Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Teze diplomové práce

Ochrana know-how a jiných kritických dat podniku v digitální době

Autorka: Bc. Jana Urbanová

Vedoucí práce: Ing. Olga Regnerová

© 2016 ČZU v Praze

1 Souhrn

Digitální doba, jak je někdy označován začátek 21. století, se v podnikatelském prostředí vyznačuje vysokou mírou automatizace procesů, která vyžaduje digitalizaci velkého množství dat. Automatizace přináší zrychlení procesů, omezení lidských zásahů, snížení chybovosti a tím snížení nákladů a zvýšení zisků. Mezi digitalizovanými daty nechybí ani různé druhy dat důležitých pro prosperitu podniku, mimo jiné know-how v podobě různých receptů, návodů, postupů, šablon atp. Stejně tak jako jiná důležitá aktiva podniku je potřeba i tato data chránit proti zcizení či zneužití. Tato práce rozebírá různé možnosti ochrany dat reagující na známá rizika a na příkladu konkrétní společnosti analyzuje, jak je tato společnost v oblasti ochrany svých dat připravena. V závěru práce zhodnocuje aktuální stav a doporučuje, čemu by se společnost měla v oblasti ochrany svých dat dále věnovat. Samozřejmě s přihlédnutím k efektivnosti zavádění jednotlivých opatření.

2 Klíčová slova

Bezpečnost, citlivá data, know-how, obchodní tajemství, znalostní báze.

3 Cíl práce a metodika

Hlavním cílem práce je vyhodnocení rizik pro uchovávání a ochranu kritických důvěrných dat podniku a sestavení metodiky pro jejich ochranu.

Dílčími cíli jsou:

- Prokázání důležitosti vlastnictví unikátního know-how, ukázka příkladů z praxe.
- Identifikace dalších dat, která je potřeba chránit před ztrátou, zcizením či zneužitím.
- Identifikace rizik poplatných aktuálnímu trendu digitalizace.
- Návrhy a volba efektivních nástrojů pro ochranu dat.

Diplomová práce je rozdělena na část teoretickou a část praktickou. Teoretická část definuje názvosloví, jednotlivé pojmy a vztahy mezi nimi. Popisuje relevantní zákonné normy, přednáší základní principy ze studované odborné literatury tištěného i elektronického charakteru, přičemž se zaměřuje na různé druhy dat důležitých pro prosperitu podniku a potřebu jejich ochrany včetně metody analýzy rizik.

Praktická část přebírá metodiku ochrany danou zákonem pro potřeby zajištění bezpečnosti kritické informační infrastruktury státu. Ten je sice zaměřen především na subjekty státní správy a samosprávy a z komerčního sektoru se týká pouze omezeného množství organizací, ale svojí podstatou kompletního výčtu rizik a potřebné ochrany může sloužit jako aktuální předpis pro veškeré subjekty vlastnící nebo nakládající s důležitými daty v digitální podobě. Metodou deskripce jsou vyjádřeny oblasti rizik a k nim uvedeny možnosti ochrany včetně organizačních a technických opatření.

Praktická ukázka analýzy stavu ochrany důležitých dat je předvedena na příkladu konkrétní společnosti, u které je analýzou současného stavu a komparací proti doporučení zákonem hodnoceno, do jaké míry je společnost chráněna proti krádeži či zneužití důležitých dat. V závěru je s přihlédnutím k efektivnímu využití zdrojů navrženo, kterým tématům by se společnost v oblasti bezpečnosti dat měla dále věnovat.

4 Zhodnocení výsledků, doporučení a závěr

V podnikatelském prostředí existuje několik jasně definovaných klíčových faktorů úspěchu. Různé studie uvádějí a dále budou uvádět částečně odlišné výčty, ale nikdy by mezi těmi základními faktory neměli chybět lidé (myšleno ve smyslu kvalitních loajálních pracovníků), data/informace a know-how.

Know-how a jeho důležitost tato práce dokládá prostřednictvím reálných příkladů. Hovoří ale nejen o tom, jak dobré využití know-how přispívá k prosperitě podniku, ale také o potřebě know-how chránit. Pohled na know-how je následně formulován jako pohled na jeho formální zápis, tedy jeho vyjádření ve formě dat. Dále je tento pohled zobecněn a rozšířen o další pro prosperitu podniku důležitá data.

Digitalizace dat v podnikovém prostředí s sebou přináší mimo jiné možnosti velmi rychlého kopírování a přemísťování dat, dokumentů, nebo klidně celých databází obsahujících milióny záznamů. To má na jedné straně velmi pozitivní efekt v situacích, kdy se dějí pro společnost chtěné aktivity a procesy, ale na druhé straně to s sebou přináší obrovská rizika, pokud se někdo rozhodne škodit. A protože informace a know-how, jehož formálnímu zápisu se digitalizace také nevyhnula, patří mezi klíčové faktory úspěchu (a tím samozřejmě také neúspěchu), může libovolná společnost, která podcení ochranu svého informačního bohatství, během okamžiku přijít o značné zisky nebo dokonce o smysl své existence. Z tohoto pohledu je jasné, že chránit svá data je naprosto nezbytné.

Statistiky ukazují, že způsoby krádeží dat, kdy se někdo vloupe do objektu společnosti, aby zcizil nějaké informace, jsou svou četností zanedbatelné. Při uvažování možností zcizení dat nabízí jejich digitální podoba pro útočníky mnohem jednodušší cesty. I tady se dá ze statistik leccos vyčíst. Protože společnosti již často disponují prostředky pro oddělení vnitřní a vnější sítě a možnostmi pro přístupy pouze přes zabezpečené kanály, což je dáno relativní jednoduchostí vyřešení této problematiky zakoupením firewall zařízení, které v sobě již obsahuje vše potřebné, cílí útočníci v naprosté většině případů zjištěných útoků na uživatele. Je totiž mnohem jednodušší zajistit si informace o uživateli a pokusit se zcizit jeho přihlašovací údaje tak, aby se útočník mohl vydávat za něj. Stačí si představit využití sociální sítě LinkedIn pro zjištění toho, kdo v pro útočníka zajímavé firmě pracuje na pozici s vysokým oprávněním, následně přes další sociální sítě jako Facebook, Instagram, či dnes velmi oblíbené portály evidující sportovní výkony (včetně tras a časů) amatérů zjistit, jaké má onen pracovník pravidelné návyky, kde bydlí a další podrobnosti. S těmito informacemi a faktem, že má dnes

téměř každý minimálně pracovní e-mail v mobilním telefonu, trendu BYOD a častému využívání federací identit (princip mimo jiné umožňující přihlašování do online systémů prostřednictvím již existující ověřené identity například ze systémů Google nebo Facebook) či dalších z pohledu bezpečnosti rizikových vymožeností poslední doby, má zkušený kybernetický zločinec velkou šanci, že pokud nebudou systémy s citlivými daty dobře zabezpečeny, najde způsob, jak se do nich dostat. Proto je potřeba své IT prostředí a i veškerá důležitá data nejen dobře zabezpečit proti známým rizikům, ale také sledovat trendy v oblasti bezpečnosti, aby při příchodu nových rizik a s nimi nových možností ochrany, byla společnost dobře připravena.

Analýzou aktuální situace v oblasti zabezpečení dokumentů v AMI Praha bylo zjištěno, že ve společnosti je zaveden procesní systém řízení a je nastavena klasifikace dat. Procesy jsou certifikovány dle ISO 9001 a ISO 27001 a na dodržování procesů dohlíží specializovaný manažer ISMS. Dále je ve společnosti využívána metoda analýzy rizik CRAMM. Bezpečnost je zajišťována i několika technickými prostředky, mezi které se řadí výkonný firewall oddělující komunikaci vnější a vnitřní sítě, antivirový program instalovaný na veškeré počítače a servery, šifrování pevných disků, systém pro automatické řízení uživatelských účtů, oprávnění a rolí a VPN pro vzdálený přístup.

Naopak bylo šetřením zjištěno, že ve společnosti nejsou zavedeny nástroje pro pokročilou autentizaci uživatelů, řízení přístupu administrátorů či vyhodnocování bezpečnostních událostí v reálném čase. Doporučením pro společnost AMI Praha je zvážení přidání alespoň dalšího faktoru autentizace při přístupu k nejkritičtějším informačním systémům, případně při přístupu administrátorů s vysokou úrovní oprávnění. Zavádění ostatních chybějících nástrojů by pro zkoumanou společnost bylo vzhledem k licenčním a implementačním nákladům neefektivní.

Dále bylo šetřením zjištěno, že přes poměrně silné zabezpečení informačních systémů a dat v počítačích chybí pokročilejší mechanismus pro ochranu důvěrných dat v mobilních telefonech. Tato problematika je standardně řešena prostřednictvím nástrojů MDM (Mobile Device Management), které v mobilních zařízeních umožňují zabezpečit aplikace i data. Ani tento nástroj není ve zkoumané společnosti nasazen a to může být, především kvůli benevolenci k současnému trendu využívání osobních zařízení pro firemní účely (BYOD – Bring Your Own Device), potenciálním rizikem.

5 Seznam vybraných použitých zdrojů

- Distrikt Court of Maryland v soudním rozhodnutí z roku 1946: ČADA, Karel, Obchodní tajemství a know-how. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, ISBN 80-85100-67-3
- ČADA, Karel; *Obchodní tajemství a know-how*. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, ISBN 80-85100-67-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002, ISBN: 978-80-245-1920-3
- MAREK,Karel; Licenční smlouva (k předmětům průmyslového vlastnictví). Bulletin advokacie. 2008, roč. 19. č. 7-8, ISBN 978-80-7208-922-2
- SKÁLA, Karel; Nekalá soutěž: Její podstata a stíhání podle zákona ze dne 15. července 1927, č. 111 Sb. z. an. Praha: Praetor, 1927, s. 185 an. ČADA, Karel; Obchodní tajemství a know-how.1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, ISBN 80-85100-67-3
- SLÁMA. Jiří, Licenční smlouva. Bulletin advokacie. 2008, roč. 19, č. 12, ISBN 978-80-7239-206-3