Ochrana know-how

Know-how protection

Bc. Jan Horsák

Diplomová práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

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

Jméno a příjmení:	**Bc. Jan HORSÁK**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Ochrana know-how**

Zásady pro vypracování:

Cílem diplomové práce je vymezení problematiky a způsobů komerční detektivní ochrany před únikem informací v oblasti intelektuálních hospodářských nehmotných statků společnosti, příp. stanovení požadavků na ochranu, včetně právních a dalších aspektů souvisejících s vykonáváním detektivní činnosti. V práci bude využito bezpečnostní analýzy, bezpečnostního plánování, volně dostupných internetových informačních zdrojů, odborné literatury a interních firemních materiálů dle možností.

1. **V úvodu diplomové práce v rámci východiskové hypotézy specifikujte zkoumaný problém -- komerční detektivní ochrana před únikem informací v oblasti intelektuálních hospodářských nehmotných statků (know-how).**
2. **Analyzujte důvody a význam ochrany know-how.**
3. **Vymezte možnosti a způsoby ochrany know-how v rámci komerční detektivní ochrany v rámci bezpečnostní analýzy a bezpečnostního plánování v prostředí konkrétní společnosti.**
4. **V praktické části diplomové práce zpracujte vlastní návrh ochrany know-how pro konkrétní ekonomický subjekt.**
5. **V závěru diplomové práce zhodnoťte výsledky analýzy zkoumaného problému, včetně vlastního přínosu.**

Rozsah práce: 80

Rozsah příloh:

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

Seznam odborné literatury:

1. **BRABEC, F. a kol.: Bezpečnost pro firmu, úřad, občana. Public History, Praha 2001.**
2. **BRABEC, F. a kol.: Soukromé detektivní služby. Eurounion, Praha 1995.**
3. **BRABEC, F. a kol.: Ochrana bezpečnosti podniku. Eurounion, Praha 1996.**
4. **DOSEDĚL, T. 21 základních pravidel počítačové bezpečnosti. 1. vyd. Computer Press,a. s., 2005. 56 s. ISBN 8025105741**
5. **DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. 1. vyd. Computer Press, a. s., 2004. 200 s. ISBN 8025101061**
6. **FOOT, M., HOOK, C.: Personalistika. Computer Press, Praha 2002.**
7. **JAŠEK, R. Informační a datová bezpečnost. 1. vyd. Academia centrum UTB, 2006. 140s. ISBN 8073184567**
8. **KAMENÍK, J., BRABEC, F. a kol.: Komerční bezpečnost (Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur). ASPI, Praha 2005.**
9. **MACEK, P. a kol.: Bezpečnostní služby. Policie History, Praha 2001.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **19. února 2010**

Termín odevzdání diplomové práce: **7. června 2010**

Ve Zlíně dne 19. února 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cílem této diplomové práce je seznámit čtenáře s problematikou týkající se ochrany know-how. Práce řeší problematiku zabývající se možné ochrany know-how ve společnosti. Práce je rozdělena na dvě hlavní části a to na teoretickou a praktickou. V teoretické části seznamuji s pojmy, důvody a významem ochrany know-how. Dále se zabývám analýzou rizik a právními aspekty souvisejícími s ochranou know-how. V praktické části představuji nabízené způsoby ochrany know-how detektivními službami. Pokouším se nastínit modelový způsob ochrany know-how v prostředí konkrétní společnosti. Z daných metod jsem vyvodil svá vyhodnocení.

Klíčová slova:

ochrana know-how, ochrana dat, únik informací, detektivní služby, metody ochrany dat, zabezpečení informací.

ABSTRACT

The aim of this diploma thesis is to acquaint readers with problems regarding to know-how protection. The work solves problems dealing with a posible of know-how protection in the society. The work is divided into two main parts both theoretical and practical. In the theoretical part I acquaint readers with concepts, reasons and a substance of know-how protection. In the practical part I present offered mays of know-how protection by detective services. I try to outline here a model way of know-how protection in the setting of the concrete society. I have drawn my evaluation from given methods.

Keywords:

know-how protection, data security, leak, detective services, methods for data protection, information security.

Děkuji vedoucímu mé diplomové práce panu PhDr. Mgr. Stanislavu Zelinkovi za odborné vedení, za cenné připomínky, rady a čas, který mi věnoval při konzultacích této diplomové práce.

Dále bych rád poděkoval mé rodině, která mě podporovala po celou dobu studia.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou/bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Držkové …….

podpis diplomanta

OBSAH

ÚVOD

Bezpečnost dat a informací se dnes stále častěji stává námětem diskusí nejen odborné, ale i laické veřejnosti. Diskrétní informace mají stále vyšší hodnotu, která ovšem neodpovídá skutečnostem, vynaložených k jejich ochraně.

Otázku bezpečnosti řeší lidstvo již od svého vzniku. Ať už to byly obranné systémy zajišťující bezpečí hradů či technologie používané na výrobu nedobytných trezorů. Ve srovnání s těmito případy byla otázka bezpečnosti informací poměrně pozadu. Bylo to způsobeno hlavně špatnou informovaností o této oblasti. Avšak za posledních deset let se společnost rapidně začíná systematicky zabývat otázkou bezpečnosti dat a informací. Informace v počítačové či jiné podobě představují mnohonásobně vyšší hodnotu a obvykle mají pro chod organizace zásadní význam. Představte si jen následky zcizení vývojových informací například konkurencí.

Tato diplomová práce bude mít za ambici stát se průvodcem v tajemném světě informační bezpečnosti. Pokusím se odhalit možné úniky informací ve společnosti. Na základě podrobné bezpečnostní analýzy následně doporučím vhodná bezpečnostní opatření a postupy, které možnost úniku informací minimalizují. Problematika bezpečnosti dat je nikdy nekončící proces a musí se operativně přizpůsobovat rozvoji a nasazování nových technologií.

V dnešní době není žádné bezpečnostní opatření dokonalé a čím citlivější jsou informace, se kterými pracujeme, tím smysluplnější jsou prostředky, čas i investice vložené do takovýchto opatření.

I. TEORETICKÁ ČÁST

1 SPECIFIKACE POJMŮ

1.1 Pojem nehmotné statky

Výraz nehmotné statky se dříve používal i v soudobém českém právu, ale dnes se s nim setkáváme jen v teorii. Právní ochrana nehmotných statků se zakládá na společných zásadách, které jsou příznačné a promítají se i v právu mezinárodním.

K tomu, aby byl jakýkoli nehmotný statek předmětem práva, je zapotřebí, aby byl svým původcem vyjádřen v objektivně (tj. smysly) vnímatelné podobě, což se fakticky rovná jeho zhmotnění (materializaci) v obecném významu. V dnešní době probíhá značný proces komercializace nehmotných statků, v jehož důsledku jsou do oblasti obchodu neustále vtahovány nové nehmotné statky, což vede i k rozvoji práva samého.

Je zapotřebí od nehmotných statků odlišovat činnosti, které vedou k jejich vzniku.

Jedná se o činnosti:

- tvůrčí povahy (o tvorbu),
- činnosti jiné, zvláště hospodářské.

Pokud budeme vycházet z našeho právního řádu je pojem nehmotný statek blízký k pojmu „duševní vlastnictví“, ale obsahuje širší obsahové pojetí. Je širší proto, neboť jejich povahové vymezení obsahuje nejen nehmotné (ideální) majetkové hodnoty, ale i nehmotné (ideální) hodnoty osobní, tzn. nemajetkové hodnoty. Nehmotným statkem ve smyslu právním je tedy i osobnost fyzické osoby a její obdoba u osoby právnické.

Zásadní rozdíl tedy spočívá mezi obsahem (a rozsahem) našemu právnímu řádu známého pojmu duševní vlastnictví a teoretického koncepčního pojetí nehmotných statků. Na shora uvedeném pojetí můžeme provést následující klasifikaci nehmotných statků:

- nehmotné statky osobní povahy,
- duševní vlastnictví
  - a) literární a jiné umělecké vlastnictví,
  - b) průmyslové vlastnictví.

S pojetím, které víceméně vychází ze stejné nebo podobné klasifikace, se můžeme setkat kupř. v právu mezinárodním veřejném, v řadě vícestranných i dvoustranných smluv, které se týkají úpravy literárního a jiného uměleckého vlastnictví a vlastnictví průmyslového, a to v obou případech jako pojmových prvků (druhů) duševního vlastnictví.

Duševním vlastnictvím se rozumí vlastnictví duševních plodů, jež nemají hmotnou povahu, z čehož se někdy dovozuje, že se vůbec nejedná o „vlastnictví", nýbrž o svébytný předmět zvláštního práva k duševním plodům. U těch nehmotných statků, které mají osobní povahu, se právně projevuje jejich nerozlučitelnost s osobností tvůrce. Naproti tomu ty nehmotné statky, které jsou pouze majetkovými hodnotami, zcela postrádají jakékoli osobní (osobnostní) rysy. Jsou proto způsobilé zcizení.

Nehmotné statky jsou povahově dělitelné na:

- osobní (život, zdraví fyzické osoby, její soukromí, lidská důstojnost, jméno, dobrá pověst právnické osoby, literární, jiné umělecké nebo vědecké dílo, částečně vynálezy a jiné duševní plody, jež jsou výsledky technické tvůrčí činnosti, užitné vzory, průmyslové vzory atd.),
- majetkové (zvukový a obrazový záznam, rozhlasové a televizní vysílání, obchodní tajemství, důvěrná informace, osobní údaj, obchodní firma, ochranná známka, know-how atd.).

Nehmotné statky můžeme v zásadě členit do dvou tříd, a to při zvolení kritéria jejich způsobilosti být předmětem občanskoprávních vztahů:

I. nehmotné statky, které nejsou způsobilé být předměty občanskoprávních vztahů (tj. ideální nemajetkové hodnoty), jež samy o sobě nejsou penězi, jakožto všeobecným ekvivalentem, ocenitelné:
    1. předměty osobního práva na ochranu osob
        a) osobnost fyzické osoby,
        b) název právnické osoby,
        c) dobrá pověst právnické osoby
    2. předměty práva autorského a práv výkonných umělců

a) literární, jiná umělecká a vědecká díla,

b) umělecké výkony,

3. předměty některých (tzv. tvůrčích) práv průmyslových (u nichž je však zcizitelnost právně řešena zcizením udělených majetkových práv k nim – patentů, respektive osvědčení)

a) vynálezy,

b) užitné a průmyslové vzory,

c) topografie polovodičových výrobků,

d) odrůdy rostlin.

II. Nehmotné statky, které jsou způsobilé být předměty občanskoprávních vztahů (jsou samy o sobě penězi ocenitelné):

1. předměty průmyslových práv na označení

a) obchodní firmy,

b) ochranné známky,

c) označení původů,

d) zeměpisná označení,

e) zvláštní označení podniků a jejich části (označení provozoven, televizní programy – názvy stanic atd.),

f) zvláštní označení výrobků, výkonů nebo obchodních materiálů podniku (označení obalů, katalogů, reklamních prostředků atd.),

g) jiná zvláštní označení (názvy odrůd, názvy dluhopisů atd.),

2. předměty jiných průmyslových práv

a) obchodní tajemství,

b) důvěrné informace,

c) zlepšovací návrhy,

d) know-how,

3. předměty ostatních majetkových práv

a) zvukové a zvukově obrazové záznamy,

b) rozhlasová a televizní vysílání,

c) databáze,

d) osobní údaje,

e) jiné zcizitelné nehmotné statky (majetkové hodnoty).

V uvedeném výčtu jsou obsaženy jak nehmotné statky požívající zákonné (absolutní) ochrany, tak též ty nehmotné (ideální) předměty, které absolutní ochranu žádným zákonem přiznánu nemají a lze je chránit pouze relativně. Tj. v rámci závazkového právního vztahu, v němž jedna jeho strana dobrovolně přijímá závazek k určité ochraně nehmotného předmětu, jejíž obsah a rozsah je mezi stranami dohodnut. Tato relativní ochrana ovšem působí jen mezi účastníky příslušného závazkově právního vztahu a nemá žádné právní důsledky (účinky) vůči komukoli ostatnímu. Můžeme ji použít i na ochranu nehmotných statků, které samy nepožívají absolutní ochrany zvláštními zákony, ochranu soutěžně-právní, vyplývající z práva na ochranu před nekalým soutěžním jednáním (z práva nekalé soutěže).[13]

1.2 Pojem know-how

Výraz know-how je amerického původu a v překladu znamená ,,vědět jak“, ,,vědět jak na to“. V obecném pojetí představuje know-how výrobně technické poznatky, které nejsou obvykle výsledkem vědecké nebo tvůrčí činnosti. Jedná se zejména o dlouhodobé zkušenosti s optimálním průběhem určité technologie a procesu.

Zahrnuje nesporně celou řadu zkušeností nabytých především z široké oblasti techniky, ale i obchodu a podnikání. Často bývají tímto výrazem označovány výrobní zkušenosti, technická pomoc nebo technická informace. Dá se říci, že je know-how nástrojem technického pokroku a nezastupitelným činitelem při soutěži. Mnohdy mívá pro podnikatele, společnost větší význam než samotné výrobky nebo patenty. Definice know-

how nejsou v jednotlivých zemích ani v teorii jednotné. Pod pojmem know-how mnohdy bývají chápány utajované vynálezy, výsledky výzkumu, vývoje atd.. Všechny poznatky zahrnující nechráněné vynálezy i poznatky a zkušenosti získané dlouholetou praxí lze přiřadit k know-how.

Mezinárodní obchodní komora v Paříži, Komise pro mezinárodní průmyslové vlastnictví navrhla v roce 1957 tuto definici:

> Pojem know-how označuje nejen utajované postupy, ale také techniku spojenou s patentovým výrobním postupem nebo procesem, techniku, která je nutná, aby patentovaný vynález mohl být využíván, a která umožňuje majiteli patentu vy-užívat jej v širším technickém rozsahu. Tento pojem označuje praktické procesy, zvláštní vlastnosti a technické znalosti získané výrobcem jako výsledek výzkumu, které dosud nejsou známé soutěžitelům.

S definicí pojmu know-how přišel také Pan JUDr. Vladimír Laucký, který se pokusil podat jasnou definici ve skriptech Technologie komerční bezpečnosti II.:

> Know-how je soubor podstatných identifikovatelných technicko-ekonomických znalostí, metod a postupů, získaných ve výrobním procesu, výzkumu, vývoji i v dalších procesech, který umožňuje dosáhnout určitého vysokého stupně kvality, jakosti, bezporuchového provozu, efektivních postupů apod. Know-how je významným subjektem obchodního jednání, zpravidla se utajuje a pokud ne, projeví se jeho předání v hodnotě obchodní smlouvy.

Obsahem know-how mohou být prvky hmotné i nehmotné.

Mezi prvky hmotné patří:

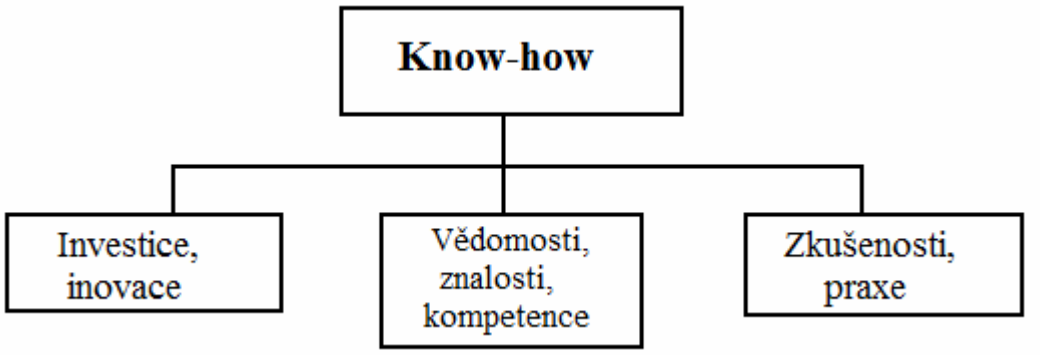
- výkresy,
- modely,
- plány,
- technická dokumentace,
- technické popisy,
- návody k výrobě a k využití,
- specifikace atd.

Mezi prvky nehmotné můžeme zařadit:

- zkušenosti získané při návštěvách závodů,
- zkušenosti získané při předávání znalostí teorie,
- zkušenosti získané z praxe atd..

Myšlenkou teoretiků je, že know-how musí být tajné. Ano, know-how by zpravidla mělo být tajné, ale nemusí se vždy jednat o utajení absolutní, tj., že je známé jen jedinému jeho uživateli. K pojmu tajné, respektive ,,SE UTAJUJE“ odborníci (Malý, Laucký) dodávají, že know-how není všeobecně známé a dostupné. Pro nejefektivnější ochranu bude stačit, je-li známe jen určitému, omezenému počtu uživatelů. Nemůžeme vyloučit případ, že někdo jiný samostatně a vlastním přičiněním dojde k totožnému know-how. Pokud se tak stane, nelze mu v tom nikterak bránit a je třeba být v tomto směru benevolentní. Nikde není psáno, že se know-how stane bezcenným, bezvýznamným, stane-li se v určité zemi obecně známým.

Know-how v sobě modelově spojuje tři základní složky:



***Obr. 1** Model know-how (inspirace Malý)*

Technologie v moderním pojetí v sobě nesporně obsahuje know-how. Poněvadž nutnou podmínkou získání know-how je v pojetí, které převažuje, dlouhodobé provozování technologie, nabyvatel technologie, který získá v rámci technologie i příslušné know-how, si osvojí technologii mnohem snadněji a rychleji, je-li vůbec toto osvojení bez příslušného know-how možné.

Vzhledem k nedostatku speciální ochrany je know-how někdy označováno jako ,,nechráněné“. Není to však zcela přesné, protože může být chráněno v rámci postihu nekalé soutěže, a to buď proti tzv. otrockému napodobení, nebo pro porušení obchodního tajemství. Na rozdíl od průmyslového vlastnictví zde neexistuje institut nucené licence,

takže odepření poskytnout know-how zájemci nelze postihnout, nebo si postihnutí vynutit, ledaže by se jednalo o jednání omezující soutěž a majitel know-how by měl monopolní nebo dominantní postavení na trhu. Zákony některých zemí totiž stanoví v tomto případě na žádost zájemce kontraktační povinnost pro majitele, tedy povinnost uzavřít smlouvu o poskytnutí know-how, tzv.nepravou licenční smlouvu. Tato možnost je ale výjimečná a je spojena vždy s úplatou za licenci.

Vzhledem k tomu, že uváděné nástroje právní ochrany i důkazní možnosti jsou poměrně slabé, je know-how chráněno obvykle utajením. Potřeba utajovat know-how se promítá do pracovněprávních vztahů (omezený přístup běžných pracovníků k dokumentaci či do utajovaných provozů, zakázky konkurenčního zaměstnání či podnikání – tzv. konkurenční doložka, zákazy prozrazení know-how) i do licenčních smluv pro případ prozrazení třetí osobě nebo jinému zneužití.

1.2.1 Nositelé know-how a členění podle podnikových činností

Pod pojmem know-how existuje i rozličná škála kompetencí. Vzhledem k tomu, že podnik představuje určitý celek, lze často jen obtížně s jistotou říci, které znalosti či dovednosti souvisejí s danou technologií a které nikoliv. Následující výčet se pokouší shrnout a setřít tyto dovednosti a znalosti ze dvou základních hledisek a to podle nositelů know-how a podle původu know-how.

Pod *podnikovým know-how* mimo jiné rozumíme:

- modely, prototypy (nechráněné),
- výkresy, plány, náčrty (nechráněné),
- inženýrské studie, přípravu investic,
- inženýring procesů,
- technickou pomoc, údržbu,
- návody, manuály, příručky, seznamy,
- marketingové studie, studie proveditelnosti (feasibility studies),
- seznamy dodavatelů, zákazníků,
- prvky komunikační politiky,

- vzdělávání a školení,
- manažerské know-how (formalizované).

Manažerské know-how neformalizované je rovněž součástí podnikového know-how, jeho nositelem je manažer nebo jeho tým. Takové know-how může být součástí poskytované technologie, např. zapůjčením manažera do partnerské firmy.

Z hlediska původu, tedy podle toho, ze které části podniku pochází dané know-how, můžeme rozlišit kompetence technické, marketingové a kompetence v oblasti řízení.

Technické know-how přímo souvisí s výrobou nebo výrobkem, dále zde zahrnujeme i zajištění výroby (pomocné provozy) a nákup surovin materiálu. Za technické know-how považujeme zejména:

- proces výzkumu a vývoje, testování prototypů,
- techniky výroby a vývoje, montáže, přípravy výroby, expedice,
- metody řízení zakázek a řízení výroby,
- metody kontroly kvality,
- metody zjišťování nákladů výroby,
- metody nákupu surovin, strojů a vybavení,
- metody řízení zásob,
- metody vzdělávání zaměstnanců ve výrobě.

Marketingové know-how zahrnuje veškeré dovednosti a zkušenosti zaměstnanců ve vztahu k trhu a k zákazníkovi ve všech souvislostech distribučních, cenových a komunikačních. Konkrétně se jedná o následující oblasti:

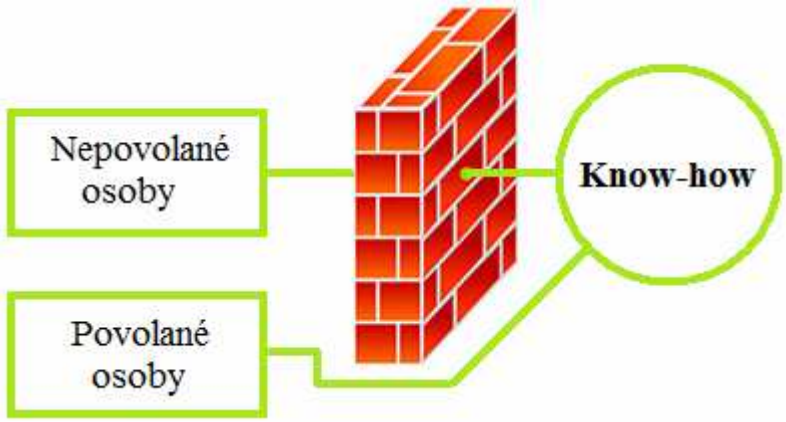
- metody výzkumu trhu, testování, odhadů prodeje,
- metody uvádění nových výrobků na trh,
- technika určování cen a cenová politika,
- reklama, podpora prodeje, vztahy s veřejností,
- techniky výběru a optimalizace distribučních cest,
- techniky organizace, vzdělávání, odměňování a motivace prodejců.

Know-how v oblasti řízení zahrnuje zejména specifické dovednosti a zkušenosti nashromážděné oddělením vrcholného managementu, účetnictví a finančního řízení, kontroly a personalistiky, tedy především:

- techniky v účetnictví a řízení nákladů,
- techniky v rozpočetnictví a v řízení cash flow,
- techniky ve výběru a hodnocení investic,
- techniky v oblasti kontroly,
- techniky přijímání a vzdělávání zaměstnanců,
- techniky odměňování,
- techniky motivace a rozvoje zaměstnanců,
- techniky plánování a kontroly.[14]

Know-how může mít mnoho podob:

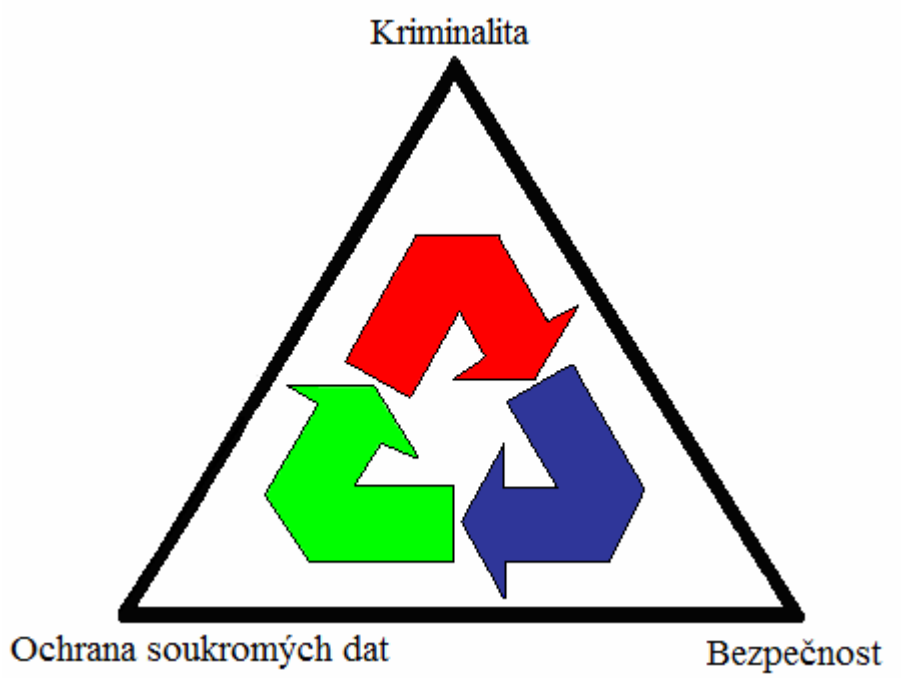
- od zkušeností s určitým zařízením, výrobkem apod.,
- až po optimální podmínky prostředí,
- snižování produkce a recyklaci odpadu atd..



Obr. 2 *Know-how není pro každého*

2 OCHRANA KNOW-HOW => OCHRANA INFORMACÍ A DAT

Počítače stále více nahrazují a podporují plno lidských činností. Vize z minulého století o digitálně propojené společnosti se stávají realitou zejména v technicky vyspělých částech světa. Počítače zpracovávají informace, které mohou znamenat moc, peníze, vědomosti a utrpení. Proto stále častěji můžeme slyšet skloňovat pojmy počítačová kriminalita, počítačová bezpečnost a ochrana soukromých dat. Všechny tři pojmy mají obdobný základ problematiky, mění se pouze úhel pohledu na danou realitu.



Obr. 3 *Trojúhelník souvislostí – zdroj Google*

V uzavřeném kruhu můžeme mimo jiné hledat slabiny implementace počítačových systémů, legislativní nedostatky, zájmy skupin a jednotlivců.

2.1 Bezpečnost informací

Bezpečnost lze definovat jako zajištěnost proti hrozbám, minimalizaci rizik a komplex administrativních, technických, logických a fyzických opatření pro prevenci a detekci neautorizovaného využití informací. I z tohoto důvodu je nutné si vymezit rámec, který má na bezpečnost informací zásadní vliv.

Bezpečnost v informačním prostředí lze zjednodušeně rozdělit na následující domény:

- komunikační bezpečnost – ochranu přenášených dat a zamezování nežádoucího datového provozu,
- fyzickou bezpečnost – ochranu před přírodními hrozbami, jako je například požár, a fyzickými útočníky, například zábranou, detektory pohybu atp.,
- personální bezpečnost – ochranu před vnitřními útočníky již při náboru, během jejich práce i po skončení pracovního poměru,
- bezpečnost informačních systémů a technologií – ochranu infrastruktury informačních systémů uchovávající data v elektronické podobě proti relevantním hrozbám typu neautorizovaný přístup, maligní software (viry, trojské koně), výpadky systému apod..

2.1.1 Základní bezpečnostní atributy v těchto doménách jsou:

- důvěrnost – prevence neautorizovaného vyzrazení dat,
- integrita – prevence neautorizované úpravy dat,
- dostupnost – prevence ztráty přístupu k datům.

Příklad ohrožení datových aktivit		
Úmyslné	**Náhodné**	**Přírodního rázu**
odhalení/odposlech	chyby a opomenutí	zemětřesení
podvod/narušení integrity	vymazání souborů	blesk
narušení dostupnosti	nesprávné směrování	požár
přisvojení/krádež	fyzické nehody	povodeň

Tab. 1 *Příklad ohrožení datových aktivit – zdroj Google*

2.2 Co se skrývá pod pojmem ochrana informací?

Pod pojmem ochrana informací si můžeme představit technologie, zabezpečení nebo procedury bránící před samotným ohrožením.

2.2.1 Proč data, informace, know-how zabezpečujeme:

- aby se informace nezničily;
- aby se k informacím dostaly jen oprávněné osoby;
- aby se zpracovávaly jen nefalšované informace;
- aby se dalo zjistit kdo informaci vytvořil, změnil či odstranil;
- aby se informace nekontrolovatelným způsobem nevyzradily;
- aby informace byly dostupné, když jsou potřebné.

2.2.2 Podstata zranitelných míst

- fyzická – umístění dostupné sabotáži, vandalismu;
- přírodní – záplavy, výpadky proudu, požáry;
- hardware / software – poruchy paměti;
- média, konkurence – krádež, zničení, nedostatečné odstranění informací, stárnutí materiálu;
- fyzikální – vyzařování (magnety);
- komunikace – útok na zprávy, spoje, komunikační kanály;
- lidský faktor – způsobuje nejvyšší zranitelnost ze všech faktorů.

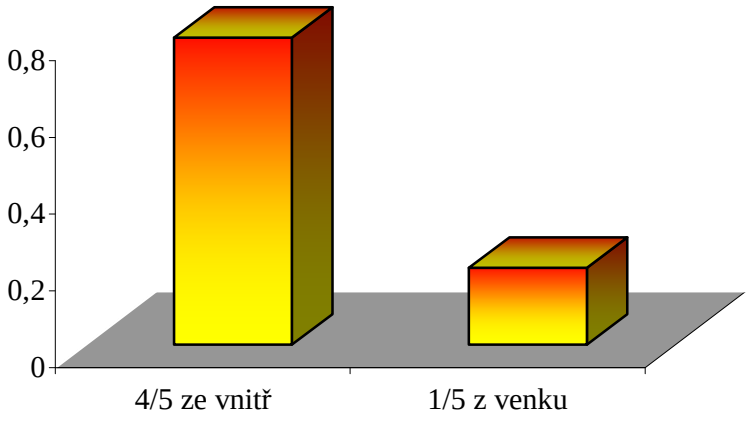
2.2.3 Způsoby ochrany know-how rozdělené podle účinnosti

- slabé – potenciálnímu narušiteli znepříjemníme život;
- střední – proti amatérovi může být účinná, ale pro profesionála je jen překážkou, kterou úspěšně překoná;
- silné – pro amatéra nepřekonatelné, pro profesionála těžce překonatelé až nepřekonatelné;

Žádná ochrana není 100%, kombinací metod jí lze zvýšit.

2.3 Nebezpečí hrozí především zevnitř

Závažným hrozivým faktem, který není rozumné přehlížet, je skutečnost, že více než čtyři pětiny útoků na informační systémy a data v nich uložená jsou klasifikovány jako vnitřní útoky.



Graf 1 *Útoky na informační systémy – zdroj McAfee*

Všechny nejsou vědomě cílené přímo zaměstnanci – jejich část je zapříčiněna:

- nedbalostí,
- neúmyslnou pomocí.

Bez ohledu na úmysl jejich důsledky bývají obvykle stejně hrozivé.

Dalším nezanedbatelným problémem je vynášení informací:

- za úplatu komerční tzv. marketingové firmy,
- spojené s odchodem zaměstnanců.

Typický český odcházející zaměstnanec, úředník apod. si sebou neopomene vzít databázi jmen a rodných čísel obyvatel, kteří spadali do jeho resortu.

Vlastní krádež dat může mít i zcela nevinnou podobu pár vytištěných papírů s citlivými informacemi (spadajícími do působnosti zákona o ochraně osobních údajů 101/2000 Sb.). S rostoucím objemem elektronicky uchovávaných dat se především jedná o hrozící problém vynášení dat v elektronické podobě.

Zde například patří:

- databáze,
- diskrétní údaje zaměstnanců,
- diskrétní údaje společnosti (firmy).

Dnes už je možné bez problémů odnést na jednom paměťovém disku část nebo dokonce všechny tyto informace. Například administrátor, který má v náplni práce spravovat a provádět pravidelné zálohování dat serveru, má z principu k systému přístup neomezený.

Samozřejmě výměnná média nejsou jediným způsobem jak lze data odnést. Skrze elektronickou poštu sice nelze nepozorovaně najednou posílat desítky či stovky megabajtů, ale rozhodně není vhodné tento kanál podceňovat.

Obr. 4 *E-mail – zdroj Google*

3 ANALÝZA RIZIK

Analýza rizik má v praxi mnohem širší využití než jen při analýze informačních systému. Například celá oblast pojišťovnictví se zakládá na práci s rizikem a tudíž na jeho analýze. Pokud toto téma zobecníme, dostaneme se k následujícímu závěru“ každý den činí lidé spousty rozhodnutí – volí mezi různými alternativami řešení daného problému, což s sebou přináší jistá rizika. Pokud se chceme rozhodovat správně, všechna tato rizika analyzujeme a na základě výsledků provedeme „správné“ rozhodnutí.

Naprosto stejná situace nastává i v případě ochrany informací uložených v rámci informačních systému. I zde 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 třeba všechna rizika a zranitelná místa systému volbou vhodných opatření omezit na minimum. Důležitost dat, informací je mnohdy obrovská a finančně nevyčíslitelná. Starost o bezpečnost informací znamená 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 je různá, od přísně tajných až po ty, které by naopak měly být zveřejněny. Bezpečnostní systém pak umožní informace strukturovat, stabilizuje v nich určitý řád.

Analýza rizik pracuje se třemi základními vstupy:

- aktiva,
- zranitelná místa,
- hrozby.

3.1 Aktiva

Informační systém spravuje určitá data či informace, která lze definovat jako aktiva. Aktivy rozumíme hmotné i nehmotné statky, které mají pro svého majitele určitou hodnotu. Jedná se o hardware (počítače, paměťové média, periferní zařízení), software (operační systémy, aplikační programy) a především informace, data (v praxi to mohou být například databáze zákazníku firmy, účetní a personální záznamy apod.). Do skupiny aktiv

se řadí také komunikační média (sítě, přenosová zařízení a média) a lidé – uživatelé systému (operátoři, uživatelé, vedoucí).

3.2 Zranitelná místa

Každé z těchto aktiv vnáší do systému určitou množinu zranitelných míst – tj. slabin, které mohou být zneužity. Zranitelným místem mohou být:

- Záležitosti fyzické podstaty (nezabezpečený vstup do budovy, nedostatečná kontrola prostor, nespolehlivé napájení, slabá ochrana proti požáru).
- Lidský faktor jako možnost toho, co mohou lidé způsobit (chyby, podvody, krádeže, vydírání, podplacení), nebo naopak co může být lidem způsobeno (poškození zdraví, smrt).
- V případě hardwaru se jedná o jeho nečekané selhání, chyby v návrhu a samozřejmě vliv prostředí, v němž je zařízení provozováno.
- I software má svá zranitelná místa, jako například nespolehlivost (špatný návrh) nebo jejich nestabilita.
- Provoz sítí je ohrožen jakoukoli formou odposlouchávání. Toto úzce souvisí se zranitelnými místy vycházejícími z hardwaru a prostředí.

Aktiva typu data lze z hlediska jejich zranitelných míst a závažnosti rozdělit do několika tříd.

3.2.1 Prozrazení informace (porušení důvěrnosti)

- Prozrazení vlastním uživatelům systému (tj. osobám, které pracují uvnitř organizace, ale nejsou oprávněny znát tyto informace).
- Prozrazení externím dodavatelům (zaměstnancům organizací, kteří mohou mít legitimní přístup k systému nebo jeho částem, ale nejsou oprávněni přistupovat k informacím – např. může jít o servisní organizace, o poskytovatele technického vybavení nebo poskytovatele datových sítí).
- Prozrazení ostatním osobám.

3.2.2 Modifikace při interaktivním a dávkovém zpracování

(například při zadávání dat do systému)

- Malé chyby (např. překlepy, duplikace vstupních dat).
- Závažné a rozsáhlé chyby (způsobené např. chybou v programu).
- Úmyslná modifikace dat (např. uložených v systému).

3.2.3 Modifikace elektronické pošty

- Vložení falešných zpráv (například vložení falešného příkazu k úhradě).
- Popření odeslání zprávy (např. odesílatel popře, že by zaslal dopis elektronickou poštou).
- Popření přijetí zprávy (např. příjemce popře, že by přijal dopis elektronickou poštou).
- Nedoručení zprávy (úmyslné nebo neúmyslné).
- Opakované zaslání téže zprávy (např. duplikace příkazu k úhradě).
- Nesprávné doručení (např. zaslání dopisu elektronickou poštou jinému příjemci).
- Monitorování provozu (zjištění skutečností, že dvě strany spolu komunikují, aniž by byl prozrazen obsah zpráv).
- Změna pořadí zpráv (např. změna pořadí dopisů).[15]

3.2.4 Nedostupnost

Následky plynoucí z faktu, že informace nejsou dostupné oprávněným uživatelům. Závažnost je závislá na době nedostupnosti těchto informací.

3.2.5 Zničení

Možnost zničení dat uživatelem patří mezi nejzávažnější zranitelná místa.

Podle závažnosti je můžeme dále rozdělit na:

- zničení dat v době od posledního úspěšného zálohování,
- úplné zničení dat včetně záložních kopií.

3.3 Hrozby

Hrozbou rozumíme reálné nebezpečí plynoucí z existence zranitelného místa včetně konkrétní pravděpodobnosti její realizace. Mezi základní zdroje hrozeb řadíme:

- Lidé – někdo může určité aktivum prostřednictvím některého zranitelného místa záměrně nebo neúmyslně poškodit (poškodit jeho integritu, tj.neoprávněně je změnit, vyzradit je, porušit jeho důvěrnost apod.).
- Nehody – například požár, lidské chyby, prasklé vodovodní potrubí, apod..
- Přírodní katastrofy – například zemětřesení, tornáda nebo povodně.

3.4 Bezpečnostní analýza

Samotná analýza pak spočívá v systematické kontrole všech možných rizik, hrozeb a určení pravděpodobnosti, že určitá hrozba bude uskutečněna.

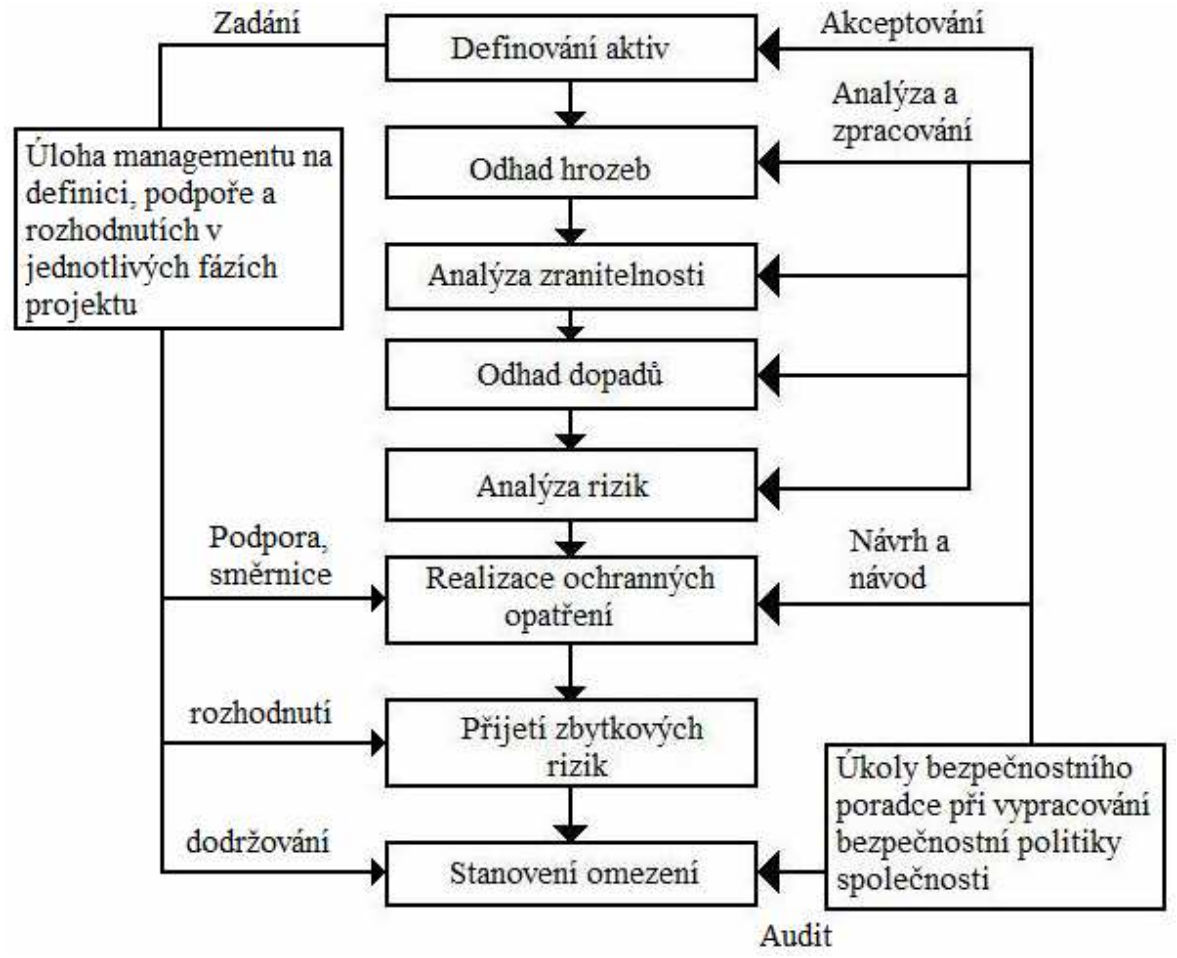
Z počátku bezpečnostní analýzy odpovídáme na následující otázky:

- kdo analyzuje,
- kde analyzuje,
- kdy analyzuje,
- jak analyzuje,
- co analyzuje,
- čím analyzuje,
- proč analyzuje.

Výstupem bezpečnostní analýzy je souhrn doporučených protiopatření, které by měly být použity proto, aby zjištěné riziko bylo sníženo na minimální možnou míru. Pro lepší představu uvedu praktický model vytvoření bezpečnostní politiky za pomocí bezpečnostní analýzy. Způsob práce spočívá ve vytvoření neformální pracovní skupiny, která bude sestavena s odborníků jednotlivých oblastí, jichž se bezpečnost dotýká. Informace se získávají formou pohovorů s jednotlivými pracovníky, zaměstnanci nebo také formou dotazníku.

V praxi platí zásada, že zpracovatel pracuje pouze s informacemi, které je organizace ochotna poskytnout.

Postup vytváření bezpečnostní politiky je následující:



***Obr. 5** Projekt bezpečnostní politiky – zdroj Ing. Michal Sláma*

Přínos projektu:[1]

- sníží se zranitelnost organizace – pokud už dojde k incidentu je k dispozici náhradní řešení a podle zpracované metodiky se zjistí příčina a přijmou se účinná ochranná opatření;
- zvýšení důvěryhodnosti pro partnerské organizace – organizace požadují po

[1] Michal Sláma. *Bezpečnostní politika.* Dostupné z WWW: <http://michal_slama.sweb.cz/security>.

svých partnerech důkazy, že se s jejich daty zachází bezpečně a nehrozí zneužití poskytnutých údajů;

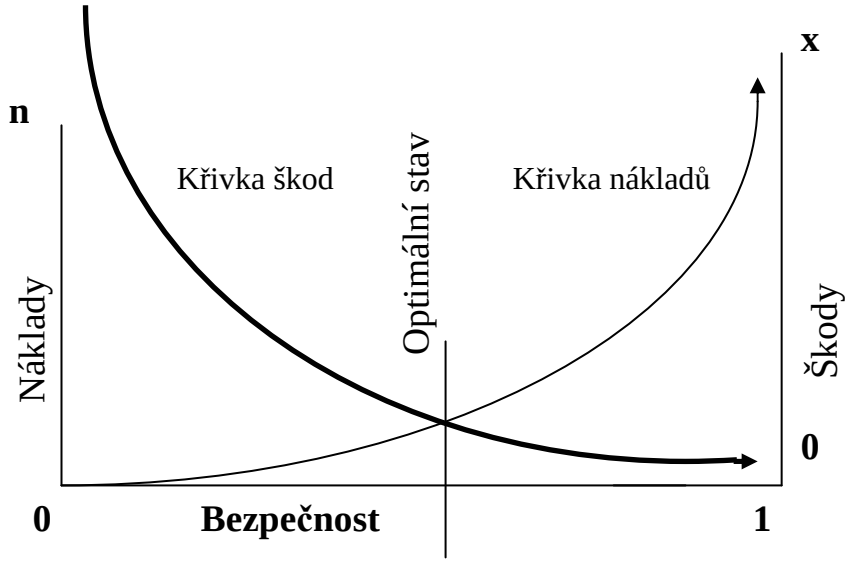
- rozpoznání a definování rizik – možnost přijetí adekvátních opatření pro zvýšení bezpečnosti;
- zlepšení organizační struktury – bezpečnost není jen záležitostí vybraných expertů, ale všech pracovníků organizace.

Dalším možným způsobem odhalení rizik je např. metodika CRAMM. Ta například používá otázky typu „Co by se stalo, kdyby…“ a předkládá scénáře možných následků nedostupnosti, úplného zničení dat, neautorizované modifikace nebo vyzrazení dat.

Protiopatření se vybírají na základě znalosti pravděpodobnosti hrozby, vyčíslení hodnoty aktiv (ve vztahu k hrozbě), ceny protiopatření a jeho zavedení do praxe. Typickým protiopatřením plynoucími z analýzy rizik jsou například:

- definování bezpečnostní politiky,
- instrukce k utajení,
- zavedení šifrování,
- zavedení přístupových hesel,
- potvrzení předávané informace,
- vedení příslušné dokumentace,
- monitorování doby přístupu,
- využití bezpečnostního poradenství,
- důvěryhodné výpočetní prostředky,
- pravidelné audity,
- detekce pokusů o neoprávněný vstup do systému,
- kontrola osob,
- procedury verifikace systému,
- zálohování a archivace,
- a další.

Všechny metody bezpečnostní, rizikové analýzy mají stejný cíl, a to dobrat se tzv. „objektivní pravdy“. Jedná se tedy o to, v jaké bezpečnostní situaci se společnost nachází.



Obr. 6 *Určení optimálních nákladů na minimalizaci rizik – zdrojLátal*

3.5 Bezpečnostní audit

Cílem bezpečnostního auditu je vyhodnotit funkčnost zavedených bezpečnostních opatření. Smyslem auditu je také posoudit celkovou bezpečnost ve světle nových technologií, a tím i nově vzniklých zranitelných míst a hrozeb. Během auditu jsou podrobně zmapovány a posouzeny všechny části informačního systému a nalezeny nedostatky a mezery v konstrukci jeho správy.

Bezpečnostní audity jsou obvykle dvojího druhu:

- Pravidelné, prováděné jako prevence pro odhalování nových zranitelných míst a hrozeb.
- Mimořádné, prováděné na žádost managementu, obvykle jako reakce na incident porušující bezpečnost organizace.

Cílem auditu není zabránit útoku, ale zjistit, zda byl nějaký útok proveden, a pakliže ano, informovat o tom, jakým způsobem. Audit samotný by měl být prováděn pracovníky, kteří jsou maximálně nezávislí. Řada organizací dává proto přednost vypracování auditu důvěryhodným nezávislým firmám, které disponují odborníky pro určitou oblast.

Obsah auditu lze shrnout do následujících bodů:

- Organizace zpracování informací – posuzuje se především oddělení jednotlivých fází nebo procesů.
- Kontrola dalšího rozvoje IS a jeho dokumentace – ověřuje se účast všech stran – od uživatelů přes systémové analytiky až po bezpečnostní managery a auditory. Důraz se také klade na metodiku testování nového IS a jeho zavedení do praxe.
- Kontrola přístupu – posuzuje se zabezpečení fyzického přístupu k hardwaru a programovému vybavení, přístup k datům, informacím a jeho zálohám a v neposlední řadě přístup ke komunikacím.
- Aplikační (procedurální a datové) kontroly – zkoumají se tři základní oblasti:
  - Zabezpečení vstupu dat do systému, jejich správnost a náchylnost k chybám, zabezpečení a prevence jejich ztrát a modifikací, kontrola přístupu.
  - Zpracování dat, tj. jak se nakládalo se zadanými informacemi během jejich zpracování. Mělo by to být možné zpětně sledovat veškeré akce s uloženými informacemi: kdo, kdy a jak s nimi zacházel.
  - Výstup ze systému, jakým způsobem jsou realizovány výstupní kontroly, kdo výsledky ověřil, jak jsou odolné vůči modifikací a zda je obdrží pouze oprávněné osoby.[15]

3.6 Legislativa

3.6.1 Vztah mezi know-how a obchodním tajemstvím

Pojem know-how je v literatuře i v praxi hojně používán a v českém právním řádu nemá legální definici. Pan Ježek v Kurzu obchodního práva definuje know-how jako soubor „*výrobních, technických, technologických a jiných poznatků a dovedností, které vedou k racionálnějšímu nebo efektivnějšímu vyřešení určitého problému a jsou podnikatelsky využitelné*“.

Tématem diskuzí zejména bývá, zda lze know-how považovat za obchodní tajemství nebo se jedná o dvě samostatné kategorie. Většina autorů má stejný názor a to takový, že jde o dvě kategorie, které se sice vzájemně prolínají, ale každá z nich obsahuje

prvky, které druhá neobsahuje. Lze tedy říci, že obchodním tajemstvím bude know-how jen tehdy, bude-li splňovat definiční znaky vyjádřené v ustanovení § 17 obchodního zákoníku. [16]

Zákonů a vyhlášek spojených s problematikou ochrany informací je v České republice několik set. Liší se svými cíli, svou působností a aspekty bezpečnosti. Já se zaměřím na zákon se kterým se běžně setkáváme v osobním životě.

Zákon č.262/2006 Sb., zákoník práce

§ 316 ochrana majetkových zájmů zaměstnavatele a ochrana osobních práv zaměstnance

(1) Zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování zákazu podle věty první je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

(2) Zaměstnavatel nesmí bez závažného důvodu spočívajícího ve zvláštní povaze činnosti zaměstnavatele narušovat soukromí zaměstnance na pracovištích a ve společných prostorách zaměstnavatele tím, že podrobuje zaměstnance otevřenému nebo skrytému sledování, odposlechu a záznamu jeho telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci.

(3) Jestliže je u zaměstnavatele dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odstavce 2, je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Zabezpečené oblasti se podle nejvyššího stupně utajení utajované informace, která se v nich ukládá, zařazují do kategorií:

a) Přísně tajné,

b) Tajné,

c) Důvěrné,

d) Vyhrazené.

Zabezpečené oblasti se podle možnosti přístupu k utajované informaci zařazují do tříd:

a) třída I, kdy vstupem do této oblasti dochází k seznámení s utajovanou informací,

b) třída II, kdy vstupem do této oblasti nedochází k seznámení s utajovanou informací.

Za naplňování zákona č. 412/2005 Sb. je zodpovědný Národní bezpečnostní úřad (http://www.nbu.cz/legislativa). Do náplně činností NBÚ patří bezpečnostní prověrky, certifikace informačních systému a kryptografických prostředků atd..

Zákon spolu s řadou vyhlášek představuje ucelenou soustavu na ochranu zvláštního druhu informací. Jsou zde podrobně popsány požadavky na bezpečnost v jednotlivých oblastech.

Další právní předpisy

– *zákon č. 40/2009 Sb., trestní zákoník*

§ 173 loupež,

§ 180 neoprávněné nakládání s osobními údaji,

§ 181 poškození cizích práv,

§ 182 porušení tajemství dopravovaných zpráv,

§ 183 porušení tajemství listin a jiných dokumentů uchovávaných v soukromí,

§ 184 pomluva,

§ 205 krádež,

§ 206 zpronevěra,

§ 207 neoprávněné užívání cizí věci,

§ 209 podvod,

§ 228 poškození cizí věci,

§ 229 zneužívání vlastnictví,

§ 230 neoprávněný přístup k počítačovému systému a nosiči informací,

§ 231 opatření a přechovávání přístupového zařízení a hesla k počítačovému sytému a jiných takových dat,

§ 232 poškození záznamů v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti,

- *zákon č. 140/1961 Sb., trestní zákon,*

§ 121 poškozování spotřebitele,

§ 149 nekalá soutěž,

§ 151 porušování průmyslových práv,

§ 152 porušování autorského práva, práv souvisejících s právem autorským a práv k databázi,

§ 199 šíření poplašné zprávy,

§ 239 porušování tajemství dopravovaných zpráv,

§ 248 zpronevěra,

§ 250 podvodu,

§ 257 o poškození a zneužití záznamu na nosiči informací,

- ochrana autorských práv – zákon č. 35/1945,

- zákon o ochraně státního tajemství č. 102/1971 Sb.,

- zákon č. 148/1998 Sb. o ochraně utajovaných skutečností,

- obchodní zákoník č. 513/1991 Sb.– ochrana obchodního tajemství.

4 NESTÁTNÍ ZPRAVODAJSTVÍ

4.1 Roviny nestátního zpravodajství[2]

Obr. 7 *Roviny nestátního zpravodajství – zdroj JUDr. Brabec*

4.1.1 Obranné zpravodajství

V obranném nestátním zpravodajství se především zajišťuje:

- personální bezpečnost,
- informační bezpečnost,
- režimová bezpečnost,
- bezpečnost technických prostředků,
- bezpečnost programových (softwarových) prostředků,
- bezpečnost komunikačních systémů,
- fyzická bezpečnost,
- ochrana před ofenzivním a vlivovým zpravodajstvím konkurence.

Zpravodajská prevence zajišťuje:

- personální prověrky,
- prověrky obchodních partnerů (odběratelů + dodavatelů),
- opatření k ochraně informací,
- ochrana proti ofenzivnímu zpravodajství konkurence,

[2] Zdrojem literatury: BRABEC, F. : *Technologie detektivní činnosti*. UTB, Zlín 2009. 160 s.

- dohled nad dodržováním režimových a organizačních opatření,
- ochrana proti vlivu konkurence a dezinformacím.

Ohrožení informační bezpečnosti	
Zvenčí	**Zevnitř**
počítačoví piráti	zaměstnanci
kyberteroristé	manažeři
hackeři	zaměstnanci a manažeři subdodavatelů a obchodních partnerů apod.
ofenzivní zpravodajství konkurence	
apod.	**!!! Největší riziko**

***Tab. 2** Ohrožení informační bezpečnosti – zdroj JUDr. Brabec*

4.1.2 Ofenzivní zpravodajství

Pan JUDr. Brabce o ofenzivním zpravodajství říká: „ *ofenzivní nestátní zpravodajství je vědou – disciplínou o rozhodování při využití informací a to v situacích, kdy několik soutěžících subjektů (konkurentů) chce dosáhnout stejných cílů a mají přitom možnost získat stejné informace*“.

Ofenzivní nestátní zpravodajství zahrnuje:

- kladení otázek nutných pro rozhodování o způsobu dosažení vytyčených cílu,
- legální a etické shromažďování informací,
- objasnění a pátrací (vyšetřující) analýzu informací,
- řízenou distribuci závěrů využitelných pro rozhodování (zpravodajství).

Podstatou ofenzivního zpravodajství je:

- odhalit strategii konkurence → využít ve prospěch vlastní společnosti,
- zajistit marketingové informace (koncepce obchodní a výrobní politiky společnosti),
- zjistit, jak si vede ekonomika konkurence,
- odhalení záměrů konkurence apod..

4.1.3 Vlivové zpravodajství

Pro vlivové zpravodajství je základním kamenem lobbying (od slova lobbyismus – cílené ovlivňování osob). Na základě lobbyingu můžeme buď informovat nebo dezinformovat zájmové prostředí. Metoda dezinformace tedy znamená ,,vpuštění,, záměrně nepravdivé zprávy např. ke konkurenci.

Příprava lobbyingu – ovlivnění:

- uvědomění si záměrů sledovaného dezinformací;
- formulace dezinformačního postupu;
- formulování (plánování) detektivní dezinformace;
- vytipování dezinformačních nosičů a informačních zdrojů;
- plán průběhu realizace detektivní dezinformace.

Vlastní realizace lobbyingu:

- proniknutí k nosiči – informačnímu zdroji cílené zprávy,
- předání cílených informací či dezinformací,
- infiltrace cílené informace či desorientační zprávy,
- získávání zpětné vazby,
- vyhodnocení účinnosti infiltrované zprávy cílené zprávy,
- analýza zpětných vazeb,
- případné zlepšení lobování,
- konec průběhu lobování.

Nelegální-protiprávní postupy olivového zpravodajství jsou:

- dezinformace při překročení míry únosnosti,
- vydírání,
- úplatky (korupce),
- zneužití něčí tísně apod..

II. PRAKTICKÁ ČÁST

5 VÍCEVRSTVÁ KONCEPCE OCHRANY SPOLEČNOSTI

5.1 Přiměřené kontroly zaměstnanců

Podle zákoníku práce zaměstnanci nesmějí bez souhlasu zaměstnavatele užívat pro svou osobní potřebu výrobní a pracovní prostředky zaměstnavatele včetně výpočetní techniky ani jeho telekomunikační zařízení. Dodržování tohoto zákazu je zaměstnavatel oprávněn přiměřeným způsobem kontrolovat.

Abychom neporušovali práva zaměstnance či zaměstnavatele, je třeba vycházet z § 316 zákoníku práce odst. 1, 2 a 3 (viz.Legislativa).

Přiměřenou kontrolu lze odůvodnit tím, aby zaměstnavatel měl přehled zda jeho zaměstnanec využívá plně svou pracovní dobu k plnění pracovních úkolů.

Přikláním se k názoru pana JUDr. Lukáše Jansy, který říká, že :„ *přiměřeně* znamená v praxi právo kontrolovat:

a) dobu strávenou na internetu a místa pohybu,

b) činnost na počítači (např. hraní her),

c) čísla příchozích a odchozích telefonických hovorů a faxových spojení,

d) obsah paměti svěřeného počítače a externích nosičů dat,

e) obsah firemní emailové schránky.

Nepřiměřeně může znamenat:

a) sledování obsahu chatu na soukromém ICQ, facebooku či skypu,

b) sledování soukromé emailové korespondence ať už prostřednictvím kamery atd..

K posouzení hranice přiměřenosti a překročení této hranice bude mít vždy rozhodující slovo výklad soudu.

5.1.1 Povinnost upozornit zaměstnance na kontrolu

Je-li dán závažný důvod spočívající ve zvláštní povaze činnosti zaměstnavatele, který odůvodňuje zavedení kontrolních mechanismů podle odst. 2 §316 , je zaměstnavatel povinen přímo informovat zaměstnance o rozsahu kontroly a o způsobech jejího provádění.

Závažným důvodem rozumíme např. to, že zaměstnanec má přístup k důvěrným či tajným informacím apod.. Zaměstnavatel o některých kontrolách své zaměstnance informovat nemusí, ale pokud se rozhodne o kontrolách informovat, může to mít pozitivní i negativní dopad. Zaměstnanci se před obavami kontroly nebudou tolik věnovat svým soukromým aktivitám, ale naopak můžou být frustrováni, stresování a to může vést k neefektivní práci.

5.1.2 Kontrola práce na počítači a pohyb na internetu

Na tuto kontrolu nemusí být zaměstnanec předem upozorněn, jelikož tyto způsoby kontroly nejsou uvedeny ve výčtu § 316 odst. 2 zákoníku práce. Stejně tak např. používání softwaru typu eDetektiv nebo Velký Bratr[3] jsou legální formou kontroly zaměstnanců.

5.1.3 Nepřiměřené kontroly můžou být problém

Pokud se zaměstnavatel dopustí neoprávněné kontroly zaměstnance a překročí mez přiměřenosti může se v takovém případě zaměstnanec bránit tím, že upozorní zaměstnavatele na protizákonný postup. Má právo se domáhat dle § 265 zákoníku práce náhrady škody. Při porušení pracovněprávních předpisů hrozí zaměstnavateli uložení pokuty oblastním inspektorátem práce.

Za úmyslné jednání zaměstnavatele sledujícího soukromou emailovou schránku zaměstnance, může zaměstnavateli hrozit trestní stíhání pro porušování tajemství dopravovaných zpráv.[17]

---

[3] JANSA, Lukáš. *PravoIT* [online]. 27.02.2009 [cit. 2010-04-14]. Způsob kontroly zaměstnanců dle nového zákoníku práce. Dostupné z WWW: <http://www.pravoit.cz/article/zpusoby-kontroly-zamestnancu-dle-noveho-zakoniku-prace>.

5.1.4 Vyhodnocení

Kontrola činnosti zaměstnance na pracovišti je důležitá, nicméně neměla by znamenat vytvoření atmosféry strachu a stresu. Je tedy vždy jen na zaměstnavateli, aby nastavil způsob kontroly do patřičné rovnováhy. Není nutné, aby se zaměstnanec obával i krátkého přístupu na internet za účelem zjištění dopravního spojení ze zaměstnání.

Vhodným řešením je, aby zaměstnavatel předem upozornil zaměstnance na monitorování jejich činností a současně dovolil při řádném plnění pracovních úkolů krátký přístup na internet.

5.2 Lze zabránit zaměstnancům v odcizení know-how?

5.2.1 Kdo je schopen se činu dopustit?

Všeobecně se říká, že pokud má ke krádeži či k poškození atd. dojít, musí být splněny tři základní rysy:

a) člověk musí mít motiv,

b) člověk musí mít příležitost,

c) člověk se musí být schopen ospravedlnit (sám před sebou).

Nejčastěji k nekalému jednání vedou pachatele tyto příčiny:

- potřebuje si udržet nákladný životní styl,
- nejsou si vědomi, že dělají něco špatného,
- mají nízký práh odolat pokušení,
- jsou najímáni ke krádeži či poškození jinou osobou (např. konkurence),
- cítí křivdu, chtějí se za něco pomstít apod..

Podle průzkumu PwC páchají tyto skutky v České republice zejména muži se středoškolským vzděláním ve věku od 31 do 40 let. Potencionálním pachatelem je ale každý z nás.

Většinu hospodářské kriminality v podniku páchají sami zaměstnanci. Zaměstnance můžeme rozdělit do dvou základních typů:

- profesionální zloději – využívají propracované metody, vše mají pečlivě naplánované a vědí, jak překonat bezpečnostní systémy;
- příležitostní zloději – využívají příležitosti, náhody a štěstí.

5.2.2 Metody prevence

Žádná metoda prevence není 100% , ale dokáže podstatně snížit riziko krádeží know-how nebo jiných hodnot. Za pomocí vhodného spojení preventivních a kontrolních opatření lze odradit profesionální podvodníky, lupiče, padouchy atd..

5.2.2.1 Školení proti nesprávnému jednání

Školení proti nesprávnému jednání navýší vědomí pracovníků, co se považuje za správné nebo nesprávné jednání. Dále upozorní na metody, kroky, jak zabraňovat a odhalovat nesprávné jednání svých kolegů. Metoda vede k vyztužení platného kodexu jednaní. Je vhodná pro členy vyššího vedení podniku, kteří nesou odpovědnost za řízení rizika souvisejícího s nesprávným jednáním vlastních zaměstnanců.

5.2.2.2 Způsoby oznámení

Přímé oznámení

Aby mohl zaměstnanec upozornit na nesprávné jednání svých kolegů, nadřízených atd. je třeba mít připravený způsob jak informaci předat. Aby se k tomu zaměstnanec odhodlal, musí vědět, že bude chráněna jeho totožnost.

Jednou z možností je zřízení tzv. schránky, kam se tyto informace dají vložit. Pokud by byla ohrožena důvěrnost člověka, co na problém upozorňuje, systém ztrácí funkčnost.

V některých státech se tato metoda může považovat za projev nedostatku loajality vůči spolupracovníkům. Metoda je to však účinná, protože 1/3 krádeží ve společnostech (zdroj MV) je odhalena na základě upozornění.

Horká linka

Zřízení tzv. horké linky je jednou z metod, jak oznámit majiteli, nadřízenému, že se kolega dopustil krádeže, zfalšování informací apod.. Anonymní způsob oznamování má své výhody:

- ulevit svědomí,
- překonat pocity tísně,
- nebezpečí se zaplést do vyšetřování,
- anonymita.

Nejideálnější řešení vidím v provozování „horké linky“ externí společností. Pocit, že svěřuji citlivé informace o spolupracovníkovi někomu cizímu považuji za bezpečnější.

Prověření uchazeče

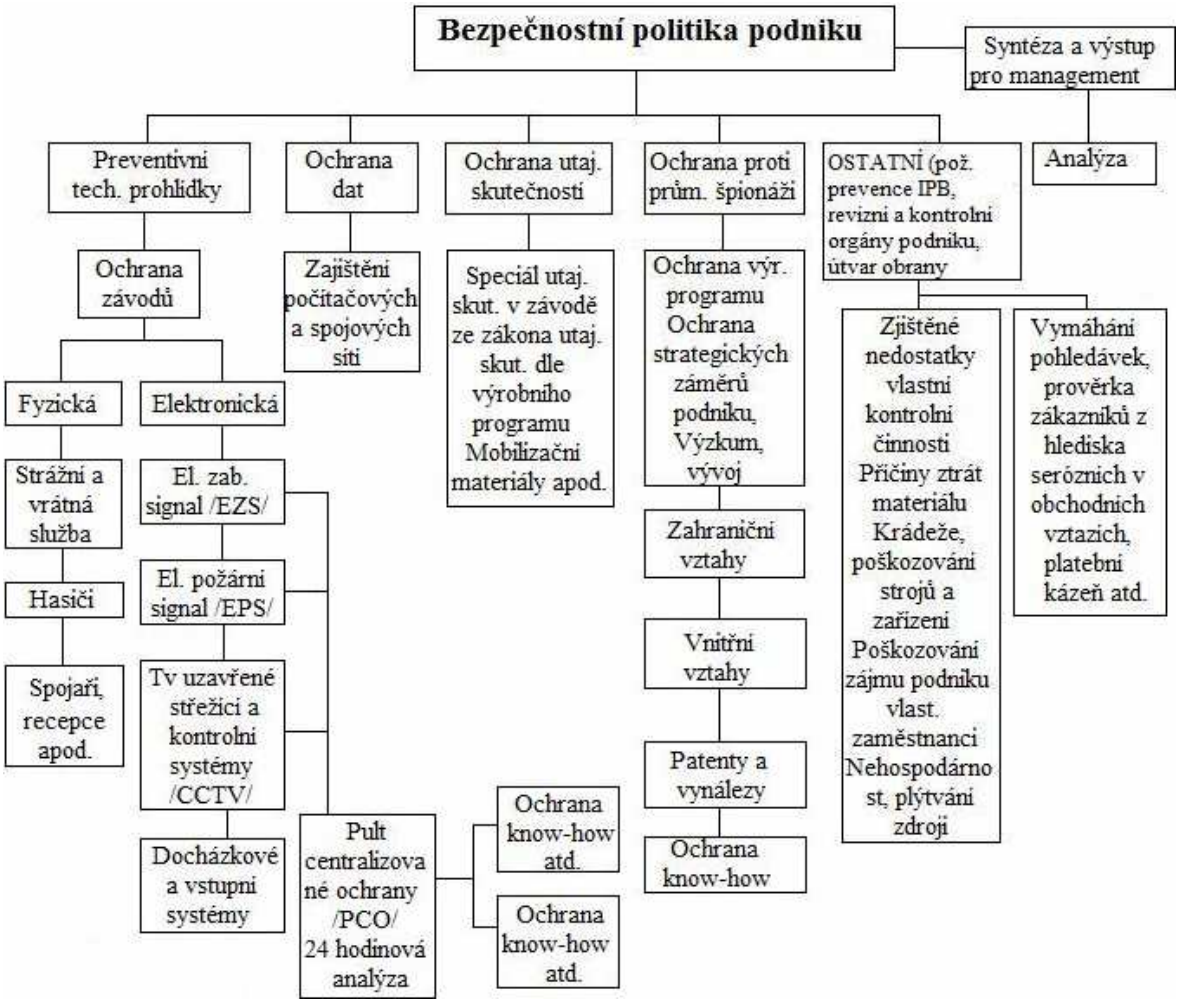
Citlivé informace vyžadují, aby s nimi přicházely do styku jen osoby, které jsou poctivé, zodpovědné a mají patřičnou kvalifikaci tuto funkci provádět. Měly by být tedy kladeny patřičné nároky na výběr zaměstnanců do těchto pozic. Pečlivý výběr vyžaduje použití metod, které uchazeče dostatečně prověří. K těmto praktikám patří metoda ověřování bezúhonnosti uchazečů. Jedná se o prověření vlastnosti uchazeče (charakter, nátura, poctivost, kvalifikace, zda byl trestně stíhán apod.).

Přestože nelze očekávat stoprocentní záruku, v praxi to poskytuje vyšší jistotu, že do společnosti nepřijímáme potenciálního zločince. Současně to může sloužit jako účinná pojistka proti tomu, aby se určité typy lidí vůbec o zaměstnání v dané společnosti ucházely. Náklady na řádné prověření jsou podstatně nižší, než následky špatné personální politiky. [18]

5.2.3 Vyhodnocení

Zaměstnanci daleko více uvažují o krádeži, poškození know-how apod. právě tehdy, když nepracují v kontrolovaném prostředí. Společnost by měla provádět pravidelné, ale i namátkové kontroly. Na pozice, které vyžadují naprostou pracovní diskrétnost je lepší dosazovat pracovníky, kteří pro podnik pracují delší dobu. V konečném výsledku je důležité, aby byl spokojen jak zaměstnavatel, tak i zaměstnanec. Zaměstnanec, který má ke své firmě pozitivní vztah, bude s menší pravděpodobností krást či poškozovat majetek zaměstnavatele a spíše se odhodlá takové jednání oznámit.

6 MODELOVÝ ZPŮSOB OCHRANY KNOW-HOW

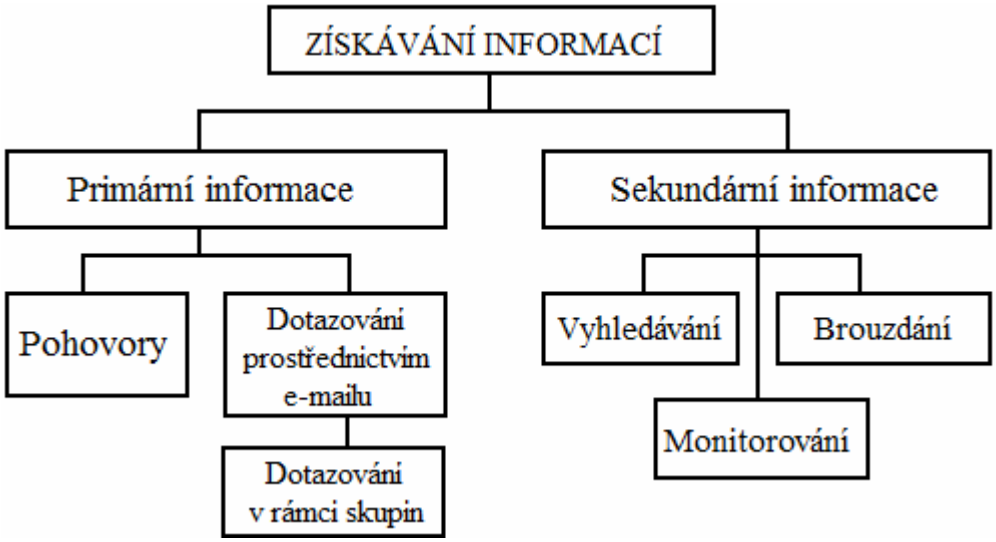


Obr. 8 *Bezpečnostní politika podniku – zdroj JUDr. Laucký*

Bezpečnostní opatření, týkající se ochrany know-how musí vycházet z:

- bezpečnostní analýzy (určíme analýzu hodnot, analýzu rizik, analýzu hrozeb a analýzu ohrožení);
- odhadu vývoje bezpečnostní situace;
- vypracování příslušných bezpečnostních projektů (režimový, technický, fyzický a také podle *JUDr. Františka Brabce* často opomíjený projekt vnitřní ochrany = detektivně – zpravodajských opatření);
- personální bezpečnosti;
- ochrany proti konkurenci;
- ochrana proti průmyslové špionáži.

Abychom mohli zvolit vhodné bezpečnostní opatření, musíme mít k dispozici dostatečné množství informací z kterých budeme vycházet. Můžeme je získat z několika zdrojů:



Obr. 9 *Získávání informací (inspirace Blažková, 2005)*

Na informace jsou kladeny zvláštní požadavky ⇒ kvalita informací :

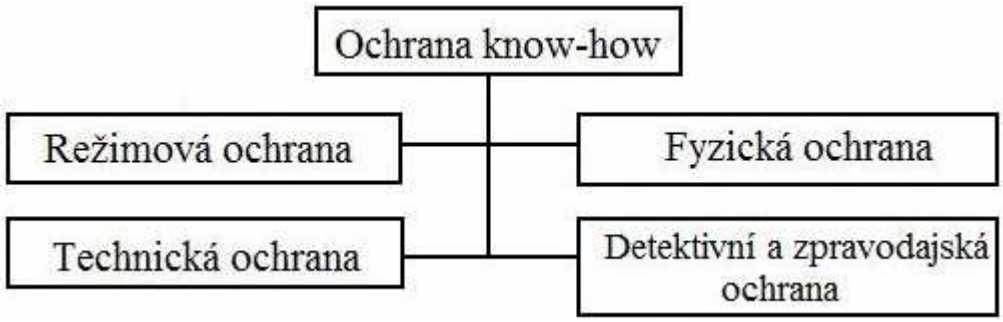
- jak je schopný informační zdroj,
- jak je spolehlivý informační zdroj,
- zda jsou informace pravdivé,
- zda je informátor objektivní,
- jak moc se mu dá věřit (důvěra v informátora).

Způsob získávání informací je obdobný i u „nastrčeného“ detektiva do společnosti. Detektiv může v podniku prozkoumávat, sledovat, pátrat apod. dvěma způsoby:

- otevřeně,
- skrytě.

Získané informace nám i jemu poslouží k efektivnímu nalezení a zvolení ochrany know-how.

6.1 Návrh ochrany know-how :



Obr. 10 *Návrh ochrany know-how (inspirace Laucký a Brabec)*

6.2 Režimová ochrana

Činnosti režimové ochrany jsou omezeny zákony, které vymezují nejen některé její úkoly, ale i oprávnění a prostředky, které mohou při ochraně podniku používat.

V Bezpečnostních zásadách ochrany podniku přišel Látal a Štantejský s definici:

Režim je administrativní, organizační a věcné uspořádaní vztahů mezi lidmi, jejich činnostmi a vlastními procesy v oblasti výkonu i řízení za účelem sladění všech prvků a s cílem dosáhnout harmonického stavu v dané společnosti.

Režim souvisí se všemi druhy ochranných opatření. Výborné mechanické a technické prostředky ochrany jsou nám k ničemu, když nebudou v provozu, protože nebude existovat systém pokynů k obsluze.

Režimová opatření se týkají:[4]

- činnosti pracovníků uvnitř podniku (vlastních zaměstnanců);
- pohybu a chování osob přicházejících zvenčí, včetně oběhů dokladů a informací uvnitř podniku (administrativní nebo spisový pořádek);
- výstupu informací, dat, dokumentů vně podniku.

[4] LÁTAL, Ivo; ŠTANTEJSKÝ, Michal. *Bezpečnostní zásady ochrany podniku : Prevence a řešení krizových situací*. Vyd.1. Praha : PROSPEKTRUM, 2001. Režimová ochrana, s. 120. ISBN 80-7175-091-3.

Všechny potřebné zásady by měly být zpracovány v patřičných organizačních dokumentech a v interních normách daného podniku. Významnou činností každého podniku je rovněž spisová služba. Jde o nástroj řešení správních agend, který musí vytvářet jednotný, účelně organizovaný systém, sjednocující pracovní postupy a respektují obecné principy i konkrétní podmínky. Spisová služba by měla být relativně stálá a pružně reagovat na změny vyvolané dynamikou pracoviště. Prvky spisové služby jsou:

- spisový plán;
- spisová registrace;
- řády, předpisy, směrnice pro spisovou agendu;
- spisové pomůcky;
- předepsané nebo užívané tiskopisy.

Režimová ochrana know-how:

- jednoznačně stanovit, které informace jsou důvěrné a tajné;
- jednoznačně stanovit prostory uložení informací;
- určit čas (dobu), jak dlouho informace chránit;
- určit osoby, které můžou a na jak dlouho s informacemi pracovat, manipulovat, případně je vynášet;
- v případě změn personálu okamžitě aktualizovat seznamy osob;
- stanovit kontroly režimových opatření – jak se budou provádět, kdo je bude provádět, kdo ponese za kontroly odpovědnost.

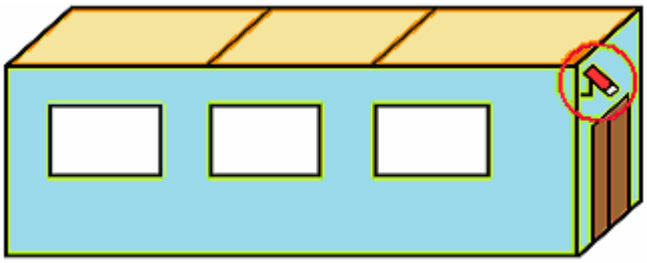
Obr. 11 *Uložení, informace, doba, aktualizace – zdroj Google*

6.3 Technická ochrana

Technická ochrana nabízí nejširší možnosti jak know-how chránit. Jednou z možností je využití technických prostředků a prvků zabezpečovací techniky:

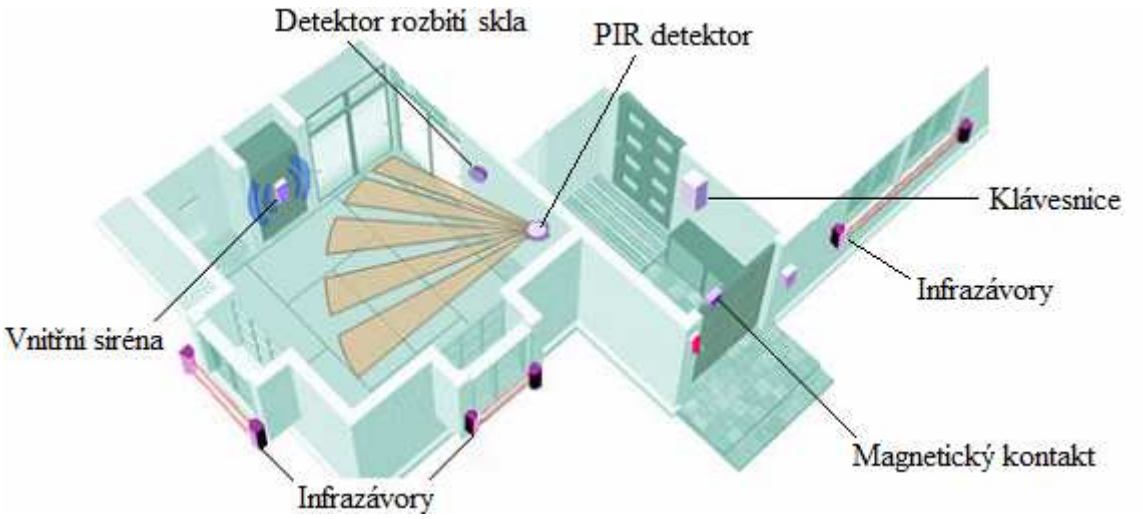
- EZS (elektronické zabezpečovací systémy),
- EPS (elektrická požární signalizace),
- CCTV (systémy průmyslové televize),
- MZS (mechanické zábranné systémy),
- přístupové systémy atd..

Nejúčinnější technické ochrany docílíme kombinací zabezpečovacích systémů (např. EZS+EPS, EZS+MZS, EZS+CCTV apod.).



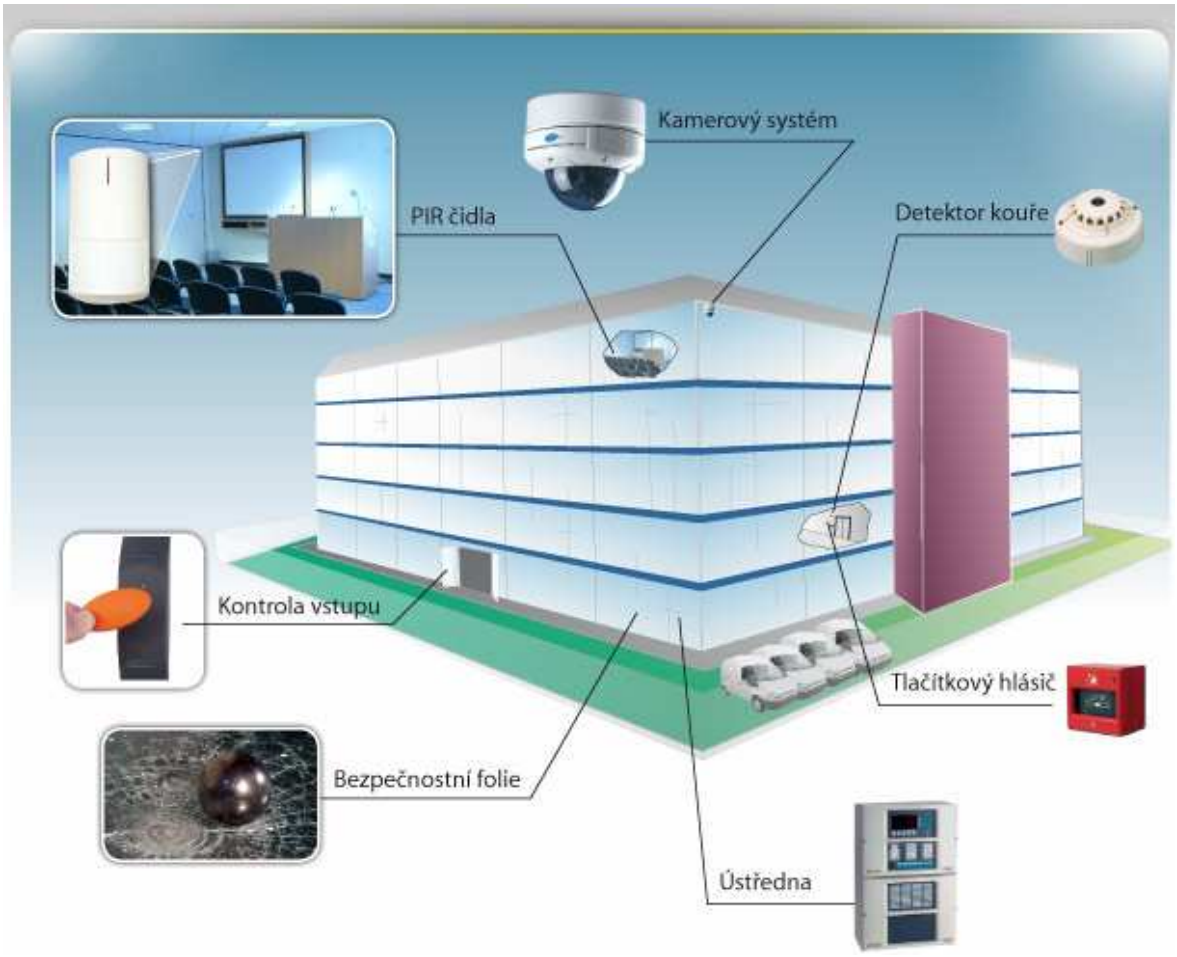
Obr. 12 *Technická ochrana vstupu pomocí kamery*

Na prostory, kde se know-how vyskytuje a skladuje by měl být kladen zvláštní důraz. Na obrázku je možný způsob vnitřního zabezpečení objektu.



Obr. 13 *Zabezpečení uvnitř objektu (inspirace Macháček L.)*

Technických prostředků lze také využít na komplexní ochranu celé společnosti.



Obr. 14 *Zabezpečení průmyslového objektu – zdroj Alcatraz*

Ochrana perimetru společnosti za pomocí EZS je vhodná především tehdy, když technická ochrana není spojena s ochranou fyzickou, anebo společnost nemá vrátného, který by prováděl pravidelné pochůzky kolem objektu.

Další metodou jak zabránit potencionálnímu útočníkovi odcizit know-how např. z počítače je zamezit mu k informacím přístup (softwarová ochrana).

6.3.1 Ochrana know-how z hlediska přístupu

Pokud je know-how uloženo v počítačové podobě, lze zamezit k neoprávněnému přístupu dvěma způsoby:

- zamezení uživateli v tom, aby jakýmkoli způsobem mohl citlivá data neoprávněně zobrazit či dokonce modifikovat;
- fyzická bezpečnost – ochrana proti krádeží apod..

Obzvlášť důvěrné a citlivé informace je třeba i šifrovat. Pokud by se nepovolaná osoba k těmto informacím dostala, bez patřičného klíče (hesla) by je neměla možnost otevřít. Útočník a narušitel může přijít k informacím buď:

- zvenčí (nedostatečně zabezpečen přístup k informacím z okolní sítě, porucha systému),
- zevnitř (zneužití hesla, špatné uspořádání přístupových práv).

Identifikace, autentizace, autorizace

Identifikace – zjištění uživatelovy identity např. zadáním hesla, či kódu.

Autentizace – ověření, zda je uživatel osobou za kterou se vydává.

Autorizace – zjištění, zda k provedení činnosti, služby má uživatel právo.

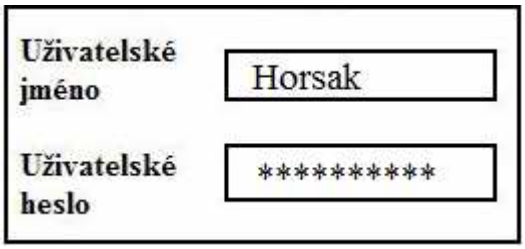
K ověření přístupu lze použít těchto metod:

- uživatel si něco pamatuje – prokáže se pomocí smluveného kódu (např. hesla, číselný kód).
- uživatel něco vlastní – uživatel se prokáže jedinečným technickým zařízením (např. čip, čipová karta, karta s magnetickým proužkem, klíč apod.).
- podle fyzických osobních charakteristik – biometrie (otisk prstu, struktura oční sítnice či analýzu hlasu).

Značným zvýšením bezpečnosti je kombinace výše popsaných metod.

Hesla

Jedná se o nejstarší způsob ověřování přístupu uživatele. Ten první zadává své uživatelské jméno a později uživatelské heslo.



***Obr. 15** Přihlášení*

Jak správně zadávat hesla:

- být mimo zorné pole ostatních osob (aby heslo nezpozorovali);
- pozor nato, zda nezadávám heslo do uživatelského jména (jiné uživatelské jméno může být zaprotokolováno do souborů);
- vyhnout se heslu složeného z jmen, příjmení a roku narození;
- vyhnou se heslu složeného z názvu měst, obcí, místa pracoviště apod..

Dobrá hesla by měla mít následující vlastnosti:

- používají velká i malá písmena abecedy;
- používají číslice a jiné znaky (interpunkce, mezery, speciální znaky – #@*);
- jsou nejlépe sedm až deset znaků dlouhá;
- netvoří žádné známé slovo;
- jsou zapamatovatelná.

Po určitém časovém období (max. několik měsíců) je vhodné heslo obměňovat.

Některé možné postupy pro výběr hesel:

- spojení dvou slov dohromady pomocí nealfanumerického znaku nebo čísla: *trikofolie, fotosklenice apod.*.
- nově vytvořená slova (spojení anglického a českého jazyka): *stultable, posteldogs, batohbooks apod.*.

Jednorázová hesla

Vyžadují zvláštní konfiguraci počítačového systému a speciální zařízení v podobě kalkulátoru, který pokaždé vygeneruje uživateli jiné heslo. Jedná se o bezpečnější způsob proti odhalení hesla. Heslo je vygenerované jen na určitou dobu (pár minut). V případě překročení doby si uživatel generuje heslo nové.

Mezi další způsoby ověřování uživatelů patří:

Čipové karty

Čipové karty jsou složeny z procesoru, integrovaného obvodu a většinou zality plastovým materiálem. Jedná se pohodlnou metodu identifikace, kde je vše uloženo na

jediném čipu. Čipové karty jsou používány i při šifrování souborů, kde mohou sloužit i jako klíč k odšifrování souborů.

Čipové karty se podle způsobů snímání dělí na dvě základní skupiny:

- kontaktní – obsahují na svém povrchu kontaktní plochy a pro svou činnost musí být vloženy do čtecího zařízení;
- bezkontaktní – nevyžadují žádný fyzický kontakt, stačí přiblížit k čtecímu zařízení. K přenosu dat a napájení používají indukční smyčku.

Čipové karty jsou poměrně rozšířené i pro běžné použití, a proto existuje několik standardů definujících jejich rozměry a funkčnost. Fyzické charakteristiky karet definuje norma ISO 7810, jejich komunikaci s okolím normy ISO/IEC 7816 (kontaktní karty) a ISO/IEC 10536 (bezkontaktní karty).

Biometrie

Biometrie je velmi starý způsob identifikace. Každý člověk má své specifické a zároveň fyziologické vlastnosti. Mezi biometrické metody patří např.:

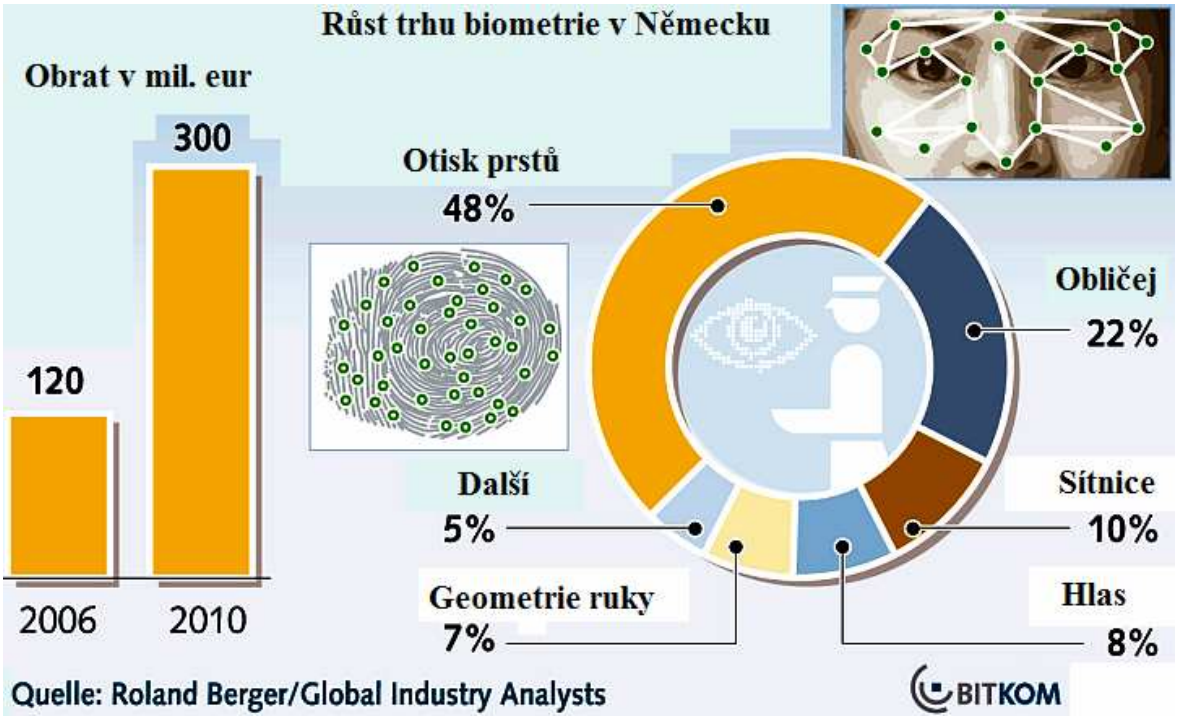
- otisk prstů,
- geometrie ruky,
- geometrie obličeje,
- vzorek oční sítnice nebo duhovky apod..

Otisky prstů jsou pro svoji spolehlivost (pravděpodobnost výskytu dvou shodných otisků se pohybuje v řádu 10^{50}) již dlouhou dobu používány pro identifikaci osob v kriminalistice.

Snímače otisků jsou založeny na principu elektrického, optického, ultrazvukového, tepelného či tlakového snímání otisku. Nejstarším typem byly křemíkové snímače, které využívaly změny elektrické kapacity mezi dvěma body snímače, podle toho, je-li mezi nimi papilární čára nebo mezera.

V dnešní době jsou nejrozšířenější optické snímače. Ty využívají změny odrazu světla od částí prstu. Jsou poměrně levné, ale spolehlivost je závislá na čistotě snímací plochy. Nejnovějším typem jsou ultrazvukové snímače, které jsou značně spolehlivé, ale

pro svou vyšší cenu relativně málo rozšířené. Ke zvýšení spolehlivosti vede kombinace snímačů s tepelnými a tlakovými senzory.



Obr. 16 *Růst trhu biometrie v Německu – zdroj Quelle*

Nevýhody identifikace podle otisků prstů:

- možnost oklamání snímače pomocí návleku na prstu (nové technologie vykazují všechny znaky živého prstu, tedy propouští teplo, pulsace krve a správná vlhkost).
- psychologický odpor některých osob (souvislost metody s kriminalistikou).

O nepříliš příjemnou, ale zato spolehlivou metodu lze považovat snímání oční sítnice. Ke snímání se používá speciální laserové zařízení. Podobná technika se využívá i při identifikaci podle oční duhovky. Jedinečnost lidské oční duhovky je udávána číslem $1/10^{78}$, tedy ještě menší pravděpodobnost výskytu dvou shodných znaků než u otisků prstů.

6.3.2 Vyhodnocení

K ověřování přístupu uživatelů se nejčastěji používá kombinace uživatelského jména a hesla. Uživatelské heslo nesmí být jednoduše odhadnutelné. Mělo by v sobě obsahovat kombinaci malých a velkých písmen, číslic i speciálních znaků. Pokud požaduji pohodlný způsob identifikace, můžu využit čipových karet. Nevýhodou čipových karet je

to, že jsou snadno odcizitelná a lehce se dají ztratit. V místech, kde je zapotřebí zvýšená bezpečnost přístupu, doporučuji používat metody biometrie. Jsou nákladnější na pořízení, ale zato velmi spolehlivé.

6.3.3 Zálohování informací a dat

Zálohování informací a dat slouží především jako „záchrana“ když se nám zhroutí systém. Jedná se o tzv. obnovu systému. V případě havárie počítače máme možnost vrátit systém do podoby ve které byl např. před hodinou.

Obnovení dat může proběhnout v úplném rozsahu, nebo se můžeme zaměřit jen na určitou část dat.

Existují dva základní druhy záloh:

- úplná záloha – záloha všech souborů;
- inkrementální záloha – záloha pouze souborů změněných od posledního zálohování.

Vyšší spolehlivost inkrementálních záloh lze dosáhnou vhodnou rotací zálohovacích medií. Princip spočívá v tom, že např. každý týden zálohujeme na jiné paměťové pásce. Metody zálohování by měly být v každém případě součástí bezpečností politiky organizace.

6.3.4 Fyzické zabezpečení informací

Pod pojmem fyzické zabezpečení informací si lze představit různé možností. Já se budu zabývat způsoby, které zabraňují pachateli v krádeži citlivých informací.

Vhodným opatřením je mít zařízení (počítač, paměťová média, disky) pečlivě uzamčené. Počítače lze mít zabudované přímo do speciálních skříní. Notebooky musí být skladovány v prostorách, kde se nepráší, není vlhko, nebo naopak příliš teplo. Doporučuje se např. uzamčení notebooků k nábytku za pomocí ocelových lanek.

K zabezpečení záloh se používají speciální druhy pancéřových sejfů, které dokáží vzdorovat i vysokým teplotám (požár). Je-li uchování dat opravdu kritickou součástí systému, je nezbytné jejich archivování na jiném místě, než se nacházejí originální data.

Servery by měly být umístěny v oddělené místnosti, do které je omezený přístup pouze pro jejich obsluhu. Vhodná je také instalace bezpečnostních zařízení včetně kamer napojených na centrální ochranu pracoviště. Samozřejmostí je napojení na systém bezpečnostních protipožárních čidel a dostatečně dimenzovaná klimatizace, která zabraňuje přehřátí počítačových systémů, které by mohlo způsobit poruchu.

Uživatel nesmí zůstat přihlášený pokud opouští své pracoviště. Měl by se ze systému buď odhlásit nebo pracovní stanici uzamknout.

6.3.5 Vyhodnocení

Pravidelné zálohování dat, nejlépe v kombinaci s rotací zálohovacích médií, zaručují větší bezpečnost i při fyzické chybě jednoho média. Jednou za čas (několik dnů až týdnů) by se měla provádět úplná záloha dat.

Fyzické zabezpečení informací je způsob prevence, jak omezit, případně zamezit narušiteli se k informacím, datům, počítačům dostat. Každá překážka v podobě zabezpečení informací může narušiteli znepříjemnit pokus se k informacím dostat nebo ho dokonce od pokusu úplně odradit.

6.4 Fyzická ochrana

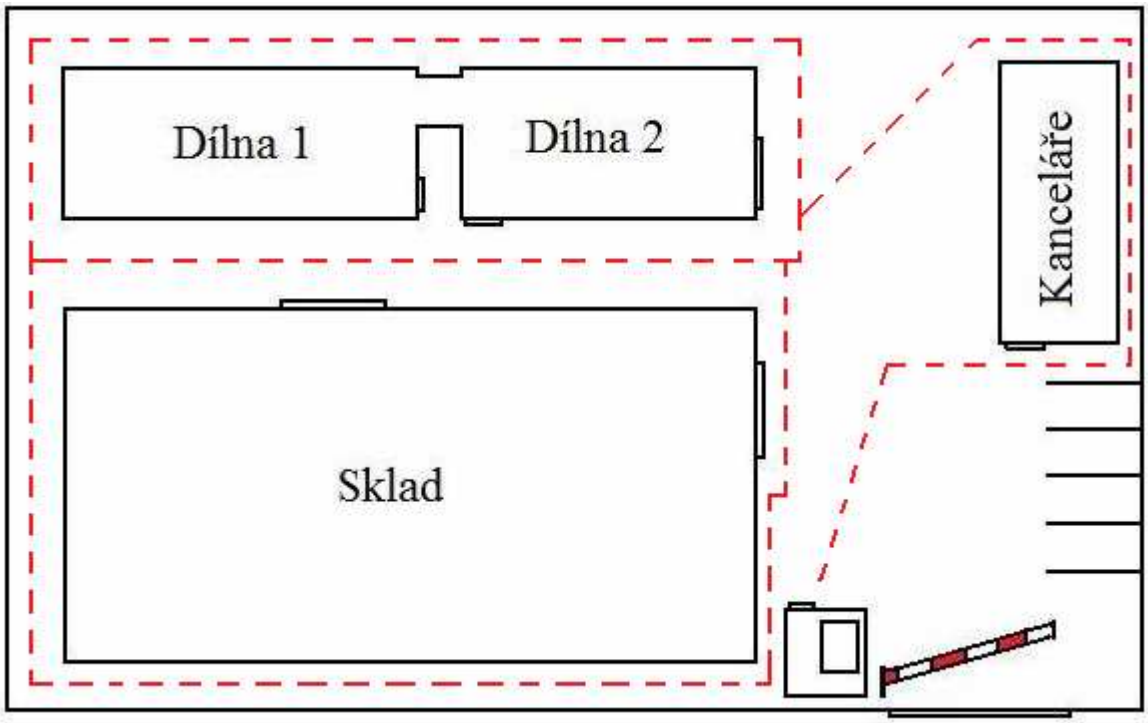
Jedná se o nejstarší formu ochrany osob a majetku. Její největší výhodou je možnost provést okamžitý zásah a odvrátit tak nebezpečí hrozící chráněnému zájmu.

Fyzická ochrana může být rozdělena podle doby provádění:

- v době pracovní doby,
- nepřetržitá ochrana,
- nárazová (namátková) ochrana.

Fyzická ochrana know-how se především týká:

- fyzická ochrana společnosti jako celku;
- fyzická ochrana vnitřních prostor, kde se know-how vyskytuje;
- fyzická ochrana prostor, v nichž se s know-how pracuje;
- fyzická ochrana míst, kde je know-how skladováno a uloženo.



Obr. 17 *Fyzická ochrana perimetru*

*** – – – * …** čárkované čáry představují trasu, kudy má fyzická ochrana projít, aby patřičně zkontrolovala perimetr objektu. Většinou se prohlídky provádí v noci (např. mezi 0.00 hod. – 05.00 hod., čtyřikrát týdně) a dle předem stanovených pokynů. Pokud je v objektu vrátný, může být jeho povinností v pravidelných intervalech okolí perimetru zkontrolovat.

6.5 Detektivní a zpravodajská ochrana

Jak uvádí pan JUDr. Brabec v Technologii detektivní činnosti je této ochraně informační bezpečnosti věnována ze strany společnosti malá pozornost. Detektivní a zpravodajská ochrana se především upíná k personální bezpečnosti. Ta je zajišťována vhodným výběrem zaměstnanců, školením zaměstnanců apod. O správnou funkčnost systému se starají pravidelné kontroly a prověrky.

Tyto prověrky je možno zajišťovat[5]:

[5] Brabec, F.: *Technologie detektivní činnosti.* UTB, Zlín 2009. 160 s. ISBN 978-80-7318-780-4

- detektivně-zpravodajskými prověrkami zaměstnanců pro organizaci významných pozicích a především středního a vyššího managementu.
- prověrky prostřednictvím psychologických auditů v personální sféře. V této souvislosti může významnou měrou přispět fyziodetekce.

Principem fyziodetekce je:

- vyvolání psychické reakce prověřované osoby na kladené diferenční (kritické) a indiferentní (nekritické) podněty.
- registrace odezvy průběhu psychických podnětů prověřované osoby na periferii organismu.
- odborná interpretace hodnot zjištěných registrací odezvy na periferii organismu.

Při fyziodetekčním vyšetření (FV) se postupuje následovně:

- připraví se FV,
- vlastní provedení FV,
- vyhodnotí se výsledky FV,
- vyvodí se závěry.

Fyziodetekčního vyšetření lze dosáhnout za pomocí přístrojů jako jsou polygrafy, analyzátory hlasu či detektory lži apod..

6.5.1 Detektor lži

Obr. 18 *Detektor lži – zdroj Google*

Vyšetřovanému jedinci se položí několik otázek, které musí být sestaveny tak, aby se na ně dalo jednoznačně a bez přemýšlení odpovědět. Výsledkem jsou křivky na obrazovce nebo papíru, z kterých specialista pozná, zda mluvil dotyčný pravdu či lhal.

Nevýhody:

- musíme mít písemný souhlas vyšetřované osoby,
- vyšetření musí provádět specialista,
- vyšetření může mít vliv na psychiku vyšetřované osoby.

Výhody:

- jasné otázky → jasné odpovědi,
- vede k objasnění trestné činnosti.

Tento způsob ochrany bych doporučil jen v krajních případech. Jako vhodná pomůcka poslouží např. když zaměstnance neoprávněně nařknu z odcizení know-how. Ten má pak možnost, alespoň částečně prokázat svou nevinu prostřednictvím tohoto přístroje.

6.6 Co nabízí detektivní kanceláře

V dnešní době je již na trhu velký počet detektivních kanceláří, které reagují na poptávku po prověrkách budoucích nebo stávajících zákazníků. Způsobů, jak je možno prověřit své zaměstnance se nabízí hned několik. Záleží na pozici zaměstnance, jakož i na míře rizika souvisejícího s výkonem jeho funkce.

Např. detektivní kancelář FALCO – HK nabízí tyto druhy prověrek zaměstnance:

„Aspirant

Ověření pravdivosti údajů uvedených v dotazníku, životopisu nebo při pohovoru, zejména prověření trestní minulosti, ověření minulých zaměstnání včetně referencí, vzdělání a praxe v oboru, prověrka v místě uvedeného bydliště.

Worker

Zjišťování skutečností, které by mohly přímo či nepřímo ovlivnit chod nebo jméno firmy. Jedná se zejména o způsob trávení volného času, zejména vyloučení či potvrzení rizika spojeného s nadměrným požíváním alkoholických nápojů a drog, hraní hazardních her nebo nezvykle vysokými finančními výdaji. Prověrka může být rozšířena o detektivní

činnost zaměřenou na odhalování trestních deliktů, počínaje drobnými krádežemi na pracovišti až po závažnou hospodářskou trestnou činnost.

Manager

Stupeň prověrky „Worker“ rozšířený o zjišťování okruhu přátel a jiných kontaktních osob, jejichž prostřednictvím by mohlo docházet k úniku informací z firmy nebo jinému poškození podniku. Tato prověrka je spojena s využitím dokumentačních a operativně technických prostředků v rozsahu, který si určuje sám zadavatel.

Inside Man

Velice efektivní způsob nasazení našeho pracovníka do firmy. Pracovník je proškolen detektivní kanceláří a vybaven veškerými potřebnými technickými prostředky. Po konkrétním zúkolování je zaměstnán ve firmě na pozici, odkud monitoruje a dokumentuje případnou trestnou činnost. Rovněž vyhledává a stanovuje veškerá rizika, na základě kterých jsou následně učiněna nezbytná opatření k zamezení trestné nebo jiné nežádoucí činnosti.

Customer

Prověrka potenciálního obchodního partnera, která může obsahovat jakýkoliv druh nebo kombinaci prověrek používaných u zaměstnanců, uchazečů nebo manažerů. Tyto prověrky jsou rovněž založeny na ověřování údajů, které obchodní partner uvedl při prvotních jednáních. Prověřují se zejména skutečné majetkové poměry, veškeré obchodní aktivity, reference od stávajících nebo bývalých obchodních partnerů, vztahy mezi jednateli, společníky a zaměstnanci, platební morálka, trestní minulost. Zároveň může být zpracována analýza propojení podniku či jeho jednatelů a společníků do jiných obchodních společností“.[19]

Mezi další prověrky patří kontrola personálu (skreening), kterou nabízí PLATINUM – SS. Zabývají se metodami kontrol personálu, které zahrnují:

- příjem do zaměstnání,
- propouštění,
- planované kontroly pracujícího personálu.

Úkolem skreeningu je najít spolehlivé a loajální pracovníky na vytyčenou pozici. Vybrat vhodného kandidáta na pozici např. práce s know-how není vůbec jednoduché.

Vedoucí podniku si tento problém začínají uvědomovat a těchto nových, efektivních metod začínají plně využívat.

Cílem těchto kotrol je odhalit činitele rizika mezi vybraným personálem.

Zabývají se např. tématy:

- kontrola pravdivosti údajů v životopise,
- skutečné (zatajované) důvody odchodů z předchozího zaměstnání,
- skutečné (zatajované) důvody nástupu do práce (rozkrádání, spolupráce s konkurencí),
- existence konfliktní práce,
- převod důvěrných informací z předchozího pracoviště dále,
- vyzrazení důvěrné informace,
- příjem úplatku, korupce,
- plánování vyděračství budoucího zaměstnavatele atd..[20]

6.7 Ochrana proti konkurenci

Zákaz konkurence je způsob jak zabránit zaměstnanci využít, resp. zneužít know-how v konkurenčním boji. V pracovněprávních vztazích je tento zákaz konkurence implementován do tzv. konkurenční doložky. Pokusím se uvést, jaká je možnost sjednání takového zákazu konkurence a jaká je jeho účinnost.

Firmy se snaží konkurenční doložkou bránit zejména úniku know-how, citlivých informací a jiných z pohledu firmy důležitých dat a postupů a jejich zneužití konkurencí, případně se brání získání výhody z efektivní činnosti zaměstnance ve prospěch konkurence.

Proto konkurenční doložka není na místě u běžných zaměstnanců, ale u těch, kteří přicházejí do kontaktu s uvedenými informacemi nebo jsou z jiných důvodů klíčoví pro firmu.

6.7.1 Konkurenční doložka

Konkurenční doložka se uvádí do pracovní smlouvy (případně dohoda o pracovní činnosti nebo provedení práce) obsažené písemné ujednání**,** jehož základní náležitosti jsou následující:

a) závazek zaměstnance zdržet se výkonu výdělečné činnosti, která by byla shodná s předmětem činnosti zaměstnavatele nebo která by měla vůči němu soutěžní povahu;

Shodnost předmětu podnikání ovšem nelze vztáhnout na celou šíři předmětu podnikání dle živnostenského listu. Nemůžeme bránit zaměstnanci, aby se zdržel jakéhokoliv zaměstnání či činnosti u jiného zaměstnavatele, pokud předmětem podnikání bude jiná činnost než kterou plnil doposud. Mělo by se vždy tedy zamezit účasti (zaměstnanecké, podnikatelské či jiné) na poskytování stejných nebo obdobných konkurenčních výrobků či služeb.

Soutěžní povahu lze pak dovozovat z faktické činnosti následujícího zaměstnavatele, jehož jednání může být konkurenční nebo konkurenci podporovat (např. poradenstvím).

b) určitá doba trvání zákazu konkurenčního jednání po skončení zaměstnání, nejdéle však 1 rok;

Stanovit délku trvání zákazu konkurence na delší dobu než je jeden rok možné není.

c) závazek zaměstnavatele platit tzv. finanční vyrovnání za dobu dodržování zákazu, a to v minimální výši odpovídající průměrné mzdě zaměstnance;

Po celou dobu, kdy zaměstnanec dodržuje zákaz konkurence, je povinen mu původní zaměstnavatel vyplácet průměrnou mzdu (bez ohledu na to, zda pracuje u nekonkurenčního zaměstnavatele nebo je nemocen). Peněžité vyrovnání je splatné pozadu za měsíční období, pokud se účastníci nedohodli na jiné době splatnosti.

d) spravedlnost požadavku zákazu konkurence;

Spravedlnost se odvíjí od povahy informací, poznatků, znalostí pracovních a technologických postupů, které zaměstnanec získal v zaměstnání u zaměstnavatele a jejichž využití by mohlo zaměstnavateli závažným způsobem ztížit jeho činnost. Takto formulovaný požadavek v podstatě znamená relativizaci platnosti každé konkurenční doložky, jelikož je nutné vždy zkoumat povahu informací a možnost ztížení činnosti

původního zaměstnavatele podstatným způsobem při jejich využití. To bude vždy na posouzení konkrétního případu konkrétním soudem.

e) možnost sjednat přiměřenou smluvní pokutu;

Bez smluvní pokuty by konkurenční doložka ztratila smysl. Největší problém činí určení výše smluvní pokuty. Zákoník práce požaduje, aby tato byla přiměřená povaze a významu konkurenční doložky, tzv. je nutné posoudit význam informací dostupných zaměstnanci, povaha jeho práce, hrozící škoda při porušení konkurenční doložky atd.

Proto vždy soudy budou posuzovat přiměřenost smluvní pokuty v jednotlivých případech a nelze obecně vztáhnout rozhodnutí na jiné případy.

Byla-li se zaměstnancem sjednána zkušební doba je možné dohodu o konkurenční doložce uzavřít nejdříve po jejím uplynutí. To znamená, že nelze donutit zaměstnance k uzavření konkurenční doložky, pokud by ji po uplynutí sjednané doby nechtěl uzavřít. Po skončení pracovního poměru zaměstnanec může konkurenční doložku vypovědět, jestliže mu zaměstnavatel nevyplatil peněžité vyrovnání nebo jeho část do 15 dnů po uplynutí jeho splatnosti.

6.7.1.1 Nevýhody takto v zákoníku práce pojaté konkurenční doložky

- povinnost zaměstnavatele vyplácet po dobu dodržování zákazu konkurence průměrnou mzdu (teoreticky by mohl zaměstnanec důvěrné poznatky sdělit konkurenci nebo pracovat pro konkurenci na základě obchodní smlouvy, aniž by původní zaměstnavatel něco zjistil);
- prokázat podezření na jednání bývalého zaměstnance může být problém;
- smluvní pokuta musí být přiměřená povaze a významu podmínek konkurenční doložky (těžko konkrétně definovat a bude vždy záležet na konkrétním případu);
- výše smluvní pokuty může být považována při soudním sporu za nepřiměřenou (rozsah škod nelze předvídat);
- zaplacením smluvní pokuty ze strany zaměstnance dochází k zániku povinnosti zdržet se konkurenčního jednání (zaměstnanec se může pohodlně zaměstnat konkurenční firmou, která za něj ochotně zaplatí smluvní pokutu);

- vymoci smluvní pokutu může trvat léta v rámci soudního rozhodování;
- možnost napadení konkurenční doložky pro její nespravedlnost;
- možnost napadení smluvní pokuty pro nepřiměřenost.

6.7.1.2 Výhody konkurenční doložky

- snadné uzavření konkurenční doložky v rámci pracovní smlouvy.[21]

6.7.2 Vyhodnocení

Konkurenční doložku bych nedoporučil jako účinný nástroj proti zneužití know-how zaměstnancem v konkurenčním boji. Pokud zaměstnanec pracuje s citlivými informace (know-how apod.), mělo by se pamatovat na zákaz konkurence již v pracovní smlouvě. Zaměstnancovi je nutno sdělit, jaké by jeho porušení např. mlčenlivosti mělo právní dopady, a že by to mohlo vést i k ukončení pracovního poměru. Všechny zákazy a nedovolené způsoby zacházení s know-how je dobré mít zpracované v pracovním řádu a vystaveny na zřetelném místě. Ideální ochranou je mít spolehlivé zaměstnance, kteří jsou patřičně motivováni a pro firmu pracují s radostí.

6.8 Jak může vypadat smlouva o know-how

Dohoda o mlčenlivosti, ochraně informací a zákazu jejich zneužití[6]

kterou uzavřely dle ustanovení § 269 odst. 2 zákona č. 513/1991 Sb., obchodní zákoník, v platném znění níže uvedeného dne

Smluvní strany:

AAA, a.s.	a	BBB, s.r.o.
Sídlem:		Sídlem:
Zapsaná v obchodním rejstříku…		Zapsaná v obchodním rejstříku…
Jednající:		Jednající:

[6] Inspiroval jsem se Markem Doležkem, *businessifo.cz(2009)*

IČ:	IČ:

Dohoda by měla obsahovat:

- co je účelem,
- co je předmětem,
- co se rozumí důvěrnými informacemi,
- obě smluvní strany se zavazují k plnění smlouvy,
- obě smluvní strany omezí počet zaměstnanců pro styk s těmito chráněnými informacemi,
- vymezí se informace na které se smlouva nevztahuje,
- veškeré informace dle smlouvy zůstanou vlastnictvím smluvní strany,
- co následuje za porušení této smlouvy,
- výše pokuty je stanovena .. Kč (slovy:…),
- doba, do kdy má být pokuta uhrazena,
- za způsobenou škodu porušením smlouvy odpovídá smluvní strana dle právních předpisů,
- kdy smlouva nabývá platnosti a účinnosti,
- na jakou dobu se smlouva uzavírá,
- změny a doplňky smlouvy vyžadují souhlas obou stran,
- právní vztahy se řídí právním řádem České republiky,
- smlouva se vyhotovuje ve dvou výtiscích (pro každou smluvní stranu 1x).

Ve Zlíně dne	Ve Zlíně dne
AAA a.s.	**BBB.s.r.o.**
……	……...

7 VŠEOBECNÁ OCHRANNÁ (PREVENTIVNÍ) OPATŘENÍ

- vytváření celkové ochranné (bezpečnostní) politiky společnosti;
- zajišťování fyzické ochrany objektů, majetku, osob a informací;
- programově-technická opatření v automatizovaných informačních systémech;
- týkající se software, hardware;
- opatření zabývající se řádného vedení příslušné dokumentace, protivirových opatření apod.;
- organizačně-režimová opatření, k nimž patří např. přesné a jasné vymezení funkcí, kompetencí, režimu na pracovištích, hierarchické úrovně pracovníků;
- personální opatření při výběru a kontrole lidských zdrojů.

Z hlediska ochrany jednotlivých objektů (prvků systému) pak lze rozlišovat následující druhy opatření:

- organizační (organizační řád, pracovní řád, technologické postupy);
- administrativní (předpisy, pokyny, směrnice apod.);
- režimová (pokyny pro činnost v krizových situacích);
- právní (preventivní, represivní);
- fyzická (předpisy stavební, elektrotechnické, vzduchotechnické a další);
- technická (pro hardware a software);
- personální (pro výběr a výchovu personálu) a sociálně – psychologické.[22]

7.1 Návrh plánu, jak vyjít z problému

Ani sebelepší prevence není stoprocentní zárukou ochrany know-how. Pokud dojde k prolomení bezpečnostních opatření např. z počítače a know-how unikne, je třeba mít po ruce plán řešení (může se jednat o krizový plán). Plán by měl být patřičně otestovaný. S testy stoupá kvalita plánu. Kvalitní plán nám pomůže, jak se co nejlépe a nejrychleji s problémem vypořádat.

Co dělat prvních 60 minut?

- člověk nesmí hned panikařit,
- nedělat hned závěry,
- snažit se nemyslet hned na nejhorší,
- postavit se k problému čelem a s čistou hlavou,
- snažit se zjistit rozsah poškození,
- v případě stanovit, koho by mohly informace zajímat,
- stanovit důsledky (přímé, nepřímé).

Co dělat prvních pár hodin?

Když už víme, které informace unikly, pokračujeme v analyzování:

- kdo se k informacím mohl dostat (zevnitř, zvenčí) a co by s informacemi mohl provést,
- prohlédneme záznamy (kdo a kdy měl k informacím přístup),
- jakou formou s informacemi zacházel (tisk, kopírování, posílání),
- uchovaní všech důkazů (pro soudní spory),
- zabezpečit místo úniku, zamknout místnosti s počítači, dokumenty apod.,
- nevypouštět informace o úniku ven,
- neinformovat o vyšetřování zaměstnance (nevíme zda to nebyli právě oni),
- čím míň osob o tom ví tím lépe (nebrzdí vyšetřování).

Co dělat prvních 24 hodin

- pokud se jedná o soukromou firmu, rozhodnout se, zda událost ohlásit,
- uvědomit si zda toho nemůže využít konkurence,
- v případě ohrožení osobních údajů kontaktovat Úřad pro ochranu osobních údajů,

- v případě úniku zvenčí, je lepší spolupracovat s policií,
- zjistit, zda nedošlo k selhání bezpečnostní opatření.

Co dělat další dny?

- je vhodné provést kontrolu všech bezpečnostních opatření,
- pokud známe viníka, vyslechnout ho,
- zjistit, co ho k tomu vedlo,
- pokud je viníkem zaměstnanec, není pravidlem, že se musí propustit,
- zjistit zda neselhalo vedení.

Je tedy nutno k problému přistupovat systematicky a měla by to vždy dělat osoba, která má patřičnou kvalifikaci nikoli amatér. Ve větších společnostech tuto funkci zastává specialista na bezpečnost tzv. bezpečnostní manažer. Pokud se jedná o rozsáhlý komplex (firmu, společnost), bývá specialistů zpravidla více.

7.1.1 Bezpečnostní manažer

Jedná se o specialistu, zaměřeného na ochranu vlastnictví, a to jak hmotného, tak nehmotného včetně osob. Bezpečnostní manažer by měl splňovat:

- schopnost se rychle a správně rozhodnout,
- pracovat systematicky,
- efektivní a flexibilní práce,
- odborník na bezpečnost (kvalifikace),
- musí dovést řešit problémy pod tlakem,
- komplexní přístup,
- klidný, vyrovnaný, všímavý atd..

Velké společnosti zřizují funkci bezpečnostního manažera a požadují po něm ucelenou ochranu společnosti. Má tedy sledovat a vyhodnocovat činnost soukromé bezpečnostní služby, navrhovat opatření proti vnitropodnikové kriminalitě. Případně

vytváří požadavky na výběrová řízení, sleduje jak jsou zaměstnanci spokojeni. Dále zřizuje anonymní oznamovací pulty či linky a zajišťuje vnitřní audity.

Pokud se jedná o menší komplex společnosti, může se nahradit funkce bezpečnostního manažera externími specialisty. Bezpečnostní odborníci provedou návrh opatření, předloží je managementu společnosti a je už jenom na nich, jak ucelenou ochranu potřebují.

7.2 Poučit se z chyb

Abychom se vyvarovali nových chyb, musíme se poučit z těch starých. To lze jen tehdy, když předchozí nesprávné kroky zanalyzujeme. Musíme identifikovat slabá místa. Jakmile nalezneme slabá bezpečnostní opatření, nahradíme je silnějšími. Tam, kde selhal systém, selhal i člověk. Z každé další špatné zkušenosti roste účinnost nových opatření.

Dnešní vynalézavost moderních lupičů je dynamická a je tedy nutné se jí přizpůsobovat. Každé rozhodnutí musí mít zvážena všechna pro a proti. Jen tak můžeme eliminovat příčiny selhání techniky, ale i nás samých.

Pro efektivní zavedení systémového přístupu bezpečnosti informací je zapotřebí:

- pochopit, co je to management rizik a jak se správně realizuje,
- naučit se zacházet s informacemi podle klasifikace jejich míry důvěrnosti,
- hodnotit efektivnost systému na základě sběru informací,
- naučit se využívat záznamů o incidentech k analýzám a dalšímu zlepšování systému.

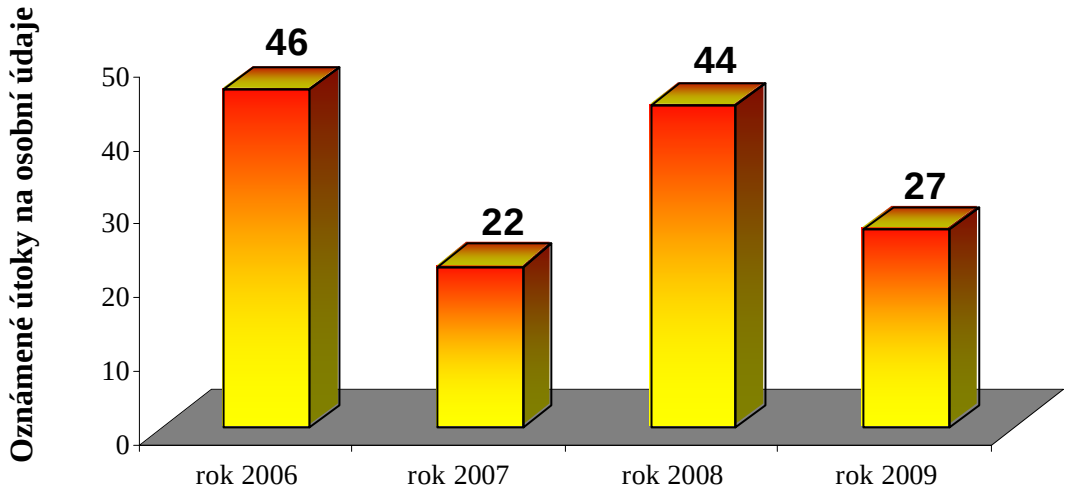
Závěrem lze říci, že nejúčinnějším řešením je prevence. Jak dokonalá prevence je, záleží hlavně na financích s kterými disponujeme.

8 STATISTIKY

Podle studie McAfee dochází při odchodu zaměstnanců z firem ve většině podniků k úniku důvěrných informací. Každý únik firemních dat stojí dotyčnou společnost průměrně 268 000 dolarů.

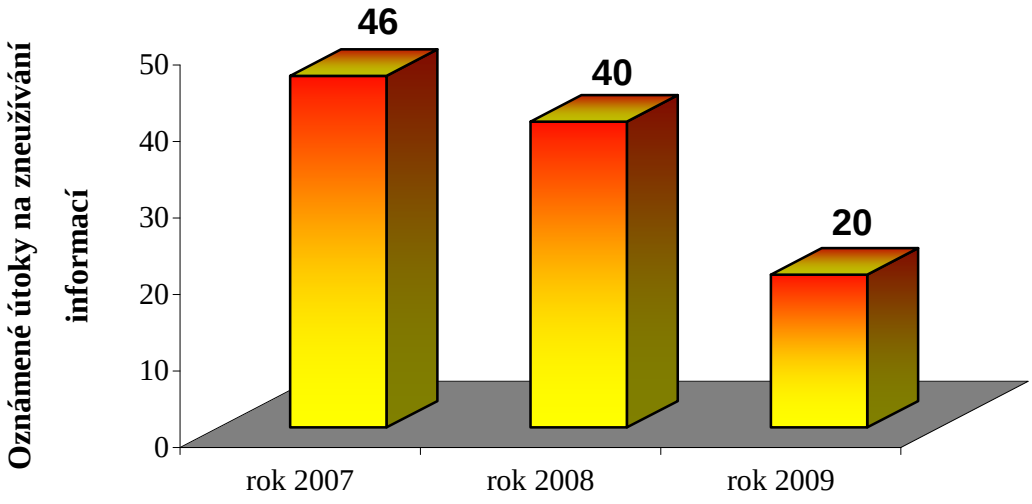
Neoprávněné nakládání s osobními údaji

Vycházím ze statistik které zveřejnilo Ministerstvo vnitra.



Graf 2 *Neoprávněné nakládání s osobními údaji – zdroj MV*

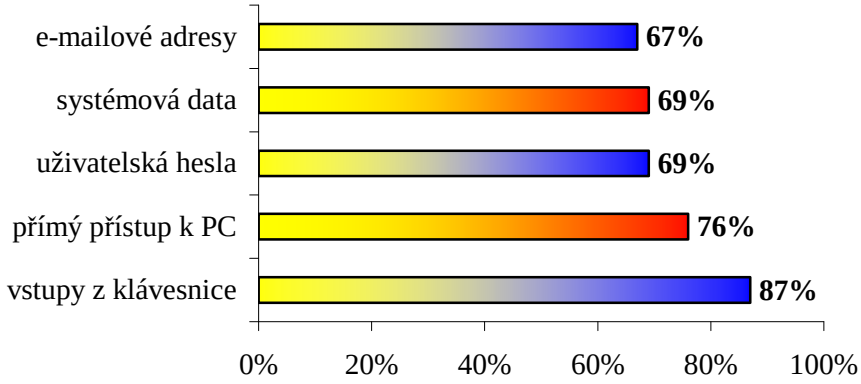
Zneužívání informací v obchodním styku



Graf 3 *Zneužívaní informací v obchodním styku – zdroj MV*

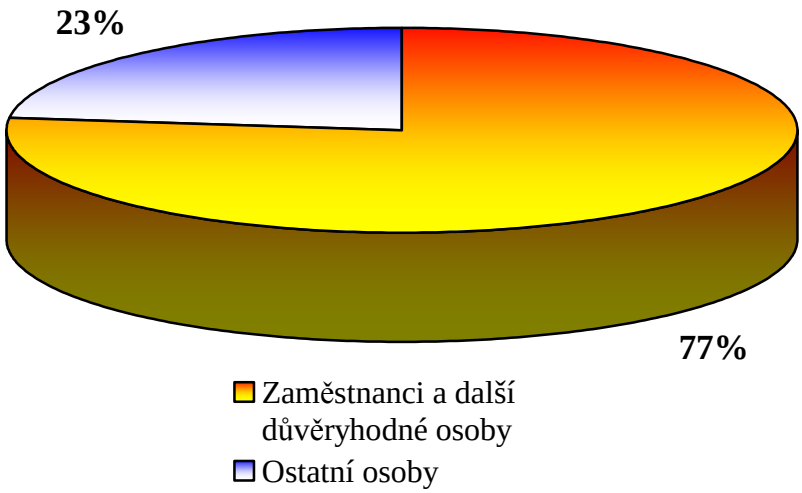
Ztráta důvěrnosti informací může mít zvláště pro komerční organizaci závažné následky. Ve většině případů jde o oslabení konkurenční pozice na trhu, ať již formou ztráty důvěry současných a potenciálních zákazníků nebo vyzrazením technologických postupů či marketingových plánů, které zajistí ostatním soupeřům oslabení konkurenčních výhod.

Hlavní cíle útoku



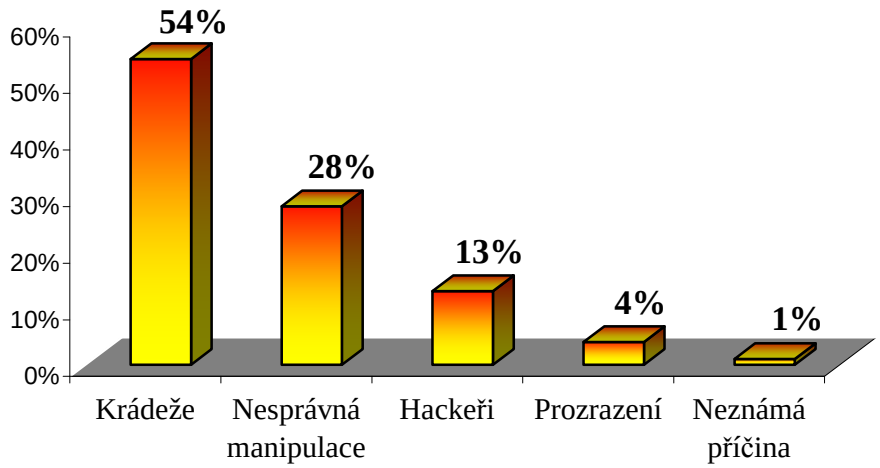
Graf 4 *Hlavní cíle útoku – zdroj Symantec*

Kdo zcizuje informace



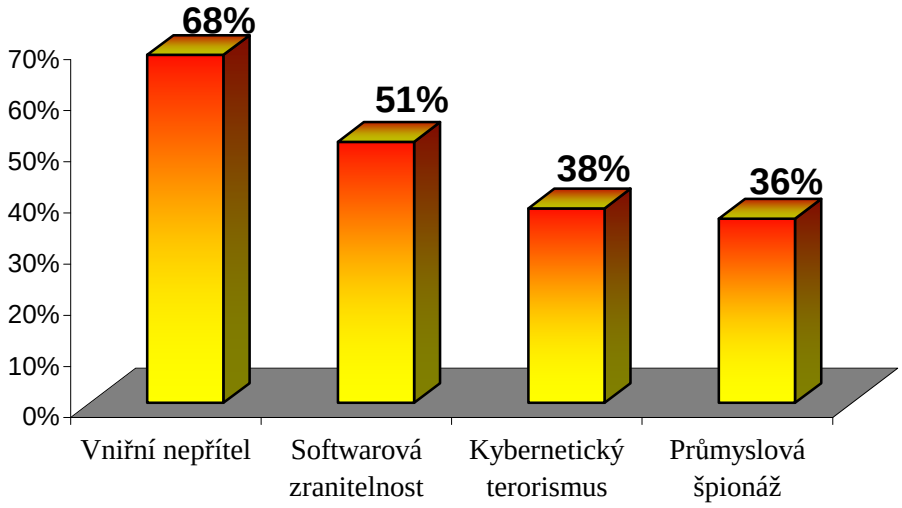
Graf 5 *Kdo zcizuje informace – zdroj McAfee*

Ztráty dat



Graf 6 *Ztráty dat – zdroj Symantec*

Nejčastější způsoby úniku citlivých informací



Graf 7 *Úniky citlivých informací – zdroj S&T*

ZÁVĚR

Cílem práce nebylo ukázat potenciálnímu narušiteli slabá místa, ale upozornit na ně majitele a osoby, které za ochranu informací nesou odpovědnost.

Přínos své práce vidím v získání základních informací o bezpečnosti a ochraně know-how. Dále v analýze rizik a právní legislativě spojené s ochranou dat. Seznámil jsem čtenáře s možnými metodami ochrany know-how za pomocí detektivních služeb, tak s metodami ochrany know-how za pomocí právní legislativy. Z daných metod jsem se snažil vyvodit vyhodnocení. Přiblížil jsem příklady možné ochrany know-how a kde to bylo možné, tak jsem se pokusil vyvodit výhody a nevýhody dané ochrany. Statistikami jsem se snažil přiblížit odkud hrozí útoky na cenné data a důvěrné informace, abychom si udělali představu, kterým směrem ochranu směrovat.

Analýzou metod jsem získal několik závěrů. Ochrana know-how je rozsáhlý problém, který má svá úskalí a je třeba chránit know-how ze široké oblasti spektra. Důležitou a často opomíjenou složkou bezpečnosti a ochrany know-how je role lidského faktoru. Na základě analýz jsem zjistil, že jsou to právě vlastní zaměstnanci, od kterých hrozí největší nebezpečí v odcizení know-how. Abychom jim alespoň částečně zabránili v nekalých úmyslech, je vhodné jim připravit prostředí, v kterém budou spokojeni a myšlenkami podvodů, krádeží atd. se nebudou zabývat. Každé prostředí má svá specifika a zvolit správnou metodu ochrany není jednoduché. Za nutné považuji aktualizovat metody na ochranu dat a přizpůsobovat se rozvoji nových technologií.

Práce mi přinesla nahlédnutí do oblasti, která byla pro mě pouhou neznámou. Setkal jsem se s novým druhem informací ve světě informační, ale i právní bezpečnosti.

Ochrana know-how je běh na dlouho trať a jedinou možností, jak se s ní co nejlépe vypořádat, je neztrácet ostražitost, pravidelně sledovat veškerý vývoj v oblasti informační bezpečnosti a neustále se mu přizpůsobovat. Je to náročný úkol, ale jen tak můžeme zajistit bezpečí pro naše důvěrné data a tím často i soukromí nás samých.

ZÁVĚR V ANGLIČTINĚ

The aim of this work was not was not only to show a protential intruder some weak points but also to draw owners and people's attention to them because they are responsible for information protection.

The contribution of my work can be seen in gaining of basic information about security and know-how protection and further in risk analysis and legal legislation connected with know-how protection. I have made readers familiar with both posible methods of know-how protection with the assistance of detective services and with methods of know-how protection with the assistance of legal legislation. I have tried to draw my evaluation from given methods. I have outlined examples of possible know-how protection and where it was possible I have tried to deduce advantages and disadvantages of given protection. I have used statistics to describe where is possible to attacks valuable data and confidential information to get the picture which ways to use for protection.

I have obtained several conclusions by analysis of methods. The know-how protection is an extensive problem which has its diffculties and it is necessary to protect know-how from a wide area of spectrum. The important and often ignored component of security and know-how protection is the role of human factor. On the basis of analysis I have found out that they are just own employees who pose a threat to stealing of know-how. To prevent them at least partly from unfair intentions it is fit to prepare for them such settings where they will be satisfied and they will not ans the idea of deceptions, thefts etc. Each setting has its specific and to choose the right method of protection is not easy. I think it is necessary to update methods for know-how protection and to accommodate to the development of new technologies.

The thesis enabled me to look into the area which was for mere unknown. I have met new kind of information in the information world and also in the legal security.

Know-how protection is a long-distance run and the only possibility how to deal with it as well as possible is do not to lose alertness and to observe regularly all progress in the area of information security and to adjust to it constantly. It is a very exacting task but it is the only way how to ensure safety for our confidential data and for our privacy.

SEZNAM POUŽITÉ LITERATURY

[1] BRABEC, F. a kol.: *Bezpečnost pro firmu, úřad, občana*. Public History, Praha 2001.

[2] BRABEC, F. a kol.: *Soukromé detektivní služby*. Eurounion, Praha 1995.

[3] BRABEC, F. a kol.: *Ochrana bezpečnosti podniku*. Eurounion, Praha 1996.

[4] BRABEC, F. : *Technologie detektivní činnosti*. UTB, Zlín 2009. 160 s. ISBN 978-80-7318-780-4.

[5] DOSEDĚL, T. *21 základních pravidel počítačové bezpečnosti*. 1. vyd. Computer Press, a. s., 2005. 56 s. ISBN 8025105741.

[6] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Computer Press, a. s., 2004. 200 s. ISBN 8025101061.

[7] FOOT, M., HOOK, C.: *Personalistika*. Computer Press, Praha 2002.

[8] JAŠEK, R. *Informační a datová bezpečnost*. 1. vyd. Academia centrum UTB, 2006. 140s. ISBN 8073184567.

[9] KAMENÍK, J., BRABEC, F. a kol.: *Komerční bezpečnost (Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur).* ASPI, Praha 2005.

[10] MACEK, P. a kol.*: Bezpečnostní služby*. Policie History, Praha 2001.

[11] MACEK, P., NOVÁK, F.*: Soukromé bezpečnostní služby*. Policejní akademie, Praha 1997.

[12] MACEK, P., NOVÁK, F.*: Privátní bezpečnostní služby*. Police History 2005.

[13] *Www.sagit.cz* [online].Sagit, a.s., 2010 [cit. 2010-04-13]. Nehmotné statky a práva k nehmotným statkům. Dostupné z WWW: http://www.sagit.cz>> Právní poradce>> Občanské právo.

[14] MALÝ, Josef. *Obchod nehmotnými statky : patenty, vynálezy, know-how, ochranné známky*. 1. vyd. Praha : C.H.Beck, 2002. 257 s. C.H. Beck pro praxi.

[15] HORSÁK, Jan. *Analýza metod a technologií používaných v procesu ochrana přenosu dat*. Zlín, 2008. 65 s. Bakalářská práce. UTB Zlín.

[16] ŠTENGLOVÁ, Ivana. *Obchodní tajemství : praktická příručka*. Praha : Linde Praha, a.s., 2005. Vztah mezi know-how a obchodním tajemstvím, s. 159. ISBN 80-7201-559-1.

[17] JANSA, Lukáš. *PravoIT* [online]. 27.02.2009 [cit. 2010-04-14]. Způsob kontroly zaměstnanců dle nového zákoníku práce. Dostupné z WWW: <http://www.pravoit.cz/article/zpusoby-kontroly-zamestnancu-dle-noveho-zakoniku-prace>.

[18] QURESHI, Sirshar Lze zabránit podvodnému jednání vlastních zaměstnanců?. In . [s.l.] : [s.n.], 19.1.2007 [cit. 2010-04-20]. Dostupné z WWW: <http://www.pwc.com/cz/cs/clanky-2007/lze-zabranit-podvodnemu-jednani-vlastnich-zamestnancu.jhtml>.

[19] *Www.falco-hk.cz* [online]. 2008 [cit. 2010-04-09]. FALCO-HK. Dostupné z WWW: <http://www.falco-hk.cz/cz_bezpecna_firma.php>.

[20] *Platinum-ss* [online]. 2009 [cit. 2010-05-01]. Kontrola personálu (skreening). Dostupné z WWW: <http://www.platinum-ss.cz>.

[21] JANSA, Lukáš. *PravoIT* [online]. 30.03.2008 [cit. 2010-04-14]. Zákaz konkurence I. - zaměstnanci. Dostupné z WWW: <http://www.pravoit.cz/article/zakaz-konkurence-i-zamestnanci>.

[22] LÁTAL, Ivo; ŠTANTEJSKÝ, Michal. *Bezpečnostní zásady ochrany podniku : Prevence a řešení krizových situací*. Vyd.1. Praha : PROSPEKTRUM, 2001. Režimová ochrana, s. 120. ISBN 80-7175-091-3.

[23] RADECKÝ, Alexandr ; DONOGHUE, Andrew; ERBEN, Lukáš. *Http://businessworld.cz* [online]. 23.10.2009 [cit. 2010-05-03]. Jak zvládnout únik informací. Dostupné z WWW: <http://businessworld.cz/it-strategie/jak-zvladnout-unik-informaci-5197>.

[24] SLÁMA, Michal . *Michal_slama.sweb* [online]. 2010 [cit. 2010-05-12]. Bezpečnostní politika. Dostupné z WWW: <http://michal_slama.sweb.cz/security>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

MV	Ministerstvo vnitra
CRAMM	CCTA Risk Analysis and Management Method
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
NBÚ	Národní bezpečnostní úřad
ICQ	I Seek You
FV	Fyziodetekční vyšetření
1x	Jedenkrát

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM GRAFŮ