Ochrana objektů, střežených podniků PKB proti průmyslové špionáži

Protection of buildings, businesses PKB guarded against industrial espionage

Martin Bezruč

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

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

Jméno a příjmení:	**Martin BEZRUČ**
Osobní číslo:	**A10192**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Ochrana objektů střežených podniky průmyslu komerční bezpečnosti proti průmyslové špionáži**

Zásady pro vypracování:

1. **Popište pojem průmyslová špionáž a její příznaky ve vybraných objektech střežených podniky průmyslu komerční bezpečnosti.**
2. **Popište cíle průmyslové špionáže.**
3. **Uveďte formy a metody průmyslové špionáže.**
4. **Popište operativní prostředky k ochraně proti průmyslové špionáži.**
5. **Objasněte budoucnost vývoje této problematiky.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti I. Vyd. 3. Zlín: Univerzita Tomáše Bati ve Zlíně, 2010, 81 s. ISBN 978-80-7318-889-4.**
2. **LAUCKÝ, Vladimír. Technologie komerční bezpečnosti II. Vyd. 2. Zlín: Univerzita Tomáše Bati ve Zlíně, 2007, 123 s. ISBN 978-80-7318-631-9.**
3. **LAUCKÝ, Vladimír. Přednášky z TKB. Zlín, 2012.**
4. **BERGIER, Jacques. Průmyslová špionáž. Praha: Orbis, 1974. Stopy, fakta, svědectví. ISBN 11-074-74.**
5. **CHURAŇ, Milan. Encyklopedie špionáže. Praha: Libri, 2000. ISBN 80-7277-020-9.**

Vedoucí bakalářské práce: **JUDr. Vladimír Laucký**
Ústav bezpečnostního inženýrství

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce pojednává o problematice Průmyslové špionáže. V teoretické části je uváděna jak metodika a formy Průmyslové špionáže, tak i ochrana před ní. Je zde také rozebrána historie a budoucnost této problematiky. V praktické části jsou zveřejněny případy Průmyslové špionáže týkající se konkurenčních bojů gigantických firem a konkurence mezi státy.

Klíčová slova: Průmyslová špionáž, Licenční a patentová politika, Cíle Průmyslové špionáže, Operativní prostředky, Obranné metody, Budoucnost problematiky, Známé útoky

ABSTRACT

This thesis deals about the issue of industrial espionage. The theoretical part includes the methodology and form of industrial espionage, as well as protection against it. It also contains the history and future of this issue. In the practical part of the published cases of industrial espionage relating to competitive fighting giant firms and competition between states.

Keywords: Industrial espionage, license and patent policy objectives of industrial espionage, operational resources, defense methods, future issues, known attack

Chtěl bych poděkovat svému vedoucímu práce, panu JUDr. Vladimíru Lauckému za jeho odbornou pomoc při tvorbě a poskytnutí odborných materiálů.

Prohlašuji, že

- beru na vědomí, že odevzdáním 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 bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk 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 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 – 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 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 bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem 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 bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Má Bakalářská práce pojednává o problematice Průmyslové špionáže. Důvodem zvolení tohoto tématu bylo především zajímavost tématu. Další věcí, která mne vedla ke zpracování, je také aktuálnost tématu a problematika oblasti této činnosti v dnešní době. Jelikož Průmyslová špionáž není otázkou jen minulosti a přítomnosti, ale především budoucnosti, myslím, že je dané téma zvoleno správně. Průmyslová špionáž vychází ze špionáže obecné, jež se provozuje již po několik staletí. Snažil jsem se zpracovat problematiku, jak z historického hlediska, tak z hlediska budoucího. Dané téma se týká nás všech a její užívání v budoucnosti je zaručena. Mými cíly bylo zpracování seznámení s problematikou a návodu pro bezpečnostní manažery. Také jsem se pokusil o seznámení s cíly Průmyslové špionáže, základními vlastnosti a operativními způsoby. Jelikož se jedná především o ofenzivní způsob získávání informací a často založené na nelegálním původu, je logické, že jsem se také snažil zmínit způsoby, jak jí zabránit. Proto jsem uvedl několik metod a zásad, které by měly být výchozí pro zajištění obrany firmy každým bezpečnostním manažerem či jinými pracovníky zajišťující bezpečnost informací, výrobního tajemství nebo hodnotného Know – How. Snažil jsem se poukázat na důležitost ochrany proti tomuto způsobu získávání informací. Jak jsem již zmínil, tato činnost nás bude provázet i v budoucnosti. Proto jsem se rozhodl zmínit a rozebrat budoucnost a odvětví, v jakém se bude Průmyslová špionáž ubírat. Zde jsem chtěl především klást důraz na jejím použití v kybernetickém prostředí, což se týká nás všech a s čímž se budeme setkávat stále častěji. Ne každého však může teoretická část přesvědčit o nebezpečí této problematiky a jejího celosvětového rozmachu. Proto jsem se rozhodl zpracovat i praktickou část. Zde jsem chtěl uvést již známé případy Průmyslové špionáže a pokusil jsem se vyhledat a zahrnout do práce ty známe, při kterých došlo k velkým ztrátám finančního charakteru. Bohužel není možnost se dostat k informacím o nejzávažnějších způsobech a činech Průmyslové špionáže. Tím je myšlena především činnost špionážních pracovníků na území cizích státu. Veškeré státy drží tyto témata v tajnosti a proto se k těmto informacím není možné dostat z postu studenta nebo normálního smrtelníka. Osobně si myslím, že se jedná o velmi závažnou činnost a to ne jen co se týče průmyslu. Proto by měl být každý člověk informován a měl by dokázat alespoň trochu předcházet možnostem špionáže. Jelikož jde naše doba stále kupředu a vyvíjí se nové technologie, budou uvedené metody Průmyslové špionáže, které jsem zvolil do své bakalářské práce již

passé. Je nesmysl si myslet, že se nás tato problematika nijak netýká a že se nemůžeme stát cílem.

I. TEORETICKÁ ČÁST

1 PRŮMYSLOVÁ ŠPIONÁŽ

1.1 Historie

Průmyslová špionáž vznikla už velmi pradávno, datuje se až do pravěku,i když pravěcí lidé si toho nebyli vědomi. Vznikaly zde boje mezi kmeny o techniku rozdělání ohně, o způsob boje proti jiným kmenům, jako např. útočit na hlavu nepřítele, až po zdokonalování pazourků, primitivní obrábění kamene atd. Dalšími dobře známými událostmi týkající se špionáže bylo získávání poznatků o hedvábí a jeho výrobě, kdy Číňané byli v této oblasti napřed před ostatními národy. Ty to samozřejmě nenechalo chladné a tak se snažili všelijakými způsoby získat technologii výroby. Tímto způsobem bychom mohli mluvit velice dlouho o výrobcích, po kterých byla dříve ve světě sháňka a které byly objektem zkoumání ze strany špionů. Ať už to byla technologie výroby řeckého ohně, který při hašení přibíral na síle, nebo způsoby výroby porcelánu, či umění výroby damascenské oceli, která ve své době byla nejlepší ocelí vůbec a pro své vlastnosti po ní samozřejmě také toužili všichni. Dodnes není zcela známa její výroba. Existuje mnoho dalších „převratných“ vynálezů, které byly lákadlem pro špióny dřívějších dob. Jedním z mnoha byl střelný prach. Tato směs dřevěného uhlí, síry a ledku byla velice žádaná pro své demoliční účinky. První známá organizace, která byla určena k obraně proti Průmyslové špionáži fungující dodnes a nese jméno Pinkertonova agentura. Pinkerton byl v té době jedním z vůbec nejlepších protišpionážních pracovníků a svou činností se podílel ve válce Sever proti Jihu. Díky svým schopnostem zabránil protivládnímu spiknutí, které by mělo za následek atentát na A. Lincolna a odříznutí Washingtonu od ostatních států Severní unie.

Obr. 1- Původní logo Pinkertonovy agentury

V otázce průmyslové špionáže se ukázali ve „špatném“ světle i vědci a vynálezci, jako byl např. T. A. Edison, který si pomocí špionáže opatřil informace, jak vyrobit Westenghousový generátor, díky němuž mohl vyrobit střídavý proud. Poté svůj vynález prodal státu New York a zapříčinil se tak o vznik prvního elektrického křesla na popravu vězňů. Dalším obdobím, kdy se hojně pěstovala špionáž, bylo období první a druhé Svět. války. Zde se soupeřilo především v přebírání technologií výroby různých zbraní, výbušnin a armádní techniky a dovedností celkově. Mezi přední špionážní tahouny patřila především Amerika a Německo. Byl to boj mezi špionážními silami. Na jedné straně se Německo snažilo zjistit veškerou produkci amerického tekutého chloru. Na druhé straně Američané díky špionáži rozluštili mnoho šifer Německé vlády. Největším úspěchem Americké kontrašpionáže té doby bylo získání obsahu aktovky jednoho vysoce postaveného německého špiona. Obsahem byla řada dokumentů, jak přitížit Americe, např. plán akcí na zrušení letecké společnosti Wrighton, plán na odkoupení muničních továren v Americe, atd. Dalšími bylo vyzrazení způsobu vyvolávání barevného filmu vynalezenou firmou Kodak.

1.2 Průmyslová špionáž

Jedná se o jedno z nejstarších odvětví lidské činnosti vůbec a je to odvětví špionážní činnosti. Pod tímto pojmem rozumíme veškerou činnost, která má za úkol obohatit subjekt vědomostmi subjektu druhého, dochází zde k získávání informací. Různé informace mají různou hodnotu a jak vysokou je určeno více faktory. Mezi takové faktory patří množství lidí disponující touto informací, znalost/neznalost lidí této informace, množství surovin, apod. Informace můžou tedy na své hodnotě jak získávat, tak ztrácet. Uvedeme-li si příklad, informace získaná od určitého subjektu ztrácí svou hodnotu, protože tento subjekt šíří tuto informaci dále mezi lidi. V dnešním světě Internetu je prakticky za pár hodin informace bezcenná. Naopak informace získává na hodnotě, známe-li ji pouze my a poptávka po ní stále stoupá. Tím stoupá i její hodnota (cena).

Jedná se o obor lidské činnosti, jež se používá všude na světě. Největšími zastupiteli, kteří tuto činnost využívají, jsou státní organizace, komerční subjekty či jednotlivé osoby získávající informace pro své vlastní účely. Pomocí Průmyslové špionáže je

možné získat tajné koncepty na výrobu, možnost zisku nové technologie, atd. Přestože Průmyslová špionáž používá mnohdy stejnou technologii jako špionáž běžná (tajné fotografie, odposlouchávací a nahrávací zařízení a jiné), nejedná se o stejně nebezpečnou činnost. V případě Průmyslové špionáže se soudy řídí zákony, které pohlíží na tuto činnost jako na konkurenční boje, což není tak úplně pravda a pro zaměstnance, v případě odhalení, to znamená pouze vyhazov, v horším případě i nějakou pokutu. Tedy nehrozí mu žádné odnětí svobody!

V případě mezinárodní bezpečnosti, vojenské a bezpečnostní technologie např. jaderného a kosmického výzkumu, chemických či biologických zbraní, nanotechnologie, apod. se jedná již o velmi závažnou trestní činnost. Zde hrozí možnost obžalování z velezrady, což může vést k odnětí svobody od 5 let až po doživotí, v některých zemích světa může dojít i k trestu smrti. Jelikož se jedná většinou již o národní bezpečnost, postihy jsou velmi tvrdé a neberou se na lehkou váhu.

Je stále více zřejmé, že boj o tzv. konkurenční předstih má za následek páchání Průmyslové špionáže, ať již z postu státních rozvědných orgánů a nebo z postu průmyslových a obchodních společností státního, polostátního nebo soukromého charakteru.

Průmyslová špionáž je dnes hojně užívána a to velmi často legálně. Touto problematikou se zabývá řada lidí pracujících ve společnostech vystupujících často pod hlavičkou Detektivní či Informační kancelář. Na tyto kanceláře je často vyvíjen tlak jak ze strany soukromníků, tak ze strany státu, který je informován o jejich veškeré činnosti. Veškerá špionáž je dnes velmi dobrým pojidlem mezi vysoce postavenými politiky, vládou a podsvětím.

V dřívější době byla zaměřena čistě na vojenskou sféru a gigantické podniky, dnes jsou velmi často cíly útoků Průmyslové špionáže soukromé objekty a ekonomická sféra celkově. Dnes chce být každý dobře informovaný a snaží se pro to udělat všechno, mnohdy i nelegálního. Proto je velmi obtížné se proti této problematice úspěšně bránit. Jedním ze slabých bodů v boji proti Průmyslové špionáži jsou tzv. kancelářské spoje. Tím myslíme veškerou komunikaci mezi kancelářemi, zde často bývá velký únik informací. Zabráněním tomu se budeme zabývat později. Mějme také na paměti, že správně fungující obrana nelikviduje útoky, pouze jim zabraňuje

v zisku správných informací a naopak využívá je k předávání informací falešných, což vede k „zmatení protivníka“.

1.3 Konkurenční zpravodajství

Počátky konkurenčního zpravodajství pocházejí z práce státní bezpečnosti a vojenských služeb. Nejedná se o špionáž ani nelegální činnost, jak si mnohdy lidé myslí, nýbrž jde o legální činnost vzniklou v 80. letech v USA. Avšak někdy je tato činnost velmi na hraně zákona, někdy ho i překračuje. Touto činností by se měl zabývat každý manažer a ne jen bezpečnostní. Pod tímto pojmem rozumíme činnost shromažďování informací, vytváření analýz a využívání externích informací. Pomocí toho vytváříme plán pro zlepšení fungování našeho podniku. Pokud provádíme konkurenční zpravodajství kvalitně a vyvozujeme z toho správně důsledky, měl by se chod naší společnosti zlepšit a zkvalitnit a také by mělo dojít k lepšímu rozhodování či schopnosti zareagování na konkurenci. Další nespornou výhodou konkurenčního zpravodajství by mělo být umožnění maximálního uspokojení zákazníka. Výhodou by také mělo být to, že jsou manažeři včas informováni o hrozícím nebezpečí nebo jsou upozorňováni na nové příležitosti v jejich pracovním odvětví. Jedná se vlastně o poskytování informací konkurenci ve vhodný čas. Firmy tím zabraňují vytvoření další konkurence. Za tímto účelem jsou najímáni detektivové, jejichž úkolem je shromažďování informací o konkurenci. Musí mít však licenci a živnostenský list na tyto služby.

Konkurenční zpravodajství je označováno zkratkou CI (Competitve Intelligence) a nedochází pouze k zabývání se konkurencí, nýbrž celým konkurenčním prostředím. Typickým systémem, jak pracovat v takové konkurenci, je vznik mateřských a dceřiných společností. Máme jednu, původní, firmu, která si za poplatek vytváří dceřiné společnosti, které pracují samostatně, avšak od mateřské společnosti dostanou základní postupy a metody pro chod společnosti. Tím je docíleno jisté obrany proti konkurenčnímu zpravodajství a naopak konkurenční zpravodajství funguje na vysoké úrovní mezi mateřskou a dceřinou společností. Příkladem může být McDonald’s.

Konkurenční zpravodajství jako takové můžeme rozdělit a to dle toho, jakým směrem se ubírá. Buďto **ofenzivním** nebo **obranným** směrem.

Obranné konkurenční zpravodajství (neboli obranné zpravodajství) se zabývá:

- Zajišťováním personální bezpečnosti, režimové ochrany, technickou bezpečnost objektů, softwarovou bezpečnost
- Zajišťování komplexní informační bezpečnosti
- Zajišťování ochrany technologických procesů, především Know – How, vynálezů, zlepšování návrhů, výzkumu, vývoje
- Zajišťování bezpečnosti v obchodních vztazích
- Aktivní ochranu proti dezinformacím a působení vlivového zpravodajství konkurence
- Aktivní ochranu proti ofenzivnímu zpravodajství konkurence

Ofenzivní zpravodajství konkurence řeší převážně:

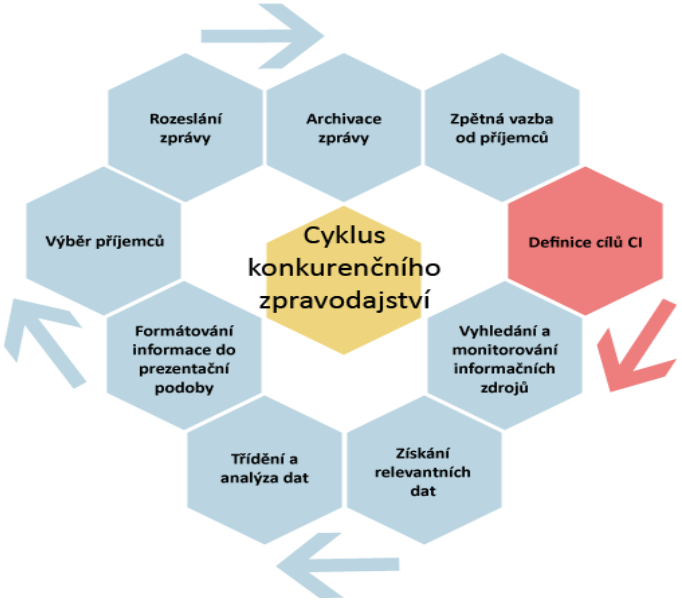
- Zajišťování informací potřebných pro podnikání
- Zajišťování informací marketingového charakteru
- Zjišťování cílených informací o konkurenci
- Zjišťování informací o potřebných technologiích
- Zjišťování informací o Know – How, výzkumu, vývoji, vynálezecké a zlepšovatelské činnosti v příslušných oborech průnikového zájmu

Další zajímavou věcí pro bezpečnostní manažery je, jaké metody využívá ofenzivní zpravodajská konkurence k docílení svých zájmů. Známe-li způsoby útoku, můžeme se poté snáze proti nim bránit. Ne vždy je však naše obrana účinná, protože ofenzivní zpravodajství využívá i pololegálních a nelegálních prostředků.

Patří sem :

1. Publikace a zprávy vydávané konkurencí a legální cestou získané zprávy o výrobních postupech, vynálezech, …
2. Informace otevřeně předávající bývalými zaměstnanci konkurenční firmy.
3. Studie trhů a zprávy od technických poradců
4. Oficiálně vytěžené prostředky informačních technologií
5. Finanční zprávy
6. Analýza výrobků konkurence
7. Zprávy obchodních cestujících a nákupčích

8. Veletrhy, výstavy, prezentace a brožury vydávané konkurencí u této příležitosti
9. Pokusy o získávání technických specialistů zaměstnaných u konkurence, přičemž se takto vyhlédnutým osobám dávají vyplňovat speciální dotazníky
10. Přímé tajné pozorování
11. Fingované nabízení zaměstnání pracovníkům konkurence bez seriozního úmyslu jejich přijetí s cílem vyzvědět závažné komerční informace či technické informace
12. Fingované jednání s konkurenční firmou vedená pod záminkou zájmu o získání licence na některý z jejich patentů
13. Používání profesionálních špionů k získávání informací
14. Přetahování zaměstnanců konkurenčního podniku s cílem získat od nich informace
15. přímé narušení vlastnických práv konkurence
16. Podplácení obchodních zástupců a jiných zaměstnanců konkurence
17. Technické průniky do informačních technologií konkurence
18. Vpašování agentů mezi zaměstnance nebo přímo technické specialisty do konkurenčních podniků
19. Ilegální odposlech u konkurence
20. Krádež plánů, vzorků a jiné dokumentace i konkurence
21. Vydírání a různé jiné formy nátlaku



Obr. 2 – Grafické zobrazení cyklu CI

Poslední částí konkurenčního zpravodajství, kterou zmíním, je tzv. Vlivové konkurenční zpravodajství často nazýváno také jako lobbing. Jedná se o čistě legální činnost, pokud nedochází k trestné činnosti v zájmu lobbingu. Hlavou celého lobbingu je zájmová skupina, často movitá, která využívá svého vlivu, financí a zaměstnanců k ovlivnění objektu, aby rozhodoval v jejich prospěch. Osobou, která je terčem této zájmové skupiny, může být politik, právník, finanční poradce, ministři, poslanci, atd. Jejich hlavní účel tohoto ovlivňování je zcela skryt nebo naopak velmi jasný. Pokud se jim podaří ovlivnit určitou osobu či skupinu, dochází k úspěšnému lobbingu a dosažení jejich cílů. Příkladem velkých lobbingů jsou např. komerční přestávky v hokeji, reklamy při Super bowlu, atd. Vlivové zpravodajství využívá různé metody k dosažení svých cílů a jak jsem již naznačil, ne vždy se musí jednat o legální činnost. Tím bychom museli přestávat nazývat lobbing lobbingem a museli ho začít nazývat korupcí. Správný lobbista by tuto hranici neměl nikdy překročit.

1.4 Know – How

Přeložíme-li toto slovní spojení do češtiny (vědět jak), dostáváme přesně to, co pro nás toto slovní spojení znamená. Podle obchodního zákoníku můžeme schopnost Know – How považovat za nehmotný statek, s kterým můžeme obchodovat, jak chceme. Ve skutečnosti se jedná o schopnosti výrobně - technické, obchodní či jiné poznatky a zkušenosti fyzické osoby či firmy. V podstatě můžeme říci, že Know – How je schopnost něco umět, tvořit, ale taky zde spadají netvořivé práce jako jsou výsledky výzkumných, vývojových, průzkumných, projekčních, apod. prací. Za Know- How můžeme také považovat všechny informace, které jsme získaly za účelem efektivnějšího vykonávání určité činnosti. S tímto druhem Know - How se setkáváme právě ve škole. Všechny tyto Know - How nejsou nijak chráněny právními předpisy a proto bývají často lehce šiřitelné. Pokud však naše Know-How je něčím výjimečné, dochází zde k tzv. Licenční a patentové politice, což samozřejmě vzbuzuje pozornost Průmyslové špionáže.

1.5 Licenční a patentová politika

Politika zabývající se patenty, patentovými smlouvami a licencemi, licenčními smlouvami. Patentová politika umožňuje udělovat patenty vydávané Patentním úřadem, čímž dochází ke vzniku ochranné známky pro náš vynález. Naším vynálezem může být software, dílo, proces, postup, výrobek, chem. látka, ve své podstatě téměř cokoliv, co jsme vynalezli, stvořili a co je něčím specifické a je použitelné v průmyslu. Jedná se o naše Know – How a udělení patentu slouží k ochraně proti odcizení. Patent je veřejná listina, která poskytuje právní ochranu pro náš vynález po dobu až 20 let. Musí být však placeny poplatky, čímž zajistíme existenci patentu. Je důležité, kterým orgánem je vydán. Tím se mění jeho působnost. Působnost může být světová, Evropská nebo jen uzemní (ČR). Získáním patentu dostaneme jak ochrannou známku pro náš vynález, tak i zajištění příjmu odpovídajícím nákladům, které jsme museli vynaložit. Průmyslová špionáž se velmi zajímá o tyto vynálezy, a pokud nebudeme své vynálezy dostatečně chránit, můžeme si být jisti, že dojde k odcizení a patentování konkurencí. Příkladem může být T. A. Edison, který odcizil postupy na výrobu zdroje pro střídavý proud a jeho následné přivlastnění pomocí patentu. Patent je tedy jedním z vůbec prvních základních ochran proti Průmyslové špionáži. Hlavou patentové politiky je Evropský patentový úřad (EPO) v Mnichově, co se Evropských patentů týče. Co se týče světových patentů, je hlavním a vůbec nejvyšším představitelem patentové politiky orgán **Úřad pro patenty a ochranné známky ve Spojených státech** (USPTO).

Co se licenční politiky týče, funguje po celém světě a hojně ji využívají veškeré firmy. Poskytování licencí je jedním ze způsobů k získání finanční hodnoty nebo jiných výhod z vynálezecké činnosti. Poskytnutím licence dáváme právo využívat náš patentovaný výrobek a tím docílit zkvalitňování tohoto vynálezu. Je možnost i přepisu patentu na jinou fyzickou, právní osobu nebo firmu. K realizaci udělení licence slouží licenční smlouva. Tou opravňuje majitel patentu možnost využití vynálezu dle uvedených zásad a nabyvatele zavazuje k řádnému placení poplatků či majetkovému vyrovnání. Umožňujeme tak možnost vytváření, prodávaní výrobků. Nedochází tedy k prodeji přímému, nýbrž pouze k jakémusi pronájmu. Často tak ale svůj vynález znehodnotíme a proto poté dochází k prodeji vlastnických práv. Český

statistický úřad dohlíží na plnění dohodnutých podmínek dle licenční smlouvy a sleduje veškeré dění na českém trhu s patenty a licencemi.

1.6 Příznaky Průmyslové špionáže ve vybraných podnicích

Příznaky Průmyslové špionáže jsou pro podniky většinou velmi podobné. Pokud dochází k jednomu z nich, můžeme si být jisti, že v našem podniku již došlo k Průmyslové špionáži nebo neustále dochází. Pak je správným řešením kontrola obrany našeho podniku a přehodnocení zabezpečení našich informací, popř. kontrola zaměstnanců a snaha o vystopování špióna. Příznaky Průmyslové špionáže jsou :

- Pokles zisků (nemusí být průkazné)
- Konkurence přichází na trh dříve nebo ve stejnou dobu s výrobkem stejného konceptu
- Zahraniční publikace zpráv o utajovaném výzkumu
- Zjištění vydání patentu na výrobek našeho konceptu
- Vydání výrobku konkurencí, jež má charakteristické rysy našeho výzkumu

2 CÍLE PRŮMYSLOVÉ ŠPIONÁŽE

Cíly průmyslové špionáže jsou především informace! Informace, které jsou nějakým způsobem prospěšné pro objekt, který Průmyslovou špionáž provozuje. Tyto informace pak hodlá zpeněžit či jinak využít ve svůj prospěch. Bavíme - li se o využití informací ve svůj prospěch, máme tím na mysli možnost předvídání budoucnosti a tím větší připravenosti nebo vytvoření vlastního výrobku na stejném základu. Cíle můžeme také nazývat kritickými místy jednotlivých podniků. V každém odvětví průmyslu jsou jiné zájmové informace a jelikož existuje spousta těchto odvětví, uvedu pouze některé. Níže zmíněné místa podniku, které se můžou stát cílem Průmyslové špionáže, jsou také zároveň prvky kritické infrastruktury státních podniků. Tyto prvky jsou stejné pro veškeré firmy pracující v těchto odvětvích, tak i pro státní podniky. Bavíme – li se o státních podnicích, může dojít při jejich napadení a zneužití (zničení) k vážné trhlině v bezpečnosti státu nebo by se mohlo jednat o tvrdý dopad na ekonomickou sféru či veřejnou správu. Dalším důsledkem může být také ohrožení základních životních potřeb obyvatelstva. V komerčních podnicích dochází „pouze“ k finanční ztrátě.

2.1 Energetika

2.1.1 Elektřina

- Softwarové a hardwarové vybavení pro řízení provozu
- Chlazení, jeho technologie a použitý materiál
- Ochrana objektu a jeho slabá místa
- Přenosové cesty (vedení) a elektrické stanice
- Technologie výroby elektřiny a její nové možnosti (vodní, větrné, jaderné, …)

2.1.2 Ropa

- Množství zpracovávané ropy
- Zdroje dodávající ropu či místa zisku ropy
- Obsah a velikost zásobníků pro ropu a celková kapacita uložené ropy
- Způsoby zpracování ropy

2.1.3 Zemní plyn

- Schopnosti přepravní soustavy
- Zdroje zemního plynu a jeho lokalita
- Schopnosti skladování

2.2 Vodní hospodářství

- Základní zásobní zdroj
- Všeobecné vodní díla
- Zpracování vody

2.3 Potravinářství a zemědělství

2.3.1 Rostlinná výroba

- Jednotlivé farmy
- Plocha a chod podniku
- Plantážní produkty a jejich kvalita
- Hnojiva

2.3.2 Živočišná výroba

- Počet chovaných kusů
- Kvalita chovu
- Krmivo

2.3.3 Potravinářská výroba

- Kvalita produktů
- Výrobní tajemství
- Způsob zpracování jednotlivých surovin

2.4 Doprava

2.4.1 Silniční, Železniční doprava

- Vytíženost

- Kvalita komunikací
- Využívání obyvatelstvem
- Průchodnost

2.4.2 Letecká doprava

- Využití cestujícími
- Používání terminálů
- Kontrola zavazadel
- Řízení letového provozu

2.5 Komunikační a informační systémy

2.5.1 Technologické prvky pevné sítě elektronických komunikací

- Centrum řízení a podpory sítě
- Řídící ústředny
- Mezinárodní ústředna
- Transitní ústředna
- Datové centra
- Telekomunikační vedení

2.5.2 Technologické prvky sítí pro rozhlasové a televizní vysílání

- Vysílače
- Řídící pracoviště pro provoz
- Datová centra
- Síť pro tyto vysílání

2.5.3 Technologické prvky pro satelitní komunikaci

- Hlavní satelitní vysílací a přijímací stanice
- Pozemní propojovací síť
- Pozemní řídící a komunikační středisko

2.5.4 Technologické prvky pro poštovní služby

- Centrální a výpočetní středisko
- Úložiště dat
- Sběrný přepravní uzel
- Poštovní dopravní infrastruktura

2.5.5 Technologické prvky informačních systémů

- Řídící centrum
- Datová centra
- Síť elektronických komunikací
- Provoz registru domény „CZ“ a zabezpečení provozu

2.6 Nouzové systémy

2.6.1 IZS

- Jednotlivé operační střediska složek
- Centrální a oblastní dispečinky jednotlivých složek

2.6.2 Radiační monitorování

- Způsoby ochrany
- Jednotlivé sítě a složky

2.6.3 Hlásná a varovná služba

- Meteorologické sítě
- Hydrologické sítě
- Geofyzikální výzkum

2.7 Pokročilá technika

- Výzkum
- Vývoj nových technologií
- Biotechnologie

- Využití ve zdravotnictví
- Využití chemických složek
- Jaderná fyzika
- Laserová technologie

2.8 Automobilový průmysl

- Výzkum
- Vývoj technologií

2.9 Zbrojní průmysl

- Vybavení státních složek
- Výzkum
- Vývoj

2.10 Kosmické centra

- Výzkum
- Vytvořené programy
- Vývoj

2.11 Finanční trh a měna

- Zdroje
- Veřejné finance
- Aplikační vybavení
- Databáze
- Státní zakázky

3 FORMY A METODY PRŮMYSLOVÉ ŠPIONÁŽE

Průmyslovou špionáž můžeme rozdělit na dvě odvětví a to na formy a nebo metody. Formami rozumíme způsoby provádění a metodami rozumíme samotné provedení. Formy špionáže se dají rozdělit dle způsobu získávání informací a mají své specifické zkratky. Jsou to následující :

HUMIT – lidské zdroje

SIGINT – radiový odposlech

IMIMT – letecký a družicový průzkum

MASINT – sledování technických příznaků

OSINT – otevřené zdroje (média)

ACINT – zvukoměrné zpravodajství

GEOINT – geologický průzkum

PHOTINT – analýza fotografií

RADINT – sledování radarového provozu

ELINT – elektronické zpravodajství

COMINT – dešifrování

FISINT – vyhledávání a ničení sítí SIGINT

FININT – finanční zpravodajství

Uvedené formy špionáže platí jak pro všeobecnou, tak i Průmyslovou špionáž. Chceme – li metody pro Průmyslovou špionáž, dělíme je v podstatě na dvě metody :

- Kopírování dokumentů a plánů
- Odposlech

3.1 Kopírování dokumentů a plánů

Tato metoda je značně jednoduchá, přesto velice účinná. Jedná se o jednorázovou metodu pro Průmyslovou špionáž, kdy má pachatel možnost zkopírovat plány či dokumenty, které obsahují citlivé informace. To je mu za jistých okolností dovoleno i z naší strany, kdy má možnost být s dokumenty o samotě. Tomu se dá vyhnout nebo alespoň minimalizovat možnost, že by taková situace mohla nastat. V horším případě se jedná o špióna uvnitř naší firmy či společnosti a v tomto případě je již daleko těžší zabránit této metodě. Kopírování se může provádět pomocí kopírovacích mechanismů, jako jsou kopírky či skenery, ale také fotografy s možností tisku fotografie ihned. Existují také obtiskové listiny, které se přiloží k dokumentu, speciálním světlem nasvítí a poté z něj lze vyvolat původní dokument. Dalším způsobem, jak lze tyto plány získat, je vyfocení fotoaparátem, ať už mobilním telefonem, tak miniaturními fotoaparáty. Ty jsou miniaturní a bývají skryty v příručních zavazadlech, v oděvech (knoflík, zip, …) či propisovacích perech, zapalovačích, atd. Tato metodika může být používána při návštěvě cizích organizací a různých exkurzích a prohlídkách. Je však důležité si uvědomit, že pokud chráníme velký prostor, je pravděpodobné, že se některé části budou nacházet i v otevřeném prostranství. Je proto potřeba zabezpečit objekt proti fotografování z dalekých míst, vyvýšených kopců. Možností je i fotografování ze vzdušných prostor. Proto je důležité chránit naše Know – How uvnitř objektu.

Obr. 3 – Kamera umístěná v propisovací tužce

3.2 Odposlech

Odposlech jako takový, se dá specifikovat jako získávání informací či odposlouchávání naší řeči či dat a to vše bez našeho vědomí. Můžeme jej dělit buďto na legální a nebo nelegální. V případě legálního odposlechu je vše prováděno ze strany státních složek a ke všemu je vydán příkaz a povolení schválené státním zástupcem a soudem. V případě nelegálního odposlechu se bavíme především o trestní činnost, která je prováděna bez našeho vědomí. Máme - li na mysli odposlech spadající pro Průmyslovou špionáž, existuje několik způsobů :

- Elektronický odposlech
- Telefonní odposlech
- Rádiový odposlech
- Počítačový odposlech

Jednotlivé odposlechy si rozebereme a také si udáme příklady a možnosti. Nutno dodat, že odposlouchávací technika je u nás velmi populární a především legální. Základní odposlouchávací zařízení se prodávají již jako hračky pro děti, ty ostatní se prodávají pod záštitou „hračky pro dospělé“. Odposlech samotný je zakázán, avšak prodej techniky k tomu určené již nikoliv.

3.2.1 Elektronický odposlech

Elektronicky odposlech vznikl pro používání elektronického přenosu. Velké množství firem stále neupustilo od používání rádiového vysílání, což se týče faxů. Faxy se stávají terčem pro jejich čtyř drátové vedení. Navíc jsou připojeny k telefonu a ty jsou umístěny všude tam, kde se vedou rozhovory a především ty důležité. Elektronický odposlech se pak také týká dálnopisů pro transakce a nebo také monitorovacích přístrojů, systémů pro ostrahu budov pro řízení. Tento odposlech je také typický pro mobilní telefony! Dnešní moderní technologie umožňují zachycování dat pomocí mikrovlnných a radiových vln. Zde dochází k velikému nebezpečí, protože právě tento typ odposlechu je velmi častý. Je to právě díky častým transakcím a datům posílaným tímto způsobem. Mezi způsoby elektronického odposlechu patří také odposlechy pomocí vedené kabeláže. Stačí se pouze dostat k tomuto vedení a nedestruktivně jej narušit. Existují možnosti odposlouchávat již všechny provedení kabeláže, včetně optického vedení.

3.2.2 Telefonní odposlech

Tento druh odposlechu je již velmi dlouho známý. Již od roku 1994 lze odposlouchávat i mobilní telefony. Ty byly velmi často označovány za bezpečné. To však tvrdili pouze operátoři. Sami výrobci přišli s metodou, jak zajistit odposlech. Telefonní odposlech je však především po drátových telefonech neboli taky pevných. To vedlo k používání drátových odposlechů. Ty musely být na telefon připevněny a sloužily tak k odposlechu hovoru. K aktivaci došlo při zvednutí sluchátka. Již jsou však minulostí. Dnešní moderní přístroje jsou již vybaveny základním obranným prostředkem proti odposlechu. Ale jedná se o opravdu základní a jednoduchý způsob, proto není problém jej překonat, máme-li základní znalosti systému.

Dalším krokem k odposlouchávání telefonů byly a stále ještě jsou nekonečné vysílače. Pod tímto pojmem si můžeme představit malou krabičku, která je připojena na telefon a při aktivaci tohoto zařízení pak můžeme slyšet veškeré zvuky v místnosti. Umožňuje také aktivaci přijímače při využití telefonu. Dnešní nekonečné vysílače jsou většinou připojeny k telefonické ústředně.

Jedním z mnoha jednoduchých způsobů odposlechu je provádění bezdrátového odposlechu. Pokud je hovor veden na nízké frekvenci, lze až do 200 metrů od místa hovoru provádět odposlech pomocí jednoduchého přijímače, který je naladěn na stejný kmitočet jako hovor. Ten je pak lehce směrovaný k odposlouchávajícímu zařízení. Tím je možné monitorovat veškeré hovory.

Obr. 4 – Odposlouchávací zařízení pro telefonní zařízení

3.2.3 Radiový odposlech

Zde se bavíme především o odposlouchávání pomocí bezdrátových štěnic, které vysílají radiové vlny k provozovateli špionáže. Štěnice mohou být jakýchkoliv velikostí a lze je velmi snadno ukrýt před zraky. I při důkladném prohledání místnosti ji nemusíme objevit. Většina těchto zařízení pracuje v pásmu 30 MHz – 25 GHz. Všeobecně platí, že čím nižší kmitočet, tím je odposlouchávací zařízení mohutnější, avšak se tím rozšiřuje dosah. Tato zařízení pracují se složitějšími typy modulací, jako jsou např. pulsní kódové, digitální, subnosné a modulace v rozprostřeném pásmu. Tím je zajištěna větší bezpečnost proti odhalení. Předchůdci těchto modulací byly modulační typy AM a FM. Ty se však v dnešní době téměř neobjevují, protože se jedná o zastaralou techniku. Nutno mít na paměti, že štěnice slouží většinou jako sekundární zdroj, tzv. odposlech je prováděn již jiným způsobem a štěnice je zde umístěna jen proto, aby byla zajištěna větší pravděpodobnost úspěchu.

Obr. 5 - Štěnice

Mezi další odposlechy pracující na bezdrátových spojích, jsou Laserové odposlechy. Ty umožňují odposlech na vzdálenost až několika kilometrů, kdy je však podmínkou přímá viditelnost. Jedná se už o velmi drahou technologii. Fungují na principu zaměření paprsku na rezonanční plochu, chvějící se ve frekvenci mluveného hlasu. Přijímaný odražený paprsek se moduluje do požadované formy a získáváme velmi čistý odposlech. Dnes již existují technologie, které již dokážou paprsek ohnout dle potřeby a tím mizí potřeba naprosto přímé viditelnosti.

Obr. 6 – Druh laserového odposlechu

Oblíbenou formou radiového odposlechu je také pasivní rezonátor. Tento 2 cm velký dutý kovový váleček je ukončen velkou anténou a dokážou pracovat bez potřeby připojeného napájení. Přijímá ozařování rezonančního kmitočtu a membrána na konci antény se pak rozechvěje.

Obr. 7 – Pasivní rezonátor

3.2.4 Počítačový odposlech

V dnešním světě moderních technologií je Počítačová kriminalita velmi „populární“ a proto je také velmi rozšířená. Proto se budeme v této kapitole touto problematikou více zabývat. Velké množství firem v dnešní době pracuje s daty a datovými úložnými centry. Tím se stávají napadnutelnými. Konkurenční firmy či útočníci tak jsou schopni lehce „záškodničit“. Další možností je také možnost lehkého zneschopnění dat či možnost zjištění informací. Firmy si často do svých vlastních řad úmyslně najímají šikovné a schopné hackery, téže označované jako „bílé límečky“,

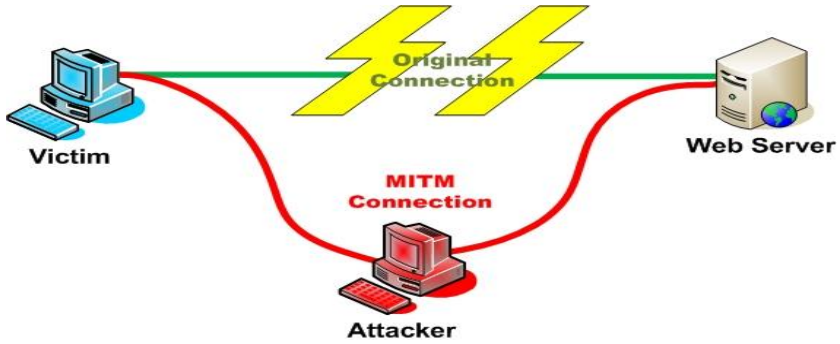
kteří danou problematiku znají a tím jsou taky schopni vytvořit ochranu. Jelikož je riziko napadení firmy pomocí počítačové techniky velmi vysoké, občas dochází až k paranoickým příznakům. Ty se projevují jako neumožnění mnoha informací pracovníkům a přístup k nim mají pouze TOP manažeři. Následkem toho vznikají tzv. Data pro data. Nutno dodat, že je tím ovlivněn chod společnosti a efektivita práce. Typickými příklady počítačové špionáže jsou :

- Napadení a likvidace počítačové sítě / databázových serverů
- Odposlech informačních kanálů / datové komunikace
- Podvržené informace / transakce

Těchto výše uvedených příkladů Průmyslové špionáže lze docílit mnoha způsoby. My si rozebereme ty nejčastější a zároveň nejnebezpečnější, protože je možné se jim naučit velice jednoduše i pro „lajka“. Uvedeme také základní možnou obranu proti nim. Jedná se o způsoby nelegálních odposlechů na počítačové síti. Je však velmi podstatné, že samotné odposlechy počítačů nemusí být vedeny vždy jen po síti Internet.

3.2.4.1 Man in the middle

Vše se děje za pomoci MAC address spoofingu. Odposlouchávání je provedeno tak, že hacker se „postaví“ mezi dva PC, servery a zachycuje data, která jsou mezi nimi posílána. Díky tomu je může také nepozorovaně měnit nebo spojení rušit. V podstatě falšujeme MAC adresy a tváříme se věrohodně, aby nám ta zařízení uvěřila. Obranou proti této metodě je zakoupení kvalitních aktivních prvků, páč ty novější již obsahují zabudovaný systém obrany, který dokáže rozluštit falšované MAC adresy.



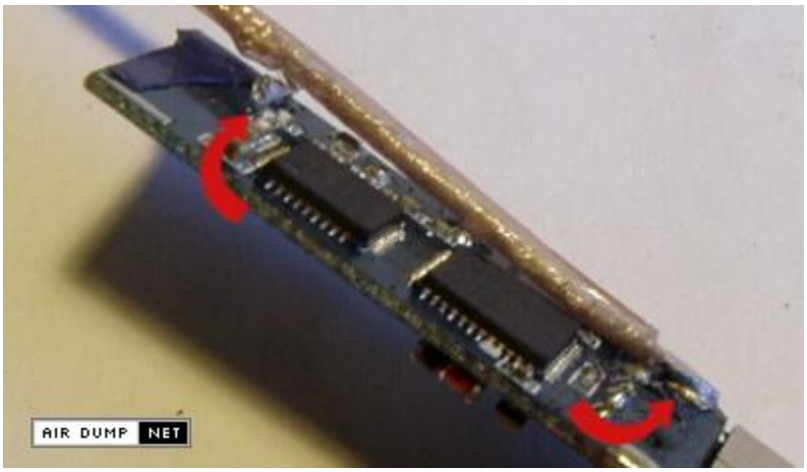
Obr. 8 – Zobrazení Man in the middle

3.2.4.2 Packet sniffing

Nejjednoduším typem sniffingu je packet sniffing. Tento typ je použitelný všude, kde síťové rozhraní a síťové karty naslouchají pouze paketům, které jsou určeny jen pro ni samostatnou. Pokud síťové rozhraní uvedeme do promiskuitního módu, dochází k odposlechnutí a uložení všech nebo vybraných dat. Vše se děje díky tomu, že síť používá síťový hardware (router, hub, …), který rozesílá pakety do celé sítě, a data jsou zpracovávána pouze počítačem k tomu určenému. Obranou jsou vhodné aktivní prvky, které minimalizují všesměrové vysílání dat.

3.2.4.3 Lokální sniffing

Jedná se o přímé odposlouchávání, které se provádí mezi dvěma počítači nebo je umístěn v protokolu TCP/IP a síťovým hardwarem na PC vybrané oběti. K tomuto je vytvořen software, který sbírá předem určená data a ukládá je a nebo je schopný je rovnou přeposlat hackerovi. Naneštěstí je většinou také schopný číst stisky na klávese, což pak může vést k snazšímu zjištění hesla. Obranou proti tomuto odposlechu je mít řádně zabezpečený PC, aktualizované spywary, firewall, antivirový software, atd. Jelikož se jedná o odposlech, k jehož chodu je potřeba záškodnický software první nainstalovat, je logickou obranou taky to, že zamezíme nepovolaným osobám k používání PC. Zabezpečíme heslem spořič obrazovky a také naše účty, různé zvolení způsobů indentifikace. Poté také logické uvažování a neinstalování neověřených programů stažených z internetu.



Obr. 9 – Bluetooth rozšířený o špionážní anténu

4 PROSTŘEDKY PROTI PRŮMYSLOVÉ ŠPIONÁŽI

Ochrana proti metodám Průmyslové špionáže lze rozdělit na :

- Ochrana proti lidskému faktoru
- Ochrana technického ražení

Před samostatným zabezpečením je nutné provést vyhodnocení rizika. Musíme si uvědomit, zda naše informace, jimiž disponujeme, jsou vzácné a dle toho předpovědět, jakou technikou bude útočník vybaven. Musíme brát v potaz také historii stavby budovy, popř. zabudování špionážní techniky do stavebního materiálu, přístupnost stěžejních prostor a kvalitu použité techniky útočníka. Tím zabráníme zbytečnému pořizování zabezpečovací techniky či zbytečného používání jistých sociálních ochran. Taky bychom si měli uvědomit, že špionáži předchází průzkum přímo na místě. Proto je vhodné tomuto zabránit.

4.1 Ochrana proti lidskému faktoru

Způsobů, jak se chránit proti Průmyslové špionáži, je hned několik. Máme – li na mysli ochranu proti lidskému faktoru, bavíme se především o ochraně uvnitř firmy proti samotným zaměstnancům. Po vyhodnocení rizika můžeme teprve přejít k samotným metodám ochrany, které jsou především organizačního ražení :

- Zvláštní režim
- Bezpečnostní služba (Pronajmutí bezpečnostní agentury)
- Fyzická ostraha (Dohled nad zaměstnanci, může být provedeno Bezpečnostní službou nebo zvlášť)
- Zálohování dat a informací (Plánované, ochrana proti odcizení či úmyslnému smazání)
- Režimy práce s datovými nosiči
- Prověření pracovníků při výběrovém řízení (provedení důkladného výslechu, grafologie, Možnost odhalení špióna)
- Častá kontrola provádění práce

- Zabránění přístupu nepovolaných osob do míst s důležitými informacemi (Přístupové systémy, biometrické systémy, zamykání dveří, …), nepovolaní ani nemusí vědět, že místnost obsahuje citlivé informace

- Přísný dohled na nespokojené zaměstnance !

- Propustkový režim

- Klíčová služba (evidence)

- Použití trezorů, bezpečnostních skříní a kufříků pro důležité listiny

- Klasifikace informací (Stanovení stupně utajení)

- Kamerový systém k dohledu nad zaměstnanci a zabránění vstupu cizí osoby

- Zabránit kontrole korespondence

- Důležité dokumenty po zužitkování zničit

- Vést dokumentaci o počtu kopií tajných dokumentů

- Počet zainteresovaných lidí snížit na minimum

- Zainteresovaní lidé by měli pracovat ve skupinkách a stejných místnostech (Minimalizace možnosti pro vnik cizích osob)

- Řádně ocenit odváděnou práci

- Kontrola řemeslníků a cizích osob v objektu (Nejlépe zajistit dohled nad nimi, umožnit jim přístup jen tam, kde je to nutné)

4.2 Technická ochrana

Touto ochranou zabraňujeme odcizení či zkopírování informací pomocí odposlechů či kamer. Na začátku zabezpečení bychom si měli taktéž zvolit míru rizika, které nám hrozí, abychom dokázali odhadnout, jakou techniku útočník použije.

Metodami technické ochrany jsou :

- Obranná technická prohlídka (OTP)
- Použití techniky zabraňující odposlechu v místnosti
- Kvalitní plášťová ochrana
- Kontrola radiového spektra
- Počítačová ochrana
- Stínění datových a komunikačních spojů
- Filtrování
- Šifrování

4.2.1 Obranná technická prohlídka (OTP)

Součást technické ochrany, prováděna před samotným zabezpečením. Jejím úkolem je odhalit nelegální špionážní techniku a zajištění prostoru proti jejímu umístění. Prohlídku provádí specialista, který musí mít osvědčení k této činnosti, za našeho dohledu a je obeznámen s touto problematikou. Jsou jisté zásady, které jsou potřeba u OTP dodržet a to:

- Zahájit v době, kdy se předpokládá aktivace odposlech. prostředků
- Zahájit i falešnou prohlídku a oklamat tak odposlech s dálkovým ovládáním
- Opakovat v určitých intervalech, nikdy však neprozradit přesný termín

- Provádět utajeně
- Výsledek je určen kvalitou použitých prostředků a pečlivostí
- Důraz na místnosti, kde se provádějí důležité rozhovory nebo činnosti
- Eliminovat možnost prozrazení průběhu OTP

4.2.2 Technické prvky proti odposlechu v místnostech

Máme tím na mysli především zařízení určené k obraně proti odposlechu. Existuje celá řada těchto přístrojů a jsou volně prodejné na trhu. Jejich hlavním principem jsou především vyzařování rušení a indikace odposlechů. Ne vždy zjistíme všechny odposlechy při obhlídce, i když jsou při ní používány níže uvedené přístroje. Níže zmíněné prvky proti odposlechu se řadí mezí obtížné na obsluhu. Proto je potřeba užívat je jen povolenou osobou, která má velké zkušenosti s touto problematikou a rozumí daným přístrojům, především Triangulaci RF spektra.

Jedním z typických přístrojů pro tuto činnost je **Radiový analyzátor**. Jeho činnost spočívá v nepřetržitém monitorování radiových vln. Je velmi rychlý a okamžitě upozorňuje na přítomnost štěnic radiového původu pomocí akustického poplachu. Pracuje dobře i v místě vysokofrekvenčního pole. Prostorová radiová štěnice patří mezi nejpoužívanější formu odposlechu.

Obr. 10 – Spektrální analyzátor

Dalším způsobem, jak zabránit ve vysílání štěnic, je **Šumový generátor.** Existuje v provedení analogovém a digitálním. Hlavním principem analogového je šum vyvolán proražením polovodičového přechodu. Šum je generován Zenerovou diodou nebo přechodem báze a emitoru bipolárního tranzistoru. Co se digitálního provedení týče, dochází k pseudonáhodnému generování signálu. Ten vznikne speciálním zapojením registrů. Slouží také ke vzniku „Růžového šumu“, který pokrývá celou část hovorového spektra. Tyto přístroje jsou k ničemu, dojde – li k otevření dveří. Proto zamykat dveře při jednání.

Obr. 11 – Šumový generátor

Triangulace RF spektra spočívá v detailním srovnání - korelaci rádiového spektra zájmového prostoru a referenčního RF spektra z několika míst dané lokality mimo tento prostor. Je to zatím nejúčinnější metoda, která umožňuje odhalit prakticky všechny aktivní rádiové odposlechy a to bez rozdílu, zda jsou analogové, digitální, šifrované. Existuje i rádiové odposlouchávací zařízení, které při použití špatné metodiky není odhalitelné ani v aktivním režimu. Tento typ odposlechů není možné spolehlivě odhalit bez použití skutečného spektrálního analyzátoru. Různá "náhražková zařízení" pracují jako běžné přehledové přijímače s velmi pomalým přelaďováním a tudíž nejsou schopna ve frekvenčně - časové doméně identifikovat signál tohoto odposlechu.

Posledním uváděným přístrojem jsou **detektory nelineárních přechodů**. Slouží ke kontrole místností, vozidel a jiných prostor před odposlechem a skrytými kamerami. Zachycuje veškeré polovodičové součástky, z nichž jsou tvořeny odposlouchávací zařízení. Jejich pořizovací cena je však vysoká a dosahuje řádu několik set tisíc.

Obr. 12 – Detektor přechodů

4.2.3 Plášťová ochrana

Další nedílnou součástí proti Průmyslové špionáži je plášťová ochrana. Můžeme jí zabezpečit místnost, objekt, vozidlo, atd. Pod pojmem plášťová ochrana, rozumíme obvodové zdi a veškeré otvory, střechy, podlahy, stropy. Velikost a šířka obvodových zdí by měla být dostatečná, aby zabránila průniku signálu. Možností vysílání šumu do zdí. Důležitou částí jsou okna. Nejmodernější přístroje dokáží dle vibrace tabule provádět odposlech i na dálku několika set metrů. Proto musí být použito kvalitní, několikavrstvé osazení okna (nejlépe místnost bez oken). Použití záclon či rolet proti odezírání ze rtů a znemožnění pořízení fotografií. Kvalitní osazení a utěsnění dveří, nejlépe silné dveře, jednokřídlé, uzamykatelné, avšak obsahující ochranu klíčové dírky a jejího utěsnění. V místnosti, kde se provádí důležité rozhovory, nesmí být krby, střešníky apod. Dobře, proti zvuku izolovaná, podlaha a stropy. Možnost použití Faradayovy klece znemožní vysílání signálů z místnosti.

4.2.4 Počítačová ochrana

Tato ochrana patří mezi vůbec nejdůležitější ochrany. V dnešní době informačních technologií se stává často napadnutelnou částí. Proto je potřeba ji v žádném případě nepodcenit. Dávat si pozor především na platby přes internetové bankovnictví. Ochrana je prováděna pomocí :

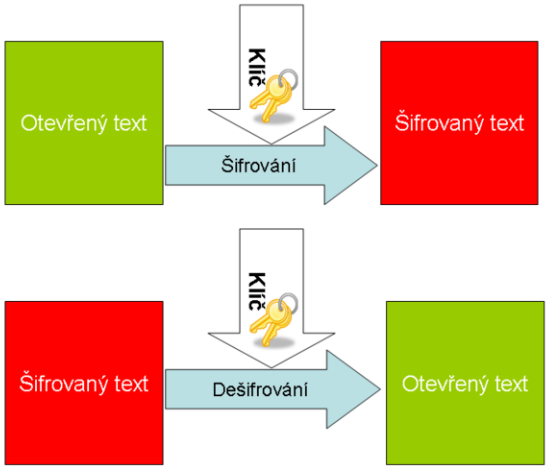
- Kvalitní firewall
- Licencovaný antivirus

- Spyware
- Antispamový filtr
- Pravidelná aktualizace
- Správné chování uživatele
- Užívání elektronických podpisů
- Certifikace, kontrola certifikace
- Kvalitní prvky pro síť a jejich zabezpečení
- Zabezpečení Acces pointu a bezdrátové sítě pomocí bezpečnostních prvků

4.2.5 Šifrování

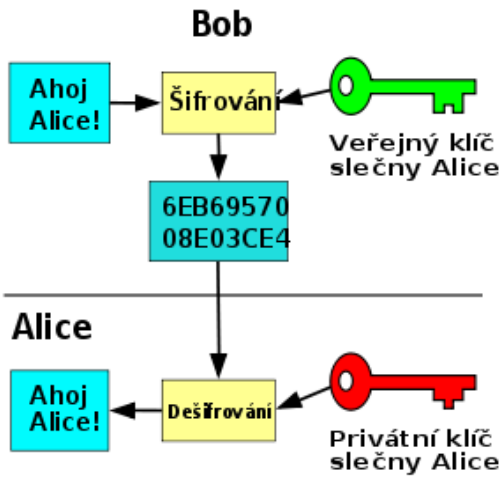
Věda, zabývající se touto problematikou, se nazývá kryptografie. Šifrování převádí informace a data do nečitelného textu pro třetí stranu. Příjemce pak tuto přijatou zašifrovanou zprávu dešifruje a dostává tak smysluplné informace nebo data. Šifry pro pozměnění textu jsou používány již od pradávna a v dnešní době je můžeme dělit na symetrické, asymetrické, hybridní a hash funkce. Jedná se o pasivní ochranný prvek proti Průmyslové špionáži, tzn. projde – li odposlech naší aktivní obranou a dojde k odposlechu, útočník dostane informace pro něj nečitelné.

Symetrickými šiframi se rozumí šifra, k jejímuž použití je potřeba jednoho klíče, pomocí nějž se text zašifruje a příjemce pak pomocí stejného klíče zprávu dešifruje. Tento klíč se musí držet v tajnosti a nejedná se o zrovna často používanou metodu. Bezpečnost této šifry je nižší, než u ostatních typů. Existují proudové šifry, kdy se text šifruje bit po bitu a blokové šifry, kdy je text rozdělen na bitová slova, které jsou doplněné bitovou šifrou, aby měla všechna slova stejnou velikost a poté dochází k šifrování blok po bloku. Typickými příklady symetrických šifer jsou DES, TRIPLE DES, IDEA, BLOWFISH.



Obr. 13 – Symetrická šifra

Dalším typem jsou **asymetrické šifry**, které používají dva odlišné klíče. Jedním je klíč veřejný a druhým je klíč soukromý. Prvním je text zašifrován a druhým dešifrován. Veřejný klíč lze někde publikovat, kdežto soukromý klíč udržujeme v tajemství. Tím je docíleno vyšší bezpečnosti, než u předešlé metody. Veřejný klíč může být veřejně publikovatelný a můžeme používat k šifraci, ale text bude rozluštitelný pouze pro vlastníky soukromého klíče. Využití při digitálních a elektronických podpisech dokumentů. Nevýhodou je náročnost na výpočetní techniku a rychlost. Typickými příklady asymetrických šifer jsou RSA, DSA, El – GAMAL, DSS (elektronický podpis).



Obr. 14 – Asymetrická šifra

Moderní technologie však přišly ještě s něčím novějším a to jsou **hybridní šifry**. Přebírají kladné vlastnosti předešlých typů a vytváří tak nový způsob šifrování bez negativních vlivů. Jejich nespornou výhodou je především rychlost, nenáročnost pro výpočetní techniku a bezpečnost. Fungují na principu rozdělení zprávy na dva celky. Jedním je text, který je zašifrovaný symetrickou šifrou a druhým je klíč, zašifrovaný asymetrickou šifrou. K výslednému textu pak musíme rozšifrovat oba celky, avšak klíč je často daleko menší a proto není pro výpočetní techniku tak náročné jej rozšifrovat. Příkladem hybridní šifry je PGP.

Posledním typem jsou **hash funkce**. Pomocí nichž dochází k zašifrování a neumožňují následné dešifrování. Velmi populární technika pro databázové systémy, kdy jsou hesla zašifrována a vychází pouze pod náhodným výsledkem šifry. Tyto výsledky mají vždy pevnou délku a neexistuje možnost, aby výsledkem dvou různých vstupů, byl stejný výstup. Tím je zvýšena bezpečnost ochrany. Příklady pro has funkce MD5, SHA1.

Šifrování má však daleko větší význam a netýká se pouze počítačových dat. Můžeme také šifrovat zprávy přenášené signály. Prvním typem tohoto šifrování byla Morseova abeceda, dnes fungují daleko vyspělejší techniky. Bezpečnostní manažeři

mají možnost využití techniky, která je připojena k mobilním telefonům a zajišťují hovor proti třetí osobě. Samotná ochrana GSM proti odposlechu je již dávno prolomena. Proto je doporučeno užití šifrovacích zařízení GSM.

5 BUDOUCNOST PROBLEMATIKY

Úroveň této problematiky každým rokem stoupá a stává se čím dál více oblíbenou. Proto je logické, že se bude hojně užívat i v budoucnosti. Samotné odvětví se bude vyvíjet ve dvou směrech, přičemž v obojí bude hlavním cílem zisk informací. Budoucnost bude jako nyní plynout ve směrech lidského faktoru a technického faktoru. Obojí se bude stále vyvíjet a budou vynalezeny nové techniky, jak Průmyslovou špionáž provádět. Velkého rozšíření se můžeme dočkat téměř ve všech odvětvích lidské činnosti. Ekonomická sféra se stává bojovým polem států a proto se dočkáme i rozmachu státní Průmyslové špionáže, která funguje již mnoho let. Můžeme také očekávat, že se do tohoto odvětví zapojí i menší státy, ještě nedotčené touto problematikou. Nutno dodat, že tyto skutečnosti budou mít také za následek vývoj kontrašpionáže, která bude zdokonalována zároveň se špionáží klasickou. Samotná Průmyslová špionáž by mohla být zcela potlačena. Kdyby v budoucnosti vznikly tzv. systémy účastnictví. Jedná se o organizované zhraňování nových technologií, metod, postupů, kdy by byli vynálezci odměněni patentem a financemi za jejjch výrobek. Následně by jejich patent byl vypuštěn do světa a byl k dispozici všem ostatním zemím. Bohužel je tato skutečnost prozatím oblastí Ideologie. Můžeme jen doufat, že se tak stane alespoň ve státní oblasti.

5.1 Lidská činnost Průmyslové špionáže

Stále se jedná o nejsnadnější způsob zisku informací a proto je nesmysl lidský faktor v této problematice zavrhnout. Problémem je především výcvik nových tajných agentů a špiónů a vznik samotných organizací, které se tím netají. Japonsko v tomto ohledu započalo velice intenzivně pracovat a to již v 80. letech, kdy došlo k budování škol pro špióny, kteří jsou cvičení metodám převleků, užívání špionážní techniky a verbální komunikaci. Již v té době dosahoval počet Japonských špiónů kolem 10 000. V dnešní době nedokážeme určit, zda disponují větším nebo nižším počtem, ale jisté je, že jsou daleko více kvalifikovanější a schopnější. Nutno dodat, že Japonsko není zrovna největší distribucí špiónů na světě, nýbrž kopírují světové velmoci a snaží se „nezahálet“ v tomto odvětví. Celosvětově vznikají a budou vznikat tréninková místa pro nové špióny a nutno dodat, že začínají zahrnovat do svých řad také nezletilé. Velkou chybou v této oblasti je také to, že spousta lidí je špatně informovaných a velice důvěřivých. Toho pochopitelně špióni zneužívají.

I přes velký současný a budoucí rozmach této problematiky je nutno říci, že vznikají již řadu let organizace bojující proti této metodice. Velkým přínosem je rozesílání informací a poskytování poradenství. V budoucnosti by se v každém podniku, jež může být potencionálním terčem špionáže, měl vyskytovat bezpečnostní manažer, který by měl být schopen této problematice zabránit. Je velmi pravděpodobné, že za tímto účelem budou vycvičování specialisté ve velkém množství a ne, jak je tomu doposud. Měly by se také objevit firemní noviny či brožury, které osvětlují tuto problematiku a měl by být dán popis obrany. Za tímto účelem se začnou pořádat i zasedání a školení.

Můžeme také očekávat, že budou stále více využívány služby soukromých detektivů a bezpečnostních agentur. Dojde také ke zvyšování kvality a schopností zaměstnanců.

Nepříjemnou částí naší budoucnosti však také budou stále častější obvinění ze špionáže, což bude mít za následek stále větší zatěžování administrativy a soudní legislativy a co se lidského faktoru týče, tak se nedá zavrhnout i zvyšování vyhrožování, vydírání a korupce. To vše povede také ke zpřísnění trestů za špionáž a snad i ke zpřísnění trestů za Průmyslovou špionáž a uvědomění si hrozby této problematiky.

5.2 Technologický vývoj

Je pochopitelné, že technologický vývoj jde kupředu s každým dnem. Proto je nesmysl si myslet, že dnes pořízené vybavení můžeme používat i za sto let. S rozmachem informačních technologií roste také způsob zisku informací po síti, což můžeme označit jako kybernetickou hrozbu. Velký rozmach můžeme očekávat ze strany počítačových hackerů, zdokonalování současných technologií a získávání dat přes celosvětově používanou síť Internet a monitorování našich myšlenek, názorů pomocí sociálních sítí. Již dnes fungují analýzy, které monitorují náš pohyb na síti, naše zájmy. To vše se tak děje legálně, jelikož se maskují za marketingové tahy, jak zajistit větší spokojenost zákazníků. Již dnešní světové organizace teroristického dopadu disponují znalci IT technologií a tím se zvyšuje stále hrozba kybernetického terorismu. S tím souvisí neustálý vývoj hardwarů, softwarů a vytváření nových

standardů (tím rozumíme schválenou technologii používanou kybernetickým prostředím).

Velkého využití můžeme očekávat také v nanotechnologii, biotechnologii, jaderné fyzice, zbrojním průmyslu a ve využívání chemických prostředků. Veškeré špionážní technologie budou zdokonalovány a minimalizace přístrojů bude neustále stoupat. Důsledkem tohoto vývoje můžeme také očekávat stále většího zásahu do soukromí, který se děje již dnes. Již nyní prostředky CCTV a družicové systémy monitorují náš veškerý pohyb. Je potřeba si uvědomit, že již dnes lze odposlouchávat veškeré naše rozhovory pomocí mobilní sítě GSM. A v blízké budoucnosti tomu nebude jinak, přestože se zvolí jiné šifrovací metody pro tyto sítě.

II. PRAKTICKÁ ČÁST

6 PRŮMYSLOVÁ ŠPIONÁŽ VE SVĚTĚ

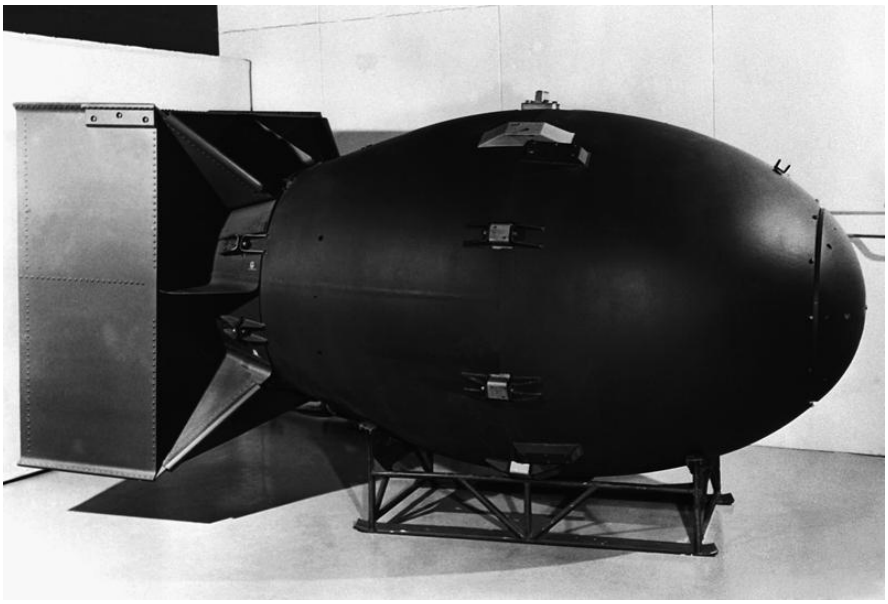
Průmyslová špionáž je zde již od pradávna. Stejně dlouho, jak funguje Průmyslová špionáž, funguje i Kontrašpionáž a techniky boje proti špionáži. Díky tomuto faktu bylo možno odhalit velkou spoustu špiónů, pokusů o špionáž a špionáží samotných. V této praktické častí se seznámíme se situacemi, které nějakým způsobem ovlivnily běh dějin, odhalily působení států na územích států jiných a vzniklé škody. Rozdělili jsme je dle období, v kterých probíhaly. Nutno dodat, že se jedná o informace často nepotvrzené oběma stranami. Fakta však hovoří jasně a je samozřejmostí, že vlády států nesmí převzít odpovědnost za jednotlivé špionážní útoky. Mohlo by to vést k velkým problémům celosvětového měřítka.

6.1 Období 2. Světové války

V tomto období se Průmyslová špionáž dočkala velkého rozmachu. Fungovala na všech frontách zemí, které zasahovaly do válečného dění. Především Rusko, Japonsko, Amerika, Francie a Německo, které v tomto období již chápalo důležitost této problematik a zavedlo trest smrti za Průmyslovou špionáž. Snažili se zjišťovat veškeré informace od výrobních tajemství, až přes dodávkové služby armád, armádní stavy, pozic jednotlivých pluků, jmen špiónů, atd. My si rozebereme pouze případy Průmyslové špionáže, která se týká především výrobních procesů.

6.1.1 Technologie atomové pumy

O tuto technologii se postaral Leslie Growes, jež vedl „projekt Manhattan“, který tak vytvořil vůbec první atomovou pumu na světě. Američané byly sice prvními, kteří ji dokázali stvořit, ale nutno dodat, že jen díky velmi dobře odvedené práci špiónů, kteří získali podklady pro tuto technologii v Německu a ve světě. Obrana tohoto projektu se dala považovat za vůbec nejlepší obranu proti Průmyslové špionáži své doby a nedokázali ji prorazit žádní celosvětově uznávaní špióni, přestože na ní pracovalo přes 600 Američanů a byly provedeny i testy odpálení. Nutno dodat, že špionáž USA v té době několikrát pozdržela vývoj atomové bomby v Německu.



Obr. 15 – Atomová puma svržena na Hirošimu

6.1.2 Enigma

Jednalo se o přístroj, který umožňoval šifrovat zprávy a tak zabránit přečtení, pokud se zpráva dostala do nesprávných rukou. Pochopitelně sloužil i k dešifrování. Byla vynalezena v Německu. Ze začátku byla použita k šifrování civilních zpráv, poté již především pro armádu. Funguje na principu několika otočných ozubených kol s velkým množstvím vnitřních vedení a na rozsvěcování „náhodných“ žárovek označených písmeny. Průmyslová špionáž zde zafungovala skvěle, protože se Polským, Britským a Americkým vědcům podařilo rozluštit tento mechanismus. Díky tomu byli schopni číst tajné zprávy Němců a podle toho jednat. Pak už jediným úkolem špiónů bylo získat dokumentaci o nastavení, což nebylo tak jednoduché. Ještě jeden velmi chytrý tah předvedla s tímto přístrojem Britská vláda. Po válce prodala veškeré přístroje Enigma rozvojovým zemím a přitom dokázala zcela utajit fakt, že jsou schopni ji rozluštit.

Obr. 16 - Enigma

6.2 Současnost

Tato část se zaměřuje na útoky blízké dnešnímu datu. Uvedu několik případů Průmyslové špionáže. Veškeré informace jsou veřejně dostupné a není problém je vyhledat. Nelze zde uvést všechny, proto vyberu jen ty největší. Průmyslových špionáží k dnešnímu datu existuje daleko více, ale vlády je drží pod pokličkou a pro normální smrtelníky je takřka nemožné se o nich dozvědět více. Můžeme pouze vést spekulace.

6.2.1 SNECMA

Jednalo se o předního evropského výrobce leteckých motorů, jež se stala obětí Průmyslové špionáže v roce 2001. Filiálka Messier – Dowty, jež byla dominantní především ve vývoji leteckých podvozků a to jak u civilních, tak vojenských letadel, ztratila důležité součástky z připravovaného koncernu bitevních letounů Rafale Marine. Výsledky následného vyšetřování služeb DST objevily Průmyslovou špionáž, avšak to ještě dlouho poté firma popírala. V podezření padlo USA a Rusko, avšak se vše v tichosti zametlo pod koberec, aby nedošlo ke skandálu. Pár měsíců poté byla firmě ukradnuta veškerá dokumentace a záznamy na výrobu podvozků Skokan. Ty umožňovaly přistát letounům na letadlové lodi i za rozbouřeného moře a vysokého větru. A to nebylo vše. Další problém vyvstal na povrch, když v pobočce

firmy zmizelo 14 počítačů, jež obsahovaly podklady pro dopravní letouny A400M. Zaměstnanci se museli zpovídat dokonce i ministru vnitra. V podezření opět padlo USA, které přišlo čas na to se stejným konceptem u svých letounů Boeing a Lockheed martin. SNECMA poté v roce 2003 ukončuje svou činnost.

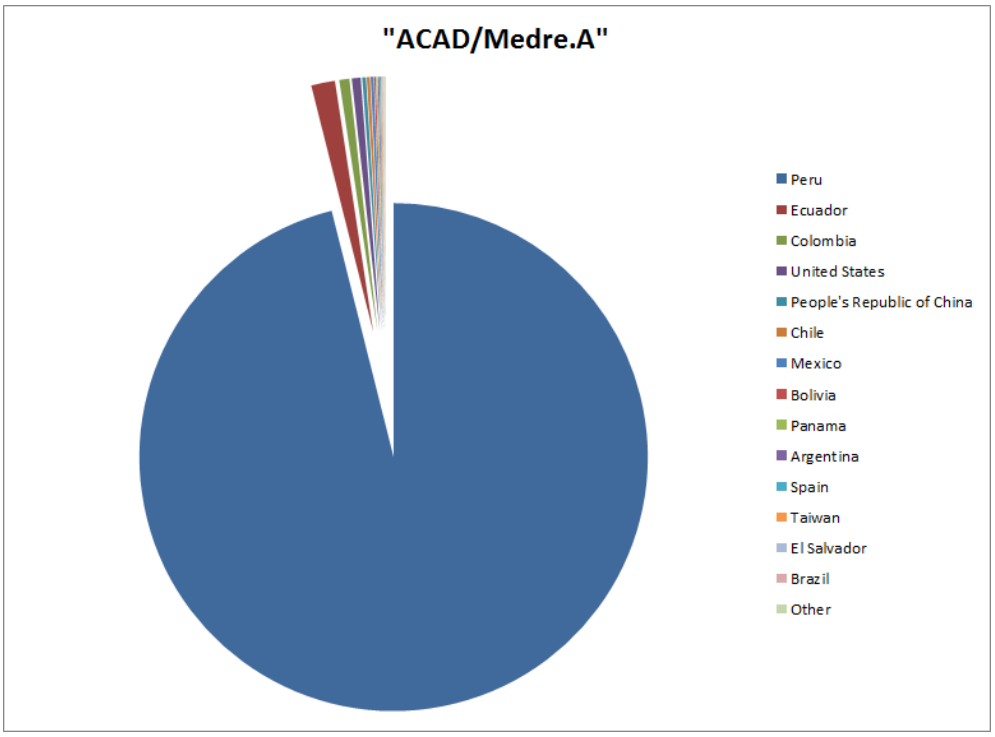
Důležitou součástí této aféry je také to, že po těchto událostech se v USA vytvořila technologie zabraňující bezpečnost a to na poli ekonomickém a vojenském.

6.2.2 Elektronické sítě Bruselu

Dalším případem Průmyslové špionáže je napadení elektronických sítí federálních úřadů v Bruselu. Útok byl veden z Číny, která mimo jiné v dnešní době patří mezi vůbec největší špionážní velmoc a užívají své finanční prostředky pro vývoj špionáže a ne pro vývoj technologií, protože se řídí heslem, že je snažší výrobu ukrást, jak objevit. Došlo dokonce i na veřejné obvinění. To vedlo k připojení se dalších států, jako bylo Německo a Británie a také FBI informovalo o ročním nárustu čínské špionáže o 10 % za poslední rok. Ministr zahraničí Číny však vše smetl ze stolu, že nejsou důkazy.

6.2.3 Acad Medre

Novým trendem Průmyslové špionáže byl v roce 2012 počítačový vir Acad Medre. Jeho úkolem je získávání a přeposílání veškeré dokumentace vytvořena v licencovaných aplikacích AutoCad. Jelikož se tento program používá k vytvoření obrazů ještě před samotnou výrobou, lze tento vir řadit mezi velmi nebezpečné pro podniky. Tento červ byl objeven v Peru, kde také napáchal nejvíce škod, protože se na něj přišlo poměrně pozdě. Následné vystopování vede opět k Číně. Zajímavostí také je, že tento červ byl umístěn přímo ve verzích AutoCad. Ty byly podle všeho zneužity k jeho šíření.



Obr. 17 – Graf napáchaných škod červem ACAD Medre

6.2.4 Automobilka Renault

Jedná se o vůbec největší aféru posledních let. Francouzská automobilka Renault, která mimo jiné vlastní i Nissan, se stala terčem Průmyslové špionáže. Stalo se tak v roce 2011, kdy firma investovala obrovské peníze do vývoje elektromobilů. Nikde se nelze dočíst, do jaké míry byla Průmyslová špionáž úspěšná. Avšak podle faktu, že automobilka propustila své tři zaměstnance, kteří pracovali na strategických pozicích, lze říci, že to byl citelný zásah. Po této skutečnosti apelovala Francouzská vláda na zvýšení zabezpečení firem, u kterých je riziko. Chvíli na to došlo k rozšiřování možných dezinformací o křivém obvinění vůči těmto zaměstnancům a zpětnému nástupu. Zda – li se tak ve skutečnosti stalo nevíme.

6.2.5 OHB Technology

Tato organizace působí především na trhu se satelitní technikou a je jedním z firem, jež přispěly svou prací k vytvoření GPS systému Galileo. Generální ředitel této firmy v roce 2009 prohlásil, že Francie patří mezi vůbec největší organizace ve světě Průmyslové špionáže a škody jsou daleko vyšší, než kdy napáchalo Rusko či Čína. Francie je také velkým konkurentem Německa ve věci špionážních satelitů, na

jejichž vývoji se neustále pracuje. Nutno dodat, že toto prohlášení uvedla USA, takže se můžeme jen domnívat, zda se nejedná o dezinformace.

6.2.6 Intel

Roku 2010 se terčem Průmyslové špionáže stal také Intel. Cílem bylo získání informací pro výrobní postupy. Tento útok byl proveden velmi promyšleně. Zároveň s napadením Intelu se stal terčem útoku i Google a používání systému MSIE 6 firemní sítě. Firma však odmítla zodpovědět otázku, zda byl útok úspěšný nebo ne. Můžeme se jen domnívat, ale jelikož Intel zveřejnil tuto informaci a je napadán takřka denně, jistým způsobem jej to určitě zasáhlo. Zda bylo hlavním cílem MSIE a ostatní útoky byly provedeny jen k zamaskování, nevíme.

6.2.7 Stuxnet

Jedná se o další vir z rodinny malwarů. Objeven byl v roce 2010 především na území Iránu a USA a jedná se o červa typického pro Průmyslovou špionáž. Úkolem tohoto viru bylo zjišťování informací o SCADA, což je technologie zabývající se monitorováním a to především v energetice a průmyslu. Největší procento napadení bylo právě v USA a to necelých 60 %. Firmě Eset, což je jednou z firem vytvářející antivirové systémy se jej již podařilo eliminovat, ale nelze říci, kolik škod stihl tento vir napáchat. Jednalo se o jednu vůbec možná největší kybernetickou hrozbu vůbec doposud známou. Nástupcem tohoto viru nenechalo na sebe dlouho čekat a byl jím další červ a to DuQu. I ten se již podařilo eliminovat, protože pracoval na velmi podobné bázi jako jeho předchůdce.

6.2.8 Trojangate

Jedná se o další z kybernetických útoků. Je typickou ukázkou Průmyslové špionáže. Stalo se tak v Izraeli v roce 2005, kdy spisovatel našel na Internetu jeho vlastní dokumenty, aniž by dokončil svou knihu a to i s poznámkami. Nic z toho nebylo nikomu poskytnuto a dokonce neměl o tom ani nikdo vědět. Následné šetření objevilo software Rona, který sloužil ke sledování a přeposílání dat útočníkovi. Pro spisovatele to byla značná ztráta, ale boom ve vyšetřování přišel teprve, když se rozpletla celá síť tohoto softwaru. Zjistila se celá řada napadených firem a nutno podotknout, že mezi ně patřili i celosvětoví giganti. Napadenými byly mimo jiné Hewlett – Packard, Ace (řetězec pro výrobu hardwarů), deník Globes, televizní

společnost HOT a také agentura Rani Rahav (mezi její klientelu patří druhý největší izraelský mobilní operátor Partner Communications) a celá řada dalších. Za vším stála jen jediná osoba, která dala vzniknout tomuto softwaru a to Michael Haephrati, který jej prodal agenturám pro provádění Průmyslové špionáže.

ZÁVĚR

Cílem této bakalářské práce bylo seznámení se s problematikou, uvedení cílů Průmyslové špionáže, seznámení se s metodami a formami a také s uvedením způsobů, jak se efektivně bránit. Během mého bádání jsem se rozhodl do praktické části zahrnout dosud světově známé případy, kdy Průmyslová špionáž zafungovala nebo k jejímž pokusům došlo. V popisu této problematiky jsem také uvedl pojmy, které s tímto tématem souvisí a to bylo vysvětlení patentní a licencované politiky a zdůvodnění výhod plynoucích z ní. Také jsem chtěl čtenáře seznámit s pojmem Know – How a objasnit Konkurenční zpravodajství. Celkovým výsledkem mého snažení bylo vytvořit návod pro bezpečnostní manažery, jež by měli být schopni úspěšné chránit své firmy a firemní zájmy. Proto jsem se snažil uvést formy a metody Průmyslové špionáže a také operativní prostředky pro boj v tomto odvětvím. Ne však pouze pomocí technických prostředků, ale také za pomoci vnitropodnikového chodu a osobního přístupu k zaměstnancům. To se mi do jisté míry povedlo, avšak si myslím, že je tato práce z pohledu budoucnosti ve velké nevýhodě. Dnešní doba jde stále dopředu a já uváděl způsoby používané v minulosti a dnes. Tyto metody však za pár let budou již zastaralé. Chtěl jsem také upozornit na problematiku kybernetického terorismu. O to jsem se pokusil v poslední části teoretické části, kde jsem se snažil také rozebrat budoucnost této oblasti z pohledu lidského faktoru. Snažil jsem se poukázat na hrozby plynoucí pro normální smrtelníky a důležitost pojmu Průmyslová špionáž. Přes všechnu snahu se mohlo stát, že jsem nepřesvědčil všechny o důležitosti této problematiky. Proto jsem se rozhodl zpracovat praktickou část, kde jsem chtěl uvést nejznámější případy dopadu Průmyslové špionáže na podniky. Pokusil jsem se vybrat ty důležité a také upozornit na hrozbu, která z nich plyne a že pole působnosti není jen v konkurenčních bojích, ale že se stává stále více zájmovou oblastí pro boj států. Mým cílem bylo změnit pohled na tuto problematiku a to aby se na ni pohlíželo přísněji i legislativně. Tím mám na mysli zvyšování trestů za provádění a také omezení prodeje techniky k jejímu provozování. Posledním cílem, který jsem si vytyčil, bylo upozornění na hrozby s rozvíjející se technologií a tím i rozvíjení se útoků přes celosvětovou síť Internet. Jelikož se dnešní společnost stále více ubírá směrem využívání moderních technologií, je logické, že dochází k jejímu rostoucímu zneužívání. Proto jsem chtěl také upozornit na tuto problematiku jako prostředek k ovlivňování dnešní společnosti. Vlastním přínosem bylo zpracování problematiky a vyhledání informací.

Především nalezení a sepsání článků o Průmyslové špionáži. Jelikož se Průmyslové špionáže nelze úplně zbavit, mělo by se podle mého názoru objevit profesionální školení bezpečnostních manažerů a zvyšovat se jejich schopnosti a kvalifikace. Mohli bychom taktéž zavést organizaci, která by alespoň v oblasti státu, vyplácela finance za patenty a oceňovala nápady. Ty by pak byly veřejně šiřitelné, čímž by Průmyslová špionáž začala postrádat smysl.

ZÁVĚR V ANGLIČTINĚ

The aim of this work was to study the issue, put the objectives of industrial espionage, apprise readers with the methods and forms of it, as well as to specify possible ways to effectively defend them. During my research, in the practical part, I decided to include the most world known existing cases of industrial espionage and also attempts which occurred in the past. In the description of this problem I also stated terms that relate to this topic and it was patented and licensed explanation and justification of the policy benefits leading from it. I also wanted to introduce the reader to the concept of Know - How and clarify the Competitive Intelligence term. The overall result of my efforts was to create a guide for security managers, who should be able to successfully protect their business and corporate interests. That's why I tried to give the forms and methods of industrial espionage and operational means to fight this espionage industry. This protection is done not only by technical means, but also with the help of internal operation and the personal approach to the staff. I think I quite succeeded but I also think that this work, from the perspective of the future, is at a great disadvantage. Today's time is still moving ahead and I featured methods used in the past and nowadays. So from this point of view, these methods will become obsolete in a few years. I also wanted to draw attention to the issue of cyber terrorism. That's what I did in the last section of the theoretical part where I tried to analyze the future of the field from the human factor's point of view. I tried to highlight the threat posed to ordinary people and the importance of industrial espionage's concept. Despite all efforts, it could happen that I did not convince everybody about the importance of this issue. Because of this, I decided to compile a practical part where I wanted to mention the most famous cases of industrial espionage and their impact on businesses. I tried to choose the most important cases and also draw attention to the threat of them and pointed out that the scope is not just in the competitive battles, but it is increasingly becoming the area of interest for fighting States. My goal was to change the perspective on this issue and the fact that it should be regarded more strictly and legally. By this, I mean to increase the penalties of implementation, and also to limit the sales of the observational technology. The last goal that I set up was to alert to the threat of emerging technologies and thus developing attacks worldwide on the Internet. As today's society is increasingly moving towards the use of modern technology, it is

logical that it is being increasingly abused. That's why I wanted to draw attention to the issue as a mean how to influence today's society. Benefit of my own work was treatment of issue and searching of informations. Especially finding and writtening of articles about industrial espionage. It's not possible to rid the world of industrial espionage, we should make proffesional courses for security managers andraise thein qualification. We can make an organization which can pay a money for new patents and appreciate an ideas. Then we can these patents make publicly for everyone. After this industrial espionage will be miss the point.

SEZNAM POUŽITÉ LITERATURY

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

[2] LAUCKÝ, Vladimír. *Přednášky z SBT*. Zlín, 2012.

[3] BERGIER, Jacques. *Průmyslová špionáž*. 1. vyd. Překlad Miroslav Brož. Praha: Orbis, 1974, 191 s. Stopy, fakta, svědectví (Orbis).

[4] I. Krizový zákon: Odvětvová kritéria pro určení prvku kritické infrastruktury. In: *432/2010*. 2011.

[5] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti I*. Vyd. 1. Zlín: Univerzita Tomáše Bati, 2003, 64 s. ISBN 80-731-8119-3.

[6] LAUCKÝ, Vladimír. *Technologie komerční bezpečnosti II.* Vyd. 1. Ve Zlíně: Univerzita Tomáše Bati, 2004, 122 s. ISBN 80-731-8231-9.

[7] CHURAŇ, Milan. *Encyklopedie špionáže: ze zákulisí tajných služeb, zejména Státní bezpečnosti*. 2., přepracované a aktualizované vyd. Praha: Libri, 2000, 431 p. ISBN 80-727-7020-9.

[8] Licenční smlouva k předmětům průmyslového vlastnictví. In: *č. 527/1990 Sb.,č. 207/2000 Sb.,č. 441/2003 Sb.,č. 478/1992 Sb.,č. 132/1989 Sb.,č. 529/1991 Sb.,č. 2*. Dostupné z: http://www.sagit.cz

[9] *Český statistický úřad: Licence* [online]. 2012 [cit. 2013-05-17]. Dostupné z: www.czso.cz

[10] Metody špionáže: Průmyslová špionáž. [online]. [cit. 2013-05-17]. Dostupné z: http://magazin.specialista.info

[11] Způsoby odposlechu mobilní komunikace. [online]. [cit. 2013-05-17]. Dostupné z: http://www.probin.cz

[12] Intel potvrdil, že se stal terčem útoku. [online]. [cit. 2013-05-17]. Dostupné z: http://computerworld.cz

[13] Ochrana proti odposlechu, odposlouchávací zařízení v praxi. [online]. [cit. 2013-05-17]. Dostupné z: http://www.triangulace.cz

[14] Nový červ napadá řídicí průmyslové systémy v USA a Íránu. [online]. [cit. 2013-05-21]. Dostupné z: computerworld.cz

Seznam použitých symbolů a zkratek

CI	Konkurenční zpravodajství
EPO	Evropský patentový úřad
USPTO	Úřad pro patenty a ochranné známky ve Spojených státech
OTP	Obranně technická prohlídka
RF	Radio – frekvenční
CCTV	Uzavřený televizní okruh
GSM	Globální systém pro mobilní komunikaci
DST	Francouzská kontrarozvědná organizace
IT	Informační technologie
FBI	Federální úřad pro vyšetřování
GPS	Globální družicový polohový systém

SEZNAM OBRÁZKŮ