Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra obchodu a financí

Diplomová práce

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

Autorka: Bc. Jana Urbanová

Vedoucí práce: Ing. Olga Regnerová

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Jana Urbanová

Provoz a ekonomika

Název práce

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

Název anglicky

A protection of know-how and other critical enterprise data in digital age

---

Cíle práce

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.

Metodika

Diplomová práce bude rozdělena na část teoretickou a část praktickou. Teoretická část definuje jednotlivé dále použité pojmy a vztahy mezi nimi. Popíše relevantní zákonné normy a přednese základní principy ze studované odborné literatury tištěného i elektronického charakteru. Budou zvolena adekvátní teoretická východiska, která budou aplikována při zpracování vlastní práce.

Praktická práce bude vycházet z charakteristiky konkrétní společnosti a popisu současného stavu řešené problematiky. Pro identifikaci a ohodnocení problémových oblastí bude použita analýza rizik a na základě hodnocení efektivnosti vynaložených zdrojů bude navrženo, které z existujících nástrojů ochrany mají být použity. Kromě metody destkripce a anylýzy budou využity metody syntézy a komparace relevantních dat.

Doporučený rozsah práce

60 – 80 stran

Klíčová slova

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

Doporučené zdroje informací

ČADA, Karel. Chránit / nechránit, to je otázka: výsledky výzkumu a vývoje, jejich ochrana a komercializace. 1. vyd. Plzeň: Alevia, 2014, 320 s. ISBN 978-80-905538-0-4.

ČADA, Karel. Know-how a obchodní tajemství. Vyd. 1. Praha: Úřad průmyslového vlastnictví, 2010, 284 s. ISBN 978-80-7282-087-0.

ČESKO. ZÁKONY ATD. Celní předpisy : celní zákon, zákon o Celní správě ČR, prováděcí předpisy, zboží porušující práva duševního vlastnictví : redakční uzávěrka 20.4.2015. Ostrava: Sagit, 2015. ISBN 978-80-7488-113-8.

HARVEY, C. Tajemství úspěchu špičkových obchodníků světa. Praha: Informatorium, 1991.

JAŠEK, Roman. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.

MALÝ, Josef. Obchod nehmotnými statky: patenty, vynálezy, know-how, ochranné známky. Vyd. 1. Praha: C. H. Beck, 1995, xiii, 257 s. ISBN 80-717-9320-5.

SPURNÝ, J. – LÁTAL, I. – URBAN, M. *Jak se bránit zločinu : jak bránit sebe, své fyzické a duševní vlastnictví před zločinem.* Praha: Státní pedagogické nakladatelství, 1994. ISBN 80-04-26581-2.

ŠTENGLOVÁ, Ivana. Obchodní tajemství: praktická příručka. Vyd. 1. Praha: Linde, 2005, 159 s. ISBN 80-720-1559-1.

Předběžný termín obhajoby

2016/17 ZS – PEF

Vedoucí práce

Ing. Olga Regnerová

Garantující pracoviště

Katedra obchodu a financí

Elektronicky schváleno dne 8. 11. 2016

Ing. Helena Čermáková, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 23. 11. 2016

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 25. 11. 2016

Čestné prohlášení

Prohlašuji, že svou diplomovou práci " Ochrana know-how a jiných kritických dat podniku v digitální době " jsem vypracovala samostatně pod vedením vedoucí diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autorka uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušila autorská práva třetích osob.

V Praze dne: _____

Poděkování

Ráda bych touto cestou poděkovala Ing. Olze Regnerové za cenné připomínky a odborné rady, kterými přispěla k vypracování této diplomové práce.

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

A protection of know-how and other critical enterprise data in digital age

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.

Summary

The Digital age, as is the beginning of the 21st century sometimes called, is in the business field characterized by a high level of automatization of its processes, which requires the digitalization of a huge amount of data. This automatization brings the acceleration of processes, both human intervention and errors reduction, and thereby it lowers the costs and increases the profits. Among the digitalized data, there are various kinds of data essential for the company prosperity such as know-how in form of various recipes, manuals, formulas, templates, etc. As it is common with other valuable assets of the company, it is also necessary to protect such data against theft or misuse. This thesis analyzes various possibilities of such data protection and does so in reaction to known risks on the example of actual company, and analyzes the readiness of this company in the data protection field. In the end, the thesis

assesses its present state and advises on what the company should do in data security field in future. That is, of course, with the particular tools implementation taken into account.

Klíčová slova: bezpečnost, citlivá data, know-how, obchodní tajemství, znalostní báze.
Keywords: security, sensitive data, know -how, trade secrets, knowledge base.

Obsah

1 Úvod

Začátek 21. století je často označován jako digitální doba. Každá doba, ve které se lidstvo kdy ocitlo, měla svá specifika a nejinak je to tomu i dnes. Věci, které dnešním lidem v produktivním věku připadají normální, by byly pro naše předky naprosto nepřestavitelné a nemuselo by se zacházet daleko do minulosti. Dokonce i ten produktivní věk se v čase znatelně mění. Naprosto zásadními rozdíly digitální doby oproti předchozím je především zapojení technologie do každodenního života všech, neuvěřitelné zrychlení většiny procesů, virtuální zkrácení vzdáleností či díky online světu umožňujícímu provádět některé operace nezávisle na čase a prostoru jejich praktické vymazání.

Z pohledu podnikatelského prostředí se sice některé aspekty podnikatelské reality téměř nezměnily, ale většina jich prošla velkými změnami a některé jsou zcela nové. Tato práce nemá za cíl rozebírat veškerá podnikatelská specifika této doby. Zabývá se kombinací know-how, které bylo součástí podnikání od nepaměti, i když třeba pod jinými názvy, a fenoménů dneška – technologickými možnostmi a důležitostí disponovat ve správném čase správnými daty a informacemi, které je navíc potřeba chránit. K tomu bude brán zřetel na další data, jejichž ochrana pro samotné fungování společností a jejich procesů není nezbytná, ale tuto nezbytnost definuje stát jako součást ochrany pro své obyvatele.

Nejde tedy jen o know-how samotné, které je v této práci chápáno především jako součást dat podléhajících vysoké míře důvěrnosti a vyjádřené a uchovávané v podobě různých postupů, návodů, znalostí apod. Tato práce se věnuje právě datům jako jednomu z fenoménů posledních desetiletí, jejich ohodnocení z pohledu důležitosti pro vlastnickou organizaci (ať již se jedná o důležitost pramenící z vlastní podstaty podnikání nebo důležitost danou legislativou) a způsobům jejich ochrany v době, kdy mají data mnohem více forem a možných lokalit pro uložení, než tomu bylo kdykoli v minulosti.

Tato práce se naopak nevěnuje klasické ochraně know-how vyjádřeného jinak než jeho formálním zápisem do formy dat. Neřeší všechny aspekty průmyslové špionáže jako rozebírání výrobků konkurence a jejich napodobování, přetahování klíčových pracovníků z jedné společnosti do jiné či jiné kopírování výrobních procesů, designů a parametrů. Neřeší ani způsoby uchovávání a předávání know-how v delším období, ve kterém dochází k změnám v pracovních týmech. Cílem je postihnout rizika a nabídnout vyčerpávající možnosti ochrany dat a dokumentů ať již se jedná o formu fyzickou (tištěné dokumenty)

nebo elektronickou (počítačová data), určit konkrétní typy nástrojů sloužícím pro ochranu proti jednotlivým rizikům a provést analýzu v konkrétní společnosti, v rámci které bude zhodnoceno, jaká rizika ošetřena jsou a jaká nikoli.

Že je pro prosperující fungování v tržním prostředí kromě jiného potřeba mít něco specifického a umět tuto specifičnost využít a ochránit proti zcizení a okopírování konkurencí, bude prokázáno na konkrétních známých případech. I bez nich si ale snad každý dokáže představit, co by znamenalo například vyzrazení receptu výroby nápoje pro společnosti jako CocaCola, RedBull či Karlovarská Becherovka. Stejně tak není potřeba dlouze vysvětlovat případné dopady vyzrazení tajných receptů, postupů, či třeba složení použitých materiálů pro jiné tržní subjekty, které si drží svou unikátnost. Nejde ale jen o tyto dlouhodobě utajené poklady. Pro společnosti je v době zuřivého konkurenčního boje zásadní i nevyzrazení parametrů nového produktu před tím, než vyjde na trh. Přestože pak jsou tyto parametry již všem jasně známé. Dnes je dokonce extrémně důležité nevyzradit ani myšlenku pro marketingovou kampaň před jejím spuštěním, protože i na ni by mohla konkurence zareagovat dříve, než je záhodno, a veškeré do kampaně vynaložené prostředky by vyšly vniveč. Dat a informací, které je potřeba v podnikatelském prostředí chránit, je zkrátka mnoho a cílem této práce je ukázat, jak k této oblasti zodpovědně přistupovat.

Z aktuálního průzkumu nadnárodní poradenské společnosti PricewaterhouseCoopers (dále jen PwC) vyplívá, že se s krádeží potýká celosvětově až třetina všech firem. Ve firmách nejčastěji kradou třicátníci s vysokoškolským vzděláním. Průzkum hospodářské kriminality provedla PwC v 6 377 firmách po celém světě a zúčastnilo se ho i 70 českých společností. Až 40 procent českých firem, které se staly obětí podvodu, přišly nejméně o 1,2 milionu korun českých.

Každá třetí firma v Česku v posledních dvou letech zaznamenala krádeže majetku či jiný způsob poškozování. V 54 procentech případů byl pachatelem někdo zvenčí, zákazník (25 %), dále obchodní zástupci či zprostředkovatelé (17 %) nebo prodejci (10 %). Ve zbytku případů kradli zaměstnanci. Interní pachatelé dle průzkumu potřebují nejčastěji tři až pět let, aby zjistili, jak v podniku fungují kontrolní mechanismy a jak je obejít. Mimo finanční ztráty dochází také k poškození dobrého jména společnosti a ke katastrofálním dopadům na morálku zaměstnanců, pokud byl pachatelem zaměstnanec. Pokud zaměstnanci vidí, že se ve firmě krade, mají pak menší zábrany si také něco přivlastnit.

Jaké jsou tedy nejčastější způsoby krádeží? Nejčastěji se jedná o finanční sektor, a to úvěrové nebo pojistné podvody. Zde se jedná jak o zákazníky, tak na druhé straně i samotné pojišťovací agenty a další zprostředkovatele. Obchodní zástupci poškozují především výrobní firmy, protože často manipulují s čísly za prodeje za účelem dosažení bonusů, nebo například neoprávněně využívají služební automobil k soukromým účelům atp. Ti otrlejší z nich si pak založí vlastní firmu se stejným oborem podnikání a parazitují tak na zaměstnavateli, který tak přichází nejen o své vlastní klienty ale také o citlivá data. V neposlední řadě se jedná o zadávání firemních zakázek, které se zadávají spřízněným firmám a fakturované zboží a služby jsou pak často předražené. Nebo se může jednat o fiktivní faktury za nikdy neuskutečněné dodávky.

Zaměstnancům se otevírá stále větší prostor k podvodům páchajícím přes počítač, a to díky stále komplikovanějším IT systémům, které umožňují dálkové přístupy, přístup k firemnímu emailu z internetových kaváren, z mobilních zařízení či práci z domova. Pokud firma zapomíná adekvátně chránit tyto systémy a v nich uložená data, může trvat třeba i rok, než na podvody firma přijde.

Zaměstnanci se snáz dostávají k firemním tajemstvím, vynálezům, projektům, technologiím či osobním údajům, které se dají zhodnotit v jejich prospěch. Své o tom vědí manažeři v české pobočce společnosti T-Mobile. Zdejší zaměstnanec ukradl a prodal osobní údaje 1,5 milionu klientů.

Firmy každoročně přicházejí v průměru o pět procent svých příjmů v důsledku nejrůznějších podvodů a machinací páchaných jak řadovými zaměstnanci, tak členy vedení či přímo majiteli firem. A to jsou již velmi silné argumenty pro zvážení možností ochrany.

2 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.

3 Teoretická východiska

3.1 Podnik

Podnik je jedním ze základních subjektů trhu, který je zakládán za účelem dosažení zisku. Podnik přeměňuje vstupy (suroviny, materiál, práce, data) na výstupy (statky a služby). Podnik představuje soubor hmotných (např. budovy), nehmotných (např. data, know-how) a osobních složek (např. schopnost pracovníků), které slouží k provozování podniku. Všechny tyto složky se promítají do hodnoty podniku např. v případě jeho prodeje. Podniky můžeme rozlišovat podle předmětu činnosti, a to na obchodní, dopravní a spojové, služební nebo peněžní. Dále je dělíme dle velikosti (malý, střední, velký) nebo dle právní formy na obchodní společnosti, podniky jednotlivce, družstva, státní podniky a ostatní formy podnikání.

Cílem podniku je mimo dosahování zisku také spokojenost zaměstnanců, rozvoj podniku, spokojenost zákazníka, zlepšování kvality, podpora charakterové činnosti, konkurenceschopnost a udržování know-how.

3.2 Know-how

Výraz know-how převzatý z anglického jazyka v překladu znamená „vědět jak“ nebo také „vědět jak na to“. V obecném pojetí lze know-how vymezit jako nehmotný statek, který je vyjádřený v objektivně vnímatelné podobě, tvoří jej poznatky, zkušenosti a vědomosti z různých oblastí společenského života. Má důležitý význam pro jeho používatele, není všeobecně známé ani dostupné, má cenu, kterou lze vyjádřit, a je využitelné třetími osobami. Žádná jediná správná definice daného pojmu neexistuje, musíme si tedy vystačit s analogií. Často je tento pojem vysvětlován jako soubor výrobních, technických, technologických a jiných poznatků a dovedností, které vedou k racionálnějšímu nebo efektivnějšímu vyřešení určitého problému a jsou podnikatelsky využitelné.[1] Mohou to být výrobní tajemství, receptury, formule, technická informace a dokumentace, které jsou nutné k výrobě určitého výrobku nebo k využití některého technologického procesu nejvhodnějším způsobem. Může to ale být i způsob dodání zákazníkovi, jedinečně řízený marketing a vlastně cokoli, co je vyřešeno unikátně a dá se to považovat za faktor úspěchu. Vymezení pojmu know-how není

[1] ČADA, Karel; *Obchodní tajemství a know-how*. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 30-33, ISBN 80-85100-67-3

v jednotlivých zemích ani v teorii jednotné. Někdy jsou sem řazeny i právně nechráněné, avšak utajované vynálezy, výsledky výzkumu a vývoje a další výsledky tvůrčí činnosti, popřípadě celé komplexy poznatků zahrnující právně nechráněné vynálezy i zkušenosti s jejich využíváním. Know-how je faktickou znalostí, kterou nelze přesně a podrobně popsat, která však, používána v akumulované formě, dává způsobilost tomu, kdo ji získal, vyrobit něco, co by jinak vyrobit nemohl, a to s přesností a účinky nutnými pro úspěšný obchod.[2]

Know-how může vznikat plánovaně, neplánovaně nebo úplně náhodně při různých příležitostech lidské činnosti, a to nejen technických, výrobních, výzkumných či vývojových.

Do know-how se naopak nepočítají osobní schopnosti spojené pouze s konkrétní osobou. Například talent určité osoby, její schopnost ani vlastnost či charakteristika. Jiným slovy know-how není to, co by nešlo od konkrétní fyzické osoby oddělit.

3.2.1 Podnikové know-how

Dovednosti a znalosti můžeme shrnout do dvou základních hledisek, a to podle nositele a původu know-how. Podnikovým know-how rozumíme například příručky, návody, marketingové studie, výkresy, plány, seznamy dodavatelů, vzdělávání a školení, nebo třeba prvky komunikační politiky. Další jeho součástí je manažerské know-how, jehož nositelem je manažer nebo jeho tým. Podle toho, ze které části podniku dané know-how pochází, můžeme rozlišit kompetence technické, marketingové a kompetence v oblasti řízení.

Technické know-how přímo souvisí s výrobou či výrobkem, dále zahrnuje zajištění výroby a nákup surovin. Považujeme za něj zejména metody řízení zakázek a řízení výroby, metody kontroly kvality, metody řízení zásob, testování prototypů, metody vzdělávání zaměstnanců ve výrobě, proces výzkumu a vývoje, techniky výroby a v neposlední řadě také metody zjišťování nákladů výroby.

Veškeré zkušenosti a dovednosti zaměstnanců ve vztahu k trhu a k zákazníkovi v souvislostech cenových, distribučních a komunikačních vyjadřuje marketingové know-how. Konkrétně se jedná o metody výzkumu trhu, testování, odhadů prodeje, metody uvádění nových výrobků na trh, techniky určování cen a cenová politika, reklama, podpora

[2] Distrikt Court of Maryland v soudním rozhodnutí z roku 1946: ČADA, Karel, *Obchodní tajemství a know-how*. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 32, ISBN 80-85100-67-3

prodeje, vztahy s veřejností, techniky výběru a optimalizace distribučních cest, techniky organizace, vzdělávání, odměňování a motivace prodejců.

V oblasti řízení know-how zahrnuje zejména specifické zkušenosti a dovednosti nashromážděné oddělením vrcholného managementu, finančního řízení a účetnictví, kontroly a personalistiky. Především tedy techniky ve výběru a hodnocení investic, techniky plánování a kontroly, techniky v účetnictví, techniky přijímání a vzdělávání zaměstnanců, techniky motivace a rozvoje zaměstnanců a techniky odměňování.

3.2.2 Právní ochrana know-how

Právní řád České republiky neobsahuje žádnou výslovnou definici know-how. I přesto je však možné tento termín najít v řadě právních předpisů a mezinárodních smluv, a to zejména o podpoře a vzájemné ochraně investic. Bohužel s ohledem na absenci výslovné definice se pak v praxi obtížně určuje, co know-how ještě je a co už není.

Právní teorie pouze vymezuje know-how jako souhrn znalostí, poznatků, vědomostí a skutečností z různých oblastí společenského života, například obchodu, výroby, techniky, služeb či ekonomiky, které mají podstatný význam pro svého uživatele a nejsou všeobecně známé a dostupné. To znamená, že se může jednat o jakoukoli nevyzrazenou informaci, znalost, zkušenost či poznatek, která je nějakým způsobem využitelná.

Z ryze právního pohledu patří know-how mezi tzv. jinou majetkovou hodnotu, která je ocenitelná penězi. S know-how lze pochopitelně nakládat. Know-how je možné vkládat do společností či sdružení, převádět (například formou koupě či darování) nebo poskytovat třetím osobám k využití (bezúplatně i za úplatu). Může být předmětem smluv o obstarání či zprostředkování know-how, součástí franšízových smluv nebo jiných (i nepojmenovaných) smluv.[3]

Nejsilnější ochranu know-how poskytuje právo průmyslového vlastnictví. Pokud tedy určitý vynález či zlepšovací návrh splňuje podmínky patentovatelnosti, představuje jeho

[3] MIROVSKÁ, Petra; Jak ochránit firemní know-how [online]. 2013 [cit. 2016-06-24]. Dostupné z: https://www.patria.cz/pravo/2279271/jak-ochranit-firemni-know-how.html

ochrana patentem mnohem lepší ochranu, než jeho pouhým utajováním. Obdobná je i situace u zapsaných průmyslových vzorů.[4]

České právo neposkytuje know-how žádnou specifickou ochranu. Know-how je však možné chránit jako obchodní tajemství, což je institut upravený obchodním zákoníkem. K tomu, aby mohla být know-how poskytována ochrana jako obchodnímu tajemství, je naprosto nezbytné, aby měl podnikatel zájem na utajení know-how a odpovídajícím způsobem jeho utajení i zajišťoval. Vůle podnikatele o utajení může být obsažena v pracovních smlouvách, v jednostranných závazcích o mlčenlivosti, ve vnitřních směrnicích, v různých závazkových smlouvách nebo i ve faktickém utajování. Příslušné organizační, technické a jiné opatření pak zajišťují vlastní utajení obchodního tajemství. Konkrétně by se mohlo jednat například o zákaz vstupu nepovolaným osobám na určitá pracoviště. Ohledně plnění těchto opatření nese důkazní břemeno podnikatel, kterému svědčí know-how chráněné jako obchodní tajemství. Bohužel podnikatelé nejsou často schopni u soudu prokázat, že skutečně efektivně zajišťují utajení know-how s využitím všech technických prostředků. Z toho důvodu pak nebývají s žalobami na poskytnutí ochrany proti porušení nebo ohrožení obchodního tajemství úspěšní.

Jen zlomek českých podniků využívá k ochraně svých nápadů patenty. V oblasti ochrany průmyslového vlastnictví patří Česko mezi podprůměrné země podobně třeba jako Polsko nebo Slovensko. Podniky totiž často vnímají patentovou ochranu jako únik informací a nedůvěřují jí. Při udělení patentu zveřejňuje firma své know-how světu, a tím může dát návod konkurenci.[5] Menší a střední firmy pak nejsou natolik kapitálově silné, aby mohly své know-how chránit v právních sporech.

K ochraně svého technického řešení mohou firmy využít buď patent, nebo užitný vzor. Častěji volí druhou variantu, protože je jednodušší, rychlejší a také levnější. Zatímco Češi v roce 2015 vynálezů přihlásili 952, užitných vzorů bylo 1446. Přitom v sousedním Rakousku byl poměr opačný s více přihlášenými patenty. Dostupnější ochrana užitným vzorem přináší více rizik a to si zahraniční firmy uvědomují. Základním rozdílem je, že

[4] MIROVSKÁ, Petra; Jak ochránit firemní know-how [online]. 2013 [cit. 2016-06-24]. Dostupné z: https://www.patria.cz/pravo/2279271/jak-ochranit-firemni-know-how.html

[5] FILIPOVÁ, Kateřina; České podniky nestojí o patenty. Právní ochraně nevěří a bojí se o své know-how [online]. 2016 [cit. 2016-06-24]. Dostupné z: http://m.ihned.cz/byznys/c1-65300920-ceske-podniky-nestoji-o-patenty-pravni-ochrane-neveri-a-boji-se-o-sve-know-how

udělení patentu předchází úřední průzkum. Posuzuje se novost řešení, vynálezecká činnost a průmyslová využitelnost. Naopak u užitného vzoru se nic podobného nezjišťuje a úřad jej rovnou zaregistruje. Mohlo by tak dojít k tomu, že se udělí ochrana i na řešení, které si registraci nezaslouží, neboť se nejedná o nové řešení.

3.3 Obchodní tajemství

Velmi blízce souvisejícím pojmem s know-how je obchodní tajemství. Podle §504 občanského zákoníku obchodní tajemství tvoří konkurenčně významné, určitelné, ocenitelné a v příslušných obchodních kruzích běžně nedostupné skutečnosti, které souvisejí se závodem a jejichž vlastník zajišťuje ve svém zájmu odpovídajícím způsobem jejich utajení. Aby určitá skutečnost byla obchodním tajemstvím, musí splňovat všechny uvedené znaky současně.

Karel Skála definuje obchodní a výrobní tajemství jako skutečnosti – zvláštnosti výrobního a obchodního podnikání – na jejichž uchování v tajnosti má podnikatel hospodářský (nikoli jen soukromý) zájem a které se též z toho důvodu v podniku jako tajemství uchovávají. Spadají sem jen takové objektivní skutečnosti výrobního a obchodního podnikání, které jsou jednomu nebo několika podnikům vlastní, nikoli takové, které nejsou vůbec anebo naopak všem konkurenčním podnikům známy. Je tedy třeba vztahu těchto skutečností k určitému podniku, není však třeba, aby šlo o nějakou zvláštnost vlastní jedině tomuto podniku. Tyto zvláštnosti musí tedy být konkurenčně ocenitelné. Nemusí to býti skutečnosti nové, stačí jen, že jsou ve veřejnosti neznámé. Rovněž výlučnost těchto skutečností není nutným předpokladem, současně v jednu dobu může mít více osob stejnou myšlenku, učinit stejný vynález apod. K pojmu tajemství se nevyžaduje, aby skutečnosti, o něž jde, byly v podniku výslovně označeny za tajné. Stačí, pokud je z okolností rozpoznatelná snaha o jejich utajení.[6]

Porušení obchodního tajemství je jedním ze způsobů nekalé soutěže podle § 2985 občanského zákoníku, spočívá v neoprávněném sdělení, zpřístupnění nebo využití obchodního tajemství, které bylo jednajícímu svěřeno, nebo o němž se dozvěděl jiným způsobem. Ten, jehož obchodní tajemství bylo porušeno, se může domáhat odstranění

[6] 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, s. 89, ISBN 80-85100-67-3

závadného stavu a především přiměřeného zadostiučinění, kterým je náhrada škody a vydání bezdůvodného obohacení.

3.4 Know-how versus obchodní tajemství

Přestože jsou si pojmy velmi podobné, nelze know-how s obchodním tajemstvím zaměňovat. Literatura a v ní většina autorů se shoduje, že jde o dva samostatné prvky. Každý z nich obsahuje prvky nenáležící do druhého a rozdíly mezi nimi lze pochytit spíše intuitivně, než aby je bylo možné charakterizovat obecnou definicí. Ani právně se nejedná o totožné termíny a nelze je tak navzájem zaměňovat, protože obchodní tajemství představuje osobitý institut obchodního práva a know-how je jeho možným předmětem. Know-how může existovat samostatně bez toho, aby bylo součástí obchodního tajemství. Porovnáním obou institutů lze dojít k závěru, že know-how je kvalifikované být součástí obchodního tajemství a je schopné být jeho podmnožinou, ale je potřeba brát v úvahu odlišné znaky, které nespadají do jejich společného průniku. Mezi tyto znaky patří například nutnost utajování obchodního tajemství, ač to není nutným znakem know-how, přestože všeobecně známé know-how je stěží obchodovatelné. Podstatnějším rozdílem je definice osob oprávněných k know-how, protože na rozdíl od oprávněných osob k právu obchodního tajemství to mohou být mimo podnikatelské subjekty i osoby fyzické a právnické, jež nejsou podnikateli. Kompetentní subjekt je oprávněn v rámci ochrany know-how použít všechny právní prostředky poskytnuté normami nekalé soutěže a je mu poskytnuta ochrana v rámci norem trestního práva.

3.4.1 Oceňování know-how a obchodního tajemství

Jak už vyplynulo z předešlých charakteristik, jde o peněžně ocenitelná majetková práva, která jsou součástí majetku podniku. Pro věcné účely je často vyžadované stanovení jejich určité hodnoty. Jejich oceňování v současné době provádí stanovení odborníci, soudní znalci, poradenské firmy a auditoři, a to podle svých zásad, úsudků a postupů.[7] Argumenty pro podobné oceňování mohou být různorodé. V praxi se většinou setkáme s potřebou stanovení hodnoty těchto práv v souvislosti se vkladem nehmotného majetku do základního kapitálu obchodní společnosti, kdy § 58 odst. 1 obchodního zákoníku stanoví, že: „Základní kapitál společnosti je peněžní vyjádření souhrnu peněžitých i nepeněžitých vkladů všech

[7] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 41. ISBN: 978-80-245-1920-3

společníků do základního kapitálu společnosti.“[8] V této definici je z pohledu know-how zajímavý pojem nepeněžitého vkladu do základního kapitálu, kterým jsou věcné vklady práv a vklady ostatní. Nepeněžitým vkladem je taktéž nehmotný statek jako obchodní tajemství či právě know-how.[9]

Dále § 59 odst. 3 obchodního zákoníku stanoví: „Hodnota nepeněžitého vkladu musí být uvedena ve společenské smlouvě, zakladatelské smlouvě nebo zakladatelské listině, nestanoví-li tento zákon jinak. Hodnota nepeněžitého vkladu do společnosti s ručením omezeným a do akciové společnosti se stanoví podle posudku zpracovaného znalcem nezávislým na společnosti, jmenovaným za tím účelem soudem.“[10] Tento nezávislý posudek znalce pak musí dle § 59 odst. 4 obchodního zákoníku pojmout popis nepeněžitého vkladu, aplikované způsoby jeho ocenění a údaj o tom, zda hodnota nepeněžitého vkladu odpovídá alespoň emisnímu kurzu upsaných akcií, které mají být vydány jako protiplnění za tento nepeněžitý vklad, nebo částce, která se má započítávat na vklad do základního kapitálu společnosti s ručením omezeným. A dále částku, kterou se nepeněžitý vklad oceňuje.[11]

Některé druhy majetku jsou pak dále oceňovány na základě zákona č. 151/1997 Sb., o oceňování majetku, ve znění pozdějších předpisů. Tento však neukládá, aby postup v něm uvedený byl použit pro tento účel, umožňuje ale na základě rozhodnutí rejstříkového soudu, aby bylo pro ocenění daného druhu nepeněžitého majetku použito způsobu podle tohoto zákona.[12] Zákon o oceňování majetku ve svém § 17 tedy jako primární stanoví způsob oceňování majetkových práv výnosovým způsobem jakožto součet diskontovaných budoucích ročních čistých výnosů vyplývajících z užívání těchto práv dle dne ocenění.[13] Jedním z důvodů pro stanovení hodnoty nehmotného majetku mohou být daňové a účetní povinnosti subjektů. Dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů se při oceňování majetku, závazků a při účtování o výsledku hospodaření účetní jednotky

[8] Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
[9] ČADA, Karel; Obchodní tajemství a know-how.1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 131, ISBN 80-85100-67-3
[10] Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
[11] Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
[12] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 38. ISBN: 978-80-245-1920-3
[13]Zákon č. 151/1997 Sb., o oceňování majetku a o změně některých zákonů, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://zakony.centrum.cz/zakon-o-ocenovani-majetku/

považují za základ veškeré náklady a výnosy, jež se vztahují k účetnímu období. Možnostem oceňování majetku pro účely účtování se konkrétně věnuje § 25 tohoto zákona, který ukládá, že nehmotný majetek (do kterého řadíme i know-how a obchodní tajemství) se oceňuje pořizovacími cenami a tím je zpravidla cena tržní. Oceňování nehmotného majetku vytvořeného vlastní činností řeší zákon o účetnictví vlastními náklady či reprodukčními pořizovacími cenami, jsou-li nižší než náklady na tvorbu, přitom se jimi chápou pořizovací ceny majetků, za které byly pořízeny v době, kdy se o nich účtuje. Z již uvedeného vyplývá, že pro účely účetnictví se zákon o oceňování majetku nepoužije.[14]

Jedním z dalších důvodů pro ocenění nehmotného majetku formou know-how a obchodního tajemství může být situace obchodní společnosti v konkurzu (také insolvenci, či likvidaci) jejíž majetek zahrnuje také významné hodnoty nehmotného charakteru. Požadavek ohodnocení nehmotného majetku obchodní společnosti zůstavitele často existuje také v případech vypořádání dědictví. Stejně je tomu i v případech přeměn obchodních společností různými formami, jako fúzí nebo rozdělování společností, také zde nastává nutnost stanovit hodnotu nehmotného majetku. Někdy pak ocenění nehmotného majetku může sloužit jeho vlastníkům coby vstupní informace pro budoucí obchodní jednání, a stejně tak je hodnota nehmotného majetku podstatným parametrem pro stanovení přiměřené satisfakce v rámci některých sporů nekalé soutěže.[15]

Zpravidla se používají tři tradiční přístupy určování hodnoty veškerého majetku (včetně nehmotných statků) tržní, výnosový a nákladový přístup. Co se týče tržního stanoviska, které přikládá váhu na charakteristiky nehmotných statků, lze konstatovat, že jeho užití přichází v úvahu, jen pokud existuje k dispozici dostatečný počet údajů o otevřeném trhu porovnatelných nehmotných statků. Je to však možné jen v podmínkách dlouhodobého a rozvinutého tržního hospodářství. Výnosový přístup je využíván především k oceňování průmyslových práv a popřípadě i jiného duševního vlastnictví. Jeho variantou může být například takzvaná licenční analogie, která předpokládá prodej ohodnocovaného nehmotného majetku prostřednictvím úplatné smlouvy třetí osobě, či poskytnutí práva k jeho

[14] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 39. ISBN: 978-80-245-1920-3

[15] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 40-41. ISBN: 978-80-245-1920-3

užívání. Na základě toho by byly placeny poplatky, a to po dobu platnosti dané smlouvy, popřípadě do konce užitečné životnosti daného technického řešení.

Také lze využít variantu přírůstku přínosu neboli zisku, tu můžeme využít v těch případech, kdy je možné prokázat, že ty výrobky, které se opírají o nehmotné vlastnictví, mají v prodejní ceně zaznamenán vyšší zisk oproti shodnému nebo podobnému výrobku konkurenta. K použití této metody je nutné mít k dispozici velký počet ekonomických údajů, a to například o výkonech a rozsahu výroby, to znamená, že není jednoduché tuto metodu věcně použít. Opačnou variantou je pak metoda předpokládané ztráty výnosu neboli zisku, jejímž důsledkem je snížení dosavadního zisku, popřípadě i jeho zaniknutí. Poslední metodou daného přístupu je reziduální výnosová metoda, zde se od celkových výnosů zjištěných z celkového podnikání organizace odečítá výnos spjatý s hmotným majetkem. Výsledek pak představuje výnos předpověditelným nehmotným statkům.[16]

Tradiční nákladový přístup vycházející ze skutečně vynaložených nákladů se pro tržní oceňování nehmotných statků nepoužívá příliš často. Většinou jeho použití můžeme vidět spíše ve spojitosti s oceňováním ochranných známek, ty však nejsou předmětem této práce.[17]

Při oceňování nehmotného majetku je potřeba zohledňovat a zaobírat se určitými specifiky, která ovlivňují jeho hodnotu. Důležitým specifikem je časové hledisko, vztah mezi hodnotou času a nehmotným majetkem. Know-how i obchodní tajemství můžeme zařadit pod technická řešení, která jak je známo časem postupně zastarávají, a tím také ztrácí na své hodnotě. Na úplném začátku, a to ať v době vytvoření, přihlášení k ochraně nebo v době zveřejňování, má takovéto ve své podstatě nové technické řešení stoprocentní hodnotu, ale po jeho uvedení a využití na trhu začíná pomalu jeho hodnota klesat. Zde začne fungovat konkurence, která okamžitě začíná hledat způsob, jak obejít patentovou ochranu, a začíná s vývojem obdobného a pokud možno také lepšího řešení. V momentě, kdy se jí to podaří, začnou hodnoty předmětného technického řešení prudce klesat.[18]

[16] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 42 - 43. ISBN: 978-80-245-1920-3
[17] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 43. ISBN: 978-80-245-1920-3
[18] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 46 - 47. ISBN: 978-80-245-1920-3

Specifikem oceňování nehmotného majetků je zvažování rizik, která souvisejí s jeho budoucím vývojem. Pro vyjádření míry rizik se stanovují koeficienty nebo míry kapitalizace, případně se provádí ocenění ve více variantách, které zohledňují možné kladné a záporné okolnosti a jejich závažnosti. V nynější době je dle přílohy č. 16 k vyhlášce č. 3/2008 míra kapitalizace pro účely zákona o oceňování majetku pro majetková práva stanovena na 12%, přitom při porovnání této výše s dalšími položkami u rozdílných statků můžeme vidět, že rizikovost při oceňování nehmotných statků je nadprůměrná (ze všech nejvyšší). Jde tedy o pracné jednání v oblasti oceňování nehmotného majetku, které by nemělo být zanedbáváno.[19]

Při oceňování můžeme využívat zjišťování podílu na výrobě, to ale nebývá vždy úplně jednoduché vzhledem ke komplexním ekonomickým údajům. Ty většinou zahrnují výrobky jakékoli povahy, myšleno i výrobky jiné povahy než ty, jenž souvisí s oceňovacím právem. Zde pak chybí potřebný kauzální vztah mezi oceňovaným předmětem a ekonomickými údaji. Také je nutné stanovit podíl oceňovaného práva či nehmotného majetku na výrobku, výrobě, službách nebo zařízení, kde je možné znovu narazit na nepříjemnosti v souvislosti s počtem průmyslově chráněných předmětů účastnících se na jejich produkci. K tomuto je nutné provádět u mnoha výrobků technickou analýzu konstrukčního, technologického a dalšího řešení s důrazem na kvalitativní a funkční aspekty, ty by měly převládat nad aspekty mechanickými a dále pak přiřazovat daným znakům výrobků znaky nároků z vybraných průmyslově chráněných předmětů.[20] Při oceňování těchto předmětů je možné zohledňovat také náklady vynaložené na samotnou ochranu, například správní poplatky, odměna autorům či původcům ochrany, právní zastoupení apod. Nicméně z pohledu zanedbatelné výše těchto nákladů nemají ve většině případů vliv na hodnotu předmětů oceňování.[21]

3.4.2 Licenční smlouva k užívání know-how a obchodního tajemství

V praxi často dochází k tomu, že obchodní tajemství je poskytnuto k užívání jiné osobě, než jakou je majitel podniku, respektive obchodního tajemství. Toto užívání je potřeba zpravidla

[19] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 49. ISBN: 978-80-245-1920-3
[20] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 50-52. ISBN: 978-80-245-1920-3
[21] ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 52-55 ISBN: 978-80-245-1920-3

smluvně ošetřit. Na to jsou různé způsoby. Jedním je například uzavření smlouvy o nájmu podniku dle § 488 obchodního zákoníku, jejíž sjednání zároveň prokazuje existenci zákonné licence k využívání obchodního tajemství. Pokud ale podnik pouze poskytuje obchodní tajemství bez ujednání nájmu podniku, tak je obvykle nutné smluvně upravit užívání tohoto samotného tajemství. To je možné provést uzavřením licenční smlouvy k předmětům průmyslového vlastnictví dle § 508 až 515 obchodního zákoníku, případně sjednáním smlouvy inominátní (tzv. bezejmennou) dle § § 269 odst. 2 obchodního zákoníku. Podle právních teoretiků je velmi sporné se rozhodnout, která z těchto smluv je výhodnější volbou. Například P. Hajna je toho názoru, že povolení k užití obchodního tajemství se poskytuje zvláštní licenční smlouvou, která také bývá označována za nepravou licenční smlouvu. Jelikož podmínky zákon výslovně neupravuje, muselo by se proto jednat o inominátní kontrakt a při koncipování této smlouvy by se mohly strany inspirovat ustanovením § 508 a násl. obchodního zákoníku o licenční smlouvě k předmětům průmyslového vlastnictví.[22] Dále například podle K. Eliáše smluvní typ není výslovně upraven a zřejmé je jen to, že tajemství není prodejné na základě kupní smlouvy, jelikož jejím předmětem může být jen věc.[23] Příčinou rozporů je především nerozhodnost, zda zařadit obchodní tajemství mezi předměty průmyslového vlastnictví, ke kterému se vztahuje výše uvedená licenční smlouva, a také aplikace tohoto typu smlouvy. Pokud by bylo možné toto konstatovat, tak podle I. Pelikánové a J. Dědiče jde o jasný předpoklad uzavření licenční smlouvy dle § 508 a násl. obchodního zákoníku. K. Marek k tomu dodává: „Je možno zvážit, zda lze dnešní licenční smlouvu upravit tak, aby zahrnovala širší okruh vztahů (s výjimkou autorských licenčních smluv podle autorského zákona), včetně licenční smlouvy na know-how zahrnující např. technologické postupy či materiálové složení přísad zboží, které nejsou chráněny průmyslovými právy.“[24]

Pokud se zaměříme na uzavírání výše uvedené licenční smlouvy, je potřeba si uvědomit, že musí splňovat některé předpoklady. Smlouva musí být uzavřena v písemné formě, je nutné upřesnit smluvní strany a specifikovat jejich práva, podle kterých se výkon poskytuje,

[22] ŠTENGLOVÁ, I. – DRÁPAL, L. – PÚRY, F. et al. Obchodní tajemství: Praktická příručka. Praha: Linde Praha, a.s., 2005. s. 25. ISBN 978-80-89447-26-8
[23] ŠTENGLOVÁ, I. – DRÁPAL, L. – PÚRY, F. et al. Obchodní tajemství: Praktická příručka. Praha: Linde Praha, a.s., 2005. s. 25-26. ISBN 978-80-89447-26-8
[24] MAREK,Karel; Licenční smlouva (k předmětům průmyslového vlastnictví). Bulletin advokacie. 2008, roč. 19,č.7-8, s. 27. ISBN 978-80-7208-922-2

vymezit rozsah, upřesnit území jeho poskytnutí a určit cenu. Smlouvu je možná sjednat jako nevýhradní či výhradní, doba jejího sjednání je upravena dispozitivně tzn., že je možné smlouvu sjednat také na dobu určitou i neurčitou. Dle obchodního zákoníku má poskytovatel licence povinnost bez zbytečného odkladu po uzavření licenční smlouvy poskytnout nabyvateli informace a podklady potřebné k výkonu práva podle této smlouvy a má také povinnost udržovat dané právo po celou dobu trvání smlouvy, pokud to povaha tohoto práva vyžaduje. Naopak nabyvatel má povinnost utajovat poskytnuté informace a podklady před třetími osobami, a to i po skončení smlouvy až do té doby, než se stanou obecně známými.[25] Podle úpravy obchodního zákoníku má poskytovatel oprávnění k výkonu práva, které je předmětem smlouvy a má právo poskytnou ho jiným osobám, ale pokud by byla licenční smlouva sjednána jako výhradní, nebyl by oprávněn nakládat s jejím předmětem ani jeho poskytovatel.[26]

Jelikož jednou z problematických otázek spojených s institutem obchodního tajemství je i existence a užívání podniku bez jeho současného provozování, tak z možnosti uzavřít o jeho samostatném užívání s druhou osobou smlouvu, se dá usuzovat, že je taková situace možná.

3.5 Důvěrné informace

Obchodní tajemství a know-how ale nejsou jedinými daty, které je potřeba v podnikovém prostředí chránit. Mezi ty patří mnoho dalších dat a z nich plynoucích informací. Rozdíl mezi informacemi a daty je dle teorie informací smysl, který je k datům přiřazený. Informace jsou data obohacená o jejich význam. Například řetězec čísel 2015, 472 mil. Kč, 3,4 mld. Kč představuje z informatického pohledu nějaká data. Ale až kontext, který říká, že obrat určité společnosti vzrostl během roku 2015 z 3,4 mld. Kč o 472 mil. Kč, dává příjemci pochopitelnou informaci. Pro potřeby této práce není potřeba informace a data dále rozlišovat, bude na ně nahlíženo jednotně.

Další informace, které je v podnikovém prostředí zapotřebí chránit proti zneužití patří například:

[25] MAREK,Karel. Licenční smlouva (k předmětům průmyslového vlastnictví). Bulletin advokacie. 2008, roč. 19, č. 7-8, s. 26–28. ISBN 978-80-7208-922-2
[26] SLÁMA. Jiří, Licenční smlouva. Bulletin advokacie. 2008, roč. 19, č. 12, s. 26. ISBN 978-80-7239-206-3

- Osobní údaje, které je potřeba chránit na základě platné legislativy. Osobním údajem se dle § 4 písm. a) zákona č. 101/2000 Sb. rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.[27]
- Kritická data pro chod podniku. Nemusí jít pouze o know-how či výrobní postupy. Může jít o materiály k připravované marketingové kampani, které je potřeba uchránit před zraky a sluchy konkurence do doby, než se stane veřejnou, výroční zprávu o chodu podniku před jejím vydáním, komunikaci o chystané akvizici jiné společnosti, nebo třeba o informace zcela důvěrného charakteru typu výše platů zaměstnanců podniku apod.
- Jiné citlivé údaje, které třeba nemají pro chod podniku zásadní význam, ale mohly by jej anebo jeho obchodní partnery poškodit.

Data a informace, které je potřeba chránit, můžeme souhrnně nazvat důvěrnými daty či důvěrnými informacemi. Samotná ochrana musí být zajištěna nejen uvnitř podniku a jeho procesů, ale protože většina podniků v tržním prostředí není uzavřená pevnost a musí komunikovat se svým okolím, tak také v umístěních, do kterých se tyto informace dostávají mimo podnik. Někdy je třeba důvěrná data a informace předat obchodním partnerům, často se totiž uzavírají obchodní vztahy, při kterých je předání i těch nekritičtějších informací jako je podnikové know-how nutné. Může jít o důležité subdodávky do výrobního či jiného kritického procesu, dodání informačního systému spravujícího část procesu výroby, dodávky služeb či zboží zákazníkovi, dodávky specializovaných výrobních technologií, nebo třeba outsourcing celé výroby.

3.5.1 Smlouvy o ochraně důvěrných informací

V takovém případě se mezi spolupracujícími subjekty uzavírají smluvní vztahy obsahující úpravu ochrany důvěrných informací. Tyto smlouvy obsahují klauzule o vysokých sankcích v případě vyzrazení jakékoli neveřejné informace včetně třeba i textace samotné smlouvy a nezapomínají ani na náhradu případné škody vzniklé pochybením jedné ze smluvních stran.

[27] PAVLÁT, David; Pojem osobní údaj [online]. 2013 [cit. 2016-08-08]. Dostupné z: https://www.uoou.cz/pojem-osobni-udaj/d-1751

Smlouvy samostatně podepisované za účelem ochrany důvěrných informací se nazývají také smlouvami o mlčenlivosti, nebo souhrnně zkratkou NDA (z anglického Non-Disclosure Agreement). NDA smlouvy se často používají v situacích, kdy je potřeba předat důvěrné informace v předstihu před uzavíráním samotných obchodních smluv o spolupráci. Často je to například při výběru dodavatele při výběrovém řízení, kdy je potřeba už pro vypracování nabídky předat všem uchazečům podklady, které podnik nechce nebo nemůže jen tak zveřejnit. Uchazeči se těmito smlouvami zavazují podklady použít skutečně jen pro vypracování nabídky a následně smazat nebo vrátit. V takových situacích je na místě ohlídat, aby se i v rámci spolupracujících společností dostali k předmětným informacím jen ti pracovníci, kteří k tomu mají důvod a oprávnění.

3.6 Ochrana důvěrných informací uvnitř podniku

Ještě přesněji by se tato ochrana mohla formulovat jako ochrana důvěrných informací uvnitř podnikových procesů. To totiž lépe postihuje dnešní dobu, kdy jsou často data přenášena (přenosné počítače, externí disky, USB klíčenky, CD, ale i v tištěné podobě) nebo uložena (různá vzdálená úložiště) mimo podnik. Podnik ale musí zajistit, aby veškerá manipulace s daty, ať již těmi fyzicky vytištěnými či v elektronické podobě, odpovídala popsaným podnikovým procesům.

3.6.1 Podnikové procesy

Podnikové procesy (často i v českém podnikovém prostředí označované jako business procesy) představují sadu akcí, pravidel a definovaných pomůcek ve formě různých šablon, směrnic, manuálů, SW nástrojů či úložišť apod., které dohromady představují jakousi kuchařku pro postupování v pro podnik typických situacích. Popis všech pro úspěch podniku kritických procesů je důležitý proto, aby bylo zajištěno, že všichni pracovníci při své činnosti postupují stejně, používají stejné šablony, ukládají jednotlivé typy dokumentů na stejná úložiště a reportují stejnou formou do stejného systému (či na stejném místě). Například v případě dobře popsaného obchodního procesu je při jeho důsledném využívání zajištěno, že nabídky, smlouvy a další dokumenty vycházejí ze stejných šablon, mají stejnou formu a jsou uloženy tak, aby je kdokoli v případě potřeby nalezl.

Procesy vycházejí ze zkušeností daného podniku a jeho pracovníků a při jejich důsledném následování je zajištěno, že se aktivity dějí dle možností a znalostí podniku efektivně. Stejně tak jsou procesy doplňovány v případě výskytu nějaké chyby či nalezení možné

optimalizace, a tím je zajištěno, že se při respektování definovaných procesů stejné chyby neopakují. I podnikové procesy, které zrovna nepopisují způsob výroby produktu, patří mezi know-how podniku. Může v nich být obsažena unikátní obchodní metoda, která je v daném odvětví extrémně účinná, může v nich být schována spousta drobných detailů, které dohromady dávají fungující komplex aktivit, který přispívá k prosperitě podniku. Proto i popisy podnikových procesů patří mezi důvěrná data a je třeba je chránit.

Procesy mohou být nastaveny čistě z vůle či prozřetelnosti podniku v rámci interních směrnic nebo třeba jen jako součást nepsaných pravidel. Často se ale podnikové procesy formalizují dle některé z obecně uznávaných norem. V takovém případě se procesy nechávají certifikovat (akt ověření, že procesy odpovídají požadavkům normy), aby bylo navenek známé, že podnik funguje tak, jak normy požadují. Takové normy mohou být zaměřeny na různé oblasti podnikání nebo obecných zájmů. V Evropě a tedy i v České republice se nejčastěji certifikuje dle norem ISO (International Organization for Standardization – mezinárodní organizace zabývající se tvorbou norem). Často jsou normy označovány pod společnou hlavičkou ISO/IEC (The International Electrotechnical Commission).

3.6.2 Procesy dle ISO

Hlavní motiv pro certifikaci dle norem je prokázání certifikované organizace, že v rámci svých procesů udržuje deklarovanou kvalitu. Samotná certifikace spočívá v důsledné kontrole jednotlivých aktivit, které v organizaci probíhají, jestli odpovídají nastaveným procesům. Stejně tak jsou všechny nastavené procesy podrobeny kontrole, jestli odpovídají požadavkům norem. Norem ISO je celá řada, ale pro téma této práce jsou nejzajímavější tyto tři:

- ISO 9001(standard pro systém managementu kvality),
- ISO 20001 (management služeb pro informační technologie)
- ISO 27001 (standard, který definuje požadavky na systém managementu bezpečnosti informací).

3.6.2.1 ISO 9001

První zmínky o potřebě vzniku této normy se datují ve 20. létech minulého století. Rozjížděla se sériová výroba a bylo potřeba systémově zajistit stabilní kvalitu výroby tak, aby se

nemusel testovat každý vyrobený kus produktu. Publikace prvních norem se začaly vyskytovat po druhé světové válce. Přístup jednotlivých zemí a korporací se ale lišil. Norma ISO 9001, která dnes patří k nejpoužívanějším, vznikla ve Velké Británii v 80. létech minulého století. Následně byla rozšířena do celé Evropy a spolu s tím vznikly i první nezávislé certifikační autority (společnosti s privilegiem certifikovat).

Dle normy vedení certifikované společnosti samo definuje své plány a cíle pro dosažení kvality výroby. Nastaví se procesy a s jejich pomocí jsou cíle postupně dosahovány, přičemž účinnost procesů je měřena a procesy jsou na základě tohoto měření a vyhodnocování v čase optimalizovány. ISO 9001 reflektuje principy řízení dokumentace, infrastruktury a lidských zdrojů. Zavádí či optimalizuje procesy interakce se zákazníky, hodnotí dodavatele a měří výkonnost procesů. Na jejím základě jsou zaváděny interní audity, které slouží jako pravidelná zpětná vazba k procesnímu řízení.

3.6.2.2 ISO 20001

ISO 20001 je standardem pro systém řízení v oblasti služeb poskytovaných prostřednictvím informačních technologií. Základem této normy je ITIL (Information Technology Infrastructure Library). ITIL je soupisem nejlepších zkušeností (v IT branži používané mezinárodně známé označení best practice) používaným ve firmách zabývajících se dodávkou služeb prostřednictvím nebo se zásadním využitím informačních technologií.

V rámci této normy je definován princip identifikace procesů, které jsou nezbytné pro dodávku bezvadných služeb v oblasti informačních technologií. Jsou definovány procesy a jejich vzájemné působení. Je také požadován systém pravidelných interních auditů, které slouží pro získání zpětné vazby umožňující kontinuální optimalizaci a porovnávání úrovně IT služeb se standardy na trhu (benchmarking – mezinárodně často používané označení z anglického jazyka).

3.6.2.3 ISO 27001

Standard definující požadavky na systém řízení bezpečnosti informací, především pak řízení bezpečnosti důvěry informací pro zaměstnance, procesy, IT systémy a strategii firmy.

Norma se zabývá například ochranou státem definovaných citlivých dat (osobní údaje) a zaručuje soulad s platnou legislativou. Zavedení ISO 27001 s sebou přináší systémový přístup k ochraně dat a zásadně napomáhá snížit riziko krádeže či zneužití důvěrných dat.

3.7 Analýza rizik

Pokud bychom toto téma zobecnili, dostaneme se k závěru, že každý den činí lidé spousty rozhodnutí a volí mezi různými alternativami řešení daného problému, což s sebou přináší jistá rizika. Pokud se chceme rozhodovat správně, všechna tato rizika rozebíráme a na základě výsledků provedeme tzv. správné rozhodnutí. Stejná situace nastává i v případě ochrany informací v podniku. I tady je nutné počítat s jistými riziky, jako například když některá osoba změní nebo vymaže záznamy z firemní databáze, případně dojde k selhání zařízení. Proto je potřeba všechna tato rizika a zranitelná místa systému volbou vhodných opatření omezit na minimum. Důležitost dat a informací je mnohdy veliká a finančně nevyčíslitelná. Bezpečnost informací znamená starost a komplexní zájem o dokumenty, data a software, který se v podniku používá, dále o způsob práce s daty, vnitropodnikovou komunikaci a spolupráci.

Citlivost informací vůči cizím zájmům může být různá, od přísně tajných až po ty, které by naopak měly být zveřejněny. Bezpečnostní systém pak umožní informace strukturovat a stabilizuje v nich určitý řád. Analýza rizik pracuje se třemi základními vstupy, jimiž jsou aktiva, zranitelná místa a hrozby.

Mezi aktivity jsou řazeny hmotné i nehmotné statky, které mají pro svého majitele určitou hodnotu. Jedná se o hardware (počítače, paměťová média, periferní zařízení), software (operační systémy, aplikační programy) a především informace a data. Dále sem patří také komunikační média (sítě, přenosová zařízení a média) a lidé, tedy uživatelé systému (operátoři, uživatelé, vedoucí). Každé z těchto aktiv vnáší do systému určité množství zranitelných míst a ta mohou být zneužita. Zranitelným místem mohou být záležitosti fyzické podstaty, lidský faktor, selhání hardwaru, vliv prostředí, nespolehlivost a nestabilita softwaru, odposlouchávání sítí

Aktiva typu data lze z hlediska jejich zranitelných míst a závažnosti rozdělit do několika tříd. Prvním může být porušení důvěrnosti a prozrazení informace, to se může týkat jak vlastních uživatelů systému, tak externích dodavatelů, nebo prozrazení ostatním osobám. Dalším je modifikace elektronické pošty, jako je vložení falešných zpráv, popření odeslání nebo přijetí zprávy, nedoručení zprávy, nesprávné doručení atd. Další třídou je nedostupnost – následky plynoucí z faktu, že informace nejsou dostupné oprávněným uživatelům. Mezi nejzávažnější rizika patří zničení dat uživatelem. Jako hrozba je pak označováno reálné

nebezpečí plynoucí z existence zranitelného místa včetně konkrétní pravděpodobnosti její realizace. Mezi základní zdroje hrozeb jsou řazeni lidé, nehody a přírodní katastrofy.

3.8 Citlivá data

Citlivá data nelze bezpečně poznat, každá organizace si musí sama určit, co právě pro ni jsou citlivá data. Bezpečnostní standart SEC 501 definuje citlivá data jako: „Jakákoliv data, jejichž kompromitace porušením utajení, integrity nebo dostupnosti může mít zásadní dopad na zájmy dotčené strany, průběh programů organizace nebo soukromí jednotlivci. Citlivost dat je přímo úměrná škodám, které mohou vzniknout jejich kompromitací. Organizace musí klasifikovat každý IT systém příslušným stupněm citlivosti, a to dle nejcitlivějších dat, která systém skladuje, zpracovává nebo přenáší.“[28] Citlivá data potřebujeme chránit, a to je možné různými způsoby. Jejich volba záleží na mnoha faktorech, jako je například citlivost dat, potřeba jejich dostupnosti apod.

Aby byla ochrana dat skutečně silná, je potřeba nastavit komplexní systém využívající mnohé techniky ochrany, které dohromady reagují na mnoho různých typů rizik. Jedním ze základních způsobů je omezení přístupu na základě rozhodnutí a vypracování, kdo a za jakých podmínek k datům může. Další možností eliminace možnosti, že se k datům dostane neoprávněná osoba, je šifrování dat. Případný útočník se bez znalosti hesla, dešifrovacího klíče a dešifrovacího algoritmu dostává pouze ke shluku znaků, nikoliv ke skutečným datům či informacím.

Podrobně se různým známým typům rizik komplexnímu setu bezpečnostních opatření věnuje praktická část této práce.

[28] PŘIBYL, Tomáš; ICT Security. Citlivá data: hlídáme utajení, integritu i dostupnost [online]. 2010 [cit. 2016-08-08]. Dostupné z: http://www.ictsecurity.cz/11101-mngmnt-citlivych-dat-dlpecmdmsaaa/citliva-data-hlidame-utajeni-integritu-i-dostupnost.html

4 Praktická část

4.1 Příklady dobře využitého know-how

V následujících kapitolách jsou popsány obecně známé příklady dobře využitého know-how pro prosperitu daných společností.

4.1.1 Apple

Pro ukázku toho, jak je know-how podniku důležité pro jeho dlouhodobý rozvoj a co ve spojení s vizí, nadšením pro věc, neutuchající vytrvalostí a správným načasováním dokáže, může posloužit společnost Apple Inc. z kalifornského Cupertina. Tento technologický gigant má v moderním světě svou nezaměnitelnou pozici. Společnost letos oslavila 40 let na trhu. Za tu dobu slavila historické úspěchy a zažila téměř likvidační zklamání. Za obojím stála postava absolutního vládce. Steve Jobs dostal společnost od založení v garáži svých adoptivních rodičů (společnost založili 3 společníci, přičemž vedle Jobse měl především Steve Wozniak zásadní podíl na rozvoji společnosti) nejprve na burzu a nakonec z ní vytvořil nejhodnotnější společnost na světě (hodnota v roce 2016 je odhadována přes 100 miliard amerických dolarů). Kde za tímto úspěchem hledat know-how? U Jobse byl základ pravděpodobně v navštěvování hodin grafiky a designu při jeho jinak v klasickém pojetí neúspěšném studování v Portlandu na Reed College a také v jeho silnému sklonu k východním učením. Díky těmto dispozicím měl touhu dělat vše krásné, dokonalé a pokud možno co nejjednodušší. Jobs měl představu, že přivede osobní počítače do každé domácnosti a rozhodně se dá říci, že byl u toho, protože to byl především konkurenční boj, který v té době táhl pokrok kupředu. I když svět nakonec za společnost, která to dokázala, považuje jiného giganta – společnost IBM. Menších či větších úspěchů měl Apple více, ale skutečně převratný počin předvedla v roce 1984. V té době přišla s počítačem Macintosh, který byl jako vůbec první ovládaný v grafickém uživatelském rozhraní (GUI – graphic user interface) a ovládaný myší. Myš jako takovou vymyslela společnost Xerox, ale Jobsovým nápadem bylo jí využít v grafickém prostřední pro ovládání tak, jak ho známe dnes. Byla to právě jeho touha usnadnit uživatelům práci a udělat jí jednodušší a příjemnější.

Obrázek 1 - Logo společnosti Apple

Zdroj: https://twitter.com/apple

Byla to Jobsova filozofie a dodnes je to součástí know-how společnosti Apple, že je třeba dělat krásné vše, třebaže to je pro zákazníka při klasickém použití neviditelné. Začalo to trváním na dobře zpracovaných tištěných spojích, pěkné krabici prvního počítače a je to vidět na dnešní kultuře celé společnosti i prodejního procesu. Dokonalé musí být vše. Samozřejmostí je samotný produkt, ale v Apple si dávají velmi záležet i na jeho představení, na jeho obalu, Jobs trval na tom, že i rozbalování nového produktu musí být pro zákazníka zážitkem, ale i na prodeji, kdy sítě prodejen Apple podléhají přísným požadavkům, aby vypadaly jednotně, moderně a naprosto čistě. Jobs dokonce to samé očekával i od vlastní montážní linky, vše muselo být naprosto čisté a ideálně bílé. Že jsou i dnešní produkty tvořeny s důrazem na jednoduchost ovládání je vidět na první pohled. Minimum ovládacích prvků (například na telefonu iPhone jediné ovládací tlačítko pro kompletní navigaci), intuitivní prostředí, dohromady vyladěný software a hardware. Na telefonech Apple je to ostatně znát nejvíce. Zatímco iOS (operační systém pro telefony Apple) je použitý pouze u iPhone telefonů, a tudíž je možné naprosto přesně využít možnosti na míru stavěného zařízení (hardwaru), konkurenční Android od společnosti Google je vyvíjen s cílem využití na stovkách zařízení a tedy musí být více univerzální. A výsledek? Při testování intuitivnosti ovládání dětmi byl iPhone v rukách nejmenších uživatelů nadšeně využíván a děti překvapovaly tím, co všechno s ním dokázaly a kam až se dostaly. U Androidu se většinou brzy zasekly a nemohly dál.

Z příběhu společnosti Apple lze vyčíst, že Steve Jobs díky své povaze a vlastnímu know-how, které dokázal vnuknout své společnosti, vytvořil korporaci, která změnila svět, tedy minimálně ten technologický. Vytvořil společnost, která jej přežila (Jobs zemřel v roce 2011) a která, pokud si zachová principy svého zakladatele, bude dlouho mezi špičkou

technologických firem. Vytvořil takovou kulturu své značky a produktů, že má pravděpodobně jedny z nejloajálnějších zákazníků na světě, pro které počítač není jen počítačem, ale i tím vším okolo. Know-how společnosti Apple je ukryté v mnoha technologických postupech výroby, ale za úspěchem jejích produktů stojí v minimálně stejné míře i znalost toho, jak produkty dostat mezi lidi a ty totálně pobláznit, aby už nikdy nechtěli nic jiného.

4.1.2 Plzeňský Prazdroj

Pro další příklad ukázkově využitého know-how můžeme použít lokálního výrobce piva Plzeňský Prazdroj. První zmínky o městském pivovaru v Plzni sahají až do roku 1501, kdy ale kvalita produktu ještě nebyla valná a přispěla k rozhodnutí postavit pivovar nový – předchůdce Plzeňského Prazdroje. Historie se začala psát roku 1839, kdy se měšťané v Plzni rozhodli postavit vlastní nový pivovar. O tři roky později byl dokončen Měšťanský pivovar Plzeň a započal obdivuhodný příběh. První sládek Josef Groll byl povolán z Bavorska, aby uvařil pivo bavorského typu. První várka se mu nepovedla dle jeho představ, protože nepočítal se specifickými místními surovinami (měkká voda, žatecký chmel, světlejší slad připravovaný anglickou technologií), ale sklidila velký úspěch. Tak vzniklo pivo, kterému se dodnes po celém světě říká pivo plzeňského typu (světlé spodně kvašené pivo vařené dle plzeňské receptury). Pivovar si pak postupně nechal zaregistrovat obchodní známky Pilsner Bier – Plzeňské pivo (1859) a Plzeňský Prazdroj – Pilsner Urquell (1898). Pivovar záhy po svém založení získal úspěch v Praze následovaný dalšími úspěchy ve Vídni či Paříži.

Obrázek 2 - Logo společnosti Plzeňský Prazdroj

Zdroj: https://www.prazdroj.cz

V novodobé historii Plzeňského Prazdroje došlo po druhé světové válce ke znárodnění a sloučení s konkurenčním plzeňským Akciovým pivovarem pod hlavičku národního podniku Plzeňské pivovary. Po Sametové revoluci pak vznikla akciová společnost a nakonec v roce 1994 společnost s dnešním jménem. Následně byl pivovar prodán jihoafrické společnosti South African Breweries, která se následně sloučila s americkou Miller Breweries a vznikla

společnosti SABMiller s centrálou v Londýně. Nový majitel avizoval, že se k pivovaru bude chovat jako k rodinnému stříbru a naštěstí tak i postupoval. Prazdroj se postupně rozšiřoval a do skupiny převzal další pivovary – Radegast a Velké Popovice. Důležité je, že si po celou dobu své existence Plzeňský Prazdroj uchoval své know-how výroby svého produktu. Že se to vyplatilo, dokazuje nejen unikátní postavení ve střední Evropě s prodaným ročním objemem deseti miliónů hektolitrů piva v roce 2015 (piva pod značkou Pilsner Urquell z toho jsou 2 miliony hektolitrů), ale také ekonomické výsledky. V roce 2015 společnost dosáhla tržeb 14,4 miliardy Kč a zisku 3,7 miliardy Kč.

Nyní je Plzeňský Prazdroj opět na prodej. Může za to převzetí mateřské společnosti největším světovým výrobcem piva – společností Anheuser-Busch InBev. Evropská komise schválila transakci pouze s podmínkou, že nově vnikající subjekt prodá pivovarnické aktivity společnosti SABMiller v Evropě, tedy i Plzeňský Prazdroj. Zájemců je dost a přes různé iniciativy snažící se přimět vládu ČR k odkoupení zpět do vlastnictví státu to vzhledem k ceně vypadá opět na zahraničního vlastníka.

Podobných případů, kdy je know-how dané společnosti klíčem k úspěchu, bychom nalezli mnoho. Že je v podmínkách tržní ekonomiky plné nemilosrdné konkurence zapotřebí know-how chránit, aby konkurence jednoduše unikátnost nezkopírovala, je již také jasné. Jistě existují i společnosti, které žádné specifické know-how nevlastní a také přežívají či dokonce prosperují (i když na prosperování bez unikátních znalostí, postupů či procesů nebo použitého materiálu už to jistě nějaké know-how chce), ale ani pro ty není od věci se zaměřit na ochranu některých v rámci podnikání zpracovávajících dat. Na to, jak k této problematice přistupovat, jsou zaměřeny další kapitoly této práce.

4.2 Zkoumaná společnost AMI Praha a. s.

Pro účely ukázky možností ochrany know-how a dalších ochranu si zasloužívších dat bude použita konkrétní společnost z českého prostředí. Pomůže to lépe vykreslit reálnou situaci, ve které se společnost může vyskytovat, a to jak z pohledu potřeby ochrany specifických druhů informací a dat, tak co se týká efektivity jednotlivých bezpečnostních opatření. V této práci nebudou řešeny ostatní předpoklady dalšího úspěšného fungování zkoumané společnosti. Bude pouze analyzováno, s jakými daty společnost nakládá, co považuje za své klíčové faktory úspěchu, a bude navrženo, jak by mohla či měla postupovat v oblasti zachování důvěrnosti pro ni klíčových dat tak, aby to neohrozilo její další existenci.

Společnost AMI Praha je malou českou společností působící v oblasti informačních technologií a fungující od roku 1996. Původně byla založena jako webová agentura nabízející internetové prezentace firmám na českém trhu a jak říkají služebně nejstarší pracovníci této společnosti, na začátku to bylo především o jakési evangelizaci trhu. Pojem vypůjčený z křesťanství může znít velmi silně, ale v době, kdy o internetu nikdo nic nevěděl, si opravdu obchodníci snažící se prodat služby internetové firmy mohli připadat jako věřící jedinci seznamující nekřesťany s evangeliem. Internetová prezentace tehdy nebylo nic, co by jako dnes uměl postavit téměř každý středoškolák, a platily se za ně horentní sumy. Představa, že se něco takového snažíte prodat vedoucímu pracovníkovi, který si prostřednictvím internetu teprve navyká posílat e-maily, není příliš lákavá. Společnost AMI Praha byla od začátku svého působení poměrně úspěšná a poskytovala své služby zvučným klientům typu Unipetrol, CAC leasing (dnes UniCredit Leasing) nebo Bank Austria Creditanstalt (dnes UniCredit Bank).

Obrázek 3 - Logo společnosti AMI Praha a. s.

Zdroj: http://www.ami.cz

Přibližně dva roky po přelomu tisíciletí si ale management společnosti začal uvědomovat, že jen s internetovými prezentacemi to nepůjde. Konkurence byla veliká a začaly se objevovat i malá uskupení internetových nadšenců, kteří vytvářeli tzv. garážové webové agentury. Pod tímto pojmem byly myšleny miniaturní firmy často ani nemající kanceláře, ve kterých pracovníci fungují z domova (často domova svých rodičů) a navíc všichni pracovníci včetně managementu jsou také realizátoři. Pro zavedené společnosti s více zaměstnanci, managementem, obchodníky, recepcí, ustálenými procesy a především nájmem za kanceláře taková konkurence představuje veliké riziko v cenotvorbě. Bylo jasné, že tyto společnosti musely nabídnout něco více. Na jedné straně to byla garance dokončení velkých projektů ve smluveném termínu, garance nejvyšší možné kvality, zastupitelnost jednotlivých rolí realizátorského týmu, diametrálně odlišný servis při poskytování služeb a

v neposlední řadě support v režimu, který si zmíněná malá uskupení nemohla dovolit – například technická podpora při provozu internetové prezentace 24 hodin denně 7 dní v týdnu s garantovanými reakčními dobami. V AMI Praha ale šli dále a z internetové firmy udělali adopcí nových technologií a kompetencí malou softwarovou společnost. Začali část svých řešení stavět na platformě Java EE (Java Enterpsise Edition – v té době jeden z nejrozšířenějších programovacích jazyků pro tvorbu tzv. enterprise solutions, tedy česky podnikových řešení). Cílem již nebylo uspokojit pouze marketingové potřeby klientských společností při jejich snaze zaujmout trh, ale podpořit a především zautomatizovat interní procesy klientů. Přerod podnikatelského plánu se podařil, ale vývoj šel ještě dál. Zásadní změna v podobě zúžení zaměření přišla kolem roku 2008, kdy společnost AMI Praha s partnerem Sun Microsystems (nadnárodní výrobce IT) nasadily nástroj pro řízení uživatelů, jejich oprávnění a rolí v prostředí skupiny ČEZ. Bylo to tehdy největší nasazení nástroje tohoto typu ve střední Evropě a poznamenalo to další směřování AMI Praha. V té době se tato společnost začala zaměřovat především na dodávku podobných řešení, která jsou při automatickém přidělování a odebírání oprávnění do IT systémů v organizaci zaměřená primárně na bezpečnost.

Dnes má společnost AMI Praha přibližně 35 pracovníků (aktuální počet se liší dle souběžně běžících projektů) a je, jak se sama prezentuje, lídrem českého trhu v oblasti nasazování řešení pro řízení oprávnění jak k IT systémům, tak k datům na diskových úložištích. Pro potřeby této práce je AMI Praha ideální kandidát pro analýzu. Se svým zaměřením na bezpečnost má nasazené některé nástroje chránící data, ale jak to dle přísloví o kovářově kobyle bývá, ne všechny. Má nastavené procesy řízení dle norem ISO 9001 a ISO 27001 a přitom jde pořád o malou společnost s procesy dostatečně jednoduchými a nesvázanými byrokratickými administrativními povinnostmi. Z těch je jednoduše čitelné, s jakými daty je ve společnosti nakládáno a která z nich je potřeba chránit.

4.2.1 Data zpracovávaná v AMI Praha

Při studiu procesů, které společnost AMI Praha implementovala při zavádění ISO norem, lze nalézt důvěrná data, se kterými společnost pracuje a která chrání tak, aby nebyly vyzrazeny konkurenci nebo veřejnosti. Samotné procesy jsou také v režimu ochrany označeny jako důvěrné, proto je tato práce neuvádí. Obecná povaha dat, která se v procesech vyskytuje

v některém z ochranných režimů, ale uvést lze. Samotné stupně ochrany jsou zde definovány tři:

- Bez označení – tedy dokumenty a data, které společnost volně sdílí interně i vně společnosti. Jsou to většinou obecně známé skutečnosti, nebo třeba informace, které společnost sama publikuje, aby na sebe upoutala pozornost.
- Interní – dokumenty a data, které jsou volně sdíleny uvnitř společnosti ale již ne mimo společnost. Může k nim tedy libovolný pracovník AMI Praha. Jsou to různé návody, postupy, interní směrnice, obecné informace apod.
- Důvěrné – dokumenty a data, které podléhají nejvyššími stupni ochrany. Mohou k nim pouze pověření pracovníci, kteří je potřebují k výkonu své práce. Některé tyto dokumenty jsou sdíleny mimo společnost, ale opět pouze v důvěrném režimu. To se týká především nabídkových dokumentů, prostřednictvím kterých společnost nabízí své služby zákazníkům, a také smluv, které společnost uzavírá se svými obchodními partnery. Do kategorie důvěrné bez sdílení se třetími stranami patří mimo jiné veškeré osobní údaje zaměstnanců, zaměstnanecké smlouvy, informace o obchodních příležitostech, obchodní kontakty, obchodní plány a strategie, know-how v podobě výrobních postupů, různé metodiky, již zmiňované procesy, šablony dokumentů používaných při kalkulacích a realizacích a spousta dalších dokumentů a dat, jejichž zveřejnění by mohlo společnost poškodit. Patří sem ale také data, ke kterým se společnost dostala díky realizaci projektů u zákazníků a jejichž zabezpečení je pod velkými sankcemi zajištěno ve smlouvách upravujících podmínky realizace či samostatných ujednáních o ochraně důvěrných informací. Někdy je potřeba, aby se tato data poskytla dále subdodavatelům v daném obchodním případu. Potom je třeba, aby byly i s těmito subdodavateli uzavřeny smlouvy se stejnými nebo přísnějšími parametry.

Je zde počítáno s různou formou existence dat. Zde je základní rozdělení jednoduché, existuje:

- fyzická podoba, tedy například vytištěný dokument,
- elektronická podoba, u které je způsobů uložení mnohem více.

Chránit je samozřejmě potřeba všechny formy dat. S tím, jak přicházejí další a další možnosti uložení, se stává disciplína jejich ochrany stále větší výzvou, se kterou společnostem pomáhají specializovaní dodavatelé.

4.3 Přístup k zabezpečení dat proti zneužití

V první řadě je potřeba, aby si management společnosti uvědomil, že je potřeba data chránit. Prvotní impulz může mít mnoho podob. Tam, kde je uchovávané zásadní výrobní know-how v podobě specifického receptu nebo výrobního postupu, si většinou potřebu ochrany dávno uvědomují. Jinde je potřeba nějaký spouštěč, který společnost přinutí. V lepším případě to může být auditní nález, který ještě nemusí mít zásadní následky, ale třeba jen doporučení bez jakýchkoli sankcí. Může to být i jen proces zavádění řízení dle ISO norem, které v sobě požadavky na ochranu obsahují. Často je to ale až bezpečností situace, kdy již k nějakému zneužití dat dojde, která společnost přinutí jednat. Dle zkušeností pracovníků AMI Praha je za poptávkou po službách z oblasti bezpečnosti téměř vždy nějaký problém, buď již velmi rozezlený auditor, nebo incident často právě pro ignorování nálezů z auditů.

Když už se společnost rozhodne, že nebude spoléhat na dobrou morálku všech okolo a raději své know-how a další citlivá data zajistí, musí začít především u sebe doma. Je potřeba vytvořit systém směrnic neboli bezpečnostní politiku, která mimo jiné formálním způsobem definuje, kdo k čemu a v jakém okamžiku má jaká práva. Je potřeba brát zřetel i na konkrétní fázi životního cyklu dokumentů či dat, protože je mnoho těch, u kterých se potřeba zajištění v čase mění. Například taková výroční zpráva o hospodaření společnosti je ve fázi svého vzniku důvěrným dokumentem, jehož zveřejnění by mohlo společnost poškodit. Naopak po zveřejnění ve správném čase se již jedná o dokument, ke kterému má (u určitých forem podnikání) ze zákona přístup jakýkoli zájemce. Směrnice také stanoví, kde a v jaké podobě mají být data uložena, ať už se jedná o uložení fyzických dokumentů nebo elektronických dat. Stejně tak by mělo být, ať již z předmětné směrnice nebo nějakého vnitřního řádu společnosti, což je vlastně také směrnice, všem jasné, jaké postihy čekají na toho, kdo se proti směrnici proviní. Celý tento systém směrnic ještě přímo žádná data neochraňuje, ale vytváří formální prostředí navázané na legislativní rámec právního státu, ve kterém všichni pracovníci ve společnosti vědí, co a se kterými dokumenty či daty mohou a co již nemohou dělat a co je čeká v případě, že budou konat něco proti společnosti. Společnosti to dává možnost při přistižení provinilce perzekuovat, což už samo o sobě odradí mnoho rozumně

smýšlejících lidí od případného pokušení. Samozřejmostí je, aby každý ve společnosti předmětné směrnice podepsal, nebo alespoň podepsal záznam o proškolení. Dále je nezbytné míti s pracovníky podepsané pracovní smlouvy, ve kterých je minimálně odkaz na dodržování interních směrnic.

Ve společnosti AMI Praha je výše popsaný systém směrnic vytvořen a je formálně zachycen v dokumentaci jednotlivých procesů řízení. Jeho dodržování je pravidelně kontrolováno v rámci několika auditů, které ve společnosti díky certifikaci na normy ISO každoročně probíhají. Smlouvy a záznamy o proškolení směrnicemi jsou podepisovány nejen se všemi pracovníky, kteří se ve společnosti vyskytují, ale také se všemi subdodavatelskými společnostmi, které se účastní projektů pro koncové zákazníky, případně dodávají služby pro potřeby AMI Praha.

Když je vytvořen formální rámec, je na řadě přijetí takových praktických opatření a využití takových nástrojů, které zajistí bezpečnost důvěrných dat v případě, že se někdo rozhodne formální rámec ať již vědomě nebo nevědomky obejít.

4.4 Ochrana dokumentů

U tištěných dokumentů je ochrana poměrně jednoduchá a více méně se neliší od toho, co byli zvyklí praktikovat v nedávné minulosti. Většinou jde pouze o kritičnost chráněných dokumentů, od které se odvíjí počet zámků, za kterými jsou dokumenty uchovávány. Ty nejdůležitější dokumenty se mohou uschovat v bankovním trezoru, méně důležité v trezoru v prostorách kanceláře společnosti, pro některé stačí zamčená zásuvka pracovního stolu v kanceláři. U větších podniků, provozů a strategických zařízení je možné se potkat s termínem ochrana perimetru. Jde o zabezpečení objektu nebo celého areálu tak, aby se po něm nemohl pohybovat nikdo neoprávněný. Tato problematika ale již přesahuje téma této práce, proto nebude detailně rozebírána.

AMI Praha ani její pracovníci nemají bezpečnostní prověrku Národního bezpečnostního úřadu a nepracují s informacemi podléhajícími vysokému stupni utajení, proto pro většinu dokumentů stačí běžný uzamykatelný kancelářský nábytek. V tomto smyslu hovoří i interní firemní procesy. Každý vlastník konkrétního výtisku dokumentu je zodpovědný za jeho uzamčení a zajištění, aby se k němu nedostal nikdo neoprávněný. Ve větších společnostech mohou být zavedeny i systémy, které umožňují odemykání zámků jednotlivých kanceláří

pouze pověřeným pracovníkům. To může být řešeno systémem klasických zámků a klíčů, případně moderněji systémem vstupních karet, které mohou obsahovat několik úrovní oprávnění s nastavením pověření na jednotlivé dveře v objektu. V případě potřeby sofistikovanějšího zabezpečení se instalují různé autentizační (proces ověřování identity) prostředky. Moderní technologie umožňují nejen dnes již standardní čtení otisků prstů, ale načítají celé dlaně, čtou a ověřují dle rohovky či krevního řečiště. Především poslední dvě jmenované varianty patří ke špičce v oboru. Nejen, že jsou velmi těžko zfalšovatelné (například u krevního řečiště případným škůdcům nepomůže ani hrubé násilí, pro načtení dlaně je nutné, aby v ní proudila krev), ale jsou bezkontaktní a je tak možné je využít i v provozech, kde není zcela čisto. Toto už ale není realita společnosti AMI Praha. Jak bylo zmíněno, zde si majitelé a management vystačí s mnohem jednoduššími technologiemi.

4.5 Elektronická data

Zde je situace s ochranou mnohem složitější. Elektronická data jsou dnes totiž všude kolem nás. A pokud je společnost chce uchránit proti zneužití, musí zajistit všechna místa, kde se tato data vyskytují, a zajistit, aby se nedostala nikam, kde je chránit nedokáže. Umístění, kde se firemní data nejčastěji mohou vyskytovat:

- Data v infrastruktuře společnosti:
    - aplikace a systémy,
    - databáze,
    - sdílené souborové systémy.
- Data mimo infrastrukturu společnosti (infrastruktura dodávaná formou služby):
    - aplikace a systémy,
    - databáze,
    - sdílené souborové systémy.
- Data mimo infrastrukturu na zařízeních ve vlastnictví společnosti:
    - PC a notebooky,
    - mobilní telefony,
    - USB disky a klíčenky,
    - CD, DVD apod.
- Data na jiných zařízeních:
    - osobní notebooky pracovníků,

- osobní mobilní zařízení pracovníků,
- osobní přenosná úložná zařízení pracovníků.

Možností a úhlů pohledu na to, jak elektronická data v podniku chránit, je opravdu mnoho. Pro základní výčet oblastí a nástrojů, které do nich zapadají, je možno využít Zákon o kybernetické bezpečnosti (zákon č. 181/2014 Sb., účinný v ČR od 1. 1. 2015, dále také jen ZoKB). Ten stanovuje, co musejí zajistit organizace (úřady, podniky), které provozují takzvanou kritickou informační infrastrukturu státu, případně významné informační systémy. Práce v následující části vychází z doporučení, jak důležité IT systémy a důvěrná data, povahou podobná těm, která jsou předmětem této práce, mají dle zákona chránit výše zmíněné subjekty. Práce vychází také z toho, že zákonodárci při své snaze zajistit bezpečnost systémů kritických pro základní fungování státu vzali do úvahy veškerá v daném okamžiku známá rizika. Proto tato práce tento legislativní předpis přejímá a bere ho za směrodatnou aktuální metodiku přístupu k ochraně dat na základě ohodnocení známých kybernetických rizik. Bezpečnostní opatření jsou v zákoně dělena na organizační opatření a technická opatření.

Organizačními opatřeními dle ZoKB jsou:

- systém řízení bezpečnosti informací,
- řízení rizik,
- bezpečnostní politika,
- organizační bezpečnost,
- stanovení bezpečnostních požadavků pro dodavatele,
- řízení aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
- řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
- akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,

- řízení kontinuity činností a
- kontrola a audit kritické informační infrastruktury a významných informačních systémů.

3) Technickými opatřeními dle ZoKB jsou:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací a
- bezpečnost průmyslových a řídicích systémů.

Pro výčet povinností zainteresovaných organizací v oblasti zaměření této práce je vhodné využít vyhlášku 316/2014, která nese krkolomný název „Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti“ a konkrétně její Hlavu 1 a Hlavu 2 – výše zmíněná organizační a technická opatření. Tato část vyhlášky obsahuje řadu paragrafů, které popisují jednotlivé oblasti bezpečnosti a konkrétní požadavky, které je třeba řešit. Problematika řešená zákonem a jeho vyhláškou představuje komplexní zajištění bezpečnosti použitelné pro nejdůležitější aktiva státu. Jakýkoli jiný subjekt tedy může vzít tento kompletní výčet jako doporučení a přizpůsobit si ho svým potřebám, podle závažnosti dopadů při narušení bezpečnosti v jeho podmínkách. Zatímco organizace provozující kritickou infrastrukturu státu nebo státem definované významné informační systémy musejí splnit všechny požadavky, ostatní subjekty mohou vyhodnotit přínosy zavedení jednotlivých doporučení a s přihlédnutím k efektivitě ochrany si vybrat jen ty, která pro ně dávají smysl.

Dále v textu jsou popsány jednotlivé dílčí oblasti dle rozdělení v zákoně a u každého paragrafu je přidán výsledek zkoumání a řešení dané problematiky ve společnosti AMI Praha. Cílem je shromáždit dostatek dat k následnému posouzení, jestli je bezpečnost dat ve zkoumané společnosti na dostatečné úrovni, kde jsou případná slabá místa, na kterých je potřeba zapracovat, a jak efektivní by vzhledem k přínosům (nebo spíše eliminaci hrozících rizik) a nákladům bylo další zabezpečení.

4.6 Organizační opatření

Organizační opatření stanovená v ZoKB mají za cíl nastavit v institucích a společnostech formální rámec v podobě souboru politik a nařízení, bezpečnostní organizační struktury a požadavků na konkrétní bezpečnostní oblasti tak, aby byla zajištěna prevence před kybernetickými bezpečnostními riziky a byly nastavené procesy obnovy a nápravy v případě, že i přes opatření dojde k bezpečnostním incidentům.

4.6.1 § 3 Systém řízení bezpečnosti informací

Organizační opatření v uvozujícím paragrafu (třetí paragraf vyhlášky, kterým začíná výčet organizačních opatření) vynucují stanovení základního rámce pro řízení bezpečnosti. Konkrétně jde o:

- stanovení hranic ochraňovaného systému,
- řízení rizik,
- vytvoření bezpečnostní politiky,
- monitoring účinnosti těchto opatření,
- vyhodnocování účinnosti bezpečnostní politiky,
- provádění bezpečnostních auditů,
- vyhodnocování celého systému řízení bezpečnosti informací,
- aktualizace tohoto systému,
- řízení provozu a zdrojů systémů řízení bezpečnosti informací.

Tento základní rámec je detailněji rozepsán v dalších paragrafech, kde je i v jednotlivých bodech zhodnoceno, jak se s daným tématem pracuje ve společnosti AMI Praha.

4.6.2 § 4 Řízení rizik

Řízení rizik je bezpochyby jedním ze základních kamenů celé problematiky ochrany dat. Ať již jde o organizaci nebo jednotlivce, aby se bylo možné chránit, je potřeba vědět, proti čemu

ochrana slouží a jaké jsou případné následky, pokud ochrana nebude dostatečná. Zákon v této oblasti požaduje:

- vytvoření metodiky pro identifikaci a hodnocení aktiv a rizik, která musí obsahovat kritéria přijatelnosti jednotlivých rizik,
- samotnou identifikaci a hodnocení aktiv,
- identifikaci rizik při zohlednění hrozeb zranitelnosti, a to včetně posouzení dopadů,
- vydání prohlášení o aplikovatelnosti, které obsahuje přehled vybraných a zavedených bezpečnostních opatření,
- zavedení plánu zvládání rizik, který musí obsahovat:
    - cíle a přínosy bezpečnostních opatření pro zvládání rizik,
    - určení osoby zajišťující prosazování bezpečnostních opatření,
    - finanční, technické, lidské a informační zdroje,
    - popis vazeb mezi riziky a příslušnými bezpečnostními opatřeními a
    - termíny zavedení,
- zohlednění reaktivních a ochranných opatření vydaných Národním bezpečnostním úřadem.

Zákon dále vyjmenovává množství různých typů zranitelností a zvažuje především tyto hrozby:

- porušení bezpečnostní politiky, neoprávněné činnosti, zneužití oprávnění administrátorů,
- pochybení zaměstnanců,
- zneužití vnitřních prostředků, sabotáž,
- dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie apod.,
- nedostatek zaměstnanců s potřebnou odbornou úrovní,
- cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
- zneužití vyměnitelných technických nosičů dat.

Zákon umožňuje řídit rizika i jinými způsoby, ale subjekt spadající pod vliv tohoto zákona musí zabezpečit, že jím využívaná opatření mají stejnou nebo vyšší úroveň.

V AMI Praha k rizikům přistupují zodpovědně. Protože u svých klientů rizika často analyzují, mají jejich pracovníci znalosti, zkušenosti i nástroje k analýze ve vlastním prostředí. Od dob certifikace dle ISO procesů je v této společnosti využívána metoda analýzy rizik CRAMM (Risk Analysis and Management Methodology vytvořená společností CCTA). Metoda vyžaduje ohodnocení aktiv, jejich seskupení do logických celků a identifikaci hrozeb působících na tyto celky. Dále se prozkoumává zranitelnost systému a definují se požadavky bezpečnosti pro jednotlivé celky.

Na základě analýzy jsou při respektování hodnoty rizik a již nasazených nástrojů navržena bezpečnostní opatření. Vždy se analyzují modely systémů, nikoli systémy samotné.

4.6.3 § 5 Bezpečnostní politika

Zákon o kybernetické bezpečnosti vyžaduje stanovení bezpečnostní politiky v mnoha oblastech:

- systém řízení bezpečnosti informací,
- organizační bezpečnost,
- řízení vztahů s dodavateli,
- klasifikace aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací,
- řízení přístupu,
- bezpečné chování uživatelů,
- zálohování a obnova,
- bezpečné předávání a výměna informací,
- řízení technických zranitelností,
- bezpečné používání mobilních zařízení,
- poskytování a nabývání licencí programového vybavení a informací,
- dlouhodobé ukládání a archivace informací,
- ochrana osobních údajů,
- fyzická bezpečnost,
- bezpečnost komunikační sítě,
- ochrana před škodlivým kódem,
- nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí,

- využití a údržba nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí a
- používání kryptografické ochrany.

Ze seznamu je patrné, že oblastí ochrany, a tedy i možných hrozeb je celá řada a je jednoduché si představit, že bez různých metodik, návodů, či konzultací je pro organizaci velmi obtížené vlastními silami definovat veškerá úskalí, která v oblasti informačních technologií číhají.

V AMI Praha mají bezpečnostní politikou pokrývající minimálně do úrovně vydaných závazných směrnic pokryté všechny výše zmíněné oblasti. Některé z nich jsou pro typ organizace v podobě malé komerční společnosti nepodléhající požadavkům zákona o kybernetické bezpečnosti více relevantní a některé méně. Ale již jen z důvodu, že svým zákazníkům předmětným zákonem často argumentují, snaží se sami k jednotlivým požadavkům přistoupit maximálně poctivě.

4.6.4 § 6 Organizační bezpečnost

Z pohledu organizace řízení bezpečnosti zavádí vyhláška povinně obsazené role, které každá organizace podléhající povinnostem zákona musí mít. Jedná se o:

- manažera kybernetické bezpečnosti odpovědného za systém řízení bezpečnosti informací,
- architekta kybernetické bezpečnosti zajišťujícího návrh a implementaci bezpečnostních opatření,
- auditora kybernetické bezpečnosti provádějícího audit kybernetické bezpečnosti a
- garanta aktiva, tedy osobu pověřenou k zajištění rozvoje, použití a bezpečnosti aktiv.

Tyto role jsou povinné skutečně pouze pro předmětnému zákonu podřízené organizace a jsou jakýmsi personálně-organizačním zajištěním toho, že je kybernetické bezpečnosti věnována dostatečná pozornost. Ve standardní organizaci obsazení všech těchto rolí není nezbytné, ale je nutné si uvědomit, že od jisté velikosti společnosti či složitosti systému je vyhrazený pracovník nezbytností. Pokud totiž bude mít bezpečnost na starost někdo, pro koho to bude jen poslední z mnoha povinností, může se stát, že bude ochrana zanedbána, a

přijde se na to až po zásadním bezpečnostním incidentu, který může mít pro společnost zásadní následky.

Ve společnosti AMI Praha vzhledem k její velikosti tyto role obsazené nejsou. Je zde pouze manažer ISMS (Information Security Management System), který je zodpovědný za tvorbu a pravidelnou optimalizaci bezpečnostních postupů a také za řízení náprav a další prevence u zjištěných incidentů. Tento manažer je také pověřený za zastupování a obhajobu systému bezpečnosti při pravidelných auditech, případně funguje jako garant a jakási autorita pro ostatní pracovníky společnosti.

4.6.5 § 7 Stanovení bezpečnostních požadavků pro dodavatele

Legislativa v této části vyžaduje zavedení jasných pravidel pro dodavatele, které respektují potřeby bezpečnostní politiky a zohledňují je také u dodavatelů podílejících se na rozvoji, provozu nebo zajištění bezpečnosti informačních systémů. Pravidla mimo jiné vyžadují provedení hodnocení rizik dodávky, uzavření smlouvy o úrovni služeb, pravidelné hodnocení rizik a pravidelnou kontrolu zavedených bezpečnostních opatření včetně odstranění nedostatků.

V AMI Praha je kladen na vlastní dodavatele a subdodavatele u klientských řešení velký důraz. Úroveň služeb u řešení poskytovaných vlastním klientům musí především respektovat smluvně domluvenou úroveň služeb s těmito klienty. Aby se minimalizoval počet případů snížení kvality služeb, ať již se jedná o klientská řešení nebo dodávky pro potřeby vlastní společnosti, dochází ve společnosti AMI Praha k pravidelnému hodnocení dodavatelů. Stanovení vlastníci z řad pracovníků AMI Praha jednou za půl roku oznámkují dodavatele podobně jako ve škole známkami 1 až 4, přičemž od známky 3 je povinný komentář toho, proč je udělena tato známka. Cílem je eliminovat spolupráci s dodavateli, kteří jsou ohodnoceni známkou 4, nebo se dlouho pohybují na úrovni známky 3. Vztah k tématu této práce je jasný. Jelikož dodavatelé disponují přístupy k citlivým datům zákazníků společnosti AMI Praha či jejím vlastním, je potřeba ukončit spolupráci s těmi, u kterých není důvěra, že tato data nezneužijí, či jakkoli použijí v rozporu se smluvními ujednáními. Příkladem může být nedávno ukončená spolupráce se společností dodávající CRM (Customer relationship management) nástroj, ve kterém jsou uložena veškerá data o stávajících i potenciálních zákaznících a obchodních příležitostech. Jelikož dodavatel nepůsobil ve svém jednání příliš důvěryhodně, byla spolupráce raději ukončena dříve, než by se citlivá data dostala k jiným

zákazníkům tohoto dodavatele, kteří jsou se společností AMI Praha v přímém konkurenčním vztahu.

4.6.6 § 8 Řízení aktiv

Tato část zákona v rámci řízení aktiv vyžaduje především:

- identifikaci primárních a podpůrných aktiv a vazeb mezi nimi,
- stanovení garantů pro jednotlivá aktiva,
- zhodnocení důležitosti aktiv z hlediska důvěrnosti, integrity a dostupnosti a rozdělení do úrovní, přičemž je třeba zohlednit:
    - rozsah a důležitost osobních údajů či obchodních tajemství,
    - rozsah právních povinností,
    - rozsah narušení vnitřních řídících a kontrolních činností,
    - poškození veřejných, obchodních nebo ekonomických zájmů a možné finanční ztráty,
    - rozsah narušení běžných činností organizace,
    - dopady spojené s narušením důvěrnosti, integrity a dostupnosti a
    - dopady na zachování dobrého jména nebo ochranu dobré pověsti.

Zákon také vyžaduje ustanovení pravidel ochrany a manipulace pro jednotlivé definované úrovně aktiv.

Řízení aktiv je ve společnosti AMI Praha požadováno ne zákonem ale certifikací dle ISO. Na základě z nich vyplývajících povinností ve společnosti existuje evidence všech významných aktiv a jsou stanoveni jejich vlastníci, kteří přebírají úlohu garantů. Systém úrovní má tři stavy – veřejné, interní a důvěrné. Pro jednotlivé úrovně jsou nastaveny pravidla zacházení, které zajišťují potřebnou míru ochrany.

4.6.7 § 9 Bezpečnost lidských zdrojů

Zdánlivě jasná záležitost, která ale bez důsledného vyžadování dodržování postupů zapříčiňuje mnohé bezpečnostní nepříjemnosti. Je zde po organizacích vyžadováno:

- stanovení plánu rozvoje bezpečnostního povědomí v organizaci,
- zajištění poučení všech uživatelů (včetně administrátorů a osob zastávajících bezpečnostní role) o jejich povinnostech a o bezpečnostní politice formou

vstupních a pravidelných školení, a to včetně vedení záznamů o těchto školeních minimálně v míře popisu obsahu školení a seznamu účastníků,
- zajištění kontroly dodržování bezpečnostní politiky,
- zajištění vrácení svěřených prostředků, a především odebrání přístupových oprávnění při ukončení smluvního vztahu s uživateli, případně jejich změnu při změně postavení uživatele.

Při analyzování této oblasti v AMI Praha bylo zřejmé, že je na řízení lidských zdrojů z pohledu bezpečnosti kladen velký důraz. Je to jednak dáno požadavky certifikace a dále většinou přísnými podmínkami a sankcemi v případě porušení mnoha NDA smluv se zákazníky. Jelikož téměř všichni pracovníci společnosti přicházejí do styku s některými takto ošetřenými důvěrnými informacemi, je třeba, aby byli všichni poctivě proškoleni a o školení byl vyhotoven a uložen záznam, který může být v případě pochybení pracovníka použit jako argument, že bylo uděláno vše podle procesů. Školení probíhá primárně v tématech jednotlivých procesů nastavených dle požadavků ISO certifikace. Dále jsou všichni pracovníci seznamováni s obsahy směrnic, ve kterých je upraveno povolené zacházení s důvěrnými informacemi. V případě nasazení pracovníků na projekty s extrémně přísnými podmínkami v rámci NDA smluv jsou tito pracovníci dále proškolováni na konkrétní směrnice z bezpečnostních politik zákazníků.

4.6.8 § 10 Řízení provozu

Tato část vyhlášky vyžaduje nastavení pravidel, postupů a zodpovědností pro detekci kybernetických bezpečnostních událostí, pravidelné vyhodnocování získaných informací a reakce na ně. K samotné detekci dříve, než k událostem dojde, slouží technické prostředky popsané dále v této práci. Z organizačního pohledu je ale také třeba zajistit, aby bylo zcela jasné, co se má dít, pokud se k bezpečnostnímu incidentu schyluje, nebo již nastal.

Celá tato oblast je předmětem disciplíny označované zkratkou BCM (Business Continuity Management), která v předstihu analyzuje možné nežádoucí stavy po bezpečnostních incidentech a snaží se nastavit pravidla a postupy tak, aby se v případě výskytu takového stavu nejdůležitější procesy v organizaci nezastavily, nebo alespoň co nejdříve opět rozběhly. Kromě jasně dané posloupnosti kroků, které se mají vykonat po zjištění, že došlo k bezpečnostnímu incidentu, jsou také nastavené preventivní požadavky a aktivity a jejich požadované periodicity. Jedná se například o pravidelné zálohy, zkoušky jejich

použitelnosti, oddělování různých IT prostředí, testování funkčnosti samotných BCM procesů apod.

Protože velmi příbuznému tématu se věnuje i § 14 z organizačních opatření, je způsob řešení BCM problematiky v AMI Praha popsán na jeho konci.

4.6.9 § 11 Řízení přístupu a bezpečné chování uživatelů

V paragrafu 11 jsou vyjmenovány požadavky na řízení přístupů uživatelů k informačním systémům. Jsou požadována opatření, která slouží k zajištění ochrany údajů, které jsou používány pro přihlášení uživatelů k IT systémům a dále opatření bránící zneužití těchto údajů neoprávněnou osobou.

K řešení tohoto požadavku jsou v ideálním případě využity IT nástroje popisované dále mezi technickými prostředky. Jelikož i v AMI Praha disponují podobným nástrojem, bude řešení této oblasti popsáno dále v kapitole s příslušným technickým řešením u § 19.

4.6.10 § 12 Akvizice, vývoj a údržba

Zákon v této části vyžaduje stanovení bezpečnostních požadavků na změny informačních systémů spojené s jejich akvizicí, vývojem a údržbou. Je zde požadavek na identifikaci, hodnocení a řízení rizik souvisejících se změnami informačních systémů výše popsaného charakteru a dále na vytvoření bezpečného vývojového a testovacího prostředí. Připravované změny musejí být před uvedením do provozu bezpečně testovány.

V AMI Praha jsou dle procesů ISO nastaveny postupy pro vystavování změn v infomačních systémech, které se týkají jak vlastních systémů, tak zákaznických řešení. Je zde striktně vyžadováno, aby veškerý vývoj probíhal odděleně na vývojovém technickém prostředí, testovalo se v odděleném testovacím technickém prostředí na testovacích datech (někdy bývá jednotné vývojové a testovací prostředí) a teprve po důkladném odzkoušení dle předem stanovených testovacích scénářů se změny vystavily na produkční prostředí do ostrého provozu.

4.6.11 § 13 Zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů

Pro zvládání kybernetických bezpečnostních událostí u informačních systémů je třeba:

- zavést opatření zajišťující oznamování těchto událostí ze stran uživatelů a o těchto oznámeních vést záznamy,
- provádět vyhodnocení událostí a identifikovat kybernetické bezpečnostní incidenty,
- provádět klasifikaci a analýzu těchto incidentů,
- prošetřit a určit příčiny incidentů,
- a na základě vyhodnocení stanovit nutná bezpečnostní opatření k zamezení opakování řešeného incidentu.

Při řešení této problematiky je bezpečnější než spolehnout na oznamování všímavými uživateli nasazení sofistikovaného technického nástroje hlídajícího dění v jednotlivých systémech a na síti a z toho vyhodnocovat, jestli se neschyluje k nějaké nechtěné události. Moderní informační systémy umožňující tuto podporu a případně i zastavení činností dalších informačních systémů, pokud to bezpečnostní situace vyžaduje.

Technické možnosti systémů pokrývající tuto oblast jsou popsány včetně rozboru řešení této problematiky ve společnosti AMI Praha dále v části s technickými opatřeními u § 23.

4.6.12 § 14 Řízení kontinuity činností

Řízení kontinuity činností je srdcem výše zmíněné disciplíny BCM. V této části zákona jsou uvedeny požadavky na:

- stanovení práv a povinností garantů aktiv, administrátorů a osob zastávajících bezpečnostní role,
- cíle řízení kontinuity činností formou určení:
    - minimální úrovně poskytovaných služeb, která je přijatelná pro užívání, provoz a správu informačního systémů,
    - doby obnovení chodu, během které bude po kybernetickém bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb informačních systémů,
    - dobu obnovení dat jako termínu, ke kterému budou obnovena data po kybernetickém bezpečnostním incidentu.
- strategii řízení kontinuity činností,
- vyhodnocení možných dopadů a posouzení možných rizik,
- stanovení, aktualizace a testování plánů kontinuity činností informačního systému,

- realizaci opatření pro zvýšení odolnosti informačního systému,
- vyhodnocení případných negativních dopadů na provoz a bezpečnost informačního systému.

Potřeba v AMI Praha v otázce nastavení BCM procesů není nijak dramaticky výrazná a jsou zde prakticky nastaveny jen základní postupy pro případ výpadku některých služeb externích dodavatelů. V tomto směru je pro společnost nejdůležitější rychlé zapojení záložního připojení do sítě internet, aby nedošlo k dlouhému přerušení chodu služeb zákaznických řešení v případě, že je výpadkem postižena lokalita, kde jsou hostované servery, případně aby mohli pracovníci pokračovat ve své práci, pokud jsou výpadkem zasaženy kanceláře. Pro další podobné případy jsou jistě nastaveny i další kroky, ale jejich řešení není pro téma této práce podstatné, proto se jim nebude dále věnovat.

4.6.13 § 15 Kontrola a audit

Na závěr organizačních opatření jsou popsány požadavky na aktivity, které si každý ve spojení s podobnými opatřeními nutně vybaví – kontrola a audit. V rámci kontroly a auditu kybernetické bezpečnosti je vyžadováno:

- posouzení souladu bezpečnostních opatření předpisy, normami a legislativou,
- provedení a dokumentace pravidelné kontroly dodržování bezpečnostní politiky a zohlednění výstupů z těchto kontrol v plánu rozvoje bezpečnostního povědomí a plánu zvládání rizik.

Dále je pro informační systémy prováděna kontrola zranitelnosti technických prostředků pomocí automatizovaných nástrojů.

V AMI Praha je tato oblast řešena pravidelných ISO audity s podobnými požadavky. Audity probíhají několikrát ročně. Jendou je veden přímo pracovníkem certifikační autority, dvakrát jde i interní audity řízené interním manažerem ISMS. Cílem je ověřit postupování pracovníků společnosti dle nastavených procesů a také optimalizace procesů v praxi podle zjištěných nedostatků případně na základě legislativních či normativních změn. Audity probíhají s garanty jednotlivých procesů a vždy se věnují několika konkrétním zakázkám, které jsou zkoumány od prvotní informace v obchodním oddělení, že je nějaká příležitost, skrze veškeré výrobní aktivity až do konečné fáze akceptace díla klientem, fakturace a předání do servisního úseku.

4.7 Technická opatření

Zatímco organizační opatření se věnovala především potřebě nastavení různých pravidel, obsazení definovaných bezpečnostních rolí a vytvoření příhodného prostředí řízení bezpečnosti v organizaci, technická opatření k jednotlivým tématům stanovují konkrétní požadavky na technické bezpečnostní nástroje.

4.7.1 § 16 Fyzická bezpečnost

Tato část zákona vyžaduje přijetí opatření nezbytných k zamezení neoprávněným vstupům do prostor, kde se vyskytují chráněná data, systémy či infrastruktura a dále vyžaduje přijetí opatření předcházejících poškození, krádežím nebo zneužití předmětných aktiv či komunikačního systému. V §16 je pojednáváno jak o zabezpečení objektů, tak o ochraně uvnitř těchto objektů. Mezi prostředky ochrany jsou vyjmenovány:

- mechanické zábranné prostředky,
- zařízení elektrické zabezpečovací signalizace,
- prostředky omezující působení požárů,
- prostředky omezující působení projevů živelních událostí,
- systémy pro kontrolu vstupu,
- kamerové systémy,
- zařízení pro zajištění ochrany před selháním dodávky elektrického napájení a
- zařízení pro zajištění optimálních provozních podmínek.

Ve své podstatě je tato forma zabezpečení shodná s ochranou dat v tištěných dokumentech. Cílem je, aby se případný útočník nedostal do prostor, kde se data (ať již ve fyzické či digitální formě) či jiná aktiva nacházejí.

Zabezpečení v této oblasti ve společnosti AMI Praha je již popsáno v kapitole o ochraně fyzických dokumentů, neboť fyzická bezpečnost je v těchto případech prakticky shodná. Síla bezpečnostních prvků by měla přímo úměrně odpovídat hodnotě chráněných aktiv a již není rozhodující, jestli mají tyto aktiva fyzickou nebo digitální podobu.

4.7.2 § 17 Nástroj pro ochranu integrity komunikačních sítí

Požadavky v této části vyhlášky vyžadují zajištění bezpečného přenosu dat mezi vnější a vnitřní sítí, tedy při přenosu mezi internetovou a lokální sítí dané organizace. Je vyžadováno použití technických prostředků v podobě demilitarizovaných zón jako speciálního typu sítě

používaného pro oddělení vnější a vnitřní sítě a tím ke zvýšení bezpečnosti aplikací dostupných z internetu. V neposlední řadě jsou ošetřeny podmínky pro vzdálený přístup do interní sítě.

V případě AMI Praha je pro pokrytí této oblasti využito zařízení firewall výrobce Cisco, které slouží k řízení a zabezpečování síťového provozu mezi sítěmi s různou úrovní důvěryhodnosti a zabezpečení. Zjednodušeně se dá říct, že slouží jako mezivrstva, která definuje pravidla pro komunikaci mezi sítěmi, které od sebe odděluje. Pracovníci AMI Praha se v případě potřeby připojují do interní sítě prostřednictvím VPN (Virtual Private Network). Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů, dochází k autentizaci pracovníka a veškerá komunikace je šifrována, proto je takové propojení považované za bezpečné.

4.7.3 § 18 Nástroj pro ověřování identity uživatelů

Tento paragraf vyžaduje zavedení nástrojů pro ověřování identity uživatelů a stanovuje parametry pro přihlášení k systémům podléhajícím požadavkům zkoumaného zákona. Jedná se o počet faktorů (jedním je standardně heslo, dalším může být například kód ze SMS apod.), složitost neboli síla hesla, doba platnosti hesla a stanovuje různé podmínky pro běžné uživatele a administrátory.

Pro představu, heslo, které je dle zákona považováno za dostatečně silné obsahuje:

- minimálně osm znaků (u administrátorů 15 znaků),
- minimální složitost tak, že heslo obsahuje alespoň 3 z následujících 4 požadavků:
    - nejméně jedno velké písmeno,
    - nejméně jedno malé písmeno,
    - nejméně jednu číslici, nebo
    - nejméně jeden speciální znak odlišný od předchozích požadavků.

Nástroj pro ověření identity musí zamezovat opětovnému používání dříve používaných hesel a neumožnit více změn hesla jednoho uživatele během stanoveného období, které musí být nejméně 24 hodin, a dále musí požadovat opětovné ověření identity po určené době nečinnosti.

Řešení ověřování uživatelů v AMI Praha je popsáno u následujícího paragrafu, který řeší příbuzné téma.

4.7.4 § 19 Nástroj pro řízení přístupových oprávnění

Zde se jedná o řízení přístupových oprávnění pro přístup k jednotlivým aplikacím a datům a pro čtení a zápis dat. Zákon zde pamatuje i na řízení přístupu k operacím měnícím přístupová oprávnění.

Poslední dva paragrafy, respektive nástroje plnící jejich požadavky dohromady identifikují a řídí uživatele a jejich oprávnění napříč veškerými informačními zdroji v organizaci. V principu jde o zajištění toho, aby se uživatel dostal vždy jen k takovým informačním zdrojům, které potřebuje k výkonu své role v organizaci, a to jen v čase, kdy k nim přistupovat má.

Ve společnosti AMI Praha je řešení této oblasti naprostou povinností, protože právě nasazování systémů pro pokrytí problematiky uživatelských oprávnění je její hlavní podnikatelskou činností. Nástroje, které zajišťují automatizaci procesů spojených s vytvářením, změnou či rušením oprávnění v informačních systémech se nazývají identity manažery (oblast se nazývá anglickým pojmem identity management). Ve společnosti AMI Praha mají toto řešeno vlastním unikátním nástrojem s názvem SkyIdentity, který je jedním z celosvětově prvních plnohodnotných identity manažerů poskytovaných z cloudu (IT infrastruktura poskytovaná externím dodavatelem formou služby). Pro cloudové prostředí je využito služeb Microsoft Azure.

Pro ověření uživatelů standardně v technologicky vyspělých organizacích nasazují tzv. access manažery (oblast se nazývá anglickým pojmem access management). Jedná se o nástroje, které vyhodnotí podmínky, za kterých se uživatel přihlašuje, a na jejich základě jej buďto pustí dál, vyžádají si další faktor ověření, nebo přístup rovnou zamítnou. Může se například jednat o geografické nebo časové hledisko, které dle bezpečností politiky definuje, co je a co už není přípustné. V praxi to může znamenat, že uživatel při přihlašování z kanceláře nebo domova v pracovní době bude po zadání hesla standardně vpuštěn. Po uživateli, který se přihlašuje z domova mimo pracovní dobu, bude požadováno vložení dodatečného SMS kódu. A uživateli, který se snaží přihlásit z potenciálně nebezpečné lokality (stát na druhém konci světa), bude přístup rovnou zamítnut. Některé nástroje jsou

dokonce tak vyspělé, že vyhodnotí, pokud se nedlouho po sobě uživatel snaží přihlásit ze vzájemně vzdálených lokalit, že to nemůže být jeden a ten samý uživatel, a přístup také zamítnou.

Přestože i nástroje pro oblast ověřování identity uživatelů společnost AMI Praha svým klientům dodává, sama jej nasazen nemá, což představuje potenciální riziko. Zde dokonale platí rčení o bosé kovářově kobyle. Nasazení vlastními pracovníky by za předpokladu využití dostupného kvalitního open-source nástroje (open-source softwarové nástroje jsou zjednodušeně vyjádřeno nástroje, které se mohou v definovaných podmínkách používat bez placení licencí) pro společnost neznamenalo vynaložení velkých externích nákladů. Jediným nákladem by byl čas interních pracovníků zajišťující nasazení. Protože náročnost nasazení není dle vyjádření ředitele výrobního úseku AMI Praha nikterak zásadní, bylo by dosažení přínosů z provozování takového řešení velmi efektivní.

4.7.5 § 20 Nástroj pro ochranu před škodlivým kódem

Požadavek na ochranu před škodlivým kódem dnes řeší snad každý uživatel počítače či chytrého mobilního telefonu, který se svým zařízením přistupuje k internetu. Ve standardním módu je tato oblast řešena instalací antivirových programů. V podnikovém prostředí je tato oblast složitější o potřebu chránit nejen pracovní stanice (PC, notebook, mobilní zařízení), ale také servery, datové úložiště či komunikační prvky sítě. Existují dva hlavní přístupy. Prvním je již zmíněný antivirový program. Druhý představuje instalaci nástrojů, ve kterých se definují systémy, které jsou zakázány (tzv. black list, neboli je možné instalovat a pouštět vše, kromě potenciálně nebezpečných vyjmenovaných aplikací), nebo v přísnějším režimu systémy, které jsou jediné povoleny (tzv. white list, to znamená, že nelze nainstalovat ani spustit nic jiného, než je v seznamu).

Ve společnosti AMI Praha je tato oblast řešena důslednou instalací antivirových programů na všechny pracovní stanice, mobilní zařízení a jiné technické prostředky, která mají přístup k internetu.

4.7.6 § 21 Nástroj pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů

V rámci § 21 je po příslušných organizacích požadováno používání nástroje, který zajistí:

- sběr informací o provozních a bezpečnostních činnostech, zejména:

    - typ činnosti,
    - datum a čas,
    - identifikaci technického aktiva, které činnost zaznamenalo,
    - identifikaci původce a místa činnosti,
    - úspěšnost nebo neúspěšnost činnosti a
- ochranu získaných informací před neoprávněným čtením nebo změnou.

Dále je vyžadován záznam a jeho uchování po dobu minimálně 3 měsíců u těchto událostí:

- přihlášení a odhlášení uživatelů a administrátorů,
- činnosti provedené administrátory,
- činnosti vedoucí ke změně přístupových oprávnění,
- neprovedení činností v důsledku nedostatku přístupových oprávnění a další neúspěšné činnosti uživatelů,
- zahájení a ukončení činností technických aktiv informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury a významného informačního systému,
- automatická varovná nebo chybová hlášení technických aktiv,
- přístupy k záznamům o činnostech, pokusy o manipulaci se záznamy o činnostech a změny nastavení nástroje pro zaznamenávání činností a
- použití mechanismů identifikace a autentizace včetně změny údajů, které slouží k přihlášení.

Navíc je zde také požadavek na synchronizaci systémového času všech prvků kritické informační infrastruktury.

Tato část zákona se věnuje především administrátorům a jejich aktivitám. Vychází z předpokladu, že je potřeba hlídat i hlídače, který by bez toho měl téměř neomezené možnosti. Kromě toho, že by si mohl kdykoli nastavit jakákoli práva, mohl by i následně smazat záznamy o tom, že těmito právy disponoval. Pak by byl jako pachatel případného zcizení dat prakticky nedohledatelný. Nástroje naplňující představy zákona v této oblasti jej ovšem dokonale hlídají. Zaznamenávají jeho aktivity napříč administrovanými systémy a v případě, že přistupuje k nějakému obzvlášť kritickému, jsou schopny zachytávat stisky kláves při jeho práci, případně rovnou nahrávat (v pravidelných intervalech fotit) jeho obrazovku. Jde

tedy především o prevenci, kdy administrátor, který ví, že je jeho aktivita zaznamenávána, nebude vědomě konat žádné nekalé činnosti, které by byly snadno odhalitelné. Nástroje hlídající administrátory se označují jako PIM (Pivileged Identity Manager) nebo PAM (Privileged Access Manager). Jejich pořízení se svou cenou pohybuje v řádech miliónů českých korun a doporučují se tam, kde je zneužití kritických systémů či dat skutečně velkým rizikem.

Společnost AMI Praha tyto systémy nasazuje svým zákazníkům, nicméně vyhodnotila, že systémy s potřebou sofistikovaného hlídání administrátorů sama nepotřebuje, nasazení by pro ni nebylo vzhledem k ceně nasazení a dosaženým benefitům efektivní, a tedy je nevyužívá.

4.7.7 § 22 Nástroj pro detekci kybernetických bezpečnostních událostí

Paragraf 22 se zaměřuje na kybernetické bezpečnostní události v celé infrastruktuře organizace a vyžaduje nástroj pro detekci bezpečnostních událostí, který je v případě potřeby schopen zablokovat komunikaci mezi vnitřní a vnější sítí, případně v rámci vnitřní sítě nebo serverů.

4.7.8 § 23 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí

Tento paragraf navazuje na předchozí a rozšiřuje jím řešenou problematiku o potřebu sběru a průběžné vyhodnocení kybernetických bezpečnostních událostí a dále požaduje:

- integrovaný sběr a vyhodnocení kybernetických bezpečnostních událostí,
- poskytování informací pro určené bezpečnostní role o detekovaných událostech,
- nepřetržité vyhodnocování aktuálního stavu,
- pravidelnou aktualizaci nastavení pravidel pro vyhodnocování a včasné varování, aby byly omezovány případy nesprávného vyhodnocení událostí nebo případy falešných varování,
- využívání informací, které jsou připraveny nástrojem pro sběr a vyhodnocení kybernetických bezpečnostních událostí, pro optimální nastavení bezpečnostních opatření informačního systému.

Poslední dva paragrafy s ochranou know-how, potažmo jiných citlivých a důvěrných dat zdánlivě nesouvisí. Opak je pravdou. Jedná se o ochranu proti hrozbám, pro jejichž odhalení je třeba znát logiku interních procesů organizace, a navíc mít možnost vyhodnocovat logy

(data o událostech) z různých systémů v reálném čase. To umožní odhalit například situace, kdy pracovník, který má standardně přístup k souborové složce s citlivými daty (to mohou být třeba popsané výrobní postupy) a standardně pracuje s jedním či dvěma soubory denně, najednou otevírá stovky souborů. V tu chvíli je mu potřeba okamžitě zamezit přístup a notifikovat jeho nadřízeného případně bezpečnostní složky. Může to být známka toho, že si soubory někam kopíruje, případně jejich obsah zaznamenává digitálním fotoaparátem.

Nástroje, které pokrývají tuto problematiku, se řadí do skupiny SIEM (Security Information and Event Management) a ani jejich nasazení nepatří k nejlevnějším. V základním módu, kdy jsou jen zaznamenávány logy a ty vyhodnocovány základní logikou, se jedná o statisíce Kč, u pokročilých, které obsahují i bázi známých kombinací souběžných událostí značících nekalé chování (tedy vlastně takové know-how výrobce tohoto nástroje), se pak pořizují v řádech miliónů Kč.

Mimo jiné finanční náročnost pořízení takového nástroje, ale i malé množství systémů s citlivými daty jsou pro společnost AMI Praha důvody, proč, přestože jej nabízí a nasazuje svým zákazníkům, jej sama nasazen nemá.

4.7.9 § 24 Aplikační bezpečnost

Že jsou aplikace dostupné z vnější sítě (převážně internetu) bezpečné, musí být potvrzeno testováním, a to před jejich spuštěním v ostrém provozu a také po každé zásadnější změně v oblasti zabezpečení. A právě to je požadavkem obsaženým v paragrafu s pořadovým číslem 24.

Aplikace se musí testovat proti:

- neoprávněným činnostem,
- popření provedených činností,
- kompromitací,
- neautorizovanou změnou.

Dále je třeba testovat procedury po provedených úkonech (tedy tzv. transakce) před:

- jejich nedokončením,
- nesprávným směrováním,
- neautorizovanou změnou předávaného datového obsahu,

- kompromitací,
- neautorizovaným duplikováním,
- opakováním.

Standardně se pro tyto účely provádí penetrační testy. Penetrační test je v informačních technologiích používaná metoda testování a hodnocení zabezpečení počítačových zařízení, systémů nebo aplikací. Provádí se nedestruktivním testováním, simulací možných útoků na tento systém, jak zevnitř, tak zvenčí. Tester v principu napodobuje hackera (člověka snažícího s cílem vlastního prospěchu prolomit zabezpečení počítačových zařízení) a snaží se identifikovat a otestovat slabá místa v zabezpečení.

V AMI Praha jsou používané aplikace, které prošly testováním v režii jejich dodavatelů. Aplikace, které v AMI Praha vznikají pro potřeby zákazníků, jsou testovány tehdy, pokud zákazník vyhodnotí, že je potřeba zajistit vysoké bezpečnostní standardy a aplikace je volně dostupná z internetu. Aby byla zajištěná nejvyšší kvalita testování, využívá společnost AMI Praha pro penetrační testy specializovaného dodavatele, který se zaměřuje primárně na tuto oblast bezpečnosti IT.

4.7.10 § 25 Kryptografické prostředky

Pro použití kryptografické ochrany zákon stanoví

- úroveň ochrany relevantní pro typ a sílu použitého algoritmu a
- pravidla kryptografické ochrany při přenosu po počítačových sítích nebo při uložení na mobilní či vyměnitelné nosiče dat.

To vše při respektování potřeb vyplývajících z hodnocení rizik dané organizace. Prostředky musí zajistit ochranu důvěrnosti a integrity předávaných nebo ukládaných dat a identifikaci uživatele, který předmětné činnosti vykonal.

Při použití kryptografických prostředků musí být nastaven systém správy klíčů, který zajistí generování, distribuci, ukládání, archivaci, změny, ničení, kontrolu a audit klíčů, přičemž kryptografické algoritmy musí být odolné.

V AMI Praha jsou využívány kryptografické prostředky pro šifrování dat na veškerých pevných discích v počítačích všech pracovníků. Dále jsou zašifrovány sdílená úložiště, na kterých se vyskytují ochranu vyžadující data. Potenciálně slabším místem je absence

směrnice a nástrojů vyžadující a umožňující automatické šifrování dat při kopírování firemních dat na externí pevné disky (například dnes velmi oblíbené flash disky).

4.7.11 § 26 Nástroj pro zajišťování úrovně dostupnosti

Tato část zákona řešícího kybernetickou bezpečnost pro kritické či významné systémy v rámci kritické informační infrastruktury státu se vztahuje na dostupnost systémů a v nich obsažených dat a informací. Vzhledem k tomu, že tato práce pojednává o ochraně dat a informací a dostupnost z tohoto pohledu není zásadní, nebude ani dále rozebírat prostředky používané pro zajištění dostupnosti a ani zkoumat, jakým způsobem je dostatečná dostupnost zajištěná ve společnosti AMI Praha.

4.7.12 § 27 Bezpečnost průmyslových a řídicích systémů

Ani poslední paragraf vyhlášky o kybernetické bezpečnosti není z pohledu zaměření této práce zajímavý. § 27 upravuje požadavky na zabezpečení informačních systémů, u kterých by neoprávněný zásah mohl způsobit ohrožení obyvatelstva. Typickým příkladem je řídicí systém jaderné elektrárny, u kterého musí být zabezpečení na maximální možné úrovni a vzdálený přístup přes internet je naprosto nepřijatelný. Ochrana know-how je proti tomuto tématu jednoduchá úloha pro začátečníky.

AMI Praha systémem spadajícím do kategorie řídících a průmyslových systémů nedisponuje, proto ani neřeší zabezpečení spadající do této kategorie.

5 Zhodnocení výsledků a doporučení

Analýzou aktuální situace v oblasti zabezpečení dokumentů, fyzických i elektronických, v AMI Praha bylo zjištěno, že ve společnosti:

- je zaveden procesní systém řízení a klasifikace dat v jednotlivých procesech,
- procesy jsou certifikovány dle ISO 9001 a ISO 27001 a na dodržování procesů dohlíží specializovaný manažer ISMS,
- je využívána metoda analýzy rizik CRAMM,
- vnitřní síť je zajištěna výkonným firewallem Cisco,
- každý počítač (server, pevné PC, notebook, tablet či chytrý mobilní telefon) je vybaven antivirovým programem,
- je využívána pokročilá metoda šifrování pevných disků,
- je zaveden systém pro automatické řízení uživatelských účtů, oprávnění a rolí v informačních systémech,
- je využívána šifrovaná komunikace typu VPN pro vzdálený přístup k firemním datům.

Naopak bylo šetřením zjištěno, že ve společnosti, přestože je sama nabízí svým zákazníkům, chybí následující nástroje.

- Access manažer zajišťující autentizaci (ověřování identity uživatelů přistupujících k aplikacím). Uživatelé jsou ověřování jen prostřednictvím zadání uživatelského jména a hesla. Doporučením pro společnost AMI Praha je zvážení přidání alespoň jednoho dalšího faktoru autentizace při přístupu k nejkritičtějším informačním systémům, případně při přístupu administrátorů s vysokou úrovní oprávnění. Tímto dodatečným faktorem může být opsání kódu zaslaného na ověřený email případně přes SMS na mobilní telefon uživatele, který se snaží přihlásit. Takové řešení ještě nutně nevyžaduje nasazení access manažer systému (při drobné úpravě je tuto funkci schopen zajistit aktuálně nasazený identity manažer) a přitom úroveň zabezpečení znatelně zvýší.
- Nástroj pro řízení přístupu administrátorů k informačním systémům. Nasazení tohoto nástroje ve společnosti, kde je počet administrátorů spočitatelný na prstech jedné ruky a která neprovozuje extrémně kritické systémy, by bylo vzhledem k licenčním

a implementačním nákladům neefektivní. V tomto ohledu by bylo dostatečné zavedení dalšího faktoru pro autentizaci administrátorů – viz předchozí bod.

- Společnost nemá nasazen ani nástroj pro vyhodnocování bezpečnostních událostí v reálném čase. Protože ale jednotlivé provozované systémy mají vlastní možnosti tvorby a vyhodnocování záznamů o aktivitě (tzv. logy) a systémů není nijak velké množství, není sofistikovaný systém pro komplexní pohled na logy v organizaci a jejich analýzu potřeba. Navíc jde o nástroj s pořizovací hodnotou minimálně vyšších stovek tisíc Kč a poměr ceny a výkonu (přínosu) v takto malé společnosti by nebyl zajímavý.

Mimo výše zmíněné doporučení vycházející z požadavků zákona pro organizace provozující kritickou informační infrastrukturu, případně významné informační systémy, a aktuálního stavu ve společnosti AMI Praha 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), která v mobilních zařízeních umožňuje zabezpečit aplikace i data a to včetně těch, které se nacházejí v emailových zprávách v emailových klientech. Ani tento nástroj není ve zkoumané společnosti nasazen a to může být, především kvůli současnému trendu využívání osobních zařízení pro firemní účely (trend je pojmenován jako BYOD – bring your own device), potenciálně nebezpečné.

Obrázek 4 - Názor českých společností na BYOD

Zdroj: http://www.businessinfo.cz/cs/clanky/byt-ci-nebyt-byod-67764.html

Možnost využívat vlastní zařízení pro práci ve společnosti je sice zajímavá jak pro pracovníka (může si pořídit zařízení dle svého uvážení bez ohledu na jeho cenu a výrobce a nemusí s sebou nosit dvě či více zařízení), tak pro společnost (šetří na nákladech za pořizování těchto zařízení), ale přináší s sebou rizika v podobě míchání firemních a soukromých dat a menší míry kontroly nad těmito daty. MDM nástroje dokáží soukromá data a aplikace striktně oddělit od firemních a kontrolu na firemními aktivy ponechávají v rukách společnosti.

6 Závěr

V podnikatelském prostředí dá hovořit o několika obecně uznávaných klíčových faktorech úspěchu. Různé studie uvádějí a dále budou uvádět částečně odlišné výčty těchto faktorů, ale nikdy by mezi těmi základními 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. Následně je tento pohled zobecněn a rozšířen o další pro prosperitu podniku důležitá data, která je potřeba chránit proti aktuálním rizikům.

Jedním z fenoménů moderní dobry je digitalizace všeho, co za současných technologických vymožeností digitalizovat jde. Digitalizace má za následek neuvěřitelné zrychlení procesů, které ve společnostech běží. Díky mobilním telefonům, elektronické komunikaci, elektronickým podpisům, automatizovaným workflow pro oběhy dokumentů a dalším technickým vymoženostem se doba zrychlila natolik, že dnešní vrcholový manažeři musejí často během jediného týdne řešit tolik věcí a udělat tolik rozhodnutí, jako jejich předchůdci z hloubi 20. století za půl roku a déle. Kromě zrychlení s sebou digitalizace přináší i 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. Společnost AutoCont, která patří ke špičce v oblasti dodávání bezpečnostních řešení na českém trhu, v jedné ze svých aktuálních marketingových kampaní připomíná, že k vyřazení či zneužití jednoho systému stačí jeden uživatel, jedna minuta a jedna nebo velmi malé množství uživatelských operací. Naproti tomu k opětovnému rozběhnutí je potřeba jedno celé IT oddělení a minimálně jeden den práce všech jeho členů (v lepším případě). Následky takového incidentu mohou být různé a

náklady na jeho řešení jdou od nákladů na čas pracovníků IT oddělení během oprav do astronomických částek, záleží jen na typu útoku a zpronevěřených datech. Z tohoto pohledu je jasné, že chránit svá data je naprosto nezbytné.

Jenže i když už je jasná potřeba a společnost se rozhodně chránit, není situace vůbec jednoduchá. V každém daném okamžiku si můžete být jistí, že se chráníte jen proti hrozbám, které jsou známé. Jenže technologie a vynalézavost útočníků jdou stále kupředu. Statistiky ukazují, že klasické způsoby krádeží, kdy se někdo vloupe do objektu společnosti, aby zcizil informace, jsou svou četností zanedbatelné. Při uvažování možností zcizení dat a v nich uloženém know-how nabízí jejich digitální podoba pro útočníky mnohem jednodušší cesty. I tady se dá ze statistik leccos vyčíst. Protože vnitřní sítě mají již společnosti často dobře zabezpečené prostředky pro oddělení vnitřní a vnější komunikace a možnostmi pro přístupy pouze přes zabezpečené kanály, což je dáno relativní jednoduchostí vyřešení této problematiky zakoupením jednoho robustního 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.

7 Seznam použitých zdrojů

Knižní zdroje:

- Distrikt Court of Maryland v soudním rozhodnutí z roku 1946: ČADA, Karel, Obchodní tajemství a know-how. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 32, ISBN 80-85100-67-3
- ČADA, Karel; *Obchodní tajemství a know-how*. 1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 30-33, ISBN 80-85100-67-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 41. ISBN: 978-80-245-1920-3
- ČADA, Karel; Obchodní tajemství a know-how.1. vydání. Praha: Úřad průmyslového vlastnictví, 1997, s. 131, ISBN 80-85100-67-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 38. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 39. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 40-41. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 42 - 43. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 43. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 46 - 47. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 49. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 50-52. ISBN: 978-80-245-1920-3
- ČADA, Karel; Oceňování nehmotného majetku. Praha: Oeconomica, 2002. s. 52-55. ISBN: 978-80-245-1920-3
- MAREK,Karel; Licenční smlouva (k předmětům průmyslového vlastnictví). Bulletin advokacie. 2008, roč. 19. č. 7-8, s. 27. ISBN 978-80-7208-922-2
- MAREK,Karel. Licenční smlouva (k předmětům průmyslového vlastnictví). Bulletin advokacie. 2008, roč. 19, č. 7-8, s. 26–28. 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, s. 89, ISBN 80-85100-67-3
- SLÁMA. Jiří, Licenční smlouva. Bulletin advokacie. 2008, roč. 19, č. 12, s. 26. ISBN 978-80-7239-206-3

- ŠTENGLOVÁ, I. – DRÁPAL, L. – PÚRY, F. et al. Obchodní tajemství: Praktická příručka. Praha: Linde Praha, a.s., 2005. s. 25. ISBN 978-80-89447-26-8
- ŠTENGLOVÁ, I. – DRÁPAL, L. – PÚRY, F. et al. Obchodní tajemství: Praktická příručka. Praha: Linde Praha, a.s., 2005. s. 25-26. ISBN 978-80-89447-26-8

Internetové zdroje:

- FILIPOVÁ, Kateřina; České podniky nestojí o patenty. Právní ochraně nevěří a bojí se o své know-how [online]. 2016 [cit. 2016-06-24]. Dostupné z: http://m.ihned.cz/byznys/c1-65300920-ceske-podniky-nestoji-o-patenty-pravni-ochrane-neveri-a-boji-se-o-sve-know-how
- MIROVSKÁ, Petra; Jak ochránit firemní know-how [online]. 2013 [cit. 2016-06-24. Dostupné z: https://www.patria.cz/pravo/2279271/jak-ochranit-firemni-know-how.html
- PAVLÁT, David; Pojem osobní údaj [online]. 2013 [cit. 2016-08-08]. Dostupné z: https://www.uoou.cz/pojem-osobni-udaj/d-1751
- PŘIBYL, Tomáš; ICT Security. Citlivá data: hlídáme utajení, integritu i dostupnost [online]. 2010 [cit. 2016-08-08]. Dostupné z: http://www.ictsecurity.cz/11101-mngmnt-citlivych-dat-dlpecmdmsaaa/citliva-data-hlidame-utajeni-integritu-i-dostupnost.html
- Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
- Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
- Zákon č. 513/1991 Sb., obchodní zákoník, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx
- Zákon č. 151/1997 Sb., o oceňování majetku a o změně některých zákonů, ve znění pozdějších předpisů [online]. [cit. 2016-07-04]. Dostupné z: http://zakony.centrum.cz/zakon-o-ocenovani-majetku/

8 Seznam obrázků