojákovi přístup k rozsáhlému množství velmi citlivých dat a diplomatických depeší, které, ač je nepotřeboval ke své práci, měl ze svého vojenského počítače přístupné. Mohl si je tak zkopírovat, což také udělal a později předat správcům stránek Wikileaks. Opakování tohoto případu v prostředí české veřejné správy by bylo krajně nežádoucí.

Personální bezpečnost je kromě výše uvedeného zákona řešena také vyhláškou NBÚ č. 245/1998 Sb. o osobnostní způsobilosti a vzorech tiskopisů používaných v oblasti personální bezpečnosti (ve znění vyhlášky NBÚ č. 397/2000 Sb.). Ta představuje systém opatření s cílem především naplnit bod dva z předchozího odstavce. (Ivanka, 2009b, s. 79) Dále je možné zmínit zákon číslo 412/2005 Sb. o ochraně utajovaných informací a o bezpečnostní způsobilosti, na něj navazující nařízení vlády č. 522/2005 Sb. kterým se stanoví seznam utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.

Problematika bezpečnosti je v zákonech na mnoha místech upravována, avšak je také potřeba vzít v potaz, že tato legislativa, právě tak aby se adaptovala proměnlivému prostředí, se velmi rychle mění a je tedy možné, že zde uvedené informace velmi rychle zastarají a ukáží se jako neplatné. Například zmiňovaný zákon číslo 412/2005 Sb. je právě projednávaný v rámci jeho možné aktualizace. Pro význam této práce má především význam první zmiňovaný zákon.

Příslušný informační systém veřejné správy by měl být, obdobně jako osoby, certifikován NBÚ pro použití s klasifikovanými daty. Bezpečnostní prověření může získat i právnická osoba za splnění určitých podmínek. Nicméně, i sebelepší prověrky nemohou vyloučit selhání právě lidského faktoru. (Lidinský, 2008, s. 98, 100) Pro účely zpracování a uložení utajovaných informací jsou digitální informační systémy, oproti listinným podobám jejich uchovávání, určitě velmi výhodné, nicméně zde především je důležité dodržovat zmíněné pravidlo a snahu o co nejkvalitnější oddělení a zabezpečení systému oproti prostředí.

V soukromoprávní sféře práva se utajováním informací zabývá zákon číslo 513/1991 Sb. obchodní zákoník (Česko, 1991), který se zabývá problematikou ochrany dat a informací v podobě obchodního tajemství, které v § 17–20 definuje a v § 51 rozebírá jeho porušení. Respektive také § 504 zákona č. 89/2012 Sb. občanský zákoník (Česko, 2012).

České právo zná také zákon číslo 227/2000 Sb. o elektronickém podpisu a změně některých dalších zákonů (zákon o elektronickém podpisu) (Česko, 2000b). Tento předpis defi-

nuje zaručený elektronický podpis a další pojmy, jako jsou certifikáty a jejich poskytovatele, nejen pro potřeby veřejné správy. Stanovuje také požadavky pro elektronický podpis, mezi kterými jsou kupříkladu jednoznačná identifikace autora zprávy nebo možnost zjištění následných úprav zprávy. (Jašek, Dolejšová a Rosman, 2007, s. 88, 93)

Zákon číslo 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů (Česko, 2000) se dotýká soukromých i veřejných organizací a nehledí na podobu, v jaké je informační systém a v něm uchovávané údaje, veden. Jeho cílem je ochrana údajů označených jako citlivé (definuje je) a pokud informační systém spravuje takovéto údaje, musí mít registrovaného správce. Správce je odpovědný za systém a měl by být registrovaný u Úřadu pro ochranu osobních údajů. (Jašek, Dolejšová a Rosman, 2007, s. 92)

K zajištění ochrany osobních údajů před jejich zneužitím patří i povinnost mlčenlivosti. Ta se týká všech osob přicházejících s těmito daty do styku a povinnost mlčenlivosti nepokrývá jen data samotná, ale také i bezpečnostní opatření, jejichž prozrazením by byla ohrožena bezpečnost osobních údajů. Povinnost mlčenlivosti trvá i po skončení pracovního poměru nejen ve veřejné správě. Vlastní úprava mlčenlivosti je v zákonech upravena značně nejednotně a mnohdy velice komplikovaně. Je to možná způsobeno potřebou jednak údaje dobře ochránit, ale v kontrastu s tímto zároveň i vyhovět požadavkům, aby se nebylo možno přehnaně na tuto povinnost vymlouvat a v potřebných případech byly určité údaje poskytnuty. (Mates a Smejkal, 2006, s. 90)

Kromě právních úprav existuje také velké množství norem a best practices upravujících nejrůznější roviny bezpečnosti. Existují normy a koncepce řízení informačních technologií, které jsou více detailní, ITIL, více komplexní, COBIT nebo celá série ISO/IEC 27000. Nicméně tyto normy a best practices nejsou závazné ani nikterak vynutitelné, avšak nabízejí vhodná doporučení, návody a best practices a svým uživatelům mohou přinést hodnotné informace. Také, pokud se instituce nechají certifikovat dle zvolené například normy, dávají tím svým obchodním partnerům nebo klientům signál důvěryhodnosti organizace v dané problematice.

Samotné vzdělávání úředníků územních samosprávných celků, se řídí zákonem č. 312/2002 Sb. o úřednících územních samosprávných celků a o změně některých zákonů. Ten stanoví, povinnost úředníků se vzdělávat a konkrétně jmenuje jejich povinnost účastnit se vstupních a průběžných vzdělávání, přípravě a ověření zvláštní odborné způsobilosti. (Česko, 2002) Zajímavostí je, že u vstupních a průběžných školení je povinnost pouze

se účastnit, ale nepočítá se nikterak s ověřováním nabytých vědomostí, ale jinak je tomu u odborné způsobilosti, kde je již přímo jmenovaná povinnost účastnit se i na jejím ověření. Nicméně tyto povinnost nespecifikují náplň školení, která je jen z menší části bezpečnostní. Povinnost vzdělávání zaměstnanců je důležitá i z hlediska počtu osob, kterých se bezprostředně týká. Jedná se zhruba o „70 000 osob, z toho například starostové a jejich první zástupci dosahují čísla 13 000“. (Strecková, 2005, s. 75–83) Je potřeba k tomuto připomenout, že jedná se pouze o zaměstnance ÚSC, tedy nikoli plný rozsah veřejných zaměstnanců. Těch má státní správa celkem okolo 160 000, opět jedná se o hodnotu bez ostatních organizačních složek státu a příspěvkových organizací (MVČR, 2011, s. 8). Již na tomto základním počtu je vidět relativně vysoké množství zaměstnanců veřejné správy. Informace, které, ač sice ne všichni zaměstnanci, ale veřejná správa jako celek spravuje, mají nemalou hodnotu a potenciálně každý z těchto zaměstnanců, ač nemusí mít přímý přístup, může být rizikovým místem. Je proto potřeba důsledně zajistit na všech rovinách, kvalitní informovanost o možných rizicích spojených se zneužitím dat a informací a také ukázat, jak těmto rizikům předcházet. Vytvoření takovéhoto realizovatelného záměru pro veřejnou správu bude vyústěním této práce a bude nastíněno v praktické části této práce.

2.3.1 Je právní ošetření informační bezpečnosti nejen v sektoru veřejné správy dostatečné?

Identifikace zdrojů nebezpeční pro sektor veřejné správy je lehce komplikovanější. Ač zákon o informačních systémech veřejné správy zmiňuje a klade za povinnost provozovateli zajišťovat ochranu a bezpečnost informací a zajišťovat jejich důvěrnost, integritu a dostupnost, tak je potřeba počítat s tím, že nejen neznámý pachatel, ale i klient ba i samotný zaměstnanec úřadu, může mít zájem na zkopírování, smazání, změně určitých dat. Ale nejen klient, může jím být například i bývalý úředník, externí zaměstnanec, návštěva, kdokoli a jeho vazba na danou instituci ještě nemusí definovat profesionalitu, s jakou tak provede. Ona i osoba, instruovaná bývalým úředníkem, znalým prostředí, poměrů a opatření, bude schopná během velmi krátkého časového úseku, bude-li dostatečně instruovaná, vykonat pro ni zájmové úkony. (Paleček, 2006, s. 42; Černý, 2003, s. 99) A obdobně tak, jak není zřejmé, kdo by mohl být potenciálním pachatelem ve vztahu k úřadu, obdobně tak pro škody způsobené v informačním systému, daná osoba „nemusí být vůbec znalcem pro oblast informatiky“ (Jašek, 2006, s. 43). Potenciálním pachatelem je vždy nejen cizí osoba, ale tak i vlastní zaměstnanec, což vždy velmi rozšiřuje okruh rizik.

Ochranu dat je možné vnímat z hlediska právního výkladu i v rovině nejen veřejnoprávní, ale i trestněprávní (trestné činy u fyzických a právnických osob a přestupky u fyzických osob), například šíření informací vyvolávajících paniku a i v některých případech soukromoprávní (porušení autorského zákona). O ten se jedná při porušení autorských práv. V prostředí informačních systémů je značná variabilita jednání. (Mates a Smejkal, 2006, s. 64, 69, 74) A ač se tento výčet může zdát jako rozsáhlý, Mates a Smejkal (2006, s. 75) konstatují, že „veřejnosprávní ochrana informací je v rámci ČR nedostatečná“. Přispívá k tomu jednak i obtížné vyčíslení škod, které je pro právní kvalifikování některých jednání zásadní. Dále k tomuto na jiném místě jejich publikace dodávají (Mates a Smejkal, 2006, s. 56), že především „chybí výraznější nebo jasnější předpisy, které by postihovaly správce informačních systémů, například pokutami, za nedodržování předpisů“. Je to jasné tvrzení, nicméně opět vrací k otázce, podle čeho definovat onu navrhovanou pokutu, pokud, jak bylo uvedeno, je obtížné vyčíslení napáchaných škod?

2.4 Současné trendy bezpečnosti informací v personální rovině

Zaměstnanci si ponechávají firemní data a nevidí v tom nic špatného. Tak zní závěrečná tisková zpráva průzkumu, který upozorňuje, ve spojitosti s důvěrnými údaji, jak potřebné je vzdělávání. Doporučuji prostudovat tiskovou zprávu k závěrům tohoto výzkumu. (Symantec, 2013) Kromě mnohých omylů, spojených s vnímáním duševního vlastnictví a důvěrných údajů, zpráva také zmiňuje, že „organizacím se nedaří vytvořit kulturu bezpečnosti. Pouze 38 % zaměstnanců tvrdí, že jejich manažer považuje ochranu dat za obchodní prioritu, 51 % si myslí, že je přijatelné vzít si firemní data, protože jejich společnost neprosazuje striktní bezpečnostní politiky“. Právě touto prací navrhované vzdělávání zaměstnanců je řazeno jako nejvýraznější doporučení k nápravě uvedených nedostatků a zajištění vyšší bezpečnosti dat a informací. Obdobných výsledků dosahují i jiné výzkumy, kdy například společnost Microsoft ve své globální studii bezpečnostní gramotnosti poukazuje na potřebu zlepšení bezpečnostních návyků uživatelů a také na zajímavé hodnoty, že například polovina respondentů se setkala s určitým druhem rizika v digitálním prostředí, ale jen necelá třetina plánuje zrealizovat určité kroky k ochraně svých dat a pouze 38 % uživatelů se proaktivně zajímá o nové trendy ochrany osobních údajů. (CNews 2013; Microsoft, 2013)

Dle Průzkumu stavu informační bezpečnosti v České republice (DSM, 2009), dělaného každý lichý rok za spolupráce soukromé společnosti E&Y, časopisu Data Security Ma-

nagement a Národního bezpečnostního úřadu, naprostá většina dotázaných osob řadí problematiku bezpečnosti informací pouze a jen do úseku informatiky. To je již z podstaty špatně.

Tipton a Krause (2007, s. 557) ve své knize komentují, že pro některé osoby může být *zavádějící právě samotný název*, informační bezpečnost. Jakmile vnímají slovo bezpečnost, mají pocit, že o tuto oblast by se mělo starat bezpečnostní oddělení, ostraha instituce nebo právě oddělení informatiky. Že jich, vlastních řadových zaměstnanců, se tato problematika netýká.

Tento průzkum probíhá každý lichý rok a jeho účastníky jsou organizace s více než 100 zaměstnanci, kterých bylo v roce 2009 280. Účastníky jsou také organizace veřejné správy, které tvoří na výsledném počtu respondentů výrazných 24 %. Právě tento průzkum dle mnoha vyjádření představuje poměrně dobrý odraz reality, samozřejmě s výjimkou malých a středních podniků.

Z průzkumu (E&Y, NBÚ a DSM, 2009), včetně jeho odborných komentářů (Doucek, 2011, s. 231, 233, 238) vyplývají zajímavá fakta:

77 % organizací monitoruje aktivity svých zaměstnanců na internetu. Otázkou v tomto bodě je, zda jsou tyto aktivity správné, zda opravdu přispívají k větší bezpečnosti a zda tento monitoring má přímý, respektive výrazný vztah k bezpečnosti dat a informací? Nejedná se pouze o nástroj monitorování zaměstnanců s cílem navýšení jejich pracovní kázně a vyzískání motivu k postihu? Protože monitoring může mít i negativní dopady, ze strany zaměstnanců v podobě pocitů permanentní kontroly, nedůvěry ze strany zaměstnavatele. Naopak, určité volno v práci je schopné podpořit kreativitu a další následnou rychlost vykonávané práce.

Převážná většina společností upravuje své bezpečnostní standardy a normy, včetně úprav bezpečnostní politiky, až na základě známých problémů a dle trendů v oblasti informační techniky pouze 14 %. Toto je velmi výrazný prosto pro zlepšení. Kvalitnější sledování trendů umožní lépe reagovat a především predikovat a předcházet potížím. Reagování na známé je určitě správné, ale sledování trendů je neméně důležité, přínosné a úsporné.

Průzkum zodpovídal i otázku, co brání nebo jaké jsou překážky, prosazování a většímu rozšiřování bezpečnosti informací v ČR? Jeden z nejvýznamnějších důvodů zaujímajících plných 39 % odpovědí: Obecně nízké bezpečnostní povědomí.

Funkční program pro zvyšování bezpečnostního povědomí má pouze 21 % dotazovaných organizací. A přitom, zvýšení bezpečnostního povědomí představuje největší potenciál pro snížení nákladů v bezpečnosti informací (ve střednědobém horizontu) a tím podporu zásad 3E pro výkon veřejné správy.

Tato testování jsou pořádána již delší dobu a zajímavé je, že v meziročním srovnání let 2007 (E&Y, NBÚ a DSM, 2007) a 2009 je pohyb u bodu 3 pouze o jednotky procenta a stále se drží okolo podprůměrných 39 %. To rozhodně nekopíruje nárůst důležitostí informačních systémů a jejich penetrace společností a mělo by to být bráno jako maximálně alarmující. Mezi dalšími faktory uváděnými jako bránící kvalitnějšímu rozšiřování bezpečnosti informací jsou uváděny finanční náročnost 24 % (ve vzestupném trendu), nedostatečná podpora ze strany vedení organizace a také nedostatečná a nevyvážená legislativa v ČR s 14 % respektive 12 %, oba sestupný trend v řádech jednotek procent. Žádná z dalších odpovědí nepřesáhla hladinu 3 %.

Co z uvedených fakt ve stručnosti vyplývá? Z bodu 3 vyplývá nutná potřeba uceleného konceptu vzdělávání. Z bodu 2 vyplývá, že velkou výhodou by byl nástroj, pro šíření a koordinování šíření informací o známých problémech a nadcházejících trendech napříč organizacemi veřejné správy. Právě přístup k posílení těchto slabých míst bezpečnosti dat a informací, za pomoci personálního vzdělávání jako nástroje k navyšování a udržování bezpečnosti dat a informací ve veřejné správě, bude součástí toho, co nabídne tato práce v její praktické části.

Předcházející teoretická část práce nabídla významné teoretické zázemí k řešenému tématu a připravila důkladné podklady, z nichž bude vycházet následující analytická část. Následující analytická část bude na teoretických podkladech z předchozích kapitol zhodnocovat reálná a nejvýznamnější rizika pro veřejnou správu.

II. PRAKTICKÁ ČÁST

3 ZHODNOCENÍ REÁLNÝCH A NEJVÝZNAMNĚJŠÍCH RIZIK PRO VEŘEJNOU SPRÁVU

3.1 Reálná a nejvýznamnější rizika

Zhodnocování reálných a nejvýznamnějších rizik staví na důkladných podkladech teoretické části této práce a vymezuje největší rizika pro bezpečnost dat a informací v sektoru veřejné správy. Jedná se, a to nejen v tomto sektoru, především o body, ve kterých hrají určitou roli lidé a personální stránka bezpečnosti.

V rovině stanoveného zájmu této práce bylo definováno pět základních problematických rizikových okruhů:

[R1] Problematika autentizace a autorizace

[R2] Zpravodajská sociotechnika

[R3] Používání komerčních produktů placených z reklamy

[R4] Problematika práce z domova

[R5] Mobilně-lokalizační služby

3.1.1 [R1] Problematika autentizace a autorizace

Je potřeba zajistit jednoznačnou autentizaci a autorizaci uživatele (Přibyl, 2004, s. 9). Je potřeba uživatele naučit a přimět dodržovat, nesdělovat, nepůjčovat svá autentizační data a předměty jiným osobám. A tato data a předměty uchovávat na bezpečných místech. Jen tak bude zajištěna odpovídající autorizace osob, přicházejících do styku s daty a informacemi veřejné správy.

Autentizace, někdy uváděná i jako identifikace, je v podstatě ověřování identity. Že „je opravdu tím, za koho se vydává“. (Čandík, 2004, s. 9) Jedná se o porovnání určitých hodnot s jinými určitými hodnotami. Obvykle hodnot, které poskytne subjekt, jež požaduje autentizaci s referenčními hodnotami, obvykle z databáze referenčních hodnot. Na základě proběhnutí autentizace je přidělena nebo odmítnuta odpovídající autorizace přístupu a oprávnění. Autentizace může mít dva rozměry. Jednak autentizace uživatele, to je problematika, kterou diskutuje tato kapitola a jednak autentizace dat nebo dokumentů, například jejich původu, celistvosti. Obojí může zajišťovat například elektronický podpis.

(Čandík, 2004, s. 10; Mates a Smejkal, 2012, s. 283) Provádět autentizaci mohou lidské (vrátnice, výdejna) nebo informační systémy (čtečka, turniket).

Autentizace osob může probíhat (Doseděl, 2004, s. 56–58, 68; Tipton a Krause, 2007, s. 1302):

A) Důkazem znalostí – tím, co znáš – (heslo, PIN). Nevýhodou je, že uživatelé mohou heslo, PIN snadno předat, sdělit, může být okopírováno. Problémem je zde potřeba dané heslo si pamatovat. To klade nároky na paměťové schopnosti uživatelů, především vzhledem k tomu, že heslo není vhodné kamkoli zapisovat a také je vhodné jej po určitém období změnit. Dále by mělo být přiměřeně složité a tyto požadavky ztěžují zapamatovatelnost hesla. Výhodou této metody je, že není potřeba se starat o jakýkoli předmět a ochraňovat jej před ztrátou.

B) Důkaz vlastnictvím – tím, co máš – (bezpečnostní předmět, karta, čip). Problémem může být nutnost nošení daného předmětu a jeho opatrování. Dále také možnosti jeho odcizení, falšování. Výhodou je personalizovatelnost předmětů, jako identifikační karty s fotografií, nebo občanský průkaz. Výhodou je také nenáročnost na paměťové schopnosti uživatele a možnost prostým odebráním identifikačního předmětu odebrat přístup dané osobě. Není zde potřeba přenastavovat bezpečnostní systém, jako v případě odebírání hesla.

C) Důkaz vlastností – tím, co jsi nebo jakou máš fyzickou vlastnost – (sítnice, hlas, otisk kůže). Jedná se o autentizaci pomocí biometrických parametrů. Je vhodné zvolit takový prvek, který se nemění, respektive mění až v dlouhodobém období a vynechat prvky, jež se mění například podle nálady (hlas aj.). Při správném použití je tato metoda schopná zajistit vysokou spolehlivost. Kontrolován je přímo uživatel požadující autorizaci, nikoli předmět nebo znalost. Výhodou je, že identifikační údaje si nemusí osoby nikterak pamatovat ani je nosit při sobě. Nevýhodou může být proměnnost určitých prvků lidského těla v průběhu období, nemoci, stresu aj., které mohou ztěžovat úspěšnou autorizaci a použití systému.

D) Něčím, co uděláš (podepsáním se). Jedná se o relativně nově rozvíjené možnosti autentizace pomocí použití tzv. dynamického biometrického podpisu či biomechanického podpisu. Jedná se o podepsání se na čtecím zařízení, které sleduje průběh podepisování se. Jsou zde určité rozdíly, neboť při kontrole pouze výsledného podpisu, podpis se dá snadno naučit, nicméně naučit se dynamiku podpisu je obtížnější. Mezi nevýhody patří relativní složitost oproti předchozím bodům a pomalejší odbavování tohoto procesu. Někdy bývá tato metoda řazena spíše jako varianta předchozího bodu.

Každá metoda autentizace má své výhody ale i nevýhody. Jeví se proto jako nejvhodnější, kombinace několika metod zároveň, které navzájem odstraňují svoje nedostatky. Vhodná a zároveň uživatelsky přívětivá může být kombinace vlastnictví se znalostí (při zcizení karty chybí heslo). Samotné heslo, vzhledem k použití společně s kartou, může být jednodušší a ne tak náročné na zapamatování. Tato metoda je používaná například na bankovních kartách. Výhodná může být také kombinace kontrolních mechanismů, v podobě například biometrické kontroly sítnice, která probíhá automatizovaným systémem, ale tento systém je zároveň umístěn u stanoviště fyzické kontroly, například vrátnice, kde ostraha sleduje, zda není se systémem jakkoli manipulováno nebo není podváděn. Mechanismus autentizace a nastavené postupy mohou být dokonalé, ale pokud je lidé z nějakého důvodu nevyužívají nebo obcházejí, porušují nebo nedodržují jeho pravidla, bude i kvalitní zabezpečení snadné obejít. (Doseděl, 2004, s. 57)

Rizikem v tomto bodě a v rovině této práce, je neoprávněné sdílení autentizačních objektů a vlastností a také jejich nedostatečné zabezpečení proti neoprávněnému použití.

Opatřením je odpovídající vzdělávání uživatelů, které dostatečně vysvětluje potřebu zajištění kvalifikované autentizace a důležitost řádné správy autentizačních prvků. Vzdělávání, jednak úvodní a především průběžné, které zajistí dodržování potřebných pravidel.

3.1.2 [R2] Zpravodajská sociotechnika

Zpravodajská sociotechnika neboli sociální inženýrství, je „postup, taktika či metoda umění klamu, manipulace, ovlivňování a lsti s využitím znalostí a praktik psychologie, pedagogiky a sociologie“ (Brabec, 2009, s. 43). Cílem je jakákoli činnost v zájmu a dle scénáře pachatele. To, co dělá sociotechniku tak silnou metodou a sociotechniky tak nebezpečnými protivníky, je jednak jejich potenciální nenápadnost, kdy mohou dosáhnout svého cíle, aniž by si toho organizace byla vědoma a také metody a prostředky, často velmi nenápadné, za pomoci které svých cílů dosahují. Šikovný sociotechnik nebude komunikaci ukončovat okamžitě, jakmile se dověděl pro něj potřebnou informaci. (Brabec, 2009, s. 55) V neposlední řadě, to co dělá sociotechnické metody nebezpečné, je právě to, že se zaměřují na lidský faktor v cílové organizaci. A toto je právě stránka, která bývá často v organizacích podceňována.

Zde stojí za doporučení, přečíst si knihu od Kevina Mitnicka Umění klamu (Mitnick, 2003). Mitnick, sám bývalý úspěšný sociotechnik, ve své knize založené na skutečných scénářích, ilustruje a podtrhuje možnosti a rizika používání sociotechnik v nekvalitně per-

sonálně zajištěných institucích. Názorně ilustruje, že k dosažení informačních cílů leckdy není potřeba zdlouhavě překonávat technická a softwarová zabezpečení, ale za využití metod sociotechniky lze, jinak relativně dobře střežené informace, získat relativně snadno právě přes lidský faktor. Dokazuje, jak může být omylná představa zajištění dostatečné bezpečnosti dat jen za pomoci technických prostředků a že může být velice a o mnoho snazší tyto systémy obejít a dosáhnout svého cíle za použití zaměstnanců, kteří je například obsluhují.

Tipton a Krause (2007, s. 556) zvýrazňují, že to, co dělá sociální inženýrství tak úspěšné a nebezpečné, je především to, že lidé mají tendence být nápomocní. Jejich nápomocnost ještě umocňují momenty, kdy pachatel, respektive z jejich pohledu žadatel, vystupuje uctivě a působí, že pomoc opravdu potřebuje, že se bez ní neobejde, že je ztracen a bezmocný. Toho se snaží sociotechnika využít.

Brabec (2009, s. 48) k tomuto definuje šest základních, z nichž čtyři nejvýraznější zmíníme, vlastností lidské psychiky, které mají vztah k procesu aplikace sociotechniky a mohou tak přispět k úspěchu nebo neúspěchu těchto rizikových aktivit.

Autorita – kdy lidé mají tendence podřizovat se vůli mocné osoby. Toto je zesíleno u nových zaměstnanců, kteří se snaží včlenit do kolektivu a tento kolektiv také ještě dostatečně neznají. Sociotechnika toho využívá.

Sympatie – kdy lidé mají tendence vyhovět, pokud daná osoba se jeví jako sdílející obdobné zájmy, názory a životní pohled, je oběti sympatická. Pachatel se snaží dovědět o nějakém postoji, zálibě oběti a na tento navázat. Proto jsou rizikové sociální sítě s otevřeným přístupem a publikováním osobních informací. Ty jsou zdrojem bohatým na tyto informace a je zde snadné pro pachatele, dopátrat informace o potenciální oběti.

Vzájemnost – kdy se očekává automatické podřízení žádosti, pokud bylo na oplátku něco slíbeno, dáno nebo vykonáno. Operuje se s pocitem závazku, vděku. Může jít o hmotné dary, utajení určitých skutečností. Tato technika je s oblibou používaná například prodejci nádobí a jiných předmětů, kteří své zákazníky někam pozvou, něco jim dají. V těchto pozvaných osobách začne působit právě jedna z těchto základních vlastností psychiky, vzájemnost, a je jim nepříjemné, potom co něco zadarmo obdrželi, nic nekoupit. Z této vlastnosti lidské psychiky těží tito prodejci, obdobě jako zruční sociotechnikové.

Vzácná příležitost – kdy lidé mají tendenci se podřídit, když jsou přesvědčeni, že právě nyní je výjimečný okamžik. Klasická technika používaná obchodníky, na internetových

portálech, v supermarketech. Sleva, akce, výprodej. Omezené množství, pouze dnes. Dále je možné pracovat s pocitem stresu, časového nátlaku, který je velmi úspěšný. Vyvolání pocitu naléhavosti, nedostatku času a hrozícího rizika vyvolává v oběti pocit nutnosti rychle se rozhodnout a nedostává jí prostoru ke kvalifikovanému zhodnocení pachatelovi žádosti.

Útočníci se také dle Mitnicka (2003, s. 201) zaměřují především na osoby na nízkých pracovních pozicích v organizaci, protože ty si nemusí plně uvědomovat význam některých informací pro organizaci a důsledky některých činů. Zranitelné jsou osoby, které jsou rády, když se někomu zavděčí nebo někomu pomohou a také osoby sdílné a důvěřivé. S příchodem internetové a globalizované společnosti jsou tu také nové komunikační kanály, na kterých mohou probíhat tyto sociotechnické techniky a tato činnost nemusí probíhat pouze tváří v tvář oběti, úředníkovi, ale lze použít e-maily a další jiné komunikační kanály, které umožňují útočníkům snadné pozměnění své vlastní identity a manipulaci s obětí.

Není možné předpovědět všechny druhy útoků, jejich podoby a momenty, ve které přijdou, ale zaměstnanci by měli vědět, jaké druhy útoků mohu obvykle přijít, jaké se již staly a jak takové momenty vypadají. Měli by vědět, jak je odhalit a jak na ně reagovat. Pokud budou s různými možnostmi seznámeni a budou vědět, co je může očekávat, budou tak lépe připraveni jim čelit. Je potřeba podtrhnout, že sociotechnika jako taková není nikterak nebezpečnou technikou, ale nebezpečné je, že o ní lidé nevědí a tedy na ně funguje. „Platí, že většinu sociotechnických útoků je možno snadno odrazit, když se ví, na co si dávat pozor. Proto je nezbytné znát co možná nejvíce sociotechnických praktik.“ (Mitnick, 2003, s. 228) Na potřebě vědět a znát se shoduje i Brabec (2009, s. 47). Ten důrazně poukazuje, že chce-li někdo zabezpečit klíčové a důležité informace *proti riziku zneužití, je potřeba, aby právě pochopil* sociotechnické postupy a metody. Právě pochopení sociotechniky pak umožňuje předcházet těmto technikám. Je ale potřeba také upřesnit, že samotné školení není schopné dosáhnout nemožného. Především je potřeba v první řadě volit vhodné, morálně bezúhonné a konzistentní osoby na odpovědná místa odpovědných pracovníků.

Jak bylo uvedeno, má-li se těmto technikám úspěšně zabránit, dá se toho nejefektivněji docílit právě pomocí vzdělávání základního personálu. Vzdělávání je nejúčinnější metoda boje proti zneužití dat a informací pomocí sociotechniky. Je proto potřeba tyto techniky znát a vědomosti předávat dále personálu.

Rizikem v tomto bodě je obejití i jinak nejlépe propracovaných pokynů, postupů a technologií skrz nejslabší článek, zaměstnance.

Opatřením je dostatečné seznámení a pravidelné udržování vědomostí zaměstnanců o rizicích, podobách, možných cílech a další odhalování sociotechnických postupů.

3.1.3 [R3] Používání komerčních produktů placených z reklamy

V dnešní době existuje mnoho platforem a aplikací v digitálním prostředí, jejichž služby jsou poskytovány zdarma. Tyto služby jsou obvykle placeny na modelu prodeje cílené reklamy. Rizikem těchto platforem jsou:

A) jejich obliba, vedoucí k postupnému hromadění i velmi citlivých osobních údajů v těchto platformách.

B) místy nedostatečná ochrana těchto osobních údajů a zabezpečení, kdy provozovatel se již v podmínkách používání vzdává jakékoli odpovědnosti. Provozovatel tím, že je vyvázán ze zodpovědnosti pro moment ztráty jím uchovávaných dat, utrpí v případě bezpečnostního incidentu pouze v rovině pověsti, která se může sekundárně projevit do ušlého zisku. Není tedy výrazněji motivován do vyšších investic do zabezpečení a vzhledem k tomu, že jeho obchodní model je postaven na financování z reklamy, nelze to po něm ani požadovat.

C) dále že i mnoho informací z bodu A je poskytováno za přispění uživatelů k veřejnému přístupu.

Nedostatečná informační gramotnost vede některé uživatele internetu k rizikovému chování, kdy, tak jak je uvedeno v bodě A) sami vkládají mnohé osobní údaje do různých platforem sociálních sítí, ukládají data na nezajištěná cloudová úložiště nebo posílají nezabezpečenými kanály citlivá data. Tato data, nejenže mohou, díky bodu B) být napadena, ale především v platformách sociálních sítí je mnoho údajů o osobách dostupných široké veřejnosti, zadarmo a legálně. Může se jednat o zájmy dané osoby, ale i bydliště, rodinné příslušníky či jména přátel, pracoviště, data dovolených a mnohé další. Toto jsou vše údaje, které může šikovný sociotechnik dobře využít pro své potřeby. Je tedy rizikové, tyto údaje dobrovolně vystavovat na internetu, v míře větší než nutné a zpřístupnit je bez jakýchkoli restrikcí celé internetové společnosti.

Na bezpečnost služeb poskytovaných zadarmo ale není správné si ve větší míře stěžovat, protože tím, že je služba zadarmo, bývá obvykle poskytována na modelu „tak jak je“

a uživatelé, kteří nejsou se zabezpečením spokojeni, nejsou nuceni její služby dále využívat. Obdobně tak komerční a veřejné organizace.

Proto je důležitější, mít na pozoru, jaká data jsou těmto službám svěřována. Problém může nastat, pokud zaměstnanci veřejné správy budou ke komunikaci, zasílání citlivých souborů, využívat jiné než schválené spojení pro veřejnou správu nebo i používat například free mailové a jiné služby, otevřené komunikační platformy nebo free cloudové služby. Především některé zahraniční služby mohou podléhat tamější národní kontrole. Problematické by se mohlo jevit i diskutování pracovních problémů přes tyto služby. Ale především pro organizace veřejné správy, je nebezpečné, pokud zaměstnanci se velmi široce prezentují na platformách sociálních sítí. Toto dělá nejen je, ale i organizaci, potenciálně zranitelnou. (Urban, 2013; Securityworld, 2013; Gajdošová, 2013; Pelech, 2013; Fuj, 2013)

Rizikem je umisťování a komunikování pracovních dat do internetových platforem poskytovaných na bázi placení jejich provozu především z reklamy a dále poskytování vlastních osobních údajů zaměstnanci do internetového prostředí všeobecně.

Opatřením je vzdělávání zaměřené na vysvětlení rizik spojených s používáním těchto služeb pro pracovní účely a principů, na kterých tyto služby fungují a dále navyšování jejich informační gramotnosti, speciálně se zaměřením na jejich osobní bezpečnost v digitálním prostředí.

3.1.4 [R4] Problematika práce z domova

Práce z domova, ač se může zdát současným trendem, může být z hlediska bezpečnosti dat a informací velkým problémem. Týká se především soukromých společností, a v menší míře i veřejných organizací, kde práce z domova není obvyklá, ale místy lze i na ní narazit. Je proto důležité i o tomto aspektu pojednat. Rizikovým momentem, který je zde možné spatřit, je používání a připojování jinak například bezpečnostně certifikovaných zařízení, jako jsou pracovní notebooky aj. na soukromá, internetová připojení, jakými jsou domácí wi-fi připojení nebo pevné linky a celkové vynášení dat z místa působiště organizace a jejich transport do bydliště zaměstnance. Nemusí být zde totiž zaručeno, že používané datové připojení je dostatečně zajištěné a tak může dojít například ke kompromitaci určitých i jinak spolehlivých služeb organizace. Rizikem je také transport pracovního zařízení na cestě domů a zpět, které je tak vystaveno zvýšenému riziku krádeže. (Louda, 2013)

Rizikem jsou zde nezajištěná internetová připojení, možnosti používání neschváleného zařízení a samotný nadbytečný průběh transportu dat a pracovního zařízení.

Opatřením je dostatečné vysvětlení rizik a kritických míst a v návaznosti na toto odpovídající opatření a zabezpečení. Není rozhodně důvod kvůli tomuto riziku zamezit práci z domova, naopak, pokud je možno ji vykonávat, s přihlédnutím k charakteru výkonu veřejné správy toto může být složitější, lze ji po důkladném schválení i podporovat. Stačí zaměstnance důkladně poučit o rizicích, zajistit dostatečné připojení a odpovídajícím krokem zajistit moment přenosu dat, například aplikací šifrování či obdobně dle doporučení technických specialistů.

3.1.5 [R5] Mobilně-lokalizační služby

Rizikem s rozvíjejícím se potenciálem je fenomén mobilní lokalizace a služeb spojených s mobilními telefony. Takzvané chytré mobilní telefony, jsou dnes již takřka osobními počítači. Svojí výpočetní kapacitou jsou již mnohokráte dále, než byly osobní počítače před pouhými desítkami let. A tak jak dříve kolovaly fámy o možnostech mobilních telefonů ke zneužívání dat a informací, dnes se realita spíše oddaluje od fám a blíží ke skutečnosti.

Tak jak jsou chytré mobilní telefony spíše počítači, objevují se i nové trendy v podobě rizik a je potřeba reagovat odpovídajícími kroky. Banky nabízejí dvoufázové ověření při přihlašování do internetového bankovnictví. Přes počítač požádáte o zaslání kódu na váš mobilní telefon a tento kód zadáte přes počítač do systému, který vás pustí dále. Nicméně s rozvojem chytrých telefonů již opět stačí jedno zařízení, neboť zařízení jsou schopna nahradit počítač pro přístup na internet a SMS kód je zaslán na totožné zařízení. Stává se tedy z dvoufázového ověření opět pouze jednofázové ověření a oslabuje se tak autorizace k přístupu do systémů internetových bankovnictví.

Internet už není na stole ale v ruce, v mobilních telefonech (Sedlák, 2013) a ty jak jsou obdobami počítačů, mohou se i samy stát cíli útoků (Vrba, 2013). To bylo opět před určitým časem nemyslitelné. Tyto útoky, díky větší provázanosti mobilních zařízení s platebními a placenými službami, mohou být velmi nepříjemné. Může se jednat o odesílání placených SMS, drahé telefonáty aj. (Kirk, 2013). Současné chytré telefony, pokud obsahují správný kód, není pro ně problémem provádět takřka jakoukoli činnost, které jsou technicky schopny, a to za nevědomí uživatele. Tak jak se dříve jednalo spíše jen o pověru, že je potřeba mobilní telefon vypínat před odposlechem, tak dnes by se mohlo vyndávání baterie jevit jako více aktuální. Nicméně ale chytrý malware nemusí infikovat jen mobilní chytrý

telefon, ale jeho pomocí může proniknout do počítače uživatele a vzájemně se takto šířit (Janů, 2013).

Chytré mobilní telefony a počítače poskytují veliké možnosti a také velké kombinace rizika. Tak jak jsou chytré mobilní telefony počítači a mohou být infikovány škodlivým kódem, mohou se stát nástroji osobního sledování zájmových osob. Dříve běžný infikovaný počítač mohl na uživatele prozradit, zda jste online či nikoli, hrubě přibližnou polohu a všechna vaše data. Dnes, váš chytrý mobilní telefon, na vás dokáže prozradit všechna vaše data a vaši živou přesnou polohu, kde se právě nacházíte. Mobilní telefony obvykle nosíme většinou všude s sebou, jsou tedy ochotné poskytnout údaje o vaší přítomnosti, nebo nepřítomnosti na určitých místech takřka v přímém přenosu. Mohou poskytnout data a informace o časech, kdy procházíte ztemnělým parkem, kdy se ráno probouzíte anebo kudy jezdíte do práce.

Mobilní telefon ale nemusí být infikován škodlivým kódem, aby jím poskytované osobní údaje o uživatelově poloze mohly být zneužity. Nebezpečím jsou také soukromé služby, které umožňují například k aktualizaci svého profilu připojit svojí polohu. (Andress a Rogers, 2011, s. 92) Uživatelé tak dávají najevo nejen svému okolí, ale v podstatě i celému internetu, kdy se kde nacházejí. Činí tak dobrovolně, z vlastní vůle, jen nevědomi si rizika, které jejich konání představuje. Oznamují, kdy jsou doma, kdy v práci, kudy procházejí a toto nemusí představovat jen riziko pro ně samotné, nebo vykradení jejich bytu, ale potenciálně i riziko pro zaměstnance a zaměstnavatele. Vykradení bytu, nafocení při určitých aktivitách může být materiálem k pracovní kompromitaci. Oznámení o dovolené, nepřítomnosti v práci, prostorem ke kriminálním aktivitám v nepřítomnosti. Možností je opravdu mnoho, a není zde racionální důvod, tyto osobní informace o sobě dobrovolně pouštět do celého světa, kterým dnes internet skutečně je.

To vše je obří potenciál k exploitaci a neřízené používání některých služeb a technologií tak poskytuje riziko nejen veřejné správě, ale celé společnosti.

Rizikem je v tomto bodě poskytování citlivých lokalizačních údajů a snadná zranitelnost zařízení poskytujících tyto údaje.

Opatřením je vysvětlení rizik, spojených s poskytováním svých lokalizačních údajů, které povede k omezení dobrovolného poskytování těchto údajů zaměstnanci a dále k vyššímu zabezpečení jejich zařízení, které se bude snažit omezit nedobrovolná zneužití jejich mobilních zařízení.

3.2 Další dílčí rizikové body

Dále lze již jen okrajově zmínit, že mnoho mobilních služeb je dnes svázáno s povinnými účty u poskytovatele služeb. To umožňuje další snadnou vystopovatelnost a provázanost informací o uživateli. Kolektivizují se údaje o zájmech, telefonních číslech, kreditních kartách, a ač si to uživatel nemusí uvědomovat, vytváří se digitální otisk jeho identity. Ten může být přístupný i nežádoucím subjektům.

Chytré mobilní telefony nabízejí také možnosti správy elektronické pošty. I v tomto může být spatřován problém, neboť i jinak dobře zabezpečené servery s poštou tak mohou poskytnout pracovní komunikaci do ne vždy zcela dobře zabezpečených zařízení, která navíc, vzhledem k tomu, že jsou nošena takřka nepřetržitě na různá místa spolu s uživatelem, jsou vystavena většímu riziku zcizení, než například pracovní počítače umístěné v kanceláři.

3.2.1 Competitive intelligence

Neměl by také převládat klamný pocit, že získáváním informací se zabývají pouze zpravodajské služby nebo kriminální živly. Často se zapomíná na competitive intelligence. Konkurenční zpravodajství. To využívá informačních a komunikačních technologií za účelem získání informací z otevřených i skrytých zdrojů. (Požár, 2005, s. 149; Brabec, 2001, s. 218) Nejedná se o výraznější riziko, které by mohlo postihnout právě veřejnou správu, spíše se bude veřejné správy dotýkat jen okrajově. Může jít například o boj soukromých firem o veřejné zakázky. Za povšimnutí především stojí, vzhledem i ke vztahu k předchozím bodům, že competitive intelligence může získávat velké množství informací z otevřených, tedy veřejně přístupných zdrojů. Je tedy i pro veřejnou správu potřeba mít se na pozoru, kdo, kam a co publikuje, neboť při důkladné analýze veřejných zdrojů informací, lze dojít k překvapivě obsáhlým a detailní závěrům a agregovaným informacím.

3.2.2 Přenos dat v digitálních systémech

Požár (2005, s. 52) doslova uvádí, že „přenosy informací veřejnými telekomunikacemi, jsou nejslabším článkem všech informačních systémů“. Ve smyslu předchozích rizik, je potřeba věnovat pozornost, jaká data jsou přenášena kterými komunikačními kanály a nelze-li zajistit dostatečnou bezpečnost daného kanálu, je potřeba omezit hodnotu přenášených dat. Veřejná správa má svá již definovaná specifika a je vhodné při komunikaci důsledně dbát pravidel daných pojmy kryptografie a používání soukromých a veřejných klíčů. Právě kryptografie je cesta k „prevenci proti neautorizovanému odebírání nebo od-

straňování, vkládání nebo přidávání dat a informací“ a jejich celkové ochraně. (Přibyl, 2004, s. 3) Přenos dat není rizikový pouze v digitálních systémech, ale i jejich fyzický přenos je potenciálním navýšením možnosti jejich zcizení. I zde použití šifrování je schopno navýšit datovou bezpečnost.

3.2.3 Fyzická rizika

I v dnešní digitální informační době je potřeba, neopomínat samotnou problematiku fyzické ochrany dat. Nelze se soustředit pouze na dostatečné softwarové a technické zabezpečení. Je všeobecně známo mnoho případů, kdy i jinak dokonale zabezpečené informační systémy byly napadeny fyzickým útokem a data z nich byla odcizena prostým zcizením hardwarových nosičů.

Je proto důležité, aby státní instituce, jakožto instituce spravující data, neopomněly důsledné nasazení všech dostupných opatření a prvků ochrany. Je potřeba implementovat a udržovat dostatečné prvky technické ochrany, mít kvalitní režimovou ochranu a také samotné prvky vlastní fyzické ochrany. Zde opět dominuje lidských faktor. I v současné době jsou podstatné prvky, kterými jsou kvalitní strážní nebo vrátná služba.

Dostatečné zabezpečení by mělo plnit funkce, mezi kterými jsou například odrazení pachatele od vlastního úmyslu proniknout do chráněného území. Všeobecně rozšířenou, ale špatnou, fámou je to, že dobré zabezpečení pouze dává najevo to, že za ním se ukrývají důležité hodnoty a bude lákat pachatele. Ve skutečnosti pachatele, především příležitostné a situační, spíše odradí. Neboť charakteristikou výše uvedených pachatelů je, že to „prostě zkoušejí“. Tipton a Krause (2007, s. 2901) dále přidávají i zahraniční zkušenost, kdy uvádějí, že usvědčení pachatelé uvádějí, že volba jejich oběti, respektive cíle útoku, přímo souvisí se snadností, s jakou se domnívají, že útok bude snadné provést, kdy někteří uvádí, že i malý náznak zabezpečení je pro ně známkou, opustit od původního záměru a raději zvolí jiný cíl útoku a napadení. Další funkcí kvalitního fyzického zabezpečení je již samotné znemožnění vniknutí nebo odcizení. Poslední funkcí, pokud předchozí selžou, je alespoň donucení pachatele zanechat stopy, (či ještě lépe dokumentovat jeho pohyb a činnosti) které později povedou k jeho vypátrání. Se všemi body, vyjma prvního, souvisí funkce vyvolání poplachu, který povede k aktivizaci příslušných bezpečnostních složek a zamezení aktuálně probíhajícího útoku. (Brabec, 2001, s. 85, 104, 135) Fyzická strážní služba je vhodným prvkem, spolu s viditelným kamerovým zabezpečením, zjevné demonstrace takovéhoto zabezpečení a je podstatné, i tyto prvky neopomínat.

3.2.4 Vedení spisové služby

Podstatným prvkem pro ochranu dat a informací uvnitř organizace je důležitá kvalitně vedená spisová služba. Spisová služba zahrnuje systém registrace fyzických spisů, dokumentů, soubory předpisů pro spisovou službu, které pojednávají o pořádku ve spisové agendě, dále různé spisové pomůcky a také používané tiskopisy i formuláře. Její součástí, které by měla být věnována významná pozornost, je skartační činnost. Je potřeba připomenout, že pojem skartace znamená vytřiďování spisů, nikoli jejich pouhou fyzickou likvidaci, jak se bývá mylně domníváno. Jejich fyzické ničení může následovat. Předpisy spisové služby by měly být dodržovány, neboť například odpadkové koše, do kterých se dostanou nevhodné dokumenty, jsou bohatým zdrojem na informace. (Brabec, 2001, s. 221, 222)

Je vhodné se také zabývat problematikou úklidu kancelářských prostor. Kdo ho provádí, zda sám či s dozorem a obdobně. Úklidový personál má mnohé možnosti k zcizení nesprávně zabezpečených dokumentů, ale nejen ke zcizení, ale také má možnosti k instalaci nežádaných technických zařízení v budově organizace. Dokumenty a jednotlivé místnosti by měly být dostatečně dle vnitřních předpisů zabezpečené a kontrolované. Je vhodné také dodržovat clear desk policy. Je proto podstatné, aby zaměstnanci byli si vědomi a vzděláni v potřebných činnostech a tato opatření a činnosti byly pravidelně osvěžovány a udržovány napříč organizací aktivní.

3.2.5 Koncentrace informací

Jak bylo v teoretické části řádně uvedeno, žijeme v informační době a dochází k nadměrné koncentraci hodnot. S tím je potřeba se smířit a přijmout toto jako fakt. Svět se nadále globalizuje. Ale je potřeba a přinejmenším vhodné, zaujmout k tomu odpovídající opatření.

Tak jak se data a informace koncentrují, stává se, že čím dále více osob má přístup k neustále většímu množství údajů. Již ve čtyřicátých letech minulého století byl stanoven Lesliem Grovesem, v rámci projektu Manhattan, princip přepážek. Tento princip definuje, že lidé, respektive zaměstnanci, by se měli dozvídat jen to, co nezbytně potřebují ke své práci. Nikoli tedy vše, co se mohou dozvědět. I v češtině pro tento princip někdy zůstává anglické pojmenování need to know. (Laucký, 2009, s. 121) Jedná se o velmi jednoduchou myšlenku, ale s velkým potenciálem pro dnešní dobu a ochranu dat. Upustilo se snad od tohoto principu v samotné zemi, kde tento princip vznikl? V případu již jednou diskutovaného vojáka Manninga bylo právě nedodržení, respektive nenastavení principu přepážek aspektem, který umožnil tomuto vojákovy přístup k rozsáhlému množství citlivých dat

a diplomatických depeší. Ty nepotřeboval ke své práci a i přes to měl k nim umožněn přístup. Využil této možnosti, data zkopíroval a později předal jiným osobám.

Na existenci tohoto rizika a potřebě principu přepážek se shodují i čeští autoři, (Brabec, 2009, s. 143), kteří zmiňují, že potřeba aby uživatel dostával jen ty nejnutnější informace, které potřebuje, je jedním ze základních prvků budování informačních systémů. Zajištění přístupu uživatele k informacím, které skutečně potřebuje, přispívá k zajištění bezpečnosti dat a informací nejen z hlediska omezení jejich úmyslného zneužití, ale i z hlediska snížení uživatelova rizika a zodpovědnosti za omylem vykonané činy či nehody. Snahy o aplikaci tohoto principu lze nalézt i ve veřejnosprávním přístupu ke klasifikovaným dokumentům.

Jak bylo v této části důkladně zhodnoceno, mezi reálná a nejvýznamnější rizika spojená s ochranou dat a informací v institucích veřejné správy patří zejména rizika, spojená s chybami nebo nedostatky v lidských zdrojích. Nemusí se jednat vždy o vědomé zneužití možností, ale i nevědomost a nesledování trendů vývoje a včasné nereagování na změny v prostředí.

Předcházející analytická část práce zhodnotila reálná a nejvýznamnější rizika pro veřejnou správu. Na tuto analytickou část dále naváže projektová část práce, která nabídne vlastní řešení, v podobě velmi dobře udržitelného, ekonomického a realizovatelného konceptu pro uvedení do praxe. Navazující řešící část této práce reflektuje v předcházející analytické části zhodnocená reálná a nejvýznamnější rizika pro veřejnou správu a na analytickém základě nabízí vlastní projektové řešení pro přístup k těmto zhodnoceným rizikům.

4 NÁVRH MODELU BEZPEČNOSTNÍHO VZDĚLÁVÁNÍ ZAMĚSTNANCŮ VEŘEJNÉ SPRÁVY

Tato část představuje navrhované řešení, v podobě projektu navrhnutého pro instituce veřejné správy, jehož cílem je dlouhodobé udržení a další navyšování bezpečnosti správy dat a informací z personálního hlediska. Na základě důsledných podkladů prezentovaných v předchozích kapitolách, ze kterých vyplývá, že nejslabším místem zabezpečení informačních systémů, a zároveň místem, kde je v současné době ještě velmi prostoru a potřeby k největšímu zlepšení, je právě personální stránka bezpečnostní problematiky. Přispěním k možnosti zlepšení stavu v této oblasti a dílčímu naplnění cíle udržení a navýšení bezpečnosti dat a informací bude dosaženo pomocí navrhnutí modelu vzdělávání zaměstnanců veřejné správy. Jedná se také o jednu z nejefektivnějších možností, kterou je v době potřebných úspor ve výdajové stránce veřejného rozpočtu potřeba neopomenout. Návrh představuje definování osoby zodpovědné za vedení a přípravu vzdělávacích programů v každé instituci veřejné správy a dále ustanovení nové pracovní pozice, specialisty informačních systémů veřejné správy. Je představen rozvrh a základní obsah vzdělávacího konceptu spolu s modelovými činnostmi jednotlivých navrhovaných pracovních pozic.

4.1 Aktuálnost, význam a zdůvodnění projektu

Jak ukázaly nedávné útoky na český internetový prostor, digitální prostředí je snadným cílem pro záškodnická jednání. Přispívá k tomu jednak globálnost dnešního informačního systému, ale také i dostupnost prostředků a vědomostí ruku v ruce s klesajícím věkem pachatelů. V tomto prostředí se do procesu digitalizace zapojuje i veřejná správa se svými trendy v rozšiřování eGovernmentu, další podpory datových schránek a celkové digitalizace veřejné správy a jejího výkonu a poskytování veřejnosprávních služeb.

Veřejná správa je sektorem, který by měl jít v zajišťování informační bezpečnosti první a příkladem. Je to totiž právě veřejná správa, která disponuje nebývalým množstvím informací o svých občanech, každém z nás a jakákoli kompromitace, zničení nebo neoprávněná modifikace těchto údajů by mohla mít, a má, velmi nebezpečné dopady na jednotlivé životy takřka veškerých občanů. Díky propojení sítí veřejné správy skrz Evropskou unii, již nejde jen o národní občany, ale o občany celé Evropské unie.

Informace jsou klíčové a ocenit jejich hodnotu je velmi nelehké, neboť zde se nejedná pouze o samotné pořizovací náklady. Obdobně tak úniky informací lze těžko dokázat a tedy

zpravidla hodnotu něčeho oceníme, až když tuto hodnotu ztratíme. Přiměřeně k tomuto, bezpečnost je mnohdy stále vnímána jako jakási notorieta – tedy něco, co všichni znají – ale je tomu tak opravdu? Chápou tvůrci, správci aktiv a uživatelé pojem bezpečnosti stejně? Je potřeba říci, že bezpečnost se vyplácí z dlouhodobého hlediska, a také, že bezpečnost nesmí trpět na úkor zisku. V současné době se bezpečnost informací netýká pouze státu, státních orgánů a institucí, ale všech organizací a i každého jednotlivého člověka. (Mates a Smejkal, 2006, s. 64; Paleček, 2006, s. 32; Brabec, 2009, s. 127)

I sebelepší navržené bezpečnostní opatření bude neúčinné, nebude-li používáno samotnou cílovou skupinou. A i například sebekvalitnější autentizační metoda pro uživatele bude neúčinná, budou-li si tyto osoby například neoprávněně předávat autentizační klíče. Proto jsou zaměstnanci chápáni jako ústřední téma navrhovaného projektu.

4.1.1 Kulturní podklady institucí a cesta k efektivnější práci se zaměstnanci při zajišťování bezpečnosti

Pro naplnění výše uvedených bezpečnostních cílů je důležité mezi zaměstnanci vytvářet pocit sounáležitosti tak, aby zaměstnanci vnímali otázky bezpečnosti organizace, jak bylo uvedeno, jako své vlastní. (Doucek, 2011, s. 141; Dobda, 1998, s. 99) Prostor, který je vytvořen v rámci bezpečnostních školení, je k tomuto vhodným nástrojem.

Je potřeba naučit organizaci pracovat s pojmy jako jsou loajalita, hodnoty a celkový vztah k profesi, ať již za pomoci formálních nebo neformálních prostředků tak, aby byl vytvářen právě onen až pocit „sounáležitosti a kamarádství, členství v exkluzivní rodině, statusu člena a hrdosti být součástí společensky důležitého a náročného prostředí“ (Nesvadba, 2009, s. 198, 231). Bohužel v České republice stále panuje jakési pejorativní vnímání veřejné služby a je to nelehký úkol, se kterým je potřeba se potýkat. Toto se nazývá problematikou stavovské cti a kupříkladu výše citovaný Petr Nesvadba se k tomuto domnívá, že pojem stavovské cti by mohl zdařile sloužit právě jako ono vyvrcholení či integrující prvek budování celistvého morálního profilu osobnosti zaměstnance veřejné správy. Rozbor Nesvadbova pojmu stavovské cti by byl mimo rozsah této práce, nicméně jedná se o zajímavou problematiku ještě zajímavějšího autora a lze jen stručně dodat, že z jiného vnímání např. Zuzana Herzogová chápe stavovskou čest jako jakousi vědomou hrdost na příslušnost k dané profesi a uvědomělé plnění morálních povinností, které by měly regulovat výkon oné profese. Tedy jistým ideálem by bylo, kdyby zaměstnanci nežili ze své práce, ale pro svoji práci. Tak by dodržování bezpečnostních stanov nebylo vnímáno

na obtíž a zaměstnanci by sami aktivně vyhlíželi nové možnosti ke zlepšení. Nicméně v sektoru výkonu veřejné služby jde pravděpodobně spíše obtížně tohoto dosáhnout, respektive jsou vyžadovány určité typy osobností. (Nesvadba, 2009, s. 198, 231)

Zajištění bezpečnosti tedy nemůže být také pouze osamoceným úkolem pro určité oddělení, pověřené osoby, ale je potřeba, aby se bezpečnost prolínala celou institucí, včetně například oddělení lidských zdrojů, které je zodpovědné za nábor nových zaměstnanců. Bylo by vhodné, aby samotný vzdělávací proces, kromě odborného vzdělávání, pracoval i s problematikou jakéhosi mravního rozměru využití nabytých vědomostí. Jinak hrozí nebezpečí zneužívání takto nabytého vzdělání ve prospěch zločinu a vytváření dalších bezpečnostních rizik uvnitř organizace.

Je potřeba kromě odborného vzdělávání posilovat také „mravní rozměry vzdělávacího procesu. Jinak hrozí nebezpečí zneužívaní vzdělání ve prospěch zločinu a vytváření bezpečnostních rizik“ a obzvláště v „procesu výchovy, respektive vedení ostatních zaměstnanců je tento požadavek mravnosti a morálky ještě výraznější“ (Brabec, 2001, s. 33).

Samotné bezpečnostní vzdělávání, bezpečnostní trénink je vhodné uchopit jako příležitost ke změně, či úpravě kultury organizace, protože efektivita celého procesu záleží především na chování lidí. A jejich vnímání. A naopak, jejich vnímání a chování se odvíjí od toho, co znají, vědí a jak smýšlejí. Je uváděno (Tipton a Krause, 2007, s. 555, 562), že obvyklé tréninkové programy mají dopady na znalosti a vědomosti posluchačů, ale jen málokdy mají dopady a efekt na jejich smýšlení ohledně jejich vlastní odpovědnosti a toho, jak oni sami mohou přispět k bezpečnosti celé organizace.

Není pro organizaci vždy ve výsledku prospěšné, pokud probíhá výběr nových zaměstnanců pouze na základě předem definovaných požadavků, zahrnujících „pouze jejich znalosti a profesní předpoklady“ (Dobda, 1998, s. 98). Měla by se zohledňovat také a především jejich osobnost, personalita. I o něco méně kvalifikovaný zaměstnance, který však bude mít dobrou osobnost, personalitu a bude dobře působit na kolektiv, může ve výsledku být větším přínosem pro instituci než jedinec, sice oborově kvalitně kompetentní, ale který bude způsobovat interpersonální problémy. Nehledě na fakt, že pokud bude mít jedinec chuť se dále vzdělávat a učit se novým věcem, brzy se potřebné vědomosti, ve kterých na počátku zaostával, doučí a v tomto trendu může pokračovat i dále. Tedy, po nějakém čase, ten kdo bude mít kvalitní osobnost, dobře působící na kolektiv a s touhou se dále vzdělávat, může být pro instituci hodnotnějším pracovníkem než osoba sice na počátku

kvalifikovaná, ale bez touhy po dalším sebezlepšení. Avšak ale osobnostní a morální vlastnosti se však, na rozdíl od profesních, těžko v průběhu přijímacího procesu odhalují a poznávají. Nejkvalitnější výběr by měl probíhat u pozic s přístupy k citlivým údajům a vedoucích pozic, neboť právě toto jsou pozice, schopné budovat odpovídající kulturu organizace.

4.1.2 Problematika kultury a chování pro vzdělávání zaměstnanců

Proč je kultura důležitá? Kvalitní kultura organizace podporuje výkonnost celé organizace a podporuje dosahování cílů celé organizace. V případě veřejné správy je to služba občanům a plynulé fungování státu. Kultura organizace by měla mít takového ducha, který pracovníky podporuje v jejich angažovanosti, loajalitě a participaci na dosahování cílů organizace (Strecková, 2005, s. 65). Nutno podotknout, že loajalita je oboustranná. Nelze tedy budovat loajalitu ve směru od zaměstnanců, aniž by vlastní loajalitu k zaměstnancům nebyla schopna nabídnout sama instituce. Ve směru od instituce se loajalita projevuje například ve formě jistoty, že se instituce postaví za svého zaměstnance, v případě problémů aj.

Právě loajalita, jakožto „oddanost a věrnost k plnění určitých závazků“ (Nesvadba, 2009, s. 197) je silným nástrojem, schopným kvalitně motivovat pracovníky. Motivovaný zaměstnanec ví co, jak a proč má dělat, je si vědom rozsahu svých pravomocí a zodpovědnosti a vztahu ke spolupracovníkům a kvalitně reprezentuje celou instituci. Vyhýbá se nezájmu, nedbalosti či zmatku. (Laucký, 2006, s. 84, 85) Nevyhýbá se ale neznalosti a pokud se s ní setká, má zájem ji napravit vzděláváním. Je jen na jeho zaměstnavateli, poskytnout mu prostor k takovémuto vzdělávání.

Jsou-li pracovníci vhodně motivovaní a stimulovaní, mohou kvalitně odvádět svojí práci, ba i dále do ní vnášet svojí kreativitu, nápady. Nicméně osobnost člověka je složitý komplex a nikdy nelze vidět do nitra osobnosti člověka, jeho pohnutek, motivace a dále. Existují však metody a formy výběru spolupracovníků a práce s nimi, které se snaží rizika z tohoto plynoucí alespoň co nejvíce minimalizovat. Tomuto se říká řízení lidských zdrojů a je nedílnou součástí správného managementu a vykonávání zodpovědné správy bezpečnosti dat a informací. „Vedení by mělo předpokládat, že může zaměstnávat lidi, kteří svými morálními vlastnostmi neodpovídají požadavkům na ně kladeným“ (Požár, 2005, s. 150) a mohou se proto někdy chovat jinak, než by bylo žádoucí.

Chování zaměstnanců se přirozeně mění v čase a je spojené mj. s jejich vývojem vztahu k profesi. Nesvadba (2009, s. 200) uvádí několik stádií, mezi kterými jsou stádium: roz-

mělňování vstupní motivace, kdy zaměstnanec ztrácí počáteční iluze ze zaměstnání, dále stadium adaptace, které může znamenat postupné zjišťování a začleňování se do skutečných požadavků práce, kolektivu. Může také znamenat nárůst profesionality ale také s tím spojené narůstání rutiny, lhostejnosti, apatie nebo mechanického plnění požadavků a pokynů. Závěrečným stadiem je dle Nesvadby stadium profesionální deformace, kdy se jedná o jakousi opotřebovanost a hrozí syndrom vyhoření. Zaměstnanecké vzdělávání zaujímá svojí roli hlavně v první, v podobě úvodních školení, a především ve třetí a čtvrté fázi. V těchto fázích může docházet k polevování určitých bezpečnostních návyků, opomínání určitých kroků, které se mohly v minulosti jevit jako nadbytečné. V těchto fázích je důležité realizovat navrhované bezpečnostní školení.

Práce s problematikou chování a její jemná modulace v rámci vzdělávacího systému instituce je výborným nástrojem, jak posílit obranyschopnost celé instituce před riziky sociálního inženýrství. Je potřeba připomenout a zdůraznit, že bezpečnost je problémem, který týká se každého jedince. Nejedná se o abstraktní pojem. Bezpečnost je v jádru i individuálním problémem, a pokud tak bude vnímána, lidé budou na jejím zajištění pracovat tvrději a budou schopni přijmout větší zodpovědnost. Omezí se takzvaný bystander efekt, který hrozí v případě, kdy je bezpečnost organizace vnímána jako něco, co je sice součástí organizace, ale čím se má zabývat sama organizace – bez uvědomění si toho, že právě organizaci tvoří právě zaměstnanci. (Tipton a Krause, 2007, s. 521) Doseděl (2004, s. 177) dokonce uvádí, že například pro oblast počítačové bezpečnosti je problematika chování zaměstnanců dokonce nejčastěji opomíjenou oblastí zajištění bezpečnosti. Pro chování zaměstnanců je také silným činitelem jejich „sociální zázemí, rodina, přátelé, záliby nebo finanční situace“ (Dobda, 1998, s. 99). Rodinné zázemí ovlivňuje pracovní výkon a může mít podobu bludného kruhu, kdy rodinné problémy se promítají do pracovních, které si zaměstnanci nosí domů, kde se dále projevují a způsobují tak jakýsi bludný kruh. Hazardní záliby mohou mít vliv na rizikové chování, nicméně zaměstnavatel má v dnešní době ochrany osobních práv spíše menší možnosti sledování těchto prvků u svých zaměstnanců. A přitom jedná se o aspekt, se kterým pracoval již Tomáš Baťa. Ten sledoval životní styl svých zaměstnanců, a to je neméně důležité i dnes u zaměstnanců na klíčových pozicích ve vztahu k bezpečnosti a ochraně dat a informací. Pokud například začne zaměstnanec na klíčových pozicích tvořit aktivity nebo vlastnit předměty, na které by jeho příjem evidentně nestačil, měl by to být signál k decentnímu prověření jeho aktivit. Především ve veřejné správě. V jádru by se měly ale sledovat pouze základní záležitosti. Záliby a je-

jich finanční náročnost, rodinný stav. Pozorovat neobvyklá chování pracovníků a taktéž nenadálé majetkové změny poměrů.

Aby zaměstnanci nebyli sami bezpečnostním rizikem, je potřeba uspokojovat jejich potřeby a očekávání (Brabec, 2001, s. 39). Na tom závisí míra jejich zapojení se do kultury organizace, jejích bezpečnostních opatření, jejich iniciativa při ochraně aktiv instituce, loajalita. Pokud organizace nebude naplňovat očekávání a potřeby vlastních zaměstnanců, musí očekávat zvýšenou míru rizika z jejich strany. Očekávání a potřeby mohou být různé, za všechny lze zmínit odpovídající plat, pocit jistot, důležitosti vlastní práce, uznání a mnohé další. Neuspokojení těchto a některých dalších potřeba očekávání, může vést nejen k riziku v podobě snížení loajality k organizaci a kolektivu, ale také ke zvýšení potřeby sdílnosti, hledání porozumění vně organizace. (Požár, 2005, s. 67) To může být živnou půdou pro zručné sociotechniky. Celkově, jak dodává Brabec (2001, s. 31), právě společenské prostředí v organizaci, kterému se jedinec přizpůsobuje, podílí nebo snaží vyniknout (ale i naopak, snaží vyhnout) působí výraznou měrou na vznik bezpečnostních rizik. Tím je podtržen význam vzdělávání, jako nástroje k úpravě společenského klimatu organizace ale také i význam průběhu výběrového řízení. Právě tam je prvotní prostor ku zjištění motivace, potřeb, zájmů a cílů potenciálních zaměstnanců. Zda jeho potřeby a možnosti korespondují s možnostmi nabízené pozice a celé organizace. Je potřeba zabývat se nejen otázkou, zda samotný pracovník nepředstavuje bezpečnostní riziko, ale také, zda je schopen a má zájem se aktivně podílet na snižování potenciálního bezpečnostního rizika. Dalším vyšším nadstavbovým cílem je motivování nejen vedoucích, ale i liniových zaměstnanců k aktivnímu vyhledávání rizika a jeho eliminaci. Pokud nebude výběr zaměstnanců prováděn dostatečně důsledně, nelze ani od vzdělávání zaměstnanců očekávat neočekávatelné výsledky. Vzdělávání je spíše nadstavbou kvalitního personálního výběru a dalším vylepšováním personálního kapitálu organizace.

O výše uvedených problémech je zde hovořeno proto, aby bylo zdůrazněno, jak náročný je proces zajištění bezpečnosti dat a informací z personálního hlediska. Vzdělávání zaměstnanců v tomto hraje podstatnou roli, avšak i tak je součástí celého systému práce se zaměstnanci a kulturou organizace a nemůže tedy vzdělávání zůstat ojedinělým procesem, mimo celkový koncept zajištění bezpečnosti a fungování celé organizace.

Snahou je poukázat, že pro optimalizaci systému vzdělávání, v zájmu dosahování vyššího zabezpečení dat a informací v institucích veřejné správy, je pro potřeby personálního pojetí této problematiky potřeba kvalitního multidisciplinárního pojetí, zapojení společenských věd, psychologie. Nelze se soustředit pouze na technickou nebo personalistickou stránku problému, ale je nutná jejich vzájemná provázanost, spolupráce. Je potřeba, aby tyto činnosti byly koncepčně vykonávány napříč celou organizací. Přínosem jí bude kvalitní a koncepční zajištění bezpečnosti dat a informací při dosažení efektivních nákladů.

I z tohoto důvodu, nákladového hlediska, je vhodné si důvěryhodné, zaškolené a loajální zaměstnance udržovat alespoň po plný přiměřeně dlouhý životní cyklus personálu. Zaměstnanci, o kterých jsou známi jejich vlastnosti, jsou ověření, vědí co a jak, snahy o jejich udržení po přiměřenou dobu jsou i ochranou investic organizací do nich vložených. (Ortmeier, 2009, s. 144) V neposlední řadě, právě oni, pokud jsou dobře zvoleni, mohou výrazně přispět ke kvalitnějšímu budování a upevňování kultury, které se projeví přirozenou obměnou chování lidí a jejich selekcí.

Bezpečnostní vzdělávání je jednak platformou k poskytování potřebných znalostí a návyků, ale také v neméně podstatné míře, platformou ke snaze o úpravu vnitroorganizační kultury, neboť efektivita bezpečnostních opatření záleží především na chování lidí. A jejich vnímání. A i naopak, jejich vnímání a chování se odvíjí i od toho, co znají a jsou ochotni aplikovat, vědí a jak smýšlejí. Jak bylo zmíněno, obvyklé tréninkové programy mají dopady na znalosti a vědomosti posluchačů, ale jen málokdy mají dopady a efekt na jejich smýšlení ohledně jejich vlastní odpovědnosti a toho, jak oni sami mohou přispět k bezpečnosti celé organizace. (Tipton a Krause, 2007, s. 555, 562) A vzhledem k tomu, že bezpečnost a bezpečnostní opatření k jejímu zajištění jsou nejúčinnější, pokud jsou součástí celé organizační kultury, jedná se právě o důvod, proč je potřeba rozšiřovat povědomí nejen o bezpečnosti, ale i o celém bezpečnostním programu organizace tak, aby ho zaměstnanci chápali a ztotožňovali se s ním a s celou firemní kulturou (Tipton a Krause, 2007, s. 623).

Změna kultury ale není jednoduchý cíl. Vyžaduje změnu lidí. Ne fyzickou, ale duševní. Jejich smýšlení. Změnu smýšlení, uvažování, jednání a vnímání tak, aby korespondovalo s bezpečnostními potřebami organizace. Změna kultury není krátkodobým procesem a jak Tipton a Krause (2007, s. 580) jaksi nadneseně dodávají, bezpečnost by se měla jaksi stát součástí DNA organizace. Proč je tedy kultura důležitá? Kultura organizace podporuje celkovou výkonnost celé organizace – pokud je pozitivní kulturou a také opačně. Kvalitní vnitroorganizační kultura je také to, co také umožní plynule reagovat, adaptovat se celé

organizaci na nové trendy, pružně jít s dobou a bezpečnostními požadavky. (Brabec, 2001, s. 33; Tipton a Krause, 2007, s. 555, 552)

4.2 Cíl vzdělávání, projektu a řešení

Cílem projektu je nabídnout řešení institucím veřejné správy, které pomůže ke kvalitnímu dlouhodobému udržení a dalšímu navyšování bezpečnosti správy dat a informací z personálního hlediska.

Řešením postupu k danému cíli, z personálního hlediska, je návrh bezpečnostního vzdělávání pracovníků institucí veřejné správy. Návrh obsahuje rozpracované předpokládané pojetí bezpečnostního vzdělávání a nabízí institucím veřejné správy výchozí témata, reagující na identifikované hrozby z předchozích kapitol.

Cílem samotného vzdělávání je vzbudit zájem o bezpečnostní problematiku a vlastní informační bezpečnost jedinců v digitálním prostředí. Včas tak tímto upozornit na nadcházející problémy a nebezpečí, jež jsou schopné ohrozit fungování celé společnosti, která je zranitelná díky její místy až nezdravé závislosti a propojenosti s výpočetními technologiemi. Tento zájem a poskytnuté vědomosti se mohou pozitivně odrazit nejen v navýšení bezpečnosti správy dat v cíleném sektoru veřejné správy, ale i mimo tento sektor, včetně životů daných zaměstnanců. Nicméně akcent je kladen stále na sektor veřejné správy, jakožto ústřední institut výkonu státní moci a zajišťování fungování státu.

Sekundárním cílem je formou vzdělávání poskytnout vedoucím zaměstnancům platformu k úpravě vnitroorganizační kultury, vedoucí lépe k naplnění bezpečné správy svěřených dat a informací, potažmo i modulaci celého výkonu organizace.

4.3 Obsah vzdělávání pracovníků ve veřejné správě

Obsahem vzdělávání pracovníků veřejné správy je primárně reakce na identifikované hrozby R1-R5, uvedené v kapitole 3.1 a dále na všechny aspekty, které školitel uzná za vhodné. Obsah by měl být vždy aktualizován dle momentální situace.

Hlavní i sekundární obsah bude podáván takovým způsobem, aby vzbudil zájem o bezpečnostní problematiku u zaměstnanců a celkově u nich prohlubovat bezpečnostní povědomí. Principy bezpečného chování poskytnou vědomosti ke kvalitnějšímu rozlišování toho, co je a co není bezpečné, k další identifikaci potenciálních rizik či pokusů o ohrožení a také k uvědomění si vlastní hodnoty dat pro organizaci a možných rizik z jejich zneužití

plynoucích. *Tak bude vytvořen podklad k promítnutí jejich zodpovědného chování do pracovní sféry života.*

Je potřeba počítat s tím, že jak se technologie a bezpečnostní přístupy vyvíjí, musí se měnit i obsah kurzu, u kterého je potřeba, aby reflektoval současný stav. Proto tato práce nabízí pět jádrových témat, která se vyznačují současnou aktuálností a předpokladem, že ještě alespoň v krátko až středně dobém horizontu zůstanou aktuální, avšak detailní plány a obsahy, vzhledem k možnosti dlouhodobějšího uplatnění této práce, budou ponechány otevřené. Je tedy poté na cílové skupině příjemců této práce, aby byli maximálně flexibilní a doplnili tyto předkládané struktury vlastními prvky tak, aby co nejlépe jako celek reagovaly na aktuální potřeby v čase a organizaci. (Tipton a Krause, 2007, s. 552)

Ilustrativně, mezi dalšími a doplňkovými tématy by mělo být zahrnuto například kromě uvedeného rozpoznávání scénářů sociálního inženýrství a dalších R1-R5 rizik, také například chování v situacích, kdy je požadován rozhovor s médii – jak odmítnou slušně poskytnout rozhovor, odkázat na tiskové oddělení, jak neprozradit více informací než je nutných či zákonných, jak na příliš zvědavé klienty či potenciální skryté novináře – ale zároveň naplňovat základy dobré a otevřené veřejné správy. Dále základy bezpečnosti a důvěrnosti samotných informačních systémů – práce s hesly, odhlašování, listinné manipulace, transporty dat, opouštění pracoviště, clear desk policy, přítomnost klienta a obdobně. Přítomnost klienta zahrnuje problematiku například kde nechat čekat klienta či návštěvu, pokud je potřeba opustit kancelář – v kanceláři a o samotě? Nebude mít možnost nahlížet do věcí a listin, které by jí neměly být k nahlédnutí? Nebo ji nechat v kanceláři s jinými osobami? Neuslyší komunikaci, kterou by neměla slyšet? Jak je uvedeno, všechna související témata nezahrnují jen bezpečnostní problematiku, ale mají také přesahy do etické a sociální stránky veřejnosprávního působení, které odráží významnost práce s pojmem kultury organizace. Ilustrativně uvedená témata je potřeba vždy upravit tak, aby například pokud organizace již aplikuje určitý způsob bezpečnostní edukace, nedocházelo ke zdvojování témat a obdobně. Všeobecným obsahem by mělo být informování o tom, jaké jsou hrozby, jak je identifikovat a jaké se v takových situacích očekávají kroky, adekvátní reakce. Obsah může být šířen formami rozebíranými v souvisejících kapitolách a neměl by být zaměřen pouze na koncové řadové zaměstnance nebo vedoucí zaměstnance, ale na celé spektrum všech zaměstnanců instituce. (Tipton a Krause, 2007, s. 573, 622) Obsah by tedy měl mít takovou náplň, podobu a formu, která bude rozvíjet bezpečnostní povědomí za-

městnanců a vzdělávání v nich zanechá stopu a vědomosti, jak být bezpečnostně obezřetný při výkonu své každodenní práce.

4.4 Forma vzdělávání pracovníků

Otázkou je také, jaké formy edukace zvolit. Lidé mají tendence se učit buďto vizuálně, poslechem nebo pohybem. Každý jedinec směřuje k převaze v právě jedné z těchto skupin. Kvalitní vzdělávací program by měl proto vhodně kombinovat všechny tyto tři metody, aby pokryl potřeby většiny zaměstnanců a každý si odnesl co nejvíce. (Tipton a Krause, 2007, s. 2904)

Základní texty bezpečnostního vzdělávání dospělých poukazují Ortmeier (2009, s. 211), že osoby se budou lépe vzdělávat, více snažit a více se naučí, pokud naleznou v probírané látce určitou spojitost s vlastním životem, vlastním konáním. Jde tedy o to, udělat výuku jaksi osobní, provázat ji se skutečnou praxí, činnostmi na úřadě. Prezentovat probíranou problematiku na podkladech skutečných událostí, ilustrovat na realitě. Například pro ilustrování metod zpravodajské sociotechniky nebo problematiky autentizace jde toto velice dobře. Dají se velice dobře ilustrovat potenciální rizika a škody a lze i z veřejných zdrojů dopátrat mnoho skutečných případů. Jedná se o dobrou cestu, jak později tuto problematiku převést do pracovního prostředí. Nehledě také na to, že názorná ilustrace bezpečnostní problematiky a jejích dopadů i na osobní životy může být i pro mnoho osob vhodným tématem k diskusi doma, s přáteli. Tím je dosaženo dalšího šíření tématu, přemýšlení nad ním posluchači, a tedy navýšení efektivity vzdělávacího procesu a využití investovaných nákladů. Ilustrované příklady musejí být co nejjednodušší a nejsrozumitelnější, tak, aby neodradily posluchače a nezpůsobily ještě větší zmatek v jejich vnímání. Příjemce tedy musí získat co nejvěrnější, a zároveň co nejjednodušší, představy o možných situacích a právě to mu umožní představované nové informace provázat se skutečnou prací. Role posluchačů by měla být aktivní, nikoli pasivní. Je vhodné postavit tedy výuky především na diskusi, nikoli na pouhém představování informací. Louda, Grospič a Vostrá (2003, s. 183) v tomto nacházejí „princip aktivní odpovědi“, kdy uvádějí, že „vzdělání by nemělo být pouhým biflováním vědomostí“. Měly by se klást otázky a sdílet myšlenky mezi posluchači a lektorem. Ten by na ně měl reagovat, odpovídat a dále je rozvíjet a podporovat tak diskusi. U motivovaných zaměstnanců platí, že pokud něco nevědí, nebojí se zeptat. Je proto potřeba také aktivně vzbudit v posluchačích zájem o vzdělávání, motivovat je. Zde je opět vidět provázanost se zmiňovanou kulturou organizace a jejími základními součástmi.

Nesejde na tom, zda ve výsledku bude použit blended learning, gamifikace či jiné formy výuky, důležité je, aby byly dodrženy alespoň základní aspekty vzdělávání dospělých. Především takt, ohleduplnost, úcta k lidem a jejich tempu učení (Laucký, 2006, s. 64). Osobní přístup. Proto by nebylo vhodné využít jako formu výhradně e-learningu. Jako nejvhodnější se jeví empatický lektor, poskytující aktivní formy výuky, založené především na názorných ilustracích skutečných případů a diskuzích, v kombinaci s pravidelným informačním bulletinem jako podpůrným prostředkem.

4.5 Organizace vzdělávání a personální zajištění

Představované vzdělávání nemá za cíl nahradit současné vzdělávací procesy v institucích veřejné správy. Staví se po jejich bok a nabízí jim možnosti a inspiraci, jak tato školení lépe zacílit, zefektivnit a lépe je zacílit právě na bezpečnostní problematiku a aktuální dění. Navrhovaný koncept částečně doplňuje vstupní školení, ale především rozvíjí potenciál průběžných a aktualizačních školení.

4.5.1 Pozice poradce pro otázky informačních systémů veřejné správy

Vzdělávací etapy, školení, by probíhaly v určitých stupních. Bylo by vhodné, aby každá instituce veřejné správy měla pověřenou osobu zabývající se bezpečností informačních systémů z personálního hlediska. Nemusí se jednat vždy o speciálně vyhrazenou osobu jen pro tyto účely, u menších institucí tuto funkci může zastávat osoba určená primárně pro jiné účely. Pro účely této práce bude označována jako *určený pracovník*. V neposlední řadě, pokud bude na každém místě výkonu veřejné správy pověřen jeden člověk, aby věnoval například několik hodin měsíčně přípravě školení pro své spolupracovníky, bude to i pro něj určitá forma sebevzdělávání uplatnitelného později uvnitř instituce.

Dalším auxiliárním navrhovaným konceptem pro podporu uvedeného konceptu je vytvoření pozice Poradce pro otázky informačních systémů veřejné správy. Jednalo by se nikoli o technickou, ale především na soft skills založenou pozici školitele, metodika zastřešujícího celky veřejné správy České republiky.

Při kvalitním rozvrhování jeho činností bude jeho vytíženost taková, že se mu dostane času i na činnost tvorby například informačního bulletinu, osobní rozvoj a sběr nových informací. V případě, že by se ukázalo, že by jeho náplň práce byla náročnější, dalo by se později přistoupit k rozšíření jeho týmu, například o specializované osoby pro tvorbu bulletinu

nebo výjezdní školení. Stále by tak bylo dosahováno, i v případě zaměstnání více osob, značných úspor a velkého přínosu pro veřejnou správu.

Tato osoba v centrální pozici by byla tvůrcem a správcem informačního bulletinu, pravděpodobně v počátcích čtvrt až půlročního charakteru, rozesílaného orgánům veřejné správy. Ty by byly přebírány lokálními osobami pověřenými touto problematikou, jejichž úkolem by bylo postoupit tyto informace níže. Dále jeho náplní budou výjezdní návštěvy jednotlivých expozitur veřejné správy a místní vzdělávání.

Místní vzdělávání může centrální pracovník poskytovat samozřejmě pouze všeobecně, místní záležitosti by vždycky musel doučit lokální zaměstnanec a místních podmínek znalý odborník. Ale vnější host přinese novinky, vnější pohled a také minimálně zpestření pro posluchače. Mj. návštěvy externisty z centrálního úřadu by mohly být použity jako prostor a platforma ke konzultační činnosti místních bezpečnostních opatření. Dále také tím, že tento odborník z centrálního úřadu bude navštěvovat dílčí úřady, stane se tak osobou, mající možnost kvalifikovaně, na místě a s lidmi kterých se to týká, si uceleně vytvořit představu o momentální situaci napříč stavem informačních systémů ve veřejné správě České republiky. To bude velmi zásadní přidaná hodnota, která umožní účinně reagovat na nadcházející nebo očekávané problémy například zákonnými nebo podzákonnými úpravami legislativy a vyhlášek.

Výhodou tohoto centrálního řešení je také, že ušetří práci a náklady jednotlivým dílčím organizacím, které by každá musely vynakládat personální náklady na zpracování totožného. V neposlední řadě, specializací této činnosti bude možno dosáhnout kvalitnějších výsledků.

Obdobné řešení v určitém modelu již funguje, nicméně nepokrývá veřejnou správu v takto důsledném modelu. Například v resortu obrany ČR je, kromě několika pozic bezpečnostních manažerů a bezpečnostních architektů, již vytvořena samostatná pozice manažera pro školení, který řídí vzdělávání a provádí konzultace a organizuje a řídí přípravu pracovníků a uživatelů systémů KIS. (Lukáš, Hrůza a Kný, 2008, s. 99, 198)

Může se jednat na první pohled pro tuto pozici o jednoduchý cíl, nicméně s velmi složitým úkolem, který vyžaduje vysoké úsilí. Jeho úkolem bude pracovníkům pravidelně a srozumitelně vysvětlovat bezpečnostní principy a pravidla a seznamovat je s novými bezpečnostními riziky tak, aby byli schopni správně reagovat na situace, které základní dokumentace nepostihuje. Dále bude s nimi projednávat bezpečnostní incidenty, rozebírat jejich

příčiny a skutečné i potenciální následky a obdobná rizika. Jedině právě důkladným vzděláváním a systematickou komunikací s pracovníky bude možné zajistit odolnost i nejslabšího článku v pomyslném řetězu. (Doucek, 2011, s. 106)

Z pohledu této navrhované pracovní pozice jde také dozajista o nastavení určitého kvalitního komunikačního kanálu, mezi zaměstnanci veřejné správy. Vzdělávací platforma je toho vhodným nejen počátečním, ale i průběžným prostředkem.

Smyslem a cílem vytvoření této pozice je odstranění souběžného výkonu stejných činností na různých institucích veřejné správy a přispění tak ke snížení nákladů.

4.5.2 Kvalifikace a vlastnosti určených osob a poradce pro IS VS

Při výběru určené osoby v instituci veřejné správy, tedy osoby, která bude vykonávat agendu bezpečnostního vzdělávání v dané instituci, je potřeba zvolit takového zaměstnance, který má přesvědčivé a kvalitní komunikační schopnosti (Tipton a Krause, 2007, s. 546). Sice výborný, vzdělaný a orientovaný odborník, který ale není obdařen schopnostmi kvalitní reprezentace, prezentace a komunikace svůj úkol nebude schopen kvalitně splnit. Musí to být jedinec, který dokáže zaujmout posluchače. Možností je také nasadit dva prezentující. Jednoho, lépe komunikujícího, a druhého, více zkušeného, erudovaného v bezpečnostní oblasti, který bude schopen například zodpovídat otázky nebo vést diskusní část školení. Nicméně toto řešení již není tak nákladově zajímavé a nelze ho doporučit.

Problémem dnešní doby je také takzvaná politická mluva, kdy se mluví obsáhle, nikoli konkrétně. V průběhu školení by se měla pověřená osoba tomuto důsledně vyvarovat, mělo by se mluvit na příkladech, názorně ilustrovat.

Její role, by měla směřovat spíše od role školitele a instruktora k roli jakéhosi tutora, možná až mentora pro oblast bezpečnosti dat a informací v dané instituci. Mnoho lidí má například problémy se samotnou výpočetní technikou, ale není to proto, že by byly takříkajíc nespisovně řečeno hloupí. Jde spíše o to, že neměli prostor se zeptat, prostě problematiku jim nikdo dostatečně nevysvětlil, nebyl jim dán prostor pro individuální dotazy. Role někoho, kdy by byl otevřený, sdílný k zodpovězení dotazů by byla přínosnou pro celou instituci. Je to určitě funkční a prospěšné řešení, neboť z praxe je známo, že pokud zaměstnanci řeší určité problémy nebo nevědomosti mezi sebou, vzniká kolektivní atmosféra nevědomí a vzniká také prostor, kdy může být předepsaný postup, kterému nikdo nerozumí, později

nahrazen snazším, vlastním, avšak ne vždy také korespondujícím s bezpečnostními pravidly organizace.

Poradce pro informační systémy veřejné správy a ustanovení této nově vzniknutivší pozice musí jít v mezích právních předpisů. Dle zákona č. 312/2002 Sb. o úřednících územních samosprávných celků (Česko, 2002), může poskytovat vzdělávání pouze akreditovaná právnická nebo fyzická osoba nebo akreditovaný územně samosprávný celek či příspěvková organizace Ministerstva vnitra. Takováto organizace zřízená ministerstvem již existuje, pod názvem Institut pro veřejnou správu Praha. Institut je právě státní příspěvkovou organizací zřízenou Ministerstvem vnitra. Jedná se o orgán veřejné správy, který „metodicky řídí a koordinuje oblast zvláštních odborných způsobilostí jako kvalifikačního předpokladu pro výkon státní správy v přenesené působnosti“ (IVSP, 2013). Nabízí vzdělávání zaměstnancům veřejné správy ve 31 odborných správních činnostech, manažerských činnostech, ale také etice a nabízí relativně široké portfolio tematických kurzů. Nabízí i kurz pro základní pedagogickou činnost lektorů. Ten by mohl být využitelný pro trénink určených osob. Nicméně i přesto obsahuje nabídka Institutu výraznou mezeru právě v oblasti zajištění personální bezpečnosti dat a informací. Nejblíže tomuto tématu je jen jediný poskytovaný kurz, zaměřující se na všeobecný výklad zákona o utajovaných skutečnostech a administrativní bezpečnosti ochrany utajovaných skutečností. Nenabízí však žádné další ani hlubší vzdělávání ve směru, jaký prezentuje tato práce. Tato práce tedy vhodně doplňuje mezeru na trhu vzdělávání zaměstnanců veřejné správy.

Navrhovaná pozice by mohla mít, na základě výše uvedeného zákona, podobu nového akreditovaného subjektu, nebo by mohla být teoreticky začleněna pod výše zmiňovaný Institut pro veřejnou správu Praha a využít tak úspor z rozsahu.

4.5.3 Bulletin bezpečnosti veřejné správy

Navrhovaný bulletin by plnit úlohu jednosměrného komunikačního kanálu, kterým by byly předávány aktuální informace, trendy a poznatky ve směru od pozice poradce pro informační systémy veřejné správy směrem ke všem institucím veřejné správy. Vzhledem k tomu, že bulletin by byl distribuován elektronickou formou, nebyl by problém, rozesílat ho na takovéto velké množství míst. Jeho periodicita by byla v počátcích jednou až dvakrát ročně, eventuálně dle potřeby. Jednalo by se vždy o jedno vydání, psané stručně, jasně a výstižně. Byl by vždy jeden, ač například Doucek (2011, s. 105) oproti tomuto uvádí, že je spíše vhodné dělit bulletiny nebo příručky dle různých cílových skupin, aby se nesta-

lo, že informace potřebné například pro správce systému, nezahltí běžné uživatele. Je potřeba si ale uvědomit, že navrhovaný bulletin v této podobě bude rozesílán sice do všech institucí, ale do rukou určené osoby. Ta v ideálním případě přijatý bulletin prostuduje a vytvoří z něj výstupy, použitelné pro danou konkrétní instituci, a tyto výstupy bude pak dále prezentovat v instituci. Nebylo by totiž možné, aby z jednoho centrálního místa byl vytvářen bulletin pro všechny základní zaměstnance a tento bulletin byl zároveň dobře cílený, vzhledem k velkému množství a různým charakterům veřejnosprávních institucí.

Z výstupů práce poradce pro informační systémy veřejné správy by se dala vytvořit i elektronická prezentace, poskytující jakési on-line rady, a na které by mohly být více do detailu rozváděny detaily obsažené v bulletinu. Takto dostupné rady by byly dobře dostupné a mohly by poskytnout oporu zaměstnancům veřejné správy. Tuto ideu snadné dostupnosti rad podporuje i Doseděl (2004, s. 181). V počátcích by se jednalo spíše o intranetovou prezentaci, protože ač by se nejednalo o žádné utajované skutečnosti, možná by nemuselo být vhodné publikovat některé informace veřejně. Nicméně z těchto informací by se dal také později vytvořit výstup, vhodný nikoli cíleně jen pro zaměstnance veřejné správy, ale i pro běžné občany, čímž by došlo také k ještě lepšímu využití veřejných zdrojů. Takové tendence lze již dnes vysledovat z podnikové sféry určitých společností.

4.5.4 Další aspekty organizace vzdělávání

Obsah a formu vzdělávání bude nutné po určité době aktualizovat a také přizpůsobit zjištěná rizika R1 až R5 budoucím podmínkám. Je možné, že některé ze současných identifikovaných rizik přetrvají i déle do budoucnosti, nicméně lze očekávat, že tak jak některé pominout, objeví se i nová a naléhavější rizika, na která bude potřeba reagovat a poskytovat o nich odborné informace zaměstnancům veřejné správy. Lukáš, Hrůza a Kný (2008, s. 184) navrhují v oblasti bezpečnosti provádět každých 5 let celkovou hlubokou revizi, při které se bude zjišťovat, jak se změnily podmínky v informačních systémech, technologiích a zabezpečení dat a informací. Průběžné sledování vývoje trendů však poskytne včasnou aktualizaci i dříve, před tímto termínem.

Doplňkovým návrhem je možnost výstupního školení, které by poskytovalo informace, jak se chovat s nabytými informacemi a zkušenostmi, které si s sebou odnášejí zaměstnanci při přechodu do nového zaměstnání. Smyslem by bylo poskytnutí zjevných mantinelů, aby nebyly ohroženy informace z veřejnosprávní instituce, ale zároveň, aby mohli využít zkušenosti, které se za dobu svého působení naučili. Spíše by se jednalo o definování toho,

co je považováno za důvěrné a co nikoli. Ale tento návrh je spíše potřeba vnímat jako velmi doplňkový, nepovinný a založený pouze na bázi dobrovolnosti.

4.5.5 Ověřování vzdělávání

Podstatné je také přizpůsobení celého školení na míru posluchačům, respektive přesnost a jasnost je potřeba formulovat dle chápavosti příjemců a nejlépe ještě na školení si, drobnými dotazy ověřit, zda posluchači skutečně rozuměli sdělovanému tématu. A právě vzhledem k možnostem rozdílného chápání a vnímání prezentovaných materiálů na vzdělávacích cyklech, by bylo vhodné také určitým způsobem přistoupit k ověření a zpětné vazbě, zda dané vzdělávání bylo dobře koncipované a vhodně na míru konkrétním posluchačům připravené. Nabízí se možnosti testového ověření znalostí. V písemné nebo digitální podobě, obojí má své výhody i nevýhody. Avšak je tu riziko, že poté by se celý vzdělávací systém, z pohledu posluchačů, zúžil pouze do roviny vnímání toho, zda uspějí v závěrečném testu či nikoli a byla by výrazně omezena jakákoli přidaná hodnota systému vzdělávání, práce s kulturou a vlastní motivací. Nelze proto systém testování doporučit. Namísto by bylo vhodnější, přistoupit k prostému kladení dotazů ze strany lektora, dotazování, rozvinutí diskuze, ze které by šikovný lektor poznal, zda jeho posluchači porozuměli předkládanému a byl-li tedy celý vzdělávací prvek dobře koncipovaný. Takováto kontrola nepodá exaktní výsledky, ale o mnoho lépe přispěje k cíli edukace. Pokud by však z určitých důvodů bylo požadováno testové šetření, dalo by se přistoupit, jak uvádí Laucký (2006, s. 49), k možnosti ověřování například anonymním dotazníkem, zaslaným napříč zaměstnanci instituce. Takový by nevyvolával mezi zaměstnanci pocit nátlaku a nutnosti jeho úspěšného splnění a zároveň by poskytl číselné výsledky o úspěšnosti zaměstnanců v jeho vyplňování.

Nicméně lze důrazně doporučit, zakončit školení podpisem školeného, například do podoby docházkového listu. Nebo přijetí elektronického dokumentu, bulletinu, potvrzením o přijetí. Toto do budoucna výrazně omezí výmluvy na neinformovanost o daném problému, na to, že daný zaměstnanec, nebo pověřená osoba nevěděla o dané skutečnosti či o tom, že je potřeba nějakým způsobem jednat či se zdržet jednání.

4.6 Doplňkové aspekty navyšování bezpečnosti dat a informací formou vzdělávání pracovníků

4.6.1 Vzdělávání pracovníků jako součást preventivních opatření

Vzdělávání pracovníků pomáhá navyšování bezpečnosti dat a informací i z pohledu preventivního. Prevence jsou „veškeré aktivity směřující k předcházení vzniku bezpečnostních rizik“ (Brabec, 2001, s. 35) a vzdělávání pracovníků přesně takovouto úlohu plní a patří tak do kategorie preventivních opatření. (Laucký, 2004, s. 7; Brabec, 2001, s. 140) Pomáhá předcházet jednak neúmyslným činům, ale také tím, že navyšuje obezřetnost zaměstnanců, pomáhá tak eliminovat i potenciální vnější úmyslné hrozby.

Avšak je potřeba dodat, že Doucek (2011, s. 11) uvádí, že například všeobecná prevence na širokou společnost, prevence a osvěta o správném chování v digitálním prostředí, na širokou společnost moc nepomáhá. Jde o to, že lidé si nebezpečí v digitálním prostoru zatím příliš neuvědomují a skutečným rizikům, problematice systémů a skrytým hrozbám, rozumí a uvědomuje si je jen malá skupinka osob. Toto všeobecné vnímání je potřeba, aby ho prezentovaný systém vzdělávání překročil za pomoci prezentovaných nástrojů. Kladným a motivačním prvkem, sjednocujícím tématem pro vzdělávání zaměstnanců, je právě jejich poslání, výkon veřejné služby, který, na rozdíl od zmíněné široké společnosti, může působit jako výkonný motivátor k uvědomění si prezentovaných skutečností.

4.6.2 Tvorba školení jako samotné vzdělávání

Příprava vzdělávání, přebírání informací určenými pracovníky, jejich další sběr informací z internetového výzkumu, odběry odborné literatury a článků, sdílení informací mezi institucemi veřejné správy, jejich členství v odborných institucích, výzkumných útvarech a podobně, je pro určené zaměstnance i jakousi výzvou, motivací a nutností aktualizovat své vlastní vědomosti a to i tak více do hloubky, aby byli připraveni odpovídat potenciální dotazy běžných zaměstnanců. I v tomto lze spatřovat přínos bezpečnostních školení, v podobě jakéhosi i zpětného vzdělávání.

Tipton a Krause (2007, s. 601) dodávají, že je nejenom důležité, poskytovat potřebné bezpečnostní informace a vědomosti personálu, ale je také potřeba, aby kromě poskytnutí těchto možností byly pro personál vytvořeny odpovídající podmínky. Aby personál byl motivován všeobecně k pracovnímu výkonu a bezpečnostní ostražitosti a také motivován setrvat v dané organizaci. Toto je záležitostí spíše pro oddělení lidských zdrojů. Lze sou-

hlasit, že nebylo by vhodné, investovat peníze jednak do všeobecného vzdělávání a především školení určeného bezpečnostního personálu a nechat ho brzy odejít za lepším zaměstnáním. Odpovídající plat, prostředí, jsou jedněmi z podmiňujících faktorů setrvání v zaměstnání. Toto opět může navyšovat výdaje organizace, nicméně, vzhledem k tomu, že veřejná správa operuje s daty občanů celého státu, jeho právnických subjektů a mnohých dalších, právě oblast bezpečnosti není oblastí, kde by bylo vhodné jakkoli šetřit nebo právě začínat s razantnějšími úsporami a šetřením. Lukáš, Hrůza a Kný (2008, s. 8) k tomuto dodávají, že personální útvary by měly působit i při zvyšování kvalifikace a rozvoje pracovníků a tato možnost, a role personálních útvarů, byla již diskutována v předchozích kapitolách.

4.6.3 Výměna informací, komunita

Přínosné se jeví i snahy o budování jakési bezpečnostní komunity napříč institucemi veřejné správy, jejímž cílem je výměna informací, poznatků a zpráv o aktuálním dění. Určení pracovníci, nejen že by byli určeni k přebírání zpráv z bulletinu, ale jejich cílem by bylo se i dále samostatně vzdělávat a tyto informace předávat nejen zaměstnancům své domovské organizace, ale bylo by i vhodné, pokud by se právě aktivně zapojovali i do předávání poznatků mezi jednotlivými institucemi navzájem a i zpět, k poradci pro informační systém veřejné správy. Toto může být řešeno formou textových hromadných konferenčních skupin v digitálním prostoru, telefonickými rozhovory nebo využitím osobních setkání a i Laucký (2006, s. 43) dodává, že právě vzájemná výměna informací je to, co posiluje celou komunitu. Tím se dále podpoří také zpětná vazba o prováděných činnostech, nových hrozbách a jejich hodnocení (Paleček, 2006, s. 39). Tím že se umožní otevřená spolupráce a sdílení informací o případných bezpečnostních incidentech, vznikne tak efektivní monitoring rizik napříč institucemi veřejné správy.

Proto i v této práci představovaný návrh vzdělávání, tak jak je navrhovaný, podporuje výměnu informací, klade na ni důraz a považuje ji za přínosnou napříč institucemi veřejné správy. Tento koncept a podpora výměny informací celkově kvalitně zapadá a jde souběžně i se známými zahraničními koncepty best practices a awareness programů.

4.6.4 Audit, vnější poradenství

Při realizování aktivit spojených se zajišťováním bezpečnosti dat a informací ve veřejné správě, lze přistoupit i ke kroku, v rámci kterého budou přizváni vnější specialisté k vyko-

nání některých kroků. Může se jednat o audit, konzultace a další. Možnost vnějšího bezpečnostního poradenství připouští i Ivanka (2009, s. 50) a zmiňuje především vhodnost těchto kroků pro poskytnutí poradenství v oboru bezpečnosti nebo pro tvorbu bezpečnostních analýz a auditů. Právě u bezpečnostního auditu je vhodné, pokud je proveden osobou schopnou přistoupit k problematice z vnějšího úhlu pohledu a toto obdobné, platí i pro bezpečnostní konzultace, využitelné i například při tvorbě koncepcí pro bezpečnostní vzdělávání.

Právě audit je „systematický, nezávislý a dokumentovatelný proces získání důkazů a jejich hodnocení s cílem stanovit rozsah splnění kritérií“ a „audit představuje v určitém pojetí také vyšší úroveň zpětné vazby“ (Doucek, 2011, s. 174). Především poskytnutí zpětné vazby je nadmíru důležité, neboť jejím výsledkem může být stanovení možných bodů, které mohou narušovat bezpečnost dat a informací (Čandík, 2004, s. 10). Na tyto identifikované body může poté opět navázat program koncepce bezpečnostního vzdělávání a zajistit přispění k jejich eliminaci (Lidinský, 2008, s. 80; Ivanka, 2009b, s. 60).

Tipton a Krause (2007, s. 601) stanovují, že právě auditní služby je vhodné outsourcovat. Ale je základem, pro outsourcing bezpečnostních služeb, nastavení silného vztahu mezi subjekty a důsledná právní dokumentace tohoto vztahu, definovaných práv a povinností smluvních stran. Kvalitní právní ošetření, především pro outsourcing v rámci ochrany bezpečnosti dat a informací, je klíčové.

Doucek (2011, s. 135) k outsourcingu bezpečnosti informací dodává, že je nutné pro jeho implementování zvážit, která data, aktiva, přijmutím tohoto opatření budou svěřena vnějšímu subjektu a zda je takovéto riziko pro instituci účelné. Outsourcing je kromě cesty za kvalitnějšími výsledky také cestou mimo jiné právě ke snížení nákladů, a jak bylo zmíněno, není vhodné vždy dosahovat snížení nákladů za každou cenu. Především ne v bezpečnosti dat a informací ve veřejné správě. Proto musejí být vnější subjekty vybírány ke spolupráci na zajištění bezpečnosti s obzvláštní obezřetností a je vhodné je při vykonávání jejich činností vnímat z hlediska potenciálního rizika jako vlastní zaměstnance. (Požár, 2005, s. 60, 75)

Přizvání vnějších osob, konzultantů má výhodu v tom, že tyto osoby jsou schopné přinést do instituce „kritické smýšlení a zaměření na cíl“ (Norman, 2010, s. 53), které se může po nějakém čase z vlastních zaměstnanců vytratit. Interní pracovníci mají významné výhody ve znalosti prostředí organizace, znají důvěrně její chod, ale i díky tomu mohou trpět

určitým zkreslením a problémem nedostatku schopnosti pohledu na problém tzv. out of the box. Z vnějšího úhlu pohledu. A právě návštěva a konzultace nebo vykonání určitých činností ze strany externistů, může vrátit vlastní zaměstnance zpět na původní pozici kritického hodnotitele, schopného dívat se na problematiku z více úhlů a pokusit se získat odpovědi na klíčové otázky, dříve přehlédnutelnými, jednoduchými odpověďmi. Externí konzultanti a experti mohu nabídnout pohled na chod organizace z vnějších úhlů, mohou poskytnout informace a varování nad nedostatky nebo před novými hrozbami, která by vlastní zaměstnanci mohli přehlédnout a dále mohou přinést zkušenosti z ostatních organizací. Tedy mohou nabídnout i porovnání, best practices. Mají výhodu pohledu na věc out of the box. Jejich slabinou může být však právě nižší znalost chodu organizace a předmětu jejích činností. (Doucek, 2011, s. 131)

Pro oblast veřejné správy nemusejí být konzultanty externisté pouze ze soukromé sféry, i když mohou, ale může se jednat i o meziresortní výpomoci nebo výměny zaměstnanců napříč institucemi veřejné správy.

Využití schopností konzultantů uvnitř veřejné správy řeší i jednu ožehavou otázku, spojenou s outsourcingem. Tou je existence vědomostí, které by měly zůstat pouze uvnitř organizace a bylo by je tedy nevhodno je jakkoli dále šířit. Může se jednat i u veřejné správy částečně o jisté vnitroorganizační know-how, které je ale spíše aplikovatelné pro soukromou sféru. Vzhledem i k požadavku na otevřenost veřejné správy. Na druhou stranu, i zajišťování konzultantských potřeb uvnitř veřejné správy s sebou nese riziko, že veřejná správa jako celek nebude schopna se na sebe a svojí činnost podívat z vnějšího pohledu a opět ustrne v určitém bodě.

Vytvoření pozice poradce pro informační systémy veřejné správy umožní, pokud bude potřeba přijmout určitého odborníka, aby byl najat na této úrovni a jeho znalosti šířeny navrhovaným konceptem dále. To přispěje k úspoře výdajů a celkovému snížení nákladů na výdaje fungování veřejné správy a k dalšímu zajištění bezpečnosti dat a informací ve veřejné správě.

I vzhledem k právě zachování si určitého nadhledu, kritického myšlení a pohledu out of the box, bylo by vhodné, určené zaměstnance, včetně poradce pro informační systémy veřejné správy, po určitém čase obměňovat. Vhodným by se mohl jevit běžný manažerský cyklus, tedy rozmezí 3 až 5 let.

4.7 Rizika

Tím, že se v rámci tohoto představovaného konceptu nejedná o nastavování nových pravidel, neočekává se komplikace v oblasti ztížení výkonu profese. S realizací jsou spojeny náklady spojené s personálním a materiálním zajištěním, ale také náklady ušlého zisku na odbavení klientů v čase, kdy budou zaměstnanci na školení. Situace je ztížená, jak již bylo zmíněno, problémem stanovení hodnoty chráněných aktiv a tedy nelze provést exaktní vypočtení poměru nákladů a úspor. Z tohoto pohledu se školení může zdát těžko obhajitelné, nicméně je potřeba brát na vědomí, že bezpečnost nesmí jít na úkor úspor a v žádném případě tak ve veřejné správě. Minimálně lze v základu vycházet z platnosti Paretova pravidla, že 20 % nákladů při správném použití přinese 80 % kýženého efektu.

4.7.1 Strengths – Weaknesses – Opportunities – Threats analýza

Tato SWOT analýza reflektuje silné a slabé stránky postavení veřejné správy a identifikuje hrozby a příležitosti ve vnějším prostředí, která by mohla dále do budoucna ovlivnit postavení bezpečnosti dat a informací ve veřejné správě.

Strengths. Mezi silné stránky lze řadit: silné zázemí celého veřejného sektoru, projevující se dobrou strukturu, rozdělení kompetencí a pravomocí, systém řízení, odborné kvalifikace pracovníků, relativní nezávislost na ekonomickém vývoji hospodářského prostředí v zemi a ve světě.

Weaknesses, slabé stránky: fluktuace zaměstnanců, stážistů, nedostatek financí z veřejného rozpočtu, potenciální, přetrvávající neuvědomění si důležitosti odpovídající bezpečnosti a kultury organizace, neudržení tempa s bezpečnostními trendy, s tím související nižší aktuální bezpečnostní povědomí, velký objem a citlivost spravovaných dat, experti veřejné správy mohou odejít do lépe placených soukromých působišť, relativní rezistence k novým přístupům, metodám a procesům, povšechní a nekonkrétní koncepce dokumentů, neexistence osobní odpovědnosti.

Opportunities, příležitosti: posílení společenského postavení, prestiže a vnímání veřejné správy a jejího výkonu napříč společností, zlepšení hospodářského postavení státu díky efektivnějšímu výkonu veřejné správy, pozitivní přístup občanů České republiky, změny zákonů k lepšímu, dotace z fondů EU, mezinárodní spolupráce.

Threats, hrozby: velmi rychlý vývoj technologií a zdrojová náročnost na udržení tohoto tempa, špatný hospodářský vývoj státu a jeho makroekonomické prostředí, které bude vy-

tvářet tlak na další výrazné úspory ve VS, snižování popularity výkonu zaměstnání ve VS, pokles zájmu a loajality zaměstnanců, zájem soukromých firem na odvedení kvalitních zaměstnanců, zvýšený zájem o citlivá data, hrozba terorismu, pokles národní morálky a úcty k VS, změny zákonů k horšímu.

4.7.2 Analýza rizik projektu

Mezi rizika implementace projektu patří především potenciální nezájem ze strany veřejné správy. Nemusí mít zájem daný koncept implementovat a uvést do praxe, nebo jí může připadat zbytečný či duplicitní. Vše souvisí s neuvědoměním si významu bezpečnosti dat a informací. Náklady a složitost implementace se při neodborném posouzení mohou zdát jako vysoké, nicméně v porovnání s možnými úsporami je zde jednoznačný benefit kladný.

Kromě nezájmu, neochoty a neuvědomění si přínosu projektu, může být dalšími riziky neschopnost zvolit si určenou osobu, vymlouvání se na nákladovou náročnost v podobě jejího času, především v menších institucích.

Nezájem platí v případě dobrovolnosti. Pokud by byla přijata zákonná či podzákonná úprava, povinně upravující problematiku personální bezpečnosti dat a informací ve veřejné správě, v rozsahu či období tohoto konceptu, byla by jejich činnost povinná. Ve smyslu této práce se předpokládá, vzhledem k chybějící právní úpravě, že instituce se na projektu účastní dobrovolně. Právě s tímto povětšinou souvisí předchozí rizika. Pokud by byla přijata právní úprava a byla by povinnost účastnit se povinně, převážná část výše uvedených rizik by byla nerelevantních.

Mezi dílčí rizika dále patří neochota zaměstnanců účastnit se aktivně na sebevzdělávacím procesu. Zde je potřeba, aby samotné vedení šlo příkladem, nicméně i jemu může bránit ještě relativně všeobecně „nízký statut bezpečnostního personálu“ (Paleček, 2006, s. 33), daný relativně povšechně zakořeněnou představou nepotřebnosti zabývat se bezpečností dat a informací na všech úrovních organizace, mimo správcovské, včetně základních.

Klíčovým prvkem pro implementaci projektu je vytvoření hierarchické podpory shora. Podpory shora od vedení. Je důležité, aby prosazování určitých řešení, přístupu k bezpečnosti dat a informací, bylo podporováno a prosazováno z nejvyšších pater vedení organizace, respektive také z nejvyšších pater struktur uspořádání veřejné správy. Nejlépe podložených právní úpravou.

„Je důležité, aby zavázání se k určitým standardům bezpečnosti informací (ať již jakkoli z vnějšku standardizovaným nebo vnitřně ustanoveným) bylo podporováno a prosazováno z nejvyšších pater vedení organizace. Mělo by to znamenat, že vedení by mělo být nejen odpovědné za schválení potřebných kroků, opatření, směrnic a školení, ale že samo vedení by také mělo být povinno se všemi nastavenými pravidly důsledně řídit. Jenom takto je možno celé organizaci jasně ukázat, že bezpečnost informací je důležitou součástí kultury organizace a že i samo vedení považuje vydaná pravidla za správná, účelná a efektivní." (Doucek, 2011, s. 127) Toto je, dle výše citovaného autora, nenahraditelný příklad, kterým je jasně ukazováno, že přijatá pravidla jsou správná a že ten kdo je přijal, jim důvěřuje a postupuje podle nich. Tento princip je aplikovatelný ve vlastních institucích, v rovině zaměstnanci – vedení, ale také v celé hierarchii zřízení veřejné správy, v rovině dílčích institucí – a řídících orgánů. Právě tím, že budou určitá opatření k přístupu k bezpečnosti dat a informací, prosazována nejvyššími organizačními institucemi, přenesou se tyto aktivity do základních institucí veřejné správy, a dále, z jejich vedoucích zaměstnanců na úplně nejzákladnější zaměstnance veřejné správy. Právní ukotvení tomuto výrazně pomůže. (Doucek, 2011, s. 127)

Překážkou k tomuto může být, jak bylo uvedeno ve SWOT analýze, místy nedostatečná odpovědnost vedoucích pracovníků a také již zmíněný nízký statut bezpečnostního personálu (Paleček, 2006, s. 33), respektive slabé vnímání důležitosti bezpečnosti všeobecně. Proto je klíčové pro úspěch představovaného projektu mít podporu ze strany vedoucích institucí, vedení organizací a vedoucích zaměstnanců – to se projeví i ve vnímání mezi řadovými zaměstnanci (Tipton a Krause, 2007, s. 552). Tak bude dosaženo, za využití principu příkladu podpory shora, naplnění efektivity a účinnosti nejen tohoto projektu, ale všech vykonávaných činností v rámci veřejné správy zároveň s dosažením minimálních nákladů.

4.8 Nákladová náročnost realizace

4.8.1 Finanční, časové a personální prostředky

Tato kapitola nastiňuje základní rozsah odhadu časové, finanční a personální náročnosti realizace představovaného konceptu. Zabývá se pouze základním jádrovým nástinem náročnosti, neboť přesný a konkrétní propočet nákladové náročnosti realizace projektu vždy bude záviset na dané konkrétní situaci a instituci, která k realizaci přistoupí a na jejích

konkrétních podmínkách a podobě realizace projektu, pro kterou se rozhodne. Nákladová náročnost představovaného projektu má dvě fáze.

I. Samostatné vzdělávání v rámci navržených témat

Personální náklady zajišťují vlastní zaměstnanci úřadu v rámci výkonu své pracovní doby. Pouze u větších institucí by se mohlo projevit, že je potřeba speciální osoby, nicméně předpokladem je, že by si měl vystačit dedikovaný pracovník. K jeho časové náročnosti, zmíněna jsou pouze tato nová školení, není brán v potaz jejich stávající systém vstupních školení, které má každá instituce dle sebe organizované.

Povede 1x za půl roku hlavní bezpečnostní školení zaměstnanců. Na přípravu školení a vlastní vzdělávání, zároveň za pomoci materiálů poskytnutých poradcem pro IS VS, lze čas na sebevzdělávání snížit a započítat 0,5 dne/4 hod. měsíčně (při předpokladu 8hodinové pracovní doby), tedy 3 dny/24 hod. za půl roku.

Je potřeba počítat také s časem, stráveným na konzultačním školení s nadřízeným poradcem pro IS VS a obdobně na konzultačních školeních s dalšími podřízenými pracovišti a institucemi, jsou-li. Jedná se výhledově o 0,5 dne/4 hod. + 0,5 dne/4 hod. půlročně, respektive 1 den/8 hod. + 1 den/8 hod. v případech některých, především menších institucí, kdy je potřeba počítat s vysláním tohoto zaměstnance, tedy časem potřebným k cestě, orientačně v rozsahu maximálně 4 hod. obousměrné cesty.

Časová náročnost navrhovaných aktivit vychází na 10 pracovních dní ročně, respektive 80 hodin ročně při pracovní době 8 hod. denně. To je relativně velmi přijatelná časová a nákladová náročnost, vezmeme-li v potaz, že její služby, jsou nejen poskytovány dalším zaměstnancům celé dané instituce, ale především mohou mít na tuto instituci výrazně kladný bezpečnostní, potažmo ekonomický vliv.

Z času základních zaměstnanců, kteří budou školeni, je potřeba počítat 2–4 hodiny (včetně možného samostudia materiálů) z času každého zaměstnance, za půlrok. Tedy 4–8 hodin ročně. Opět, o poměru nákladů a potenciálních přínosů, platí výše uvedené.

Finanční náročnost se vyjádří jako hodinová náročnost vynásobená hodinovou odměnou zaměstnance, respektive jako ušlý zisk, v podobě nevykonané práce. Dále je potřeba započítat materiální zajištění, které nebude vyžadováno výrazně zvláštní.

Tab. 1. Časová náročnost.

pracovní den 8 hod.	měsíčně	půlročně	ročně
pověřený zaměstnanec	0,5 dne (4 hod.)	3 d. (24 h.) + 1 d. (8 h.) + 1 d. (8 h.)	10 dní (80 hod. při 8 hod. pracovní době)
řadový zaměstnanec		2 – 4 hod.	4 – 8 hod.

II. Aktivity Poradce pro informační systémy veřejné správy.

Poradce pro IS VS, zaštítěn zastřešující organizací, dojíždí školit a konzultovat do mateřských institucí veřejné správy, jakými jsou například kraje nebo další instituce veřejné správy. Tam školí a poskytuje konzultační činnost nejenom určenému pracovníkovi této organizace, ale i určeným pracovníkům dalších dílčích institucí. V tomto modelovém příkladě tedy například obcím s rozšířenou působností nebo dílčím expoziturám jiných úřadů veřejné správy. Tito určení pracovníci ORP, komunikují nasbírané zkušenosti a informace dále nejen ve svých domovských úřadech, ale i, v rámci příkladu obecního zřízení, dále do roviny základních obcí České republiky.

Názornou ilustraci vlastního mechanismu a realizovatelnosti tohoto rozvržení je možné provést například na obecním zřízení České republiky. Základních obcí České republiky je 6250, ORP 205 a krajů 14 (ČSÚ, 2012). Poradce dojíždí na 14 míst krajů, kde poskytuje svoje služby jednotlivým krajským určeným pracovníkům a určeným pracovníkům z ORP. Těch v průměru vychází 15 na kraj. Poradce tedy konzultuje a přednáší pro skupiny orientačně 16 osob. Obdobně tak určené osoby z ORP komunikují tyto nabyté vědomosti dále, do roviny základních obcí České republiky. Opět, v průměru vychází na jednoho určeného pracovníka z ORP orientačně 31 určených pracovníků základních obcí. Což je přijatelné číslo, srovnatelné s obvyklou velikostí tříd na středních školách. Díky tomuto navrhovanému systému je takto možno komunikovat bezpečnostní aktuality a informace ohledně zabezpečení dat a informací pro celé spektrum subjektů, v tomto případě 6250 obcí obecního zřízení. Obdobné schéma je aplikovatelné i na jiné instituce veřejné správy a jejich místní expozitury.

Časová náročnost pro poradce IS VS by byla jen pro tyto činnosti, při časové dotaci jednoho dne pro kraj, 14 pracovních dní půlročně a čas potřebný na přípravu. V této variantě se očekává, že poradcem poskytnuté informace budou hierarchicky, ve struktuře veřejné správy, komunikovány dále do nižších pater. Pokud by se ukázala tato varianta jako nefunkční, lze přistoupit k alternativní variantě, kdy bude poradce komunikovat napřímo i se základními jednotkami. Například na výše ilustrovaném obecním zřízení by to znamenalo potřebu komunikace se 6250 subjekty. Při možnosti setkání 30 osob a dvou prezentací denně, je časová náročnost této varianty 104 pracovních dní. Při předpokladu 252 pracovních dní v roce, je časová náročnost prezentací pod polovinou celkového pracovního času poradce. K tomu je však ještě potřeba připočítat i jiné subjekty veřejné správy, i mimo obecní zřízení a dá se předpokládat, že by větší čas pracovní doby poradce v této variantě tvořily právě prezentační činnosti. Byl by tedy většinu svého pracovního času na cestách.

Svůj zbývající čas, ať již podle varianty prvé nebo druhé, dále poradce věnuje také tvorbě informačního bulletinu, který v digitální podobě rozesílá všem jednotkám. Vzhledem k digitální podobě bulletinu jsou náklady na jeho šíření minimální. Zbývající pracovní čas věnuje sebevzdělávání, poradenské činnosti a jak již bylo zmíněno, přenosu těchto vědomostí do podoby informačního bulletinu.

Personálně je v základu tato pozice zajištěna jednou osobou. Pokud by bylo potřeba, lze přistoupit k rozšíření jeho pracovního týmu o další členy, ať již podpůrného nebo obdobně vzdělávacího charakteru. **Finanční** nároky lze vyjádřit jako odměnu tomuto zaměstnanci, respektive těmto zaměstnancům a dále je potřeba přičíst všechny potřebné provozní a režijní náklady spojené s výkonem jeho činností, včetně cestovních výdajů. Cestovní výdaje a zvýšenou časovou náročnost je také potřeba připočítat i ke kapitole I., ke všem dojíždějícím zaměstnancům. Časová náročnost věnovaná na dopravu může tvořit nárůst až 50 % základní časové náročnosti.

Výše uvedená kapitola rámcově ilustrovala předpokládané personální, časové a finanční náklady daného konceptu. Nákladový odhad byl proveden poctivě, avšak je možné ho prezentovat pouze takto všeobecně, neboť tak jak je představovaný projekt šablonou, podle které mohou cílové instituce postupovat – a upravovat si ji podle svých potřeb, tak i díky tomuto, nelze provést exaktní vyčíslení přesných nákladů. To vždy bude záležet na konkrétním pojetí a realizaci daném institucí veřejné správy. Nicméně uvedená kapitola nabídla dobrý přehled rámcové náročnosti prezentovaného konceptu a dá se uzavřít, že byla dosažena nákladová přiměřenost. Očekávané náklady na navýšení a udržení bezpečnosti dat

a informací, z pohledu personální problematiky, nepřevažují užitnou hodnotu a přínos, který předkládaný koncept může poskytnout.

4.9 Závěr a shrnutí projektu: Vzdělávání, proč je vhodné právě toto řešení?

Samotný koncept vzdělávání, jakožto cesty k navýšení bezpečnosti dat a informací skrz stránku personální bezpečnosti, byl zvolen po důkladném studiu dostupné odborné literatury. Ta z větší části potvrdila, že zvolený koncept je velmi vhodným řešením a sama ho doporučila.

Vzdělávání, průběžná realizace osvěty, jsou součástí řešení informační bezpečnosti (Požár, 2005, s. 99). Ministerstvo vnitra České republiky (2011, s. 5) definuje nedostatky současné veřejné správy, mezi kterými zmiňuje ve vybraných bodech a) vysokou míru rezistence vůči zavádění moderních metod řízení organizace, c) neexistenci standardizace jednotlivých procesních postupů a jako dílčí lze zmínit g) nedostatečnou komunikaci ústřední státní správy s územím či špatnou koordinaci komunikace, j) neexistenci osobní odpovědnosti. Bod a) souvisí s celkovou spíše pasivitou fungování určitých struktur, která se projevuje i do efektivity implementování bezpečnostních opatření, bod c) nezahrnuje pouze standardizaci bezpečnostních postupů, a v bodě j) je spatřováno jakési rozložení osobní zodpovědnosti, související právě i s v předchozích kapitolách rozebíraným mylným vnímáním, že informační bezpečnosti je sice něco, co je součástí organizace, ale netýká se jednotlivých zaměstnanců.

Dále je pro veřejnou správu stanovena povinnost se vzdělávat. Ta je zakotvena v zákoně číslo 312/2002 Sb. o úřednících územních samosprávných celků a o změně některých zákonů. (Česko, 2012)

Klíčovým slovem pro personální pojetí bezpečnosti dat a informací je slovo příprava. Je již přes šedesát let dle některých studií prokázáno, (Tipton a Krause, 2007, s. 2903), že pokud jsou osoby připraveny na to, co je může potkat, snáze se s danou situací vyrovnávají a kvalitněji jsou schopny na ní adekvátně reagovat. Jde jednak o lepší reakci s možností odvrácení probíhající události a také i o rychlejší eventuální post vyrovnání se s eventuálně proběhnutivším incidentem. Příprava v rámci vzdělávání je především silným nástrojem pro eliminaci rizik sociálního inženýrství. (Tipton a Krause, 2007, s. 2904) Zde především platí, že pokud zaměstnanci pochopí, o co v sociálním inženýrství jde, jaké používá

metody a jak probíhá, mohou se zaměstnanci lépe bránit a lépe tak ochránit aktiva instituce, pro kterou pracují.

Zde především je potřeba odvracet mylné vnímání, které panuje ve smyslu, že není potřeba znát principy fungování rizikových činností, aby bylo možno je odvrátit. Respektive jak lze parafrázovat „mylný je názor, že k tomu, abych uměl telefonovat, nepotřebuji přece znát, jak telefon funguje“ (Benda, Sodomka a Rosman, 2000, s. 8). V oblasti bezpečnosti toto není pravda. Je nutné pochopit principy, zákonitosti a na jejich znalosti budovat efektivní ochranu vlastních hodnot. Toto je důležité k pochopení a uvědomění si.

Velké procento zneužití dat mají na svědomí pracovníci vlastní organizace. Právě před nimi se dá i ochránit nejhůře. (Koch a Ondrák, 2008, s. 154) Zároveň jsou také zaměstnanci, jako nositelé znalostí, největší hodnotou společnosti a nejen rizikem, ale také klíčovým prvkem pro fungování a ochranu dat a informací (Tipton a Krause, 2007, s. 552). Lidský faktor je tedy stěžejním prvkem a to i proto, že pouze lidé mohou na základě dat vytvořit znalosti (Brabec, 2001, s. 203). A ani dokonale zabezpečený systém nezaručuje bezpečnost zcela s jistotou, i právě díky lidskému faktoru (Dobda, 1998, s. 47). Jak je názorně vidět, za nejvýznamnější rizika lze považovat především rizika, v nichž určitou úlohu hraje člověk. Posílením jeho pozice, vědomostí, znalostí a obezřetnosti bude možné dospět k posílení celkového ujištění bezpečnosti dat a informací v dané instituci.

Jak uvádí Strecková (2005, s. 9), ochrana dat a informací je ve veřejném zájmu a zvyšuje efektivnost prostředků vynaložených na fungování veřejné správy tím, že zamezuje ztrátám a tím i dalšímu navyšování nákladů. V předchozích kapitolách je dobře znázorněno, že navyšování bezpečnosti dat a informací zejména za pomoci personálního vzdělávání, je výbornou volbou. Jedná se o nejefektivnější způsob, v poměru nákladů a výkonu a to i přesto, že tento výkon nelze díky charakteru informací exaktně vyčíslit. Zvolením takového efektivního a hospodárného přístupu je dosahováno naplnění zásad 3E a dobré správy.

Avšak také z ekonomických, ale i praktických, hledisek není možné a ba ani žádoucí, chránit všechna data a informace stejným způsobem. Míru potřeby jejich ochrany definuje bezpečnostní politika. (Čandík, 2004, s. 11) Míra ochrany a použité kroky se mohou lišit dle charakteru a hodnoty daných dat a informací, aktiv, která je potřeba chránit (Jašek, 2006, s. 72).

Co se ekonomické výhodnosti daného řešení týká, určitě zde více než kde jinde platí Paretovo pravidlo, aneb tak jak 20 % všech událostí zapříčiní 80 % všech ztrát, tak 20 % úsilí a nákladů předejde 80 % potenciálních rizik (Paleček, 2006, s. 76). Vzdělávání má obrovský přidaný charakter, který uživatelům zůstane i dlouho po ukončení jejich pracovního poměru ve veřejné správě a dále tak pomáhá naplňovat sociální charakter státu. V neposlední řadě, současná technická řešení lze považovat za na relativně vyspělé úrovni, oproti tomu právě personální sféra je prostorem, kde je v současné době nejvíce možností ku dalšímu zlepšení a inovaci. Právě ve výše uvedených bodech je ukrýván velmi silný potenciál navrhovaného konceptu personálního zajištění bezpečnosti dat a informací v institucích veřejné správy.

4.9.1 Sociální aspekt vzdělávání pracovníků ve veřejné správě

Samotné vzdělávání pracovníků pomáhá k jejich lepšímu uplatnění uvnitř organizace, ale také celkově k lepšímu uplatnění na trhu práce. Veřejná správa, jakožto státní instituce sloužící občanům, by měla mít již přirozeně zájem na tom, aby, pokud bude muset propouštět své zaměstnance, aby tito zaměstnanci byli uplatnitelní na trhu práce a zapojili se do aktivního ekonomického života státu. Tedy vzdělávání zaměstnanců nepřináší pouze výhody veřejné správě jako zaměstnavateli, ale také celé společnosti, pro kterou veřejná správa vykonává svojí správu a to i poté, co již tito zaměstnanci v jejích řadách nepracují. Z pohledu zaměstnavatele, některých komerčních zaměstnavatelů především, se může zdát neperspektivní vzdělávat zaměstnance, kteří mají například brzy jít do důchodu, na mateřskou dovolenou nebo jsou absolventy a předpokládá se u nich větší zaměstnanecká fluktuace. Ale z pohledu zaměstnavatele ve veřejné správě je potřeba mít na paměti také sociální aspekty fungování státu. Vzděláváním zaměstnanců ve veřejné správě se nepřispívá pouze k samotnému lepšímu fungování veřejné správy, ale jejich vzdělávání umožňuje rozšiřování obzorů občanů, pro které veřejná správa slouží. A tedy i přes to, že ne vždy se takovéto vzdělávání musí zdát ekonomicky jako rentabilní, je dobré vzpomenout právě i na tento sociální aspekt výkonu veřejné správy. (Rosman, 2008, s. 19, 21)

4.10 Kolik bezpečnosti je dost?

Při pojednávání o bezpečnosti dat a informací je podstatné zároveň také myslet a zodpovídat si jednoduchou otázku. Kolik bezpečnosti je dost? Jde o to, aby v zájmu snahy o vytvoření bezpečného prostředí nebyla namísto dosažení tohoto cíle vytvořena pouze změť pra-

videl a opatření, která ve svém výsledku budou mnohdy i nebezpečnější než potenciální rizika. Ortmeier (2009, s. 140) nabízí pokládat si vždy otázku „je dané pravidlo opravdu potřeba?“. Mnoho pravidel v nepřehledném uspořádání vede dříve či později k jejich pozdějšímu ignorování, a to včetně těch užitečných.

Obdobně tak při vzdělávání. Je potřeba dodržet určitou přiměřenou hranici obsahu a srozumitelnosti školení. Aby nebyla, místo užitečného a efektivního přínosu posluchačům na obtíž a spíše než přínosem zdržováním od práce.

Aplikovaná opatření by měla být odůvodnitelná. A ne dražší než potenciální škody (Tipton a Krause, 2007, s. 581), nicméně toto neplatí pro všechny instituce veřejné správy, jak bylo rozebíráno. Lze však zdůraznit, že finanční aspekty by neměly být důvodem k omezování bezpečnosti. Nastavování bezpečnostních a personálně bezpečnostních opatření je o citu k přístupu a prosté univerzální aplikování best practices nebo standardů také není vhodným a vše řešícím řešením. (Tipton a Krause, 2007, s. 583) Je důležité se z pohledu zajištění bezpečnosti nedomnívat, že dostatečná implementace požadovaný bezpečnostních standardů a současné best practice, udělají dobrou práci a zajistí bezpečnost systému dat a informací. Ano, bezpečí přinesou, ale ne dostatečné. Standardy jsou kvalifikované požadavky, ale šité univerzální mírou. Každý podnik, každá veřejná instituce je unikátní a je proto potřeba, aby i implementace těchto standardů a best practices byla dále upravována dle jednotlivých potřeb, lokálních podmínek a požadavků instituce, proměnných v čase.

4.11 Nové a nadcházející rizikové fenomény

Jak bude situace vypadat v budoucnosti, je otázka spíše pro bezpečnostní futurologii. S jistotou lze snad jen tvrdit, že „budoucnost nabídne hodně prostoru pro bezpečnostní činnosti“ (Ortmeier, 2009, s. 353). Dá se předpokládat, že bude pokračovat již známý trend globalizace společnosti (Ortmeier, 2009, s. 354), se všemi jejími dopady na komunikační možnosti a i bezpečnostní rizika. Budoucnost by mohla díky komunikačním technologiím přinést silnější občanskou kontrolu, novou vlnu demokratizace ale také snadnější organizování protestů a nová nejen arabská jara. Ale zároveň i zvýšenou míru bezpečnostního rizika ze ztráty soukromí občanů. Svět se zrychluje a toto tempo by s ním měla udržovat i efektivní veřejná správa a její zabezpečení. Ta může z těchto procesů i těžit a využívat jejich výhody. Ty lze spatřovat v momentech právě určité provázanosti, kdy k prognózování pro území České republiky můžeme v rámci globalizace využít trendy, vysledované a podchycené v zahraničí.

Otázkou je, kam až toto bude směřovat. Jisté je, že získávání dat nabývá na hodnotě. Vznikají kompletní profily osob, obsahující jméno, e-mail, mobilní telefonní číslo, číslo kreditní karty a mnohé další, včetně fotografií a komunikačních partnerů, a tyto informace již nejsou jen doménou tajných služeb, ale vlastní je soukromé, obchodní a reklamní společnosti. A je na veřejné správě a zákonodárcích, aby se pokusili, alespoň částečně, dostat toto hromadění informací do určitého právního rámce. Kde je totiž hranice pro použití těchto informací a technologií pro nelegální aktivity? O to větší riziko je zde i pro veřejnou správu.

Veřejná správa bude pravděpodobně vždy z určité míry závislá na komerčních produktech. Je však jen na ní, jak spolehlivé partnery si k sobě vybere a jak bude jejich produktům důvěřovat. To samé platí o lidech, osobnostech, které budou veřejnou správu tvořit.

Dá se předpokládat, že kromě objevování nových hrozeb bude docházet k rozvoji již identifikovaných hrozeb. Studie společnost Deloitte (Deloitte, 2013) Technology, Media and Telecommunications Predictions 2013 předpovídá, že se v roce 2013 očekává až miliarda nových chytrých telefonů – tedy počítačů do kapsy. Bude potřeba se tedy skutečně odprostit od zastaralého vnímání, že mobilní telefon je něco hloupého, jiného než počítač. Bude tedy docházet k dalšímu postupnému srůstání mobilních a dříve stolních platforem, což odpovídá identifikovanému riziku R5. Zároveň se bude stále rozšiřovat připojení k mobilnímu internetu. Tedy možnost, být neustále online, připojen. Také v případě nedostatečného zabezpečení možnost být i sledován. Mluví se o internetu věcí (Vrba, 2013b), kdy předměty budou navzájem a s uživateli komunikovat. Tedy budou i monitorovatelné. Ale bude opět zajištěno, že budou monitorovatelné pouze oprávněnými subjekty? A oproti těmto komunikačním a technologickým možnostem se zároveň také očekává, že až 90 % všech hesel (Deloitte, 2013), ochraňujících přístup k těmto možnostem, bude z kategorie velmi jednoduchých, primitivních a snadno prolomitelných hesel. Bude tedy budoucnost výraznou příležitostí pro kriminalitu?

4.12 Digitální Česko 2.0

Vláda v současnosti podporuje elektronizaci společnosti i projektem Digitální Česko 2.0 (Česko, Vláda, 2013). Tento dokument, schválený v průběhu zpracovávání této práce, je pojatý jako státní politika cesty k digitální ekonomice. Nezabývá se přímo kriminalitou, snaží se podporovat informační technologie napříč společností. Samotný dokument pracuje s pojmy důvěra (v používání internetu), avšak nikoli hlouběji s pojmy bezpečnosti

(např. v používání internetu). Zmiňuje, že důvěra je důležitá až velmi klíčová při využívání služeb eGovernmentu, avšak jako politika, tento dokument zůstává pouze na všeobecné rovině a bezpečnost dále hlouběji nerozebírá a jen ji na několika místech zmiňuje. Právě jen heslovité zmínky o bezpečnosti lze letmo nalézt v úvodním manažerském shrnutí, kde je zdůrazněna „potřeba zajištění bezpečnosti a odolnosti ICT infrastruktur cestou zaměření na prevenci, připravenost a informovanost“ (Česko, Vláda, 2013). K problematice kybernetické bezpečnosti výše citovaný dokument dále zmiňuje, že si uvědomuje její důležitost, neboť se „společnost obecně stává závislejší na informačních a komunikačních technologiích“, avšak dále jen odkazuje na projednávaný návrh zákona o kybernetické bezpečnosti.

Tato politika se snaží podporovat využívání informací veřejného sektoru, kdy uvádí, že „subjekty veřejného sektoru vytvářejí, shromažďují nebo mají v držení velké množství informací“ (Česko, Vláda, 2013) a snaží se dále podporovat přístup občanů k dokumentům a výsledkům práce veřejného sektoru.

Politika obsahuje také překvapivě progresivní a správný přístup v části zmiňující model sociálních sítí. Toto je velmi správné a také koresponduje s jedním z definovaných klíčových problémů v této práci – problematikou používá služeb zdarma, placených z modelu poskytování reklamy. Politika zmiňuje tzv. „právo být zapomenut“, zejména při využívání sociálních sítí. Došlo k uvědomění si, a tato politika toto správně pojmenovává, že dnešní mladé generace občanů jsou provázeny informačními systémy již od narození a každý by měl mít právo, pokud se tak rozhodne, na výmaz svých osobních údajů ze sociálních sítí. Politika doslova vyjmenovává moment, kdy „uživatel působil na internetu v dětském věku, aniž by si byl v plném rozsahu vědom rizik spojených se zpracováním osobních údajů, a později chce tyto osobní údaje odstranit“ (Česko, Vláda, 2013). Mnohé sociální sítě obsahují totiž ve svých smluvních podmínkách ustanovení, že i poté, co je přestane uživatel užívat, mohou tyto platformy dále uchovávat a nakládat s daty jeho i dalších bývalých uživatelů, a to často po neomezeně dlouho dobu. Stát se proto bude, alespoň dle této politiky, snažit, legislativou regulovat tato jednání.

Stát prostřednictvím této politiky dále vyjadřuje podporu posilování digitální gramotnosti obyvatel České republiky, kdy mluví o tzv. e-skills, jakožto „znalostech informací potřebných ke kritickému hodnocení obsahu všech mediálních nástrojů v rámci aktivního občanství“ (Česko, Vláda, 2013). Opět však nikterak nepojednává o bezpečnosti. Zajímavě nabízí propojení informačních sítí, internetu s veřejnou správou, kdy přisuzuje internetu hodno-

tu a charakter veřejné služby. A jako k takové službě by se k ní měl stát chovat. Stát definuje, že spíše nebude zasahovat a nechá volný průběh vývoji a technologiím a bude hlídat pouze dodržování a prosazování vyjmenovaných hodnot, mezi kterými je například uvedené právo na zapomenutí.

V kontextu této práce a uvedené politiky, právě uvědomění a potřeba zaměření se na „prevenci, připravenost a informovanost“ (Česko, Vláda, 2013), může být využita jako výrazný prostor, právě pro kvalitní uplatnění projektu předkládaného v této práci.

ZÁVĚR

Práce jako celek propojila důkladné teoretické zázemí s rozsáhlým vlastním konceptem možnosti pojetí zajištění bezpečnosti dat a informací ve veřejné správě. Na teoretickém zázemí práce poukázala na aspekty probíhající digitalizace veřejné správy a pojednala o procesu probíhající digitalizace veřejné správy a společnosti. Na těchto teoretických podkladech práce dále analyticky definovala aktuální a klíčové rizikové body, aby na tyto definované body dále navázala ve své projektové části, kdy práce nabízí vlastní řešení v podobě velmi dobře udržitelného, ekonomického a realizovatelného konceptu pro uvedení do praxe. Je potřeba podotknout, že analytický výčet rizik však nelze, díky nebývalé rychlosti proměny rozebíraného prostředí, brát jako konečný, ale, jak již bylo několikrát zmíněno, je potřeba ho vnímat v kontextu roku 2013. Nicméně oproti tomuto, v praktické části práce uvedený, vlastní řešící nástin koncepce udržitelného bezpečnostního vzdělávání pracovníků veřejné správy, zpracovaný s ohledem na zásady 3E a dobré správy, nabízí přesah dlouhodobějšího horizontu, čímž naplňuje cíle práce. Práce jako celek odráží zadání práce a šířeji ho dále rozvádí.

Navyšování bezpečnosti dat a informací z personálního hlediska. Může se jednat, řečeno s nadsázkou, o trochu nevděčný úkol. Jedněmi je spatřován jako příliš zbytečný, snad až přehnaně starostlivý, druhými naopak jako velmi povšechní, nabízející jen velmi mlhavá řešení. Není tomu tak. Musíme si totiž důrazně uvědomit, že bezpečnostní opatření realizovaná skrz personální stránku bezpečnosti, zaváděná formou změny kultury, myšlení lidí, jejich motivace a jejich přístupu k bezpečnostní problematice a vlastní bezpečnosti, jsou zdlouhavým procesem, na který neexistuje jednoznačný recept. Může se tedy opravdu na první pohled jednat o relativně nevděčný, nicméně ve výsledku velmi podstatný úkol.

Nejvíce by k usnadnění této role a přístupu pomohlo, a všeobecné zkušenosti tak také ukazují, že k největšímu nárůstu péče o vlastní, zde nejen digitální informační bezpečí, dochází zpravidla po nějakém odstrašujícím incidentu. Ale zodpovězme si otázku – opravdu chceme na takový incident čekat, respektive, může si ho konkrétně veřejná správa dovolit?

Lidská společnost totiž touží po univerzálním pocitu bezpeční odjakživa, ale péče o svá data a informace je současně nechává chladnými. Neuvědomují si snad ona rizika? Právě tak jak pocit bezpečí a touha po bezpečnosti doprovázejí člověka od jeho počátků, tak právě dnes je digitální bezpečnost a počítačová gramotnost nedílnou součástí rozvoje společ-

nosti, její ekonomiky a kultury. Stává se tak součástí každodenního života a jako takovou, je proto potřeba ji reflektovat.

Tato prezentovaná práce by rozhodně neměla být chápána jako nějaký direktivní návod či kuchařka, jak se pomocí vzdělávání podaří každý informační systém automaticky zabezpečit a ošetřit a dosáhnout tak ideálního stavu zabezpečení dat a informací. Každý informační systém je v něčem odlišný a obdobně tak jeho správci a uživatelé. I každá instituce je odlišná a je tedy logické, že i opatření vedoucí k zabezpečení její bezpečnosti budou a měla by být odlišná. Avšak tato práce by měla přispět a sloužit jako základní rámec, východisko k pochopení důležitosti pojmu informační bezpečnosti, s důrazem na personální stránku problematiky a také naznačit možná uchopení tohoto problému a východiska při jeho řešení

Tento vypracovaný projekt je vytvořen jako všeobecný předpis, návrh, pro mnoho organizací veřejné správy, kterým dává možnost si na jeho základě vytvořit představu o svých individualizovaných potřebách a dle nich upravit zde předkládaný projekt. Je potřeba ale zdůraznit, že bezpečnostní vzdělávání *není všespasitelným lékem, izolovaným řešením, ale nedílnou a podstatnou součástí celého bezpečnostního systému. Součástí, která může výrazně přispět a která bývá často opomíjena.*

Taktéž je potřeba zhodnotit možnou neaktuálnost nabízeného řešení v čase. Všechna zde platná uvedená východiska jsou platná pro přelom let 2012 a 2013 a díky rychlosti vývoje technologického pokroku tomu tak v budoucnu nemusí vždy dogmaticky být. Je také potřeba zmínit, že jakékoli nekritické přebírání bezpečnostních vzorců může být obzvláště v oblasti bezpečnosti velmi problematické. Je proto potřeba k nabízenému podkladu přistupovat maximálně kriticky a tak z něj také vycházet. Jen tak poskytne cenný podklad k vlastnímu působení a kvalitnímu výkonu veřejné správy.

Je potřeba mít dále také neustále na paměti, jak již bylo zmíněno, že opatření musí býti jednoduchá. Pokud budou složitá, mohou být sama příčinou problémů a rizika.

Na některé v tomto textu uváděné jevy dosud nebyly publikovány relevantní vědecké práce a jedná se o dílčí novum. V tom lze spatřovat výraznou původnost práce a její přidanou hodnotu pro praxi.

Ústředním heslem, které by si měl čitatel odnést, je výměna informací a její podpora. To je silný nástroj posilování personální bezpečnosti dat a informací a navrhovaný koncept vzdělávání a daného specialisty je pevným nástrojem k podpoře těchto kroků.

Je potřeba také do budoucna počítat s neustálým vývojem v této oblasti a s novými a nadcházejícími rizikovými fenomény a být na budoucnost a nová rizika připraven.

Na závěr je potřeba připomenout, že pachatelé obvykle mívají náskok nejen před zákonem, ale i před bezpečnostními opatřeními. A to, čím může organizace přispět k navýšení bezpečnosti dat a informací je právě vytvoření silně motivovaného prostředí, ve kterém bude fungovat dobře nastavený systém zabezpečení. Ten bude postavený na dílčí odpovědnosti každého jednotlivého zaměstnance, který bude vzdělaný a kvalitně motivovaný. Jen tak dosáhne veřejná správa efektivity, plynulého výkonu státní správy a dostatečného zajištění bezpečnosti dat a informací.

A také mělo by být neustále na paměti, že dosažení 100% bezpečnosti je skutečně nereálné, nicméně neutuchající snahy o stálé dosažení co nejvyššího stupně bezpečnosti jsou důležité, prospěšné a žádoucí.

SEZNAM POUŽITÉ LITERATURY

ANDRESS, Jason a Russ ROGERS, 2011. *The basics of information security: understanding the fundamentals of InfoSec in theory and practice.* Amsterdam: Elsevier, xviii, 171 s. ISBN 978-1-59749-653-7.

BENDA, Radek, Petr SODOMKA a Pavel ROSMAN, 2000. *Informatika a výpočetní technika.* 2. vyd. Zlín: FaME VUT, 152 s. ISBN 8021415479.

BRABEC, František, 2001. *Bezpečnost pro firmu, úřad, občana.* Praha: Public History, 400 s. ISBN 80-86445-04-6.

BRABEC, František, 2009. *Technologie detektivních činností.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 160 s. ISBN 978-80-7318-780-4.

ČANDÍK, Marek, 2004. *Základy informační bezpečnosti.* Vyd. 1. Zlín: Univerzita Tomáše Bati, 107 s. ISBN 8073182181.

ČERNÝ, Josef, 2003. *Evropský výcvikový modul pro základní ostrahu.* Vyd. 1. Zlín: Univerzita Tomáše Bati, Fakulta technologická, 152 s. ISBN 80-7318-107-X

ČESKO, VLÁDA, 2013. *Digitální Česko v. 2.0: Cesta k digitální ekonomice* [online]. 67 s. [cit. 2013-03-21]. Dostupné z: http://www.vlada.cz/assets/media-centrum/aktualne/Digitalni-Cesko-v--2-0_120320.pdf

ČESKO, 2012. Zákon č. 89 ze dne 3. února 2012 občanský zákoník. In: *Sbírka zákonů České republiky.* 2012, částka 33, s. 1026-1365. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=6144

ČESKO, 2000. Zákon č. 101 ze dne 4. dubna 2000 o ochraně osobních údajů a o změně některých zákonů. In: *Sbírka zákonů České republiky.* 2000, částka 32, s. 1521-1532. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3420

ČESKO, 1998. Zákon č. 148 ze dne 2. července 1998 o ochraně utajovaných skutečností a o změně některých zákonů. In: *Sbírka zákonů České republiky.* 1998, částka 52, s. 6650-6672. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3159

ČESKO, 2000b. Zákon č. 227 ze dne 29. června 2000 o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu). In: *Sbírka zákonů České republiky.* 2000, částka 68, s. 3290-3297. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3456

ČESKO, 2002. Zákon č. 312 ze dne 13. června 2002 o úřednících územních samosprávných celků a o změně některých zákonů. In: *Sbírka zákonů České republiky.* 2002, částka 114, s. 6598-6612. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3933

ČESKO, 2000c. Zákon č. 365 ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých zákonů. In: *Sbírka zákonů České republiky.* 2000, částka 99, s. 4666-4671. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=3487

ČESKO, 1991. Zákon č. 513 ze dne 5. listopadu 1991 obchodní zákoník. In: *Sbírka zákonů České republiky.* 1991, částka 98, s. 2474-2565. Dostupný také z: http://aplikace.mvcr.cz/sbirka-zakonu/ViewFile.aspx?type=c&id=2510

ČESKÝ STATISTICKÝ ÚŘAD, 2012. *Malý lexikon obcí 2012* [online]. 14. prosince 2012. [cit. 2013-03-02] Dostupné z: http://www.czso.cz/csu/2012edicniplan.nsf/p/1302-12

DATA SECURITY MANAGEMENT, 2009. *Průzkum stavu informační bezpečnosti v ČR 2009* [online]. [cit. 2013-01-18]. Dostupné z: http://www.tate.cz/cz/psib-cr-2009/

DELOITTE, 2013. *TMT Predictions 2013* [online]. [cit. 2013-01-29]. Dostupné z: http://www.deloitte.com/view/en_GX/global/industries/technology-media-telecommunications/tmt-predictions-2013/index.htm

DOBDA, Luboš, 1998. *Ochrana dat v informačních systémech.* Vyd. 1. Praha: Grada Publishing, 286 s. ISBN 80-7169-479-7.

DOSEDĚL, Tomáš, 2004. *Počítačová bezpečnost a ochrana dat.* Vyd. 1. Brno: Computer Press, ix, 190 s. ISBN 80-251-0106-1.

DOUCEK, Petr, 2011. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 286 s. ISBN 978-80-7431-050-8.

ERNST & YOUNG, NBÚ a DSM, 2009. *Průzkum stavu informační bezpečnosti v ČR 2009.* Praha: TATE International, 40 s. ISBN 978-80-86813-19-6. Dostupné také z: http://www.tate.cz/files/download/PSIB_CR_2009.pdf

ERNST & YOUNG, NBÚ a DSM, 2007. *Průzkum stavu informační bezpečnosti v ČR 2007.* Praha: TATE International, 32 s. ISBN 978-80-86813-13-4. Dostupné také z: http://www.tate.cz/files/download/PSIB_CR_2007.pdf

FIALA, Miloš a Josef VILÁŠEK, 2010. *Vybrané kapitoly z ochrany obyvatelstva.* 1. vyd. Praha: Karolinum, 208 s. ISBN 978-80-246-1856-2.

INSTITUT PRO VEŘEJNOU SPRÁVU PRAHA, 2013. *O nás* [online]. [cit. 2013-01-25]. Dostupné z: http://www.institutpraha.cz/o-nas

IVANKA, Ján, 2009. *Systemizace bezpečnostního průmyslu I.* 3. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 123 s. ISBN 978-80-7318-850-4.

IVANKA, Ján, 2009b. *Systemizace bezpečnostního průmyslu II.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 86 s. ISBN 978-80-7318-863-4.

JAŠEK, Roman, 2006. *Informační a datová bezpečnost.* Zlín: Univerzita Tomáše Bati ve Zlíně, Fakulta managementu a ekonomiky, 140 s. ISBN 80-7318-456-7.

JAŠEK, Roman, Miroslava DOLEJŠOVÁ a Pavel ROSMAN, 2007. *Informační technologie ve veřejné správě.* Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 183 s. ISBN 978-8-07318-607-4.

KOCH, Miloš a Viktor ONDRÁK, 2008. *Informační systémy a technologie.* Vyd. 3. Brno: Akademické nakladatelství CERM, 166 s. ISBN 978-80-214-3732-6.

LAUCKÝ, Vladimír, 2004. *Technologie komerční bezpečnosti I.* Vyd. 2. Zlín: Univerzita Tomáše Bati, 64 s. ISBN 8073181940.

LAUCKÝ, Vladimír, 2006. *Řízení technologických procesů v průmyslu komerční bezpečnosti.* Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 101 s. ISBN 80-7318-432-x.

LAUCKÝ, Vladimír, 2009. *Speciální bezpečnostní technologie.* 1. vyd. Zlín: Univerzita Tomáše Bati ve Zlíně, 223 s. ISBN 978-80-7318-762-0.

LIDINSKÝ, Vít, 2008. *EGovernment bezpečně.* 1. vyd. Praha: Grada, 145 s. ISBN 978-80-247-2462-1.

LOUDA, Tomáš, Jiří GROSPIČ a Lenka VOSTRÁ, 2006. *Modernizace veřejné správy v Evropě a České republice: sborník příspěvků z workshopu s mezinárodní účastí. Praha 22. – 23. 11. 2005.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 351 s. ISBN 80-7380-001-2.

LUKÁŠ, Luděk, Petr HRŮZA a Milan KNÝ, 2008. *Informační management v bezpečnostních složkách.* 1. vyd. Praha: Ministerstvo obrany České republiky, 214 s. ISBN 978-80-7278-460-8.

MAREK, Jiří, 2013, Konstrukce CNC obráběcích strojů, In: *Technický týdeník.* Roč. 2013, 1-2, s. 8. Praha: Business Media. ISSN 0040-1064.

MATES, Pavel a Vladimír SMEJKAL, 2006. *E-government v českém právu.* Praha: Linde, 244 s. ISBN 80-7201-614-8.

MATES, Pavel a Vladimír SMEJKAL, 2012. *E-government v České republice: právní a technologické aspekty.* 2. podstatně přeprac. a rozš. vyd. Praha: Leges, 464 s. ISBN 978-80-87576-36-6.

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY, 2011. *Analýza aktuálního stavu veřejné správy* [online]. 78 s. [cit. 2013-01-15]. Dostupné z: http://www.mvcr.cz/soubor/analyza-aktualniho-stavu-verejne-spravy-pdf.aspx

MITNICK, Kevin David, 2002. *Umění klamu: nejslavnější hacker na světě.* Gliwice: Helion, 348 s. ISBN 83-7361-210-6.

NAVRÁTIL, Leoš, 2005. *Aktuální otázky v problematice krizového řízení.* 1. vyd. České Budějovice: Jihočeská univerzita, Zdravotně sociální fakulta, 89 s. ISBN 80-7040-794-8.

NESVADBA, Petr, 2009. *Policejní etika*. Plzeň: Aleš Čeněk, 315 s. ISBN 978-80-7380-195-3.

NORMAN, Thomas L., 2010. *Risk analysis and security countermeasure selection.* Boca Raton: CRC Taylor & Francis Group, xxv, 396 s. ISBN 978-1-4200-7870-1.

ORTMEIER, P. J., 2009. *Introduction to security: operations and management.* 3rd ed. Upper Saddle River: Pearson/Prentice Hall, xiv, 418 s. ISBN 978-0-13-512927-2.

PALEČEK, Miloš, 2006. *Prevence rizik.* Vyd. 1. Praha: Oeconomica, 257 s. ISBN 80-245-1117-7.

POŽÁR, Josef, 2005. *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 309 s. ISBN 80-86898-38-5.

PROCHÁZKOVÁ, Dana, 2007. *Bezpečnost lidského systému.* 1. vyd. V Ostravě: Sdružení požárního a bezpečnostního inženýrství, 139 s. ISBN 978-80-86634-97-5.

PŘIBYL, Jiří, 2004. *Informační bezpečnost a utajování zpráv.* Vyd. 1. Praha: Vydavatelství ČVUT, 239 s. ISBN 8001028631.

ROSMAN, Pavel a Ladislav BUŘITA, 2011. *Informatika pro ekonomy a manažery.* Vyd. 3. uprav. Zlín: Univerzita Tomáše Bati ve Zlíně, 237 s. ISBN 978-80-7454-125-4.

ROSMAN, Pavel, 2008. *Informatika pro ekonomy.* Vyd. 4., nezměn. Zlín: Univerzita Tomáše Bati ve Zlíně, 250 s. ISBN 978-80-7318-738-5.

STRECKOVÁ, Yvonne, 2005. *Faktory efektivnosti fungování veřejného sektoru a obecné poznatky o vlivu řízení veřejného sektoru na rozvoj regionů.* 1. vyd. Brno: Masarykova univerzita, 242 s. ISBN 8021036230.

SYMANTEC, 2013. *Zaměstnanci si ponechávají firemní data a nevidí v tom nic špatného, říká studie Symantec* [online]. 20. února 2013, [cit. 2013-03-02]. Dostupné z: http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20130220_01

Technický týdeník, 2013. Praha: Business Media, roč. 2013, 1-2. ISSN 0040-1064.

TIPTON, Harold F. a Micki KRAUSE, 2007. *Information security management handbook.* 6th ed. Boca Raton: Auerbach, xlvi, 3231 s. ISBN 0-8493-7495-2.

Sekundární zdroje

BRŮCHA, Filip, 2013. 8 největších bezpečnostních mýtů a pravda o nich. In: C*omputerworld* [online]. 19. února 2013, [cit. 2013-02-23]. Dostupné z: http://computerworld.cz/securityworld/8-nejvetsich-bezpecnostnich-mytu-a-pravda-o-nich-49484

CNEWS, 2013. *Microsoft: Uživatelé ignorují internetové hrozby* [online]. 5. února 2013, [cit. 2013-02-24]. Dostupné z: http://www.cnews.cz/microsoft-uzivatele-ignoruji-internetove-hrozby

FUJ, 2013. Facebook vydělává na reklamě novým způsobem. In: *E15* [online]. 28. února 2013, [cit. 2013-03-02]. Dostupné z: http://zpravy.e15.cz/byznys/technologie-a-media/facebook-vydelava-na-reklame-novym-zpusobem-961195

GAJDOŠOVÁ, Markéta, 2013. Průzkum: Neoprávněné cloudy jsou noční můrou IT. In: *Computerworld* [online]. 17. ledna 2013, [cit. 2013-02-11]. Dostupné z: http://computerworld.cz/analyzy-a-studie/pruzkum-neopravnene-cloudy-jsou-nocni-murou-it-49345

JANŮ, Stanislav, 2013. Chytrý malware pro Androidy neinfikuje smartphone, ale připojené PC. In: *CNews* [online]. 7. února 2013, [cit. 2013-02-12]. Dostupné z: http://extramobilne.cnews.cz/chytry-malware-pro-androidy-neinfikuje-smartphone-ale-pripojene-pc

KIRK, Jeremy, 2013. Android botnet sends SMS spam through Android phones. In: *Computerworld* [online]. 17. prosince 2012, [cit. 2013-02-11]. Dostupné z: http://www.computerworld.com/s/article/9234838/Android_botnet_sends_SMS_spam_through_Android_phones

LOUDA, Pavel, 2013. Pracujete z domova? Myslete i na rizika, která jsou s tím spojená. In: *Computerworld* [online]. 21. února 2013, [cit. 2013-02-22]. Dostupné z: http://computerworld.cz/aktuality/pracujete-z-domova-myslete-i-na-rizika-ktera-jsou-s-tim-spojena-49495

MICROSOFT, 2013. *MCSI: Few Consumers Change Online Habits Despite Awareness of Multiple Risks* [online]. Leden 2013, [cit. 2013-02-24]. Dostupné z: http://www.microsoft.com/security/resources/mcsi.aspx

PELECH, Tomáš, 2013. Evropané by si měli dát pozor na americký cloud. In: *Computerworld* [online]. 1. února 2013, [cit. 2013-02-11]. http://computerworld.cz/analyzy-a-studie/evropane-by-si-meli-dat-pozor-na-americky-cloud-49412

SECURITYWORLD, 2013. Sociální sítě jako hrozba pro firemní data. In: *Computerworld* [online]. 4. února 2013, [cit. 2013-02-11]. Dostupné z: http://computerworld.cz/securityworld/socialni-site-jako-hrozba-pro-firemni-data-49425

SEDLÁK, Jan, 2013. Michal Šrajer: Internet už není na stole, ale v ruce. In: *Mobilmania* [online]. 31. prosince 2012, [cit. 2013-02-12]. Dostupné z: http://www.mobilmania.cz/clanky/michal-srajer-internet-uz-neni-na-stole-ale-v-ruce/sc-3-a-1322513/default.aspx

URBAN, Petr, 2013. Organizace posílají otevřený dopis Skypu. Chtějí transparentnost. In: *CNews* [online]. 25. ledna 2013, [cit. 2013-02-09]. Dostupné z: http://www.cnews.cz/organizace-posilaji-otevreny-dopis-skypu-chteji-transparentnost

VRBA, Ondřej, 2013. Eurograbber: uživatelé Androidu a BlackBerry cílem kyber-lupičů. In: *Mobilmania* [online]. 8. prosince 2012, [cit. 2013-02-12]. Dostupné z: http://www.mobilmania.cz/bleskovky/eurograbber-uzivatele-androidu-a-blackberry-cilem-kyber-lupicu/sc-4-a-1322367/default.aspx

VRBA, Ondřej, 2013b. Internet věcí: výstřelek pro hračičky, nebo budoucí životní standard? In: *E15* [online]. 22. ledna 2013, [cit. 2013-03-02]. Dostupné z: http://zpravy.e15.cz/byznys/technologie-a-media/internet-veci-vystrelek-pro-hracicky-nebo-budouci-zivotni-standard-950357

SEZNAM PŘÍLOH

PŘÍLOHA P I: TISKOVÁ ZPRÁVA

Zaměstnanci si ponechávají firemní data a nevidí v tom nic špatného, říká studie Symantec

Aby si zaměstnanci uvědomili, že zcizení duševního vlastnictví je trestný čin, musí je společnosti v této oblasti vzdělávat

Symantec – 20. února 2013. Podle globální studie společnost Symantec (Nasdaq: SYMC) si polovina zaměstnanců, kteří opustili nebo ztratili své zaměstnání v posledních 12 měsících, ponechala důvěrné firemní údaje, 40 procent plánuje využít je ve svém novém zaměstnání. Výsledky ukazují, že postoje zaměstnanců a jejich přesvědčení o krádežích duševního vlastnictví (Intellectual Property IP) jsou v rozporu s převážnou většinou firemních politik.

Zaměstnanci považují zcizení a používání důvěrných dat nejen za přijatelné, ale také věří, že to jejich společnost nezajímá. Pouze 47 procent tvrdí, že jejich organizace v případě odcizení citlivých informací podniká patřičné akce v souladu s bezpečnostními politikami, 68 procent říká, že jejich organizace žádné kroky k zamezení zaměstnancům používat důvěrná data a informace nepodniká. Organizacím se nedaří vytvořit takové prostředí a firemní kulturu, která by podpořila zodpovědnost a závazek zaměstnanců v oblasti ochrany citlivých dat.

Hlavní zjištění průzkumu

- ***Zaměstnanci přenáší citlivá data mimo společnost a nikdy je nemažou.*** Šedesát dvě procenta říkají, že je přijatelné přenášet pracovní dokumenty do vlastních osobních počítačů, tabletů, smartphonů a on-line aplikací pro sdílení souborů. Většina nikdy nemaže údaje, které si přesunuli, protože v tom, že je mají u sebe, nevidí nic špatného.
- ***Většina zaměstnanců si myslí, že používání dat převedených od předchozího zaměstnavatele, je v pořádku.*** Padesát šest procent zaměstnanců nevěří, že používání konkurenčních důvěrných informací je trestný čin; tento omyl přináší rizika stávajícím zaměstnavatelům, kteří jsou příjemci zcizených důvěrných dat ohroženi.
- ***Zaměstnanci připisují vlastnictví důvěrných dat osobě, která je vytvořila***. Čtyřicet čtyři procenta zaměstnanců věří, že pracovník, který vyvíjí pro firmu software, má vlastnický podíl na zdrojovém kódu a je to jeho práce a vynález, 42 procent si myslí, že není trestným činem znovu použít zdrojový kód bez souhlasu v projektech pro jiné společnosti.
- ***Organizacím se nedaří vytvořit kulturu bezpečnosti***. Pouze 38 procent zaměstnanců tvrdí, že jejich manažer považuje ochranu dat za obchodní prioritu, 51 procent si

myslí, že je přijatelné vzít si firemní data, protože jejich společnost neprosazuje striktní bezpečnostní politiky.

Doporučení

- ***Vzdělávání zaměstnanců:*** Organizace musí dát svým zaměstnancům vědět, že vynášení důvěrných informací je trestné. Ochrana duševního vlastnictví by měla být nedílnou součástí školení o bezpečnosti.
- ***Prosadit podepsání dohody o ochraně důvěrných informacích (NDA):*** V téměř polovině případů interních krádeží měla organizace dohodu o duševním vlastnictví se zaměstnancem, která sice naznačuje existenci bezpečnostní politiky, ale bez pochopení zaměstnanců a účinného vynucení jejího dodržování je neefektivní. Zahrnutí jasné specifikace ochrany důvěrných informací do pracovních smluv a zajištění jejich dodržení při výstupním pohovoru vede k odpovědnosti zaměstnanců a nedochází tak k úniku firemních informací a tím i majetku firmy. Ujistěte se, že zaměstnanci jsou si vědomi, že porušení zásad bude postihováno a krádež firemních informací bude mít negativní důsledky pro ně i jejich budoucího zaměstnavatele.
- ***Monitorovat technologie:*** Implementovat politiku ochrany dat, která sleduje nevhodný přístup a používání citlivých informací a automaticky upozorní zaměstnance na porušování, což zvyšuje povědomí o bezpečnosti a odrazuje od zcizení dat.

Průzkum společnosti Symantec **„Co je vaše je i moje: Jak zaměstnanci přinášejí rizika odnášením vašeho duševního vlastnictví“** byla provedena Institutem Ponemon v říjnu 2012. Výsledky jsou založeny na odpovědích 3317 respondentů ze šesti zemí, USA, Velké Británie, Francie, Brazílie, Číny a Koreje.

O společnosti Symantec

Společnost Symantec zaujímá světové prvenství v poskytování řešení zabezpečení, úložišť a správy systémů, která pomáhají jednotlivým zákazníkům i organizacím zabezpečit a spravovat informace. Software a služby chrání komplexněji a efektivněji před více riziky a ve více místech a poskytují jistotu při užívání a ukládání informací. Společnost Symantec má ředitelství ve městě Mountain View v Kalifornii a pobočky ve více než 40 zemích. Další informace jsou k dispozici na adrese www.symantec.com.

Zdroj: SYMANTEC, 2013. *Zaměstnanci si ponechávají firemní data a nevidí v tom nic špatného, říká studie Symantec* [online]. 20. února 2013, [cit. 2013-02-27]. Dostupné z: http://www.symantec.com/cs/cz/about/news/release/article.jsp?prid=20130220_01