Masarykova univerzita
Fakulta informatiky


# Zajišťování bezpečnosti při vývoji SW

Bakalárska práca

**Marek Šanta**

Brno, jeseň 2018

Masarykova univerzita
Fakulta informatiky


# Zajišťování bezpečnosti při vývoji SW

Bakalárska práca

**Marek Šanta**

Brno, jeseň 2018

*Na tomto mieste sa v tlačenej práci nachádza oficiálne podpísané zadanie práce a vyhlásenie autora školského diela.*

# Vyhlásenie

vyhlasujem, že táto bakalárska práca je mojím pôvodným autorským dielom, ktoré som vypracoval samostatne. Všetky zdroje, pramene a literatúru, ktoré som pri vypracovaní používal alebo z nich čerpal, v práci riadne citujem s uvedením úplného odkazu na príslušný zdroj.

Marek Šanta

**Vedúci práce:** RNDr. Jaroslav Ráček

# Poďakovanie

Ďakujem vedúcemu za možnosť napísať prácu na túto podľa mňa opomínanú tému. A ďakujem všetkým, ktorí so mnou mali trpezlivosť počas jej písania

# Zhrnutie

Cieľom tejto práce je na základe legislatívy, noriem, iných zdrojov a vlastného posúdenia navrhnúť princípy zabezpečenia spoločnosti vyvíjajúcej softvér pre viacerých zákazníkov, ktorí požadujú zvýšené bezpečnostné pravidlá a navrhnúť spôsob ich implementácie v konkrétnej firme. Práca sa zameriava na fyzickú bezpečnosť, zabezpečenie dátovej infraštruktúry vrátane prenosu dát mimo nej a personálnu bezpečnosť.

## Kľúčové slová

bezpečnosť, fyzická bezpečnosť, personálna bezpečnosť, bezpečnosť infraštruktúry, ochrana utajovaných informácií, normy, legislatíva

# Obsah

# Úvod

Súčasťou vývoja softvéru je práca s citlivými informáciami. Ako citlivé informácie môžeme v danom kontexte označiť všetko, čo by mohlo v prípade ich úniku či neoprávnenej manipulácie poškodiť spoločnosť, jej zákazníka, alebo kohokoľvek iného. Môže ísť napr. o zdrojové kódy, personálne informácie, utajované skutočnosti či samotné výsledné produkty. Ochrana takýchto informácií je, pochopiteľne, kritická. Jej zlyhanie môže mať ďalekosiahle následky [1]. Tu však vidím dva zásadné problémy negatívne ovplyvňujúce aktuálnu situáciu v IT sfére.

Jedným z nich je podceňovanie alebo úplná ignorácia potreby mať správne vytvorenú a zavedenú bezpečnostnú politiku. Ide o notoricky známy problém, no aj tak sa často rieši až po nejakom odhalenom incidente [2]. Je potrebné si uvedomiť, že fatálne následky môžu mať aj na prvý pohľad banálne chyby. Z vlastnej skúsenosti viem, že nie je problém s využitím sociálneho inžinierstva získať prístup k dôležitým informáciám bez kontroly totožnosti a príslušnosti. Bez vedenia dbajúceho na bezpečnosť sa však v tomto prípade veľa robiť nedá.

Ak sa také vedenie nájde, nastáva druhý problém, ktorým je podceňovanie, resp. neuvedomovanie si niektorých aspektov bezpečnosti. Aj keď sa dá povedať, že oproti laickej verejnosti je v našom obore o niečo väčšie povedomie o bezpečnostných hrozbách vrámci informačných systémov, existujú riziká, ktoré adresované nebývajú. Podľa môjho názoru sa najmenej pozornosti sústreďuje na fyzickú, personálnu a infraštruktúrnu bezpečnosť a ich vzájomné prepojenie.

Cieľom tejto práce je popísať organizačné a technické princípy[2] zabezpečenia firmy vyvíjajúcej softvér so zameraním sa na práve tieto aspekty. a následne posúdiť existujúce zabezpečenie konkrétnej spoločnosti a navrhnúť zmeny tak, aby daným princípom odpovedali.

V prvej časti práce sa zameriavam na presnejšie vymedzenie práce a prehľad použitých zdrojov tak, aby som čitateľovi uľahčil orientáciu v nich a opísal ich určenie, či možné problémy. Následne definujem a

---

1. Napr. v roku 2017 americkej NSA uniklo množstvo nástrojov, čo malo za následok ich využitie v malvéri a napadnutie desiatok tisíc počítačov [1]
2. Je potrebné uviesť, že práca je koncipovaná ako súčasť vytvárania, resp. revidovania systému riadenia bezpečnosti informácií a nerieši komplexnú politiku.

prechádzam vybrané aspekty bezpečnosti, pričom opisujem niektoré z možných hrozieb z pohľadu útočníka.

V druhej časti prezentujem princípy, ktorými tieto a iné hrozby kontrolovať, či riešiť a posudzujem zabezpečenie konkrétnej spoločnosti a porovnávam ho okrem týchto princípov aj s požiadavkami uvedených právnych predpisov, ak je to nutné. Následne navrhujem potrebné zmeny a predstavujem základ projektovej dokumentácie na vykonanie týchto zmien.

Požiadavkou podľa zadania sú zvýšené bezpečnostné pravidlá. Preto sa mnou navrhované princípy môžu zdať prehnané - ide o pokus priblížiť sa úrovni ochrany utajovaných skutočností, prípadne vylepšiť aj tie. Avšak návrh zabezpečenia konkrétnej firmy je oproti vytvoreným princípom upravený s ohľadom na jej veľkosť, možnosti a požiadavky, ktoré som počas písania práce dostal.

V závere práce zhodnocujem, do akej miery som s prácou spokojný, či a do akej miery sa podarilo naplniť zadanie a opäť uvažujem nad situáciou v zabezpečovaní, avšak po zohľadnení informácií, ktoré som sa dozvedel v priebehu rešerše pre túto prácu.

# 1 Zasadenie práce do kontextu zabezpečovania

Bezpečnosť v organizáciách sa rieši na viacerých aspektoch a vo viacerých úrovniach. V tejto krátkej kapitole ich detailnejšie popíšem a hlbšie vysvetľujem problém, ktorý vidím. Najprv rozdeľujem bezpečnosť na viaceré časti a pri ich opise uvádzam, či sú v práci rozoberané, do akej miery a prečo.

Práca je zameraná na ochranu citlivých informácií, alebo iných aktív, ktoré môžu vznikať, alebo byť spracovávané vrámci IT firmy. A preto sú hrozbami, ktoré ma zaujímajú napr. nekalá hospodárska súťaž, či cielené zneužitie utajovaných informácií na účely ilegálnej činnosti ohrozujúcej záujmy štátu. Tie u útočníka implikujú existenciu hlbšej motivácie a úzke zameranie sa na danú spoločnosť vrátane hĺbkového prieskumu pred vykonaním útoku a využitie všetkého, čo je k dispozícii.

Bezpečnosť môžeme rozdeliť takto:

**Softvérová bezpečnosť informačných systémov** Sem patrí hlavne zabezpečenie verejného rozhrania vyvíjaných systémov a systémov používaných na vývoj. Taktiež tu môžeme zaradiť ochranu pred sieťovými hrozbami. A aj keď som už zažil vývojára, ktorý si svoj linuxový systém používaný na vývoj neaktualizoval niekoľko rokov, väčšinou sa stretávam s dostatočným pochopením dôležitosti bezpečnostných aktualizácií. Vrámci informatiky sa najviac pozornosti upriamuje práve sem. To je pochopiteľné, keďže väčšina útokov je vedená práve z vonku, pričom ciele sú náhodné a účelom je najčastejšie rýchly zárobok v dôsledku krádeže informácií, alebo vynútenej platby za službu. V práci teda túto oblasť nerozoberám.

**Administratívna bezpečnosť** Túto oblasť skvelo definuje Zákon o ochrane utajovaných skutočností a bezpečnostnej spôsobilosti[3]. Administratívnu bezpečnosť tvorí systém opatrení pri tvorbe, príjme, evidencii, spracúvaní, odosielaní, preprave, prenášaní, ukladaní, skartovaní, archivácii, prípadne inom nakladaní s informáciami. Práca rieši hlavne prepravu a prenášanie, ostatné formy nakladania s in-

formáciami sú nepriamo popísané vrámci personálnej bezpečnosti a to hlavne so zameraním sa na časté chyby. Problémom je, že pri hlbšom riešení tohoto aspektu by som už zachádzal do konkrétnych procedúr[1], ktorým sa chcem s výnimkou prenosu a prepravy vyhnúť.

**Personálna bezpečnosť** Je súhrnom opatrení, ktoré minimalizujú riziko zlyhania ľudského faktoru. Často sa o ňom hovorí ako o najslabšom článku, ale napriek tomu sa rieši minimálne. Hlavne preto som si aj tento aspekt vybral na dôkladnejšie spracovanie.

**Fyzická bezpečnosť** Sem by som zaradil všetky prostriedky, ktoré nejakým spôsobom zabraňujú neautorizovanému fyzickému prístupu k aktívam organizácie, prípadne taký prístup aspoň zaznamenajú. V práci sa tomuto aspektu venujem vo veľkej miere, keďže práve tu vídam najväčšie nedostatky.

**Zabezpečenie elektronickej infraštruktúry** Môžeme tu zaradiť zabezpečenie hardvéru informačných systémov, prvkov fyzickej bezpečnosti, alebo aj sieťové prvky a prístup k nim. K uvedomeniu si tohoto aspektu a jeho podceňovania ma viedol hlavne útok opísaný v časti *3.2.1*. V práci sa mu teda tiež venujem vo veľkej miere.

**Zabezpečenie infraštruktúry základných služieb** Sem patria všetky prvky, ktoré zabezpečujú dodávku elektrického napájania, vody, plynu a tepla. Tejto oblasti sa nepriamo, ale vo väčšej miere venujem vrámci fyzickej bezpečnosti - najväčšou hrozbou z jej pohľadu je výpadok, ktorý by mohol mať negatívny vplyv na jej funkciu.

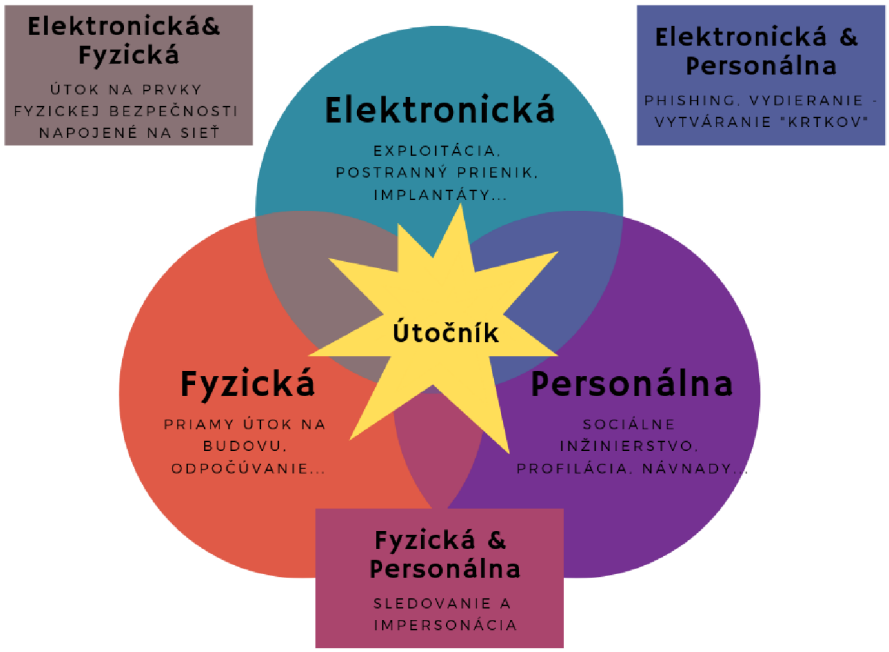
**Protipožiarne opatrenia** Zabezpečením v tomto ohľade sa myslia pokyny a prostriedky, ktoré zabraňujú požiaru, zmierňujú ho, alebo sa s ním nejakým spôsobom vyrovnávajú a to v prvom rade pre ochranu ľudského života a zdravia. Ako jediné z uvedených má detailne prepracované požiadavky, ktoré zákon vynucuje pre všetky (nielen) administratívne budovy. Tomuto aspektu sa teda v práci nevenujem,

1. Procedúrou pre účely tejto práce rozumieme presné postupy, ktoré sú vytvorené krok po kroku tak, aby ich mohol používať úplne každý. Procedúry sú spravidla veľmi špecifické pre danú organizáciu, jej časti, alebo používané zariadenia.

avšak chcem zdôrazniť jeho dôležitosť hlavne pri plánovaní fyzického zabezpečenia, ktoré nesmie byť v rozpore s požiarnou prevenciou a zároveň musí čo najviac ochrániť bezpečnosť aktív aj počas prípadného požiarneho poplachu.

## 1.1 Škálovanie bezpečnosti

V práci teda rozoberám aspekty fyzickej, infraštruktúrnej a personálnej bezpečnosti. Ako som už naznačil v úvode, problémom je aj malá pozornosť vzájomnému prepojeniu týchto oblastí a preto sa snažím, aby toto prepojenie bolo z mojej práce zreteľné.




Obr. 1.1: Ilustrácia vzájomného prepojenia elektronickej, fyzickej a personálnej stránky bezpečnosti s príkladmi útokov prezentovaná spoločnosťou *LARES Consulting*[4]

Napríklad princípy, ktoré opisujem pri personálnej bezpečnosti by boli úplne irelevantné, ak by nemali podklady v technickej realizácii prostriedkov, ktoré využívajú. Fyzické zabezpečenie by zas bolo

zbytočné riešiť, ak by sa personál správal k takýmto prostriedkom nesprávnym spôsobom.

Taktiež pri samotnom návrhu fyzických zabezpečovacích systémov sa neberie do úvahy, že často ide o informačné systémy, ktoré nejakým spôsobom využívajú okolitú infraštrktúru, ktorá je zároveň narušiteľná a útočník môže zneužiť aj tú. Tak sa v konečnom dôsledku využívajú zastaralé technológie, ktoré sú samy o sebe nebezpečné, no integrátori ich obľubujú, pretože sa svojou základnou funkcionalitou osvedčili časom.

Vzniká tak akési rozdrobovanie - škálovanie bezpečnosti, ktoré podľa mňa nefunguje. Každý si rieši svoju oblasť - programátori softvér, inžinieri zariadenia, personálni špecialisti ľudí, ale rôznym presahom pozornosť venovaná nie je.

V práci chcem ukázať, že všetky zo spomínaných oblastí nejakým spôsobom spadajú do oboru informatiky. Neviem si predstaviť, ktorému inému akademickému oboru ich priradiť v celej komplexnosti, ktorú spolu prezentujú. Veď v konečnom dôsledku ide o ochranu informácií.

# 2 Zdroje informácií pre zabezpečovanie

Kapitola obsahuje prehľad použitých materiálov týkajúcich sa informačnej a inej bezpečnosti. Predstavuje právne predpisy platné v Českej Republike normy a známe zdroje bezpečnostných chýb, ktoré je potrebné brať do úvahy pri vytváraní konkrétnych technických a organizačných opatrení. Niektoré materiály sa vzťahujú na ochranu utajovaných skutočností: daná oblasť je výkladnou skriňou rokmi osvedčených princípov zabezpečovania informácií. Tie môžu pomôcť aj spoločnostiam, ktoré s informáciami definovateľnými ako utajované skutočnosti nepracujú - ak považujú svoje aktíva za mimoriadne citlivé, nájdu tam veľmi užitočné postupy. Úskalím však je samotné utajovanie niktorých bezpečnostných štandardov, ktoré sa pri ohodnocovaní zabezpečenia podľa tejto legislatívy používajú. Pre firmu, ktorej zabezpečenie práca v druhej časti rieši však môžu byť vzhľadom na povahu jej zákaziek záväzné[1] Ich plnenie v plnom rozsahu však táto práca, pochopiteľne, neoveruje.

## 2.1 Zákon o kybernetické bezpečnosti

Zákon č. *181/2014 Sb.*[5] a s ním súvisiace vyhlášky[6][7] boli vytvárané v rokoch 2012 až 2014 vzhľadom na to, že do tej doby v ČR neexistovali dostatočné právne predpisy v tejto oblasti. Jedným z účelov zákona je stanovenie povinností správcom a prevádzkovateľom informačných systémov, ktoré sú v zákone deklarované ako kritická informačná infraštruktúra, významný informačný systém a významná sieť elektronických komunikácií. Najdôležitejšou z týchto povinností je zavedenie a vykonávanie širokého spektra bezpečnostných opatrení. Patria k nim aj prvky fyzickej, personálnej a infraštruktúrnej bezpečnosti. Zákon taktiež definuje a vyžaduje súčinnosť s národnými a vládnym CERT[2].

1. Spoločnosť rieši zákazky, ktorých súčasťou môže byť kontakt s utajovanými skutočnosťami. Konkrétnu spoločnosť, či jej zákazníkov táto práca z bezpečnostných dôvodov neobsahuje.
2. Computer Emergency Response Team - tím, ktorého úlohou je podľa zákona 181/2014 okrem iného vyhodnocovať nahlásené incidenty, poskytovať podporu a hodnotiť zraniteľnosti

Tieto opatrenia však pre väčšinu menších IT firiem nie sú záväzné - museli by spĺňať kritériá kritickej informačnej infraštruktúry podľa zákona č. 240/2000 Sb. a nariadenia vlády č. 432/2010 Sb.[8] resp. prevádzkovať priame pripojenie na inú kritickú informačnú infraštruktúru, alebo významný informačný systém[3]. Podnikatelia a organizácie sú povinné si overiť, či ich infraštruktúra tieto definície spĺňa.

Zákon sa zároveň nevzťahuje na na systémy, ktoré pracujú s utajovanými informáciami, čo je v §1 ods. 2 vyjadrené explicitne. Aj pre posudzovanú firmu však môže byť zákon podstatný, pretože nie všetky zákazky nutne implikujú prácu s utajovanými skutočnosťami a tým pádom môže systém, ktorého je zákazka súčasťou, spadnúť do pôsobnosti tohoto zákona. Ustanovenia týkajúce sa fyzickej a infraštruktúrnej bezpečnosti sa navyše nevylučujú s tými v legislatíve týkajúcej sa ochrany utajovaných informácií. V každom prípade považujem väčšinu opatrení spomenutých v zákone za dobrú prax.

## 2.2 Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti

Zákon č. *412/2005 Sb.*[3] a jeho vykonávacie predpisy predstavujú súbor mimoriadne komplexných opatrení na ochranu utajovaných informácií v ČR. Zákon bezpečnosť rozdeľuje na personálnu, priemyselnú, administratívnu, fyzickú, kryptografickú a bezpečnosť informačných, resp. komunikačných systémov. Priame opatrenia uvádzané v zákone považujem za excelentné. Zákon je v zásade postavený tak, že najslabším článkom pri vyšších stupňoch utajenia sú Národný Bezpečnostný Úrad s Národným úradom pre kybernetickú a informačnú bezpečnosť a ich proces certifikácie prostriedkov, systémov a pracovísk, resp. proces osvedčovania fyzických osôb a podnikateľov - čiže overovanie zákonom stanovených podmienok.

Tu však vidím jeden možný problém, ktorý som spomenul aj v úvode - nízka miera prepojenia aspektov. K presnejším technickým požiadavkám sa vyjadrujú vykonávacie predpisy: napr. pre fyzické prvky a informačné systémy uchovávajúce utajované informácie existujú samostatné vyhlášky[9][10] bez vzájomného prepojenia. Tak sa

3. Významný informačný systém predpokladá správu orgánom verejnej moci

môže stať, že certifikované zariadenie fyzickej bezpečnosti má z informatického hľadiska vážny problém[4]. Pritom napr. systém pre kontrolu vstupu by mal tiež spadať pod informačný systém uchovávajúci utajené informácie - jeho prístupové údaje sú podľa môjho názoru tiež súčasťou spôsobu zabezpečenia objektu, čo podľa nariadenia vlády[11] explicitne spadá pod utajované skutočnosti.

Samozrejme, vnútri týchto úradov a v organizáciách, ktorých je ČR súčasťou existujú aj utajované bezpečnostné štandardy, ktoré by to teoreticky mohli riešiť, avšak v tejto konkrétnej situácii je problém očividne koncepčný.

## 2.3 Rozhodnutie rady o bezpečnostných pravidlách na ochranu utajovaných informácií EU

Rozhodnutie *2013/488/EU*[12] je tiež súborom opatrení pre ochranu utajovaných informácií. Avšak týka sa informácií označených ako utajované informácie EÚ a je menej komplexné ako Zákon č. *412/2005 Sb.* Aj tak medzi českým a európskym prístupom nájdeme zaujímavé rozdiely: rozhodnutie rady napr. explicitne zakazuje prístup podnikateľov k utajovaným informáciám stupňa TOP SECRET, či neumožňuje prejsť previerkou fyzickým osobám, ktoré v minulosti preukázateľne užívali ilegálne omamné látky, alebo len zneužívali tie povolené. Rozdiel je aj v poňatí prenosu utajovaných informácií, ktorému sa venujem v časti *4.4*.

Ďalšou zaujímavosťou je, že v rámci ochrany informačných systémov rozhodnutie zavádza päticu ochranných línií pod názvom *hĺbková ochrana:* Odstrašenie, prevencia, odhaľovanie, odolnosť a náprava. Pritom odstrašenie vidíme skôr v normách a postupoch zameraných na fyzickú bezpečnosť. Takúto kombináciu opatrení považujem za prínosnú.

4. Konkrétnemu príkladu sa venujem v časti 3.2.1 - Rozvody a embedded zariadenia

## 2.4 Normy ISO 27000 - Systém riadenia bezpečnosti informácií

Rodina noriem ISO 27000 je súborom postupov a opatrení pre zavedenie vlastného systému riadenia bezpečnosti informácií (ďalej ISMS) spolu so samotnou normou označenou ako *ISO 27000*[13], ktorá slúži ako sprievodca celou rodinou. Zatiaľ čo *ISO 27002*[14] obsahuje všeobecnejšie požiadavky naprieč celým spektrom vrátane bezpečnosti ľudských zdrojov, fyzickej bezpečnosti, či prepravy médií a zariadení, detailne sa normy venujú len niektorým vybraným aspektom ako sú napr. siete v normách ISO *27033-x*[15].

Ako som spomenul, cieľom práce nie je vytvorenie kompletného ISMS, preto taktiež nie je cieľom dosiahnuť certifikáciu podľa *ISO 27001*, čo by bolo mimo rozsah bakalárskej práce. Zaujímajú nás hlavne povinné a odporúčané postupy v *ISO 27002*, ktoré čo najviac zvýšia bezpečnosť vrámci popisovaných aspektov.

## 2.5 Norma CEN/TS 14383-4 a normy z nej odkazované

Vzhľadom na fyzickú bezpečnosť a s ňou súvisiaci návrh budov a priestorov je pre nás najprínosnejšia norma *CEN/TS 14383-4*[16]. Zaoberá sa prevenciou kriminality pre obchodné a administratívne budovy. Norma samotná navrhuje ako hlavnú stratégiu dôslednú analýzu rizík a zraniteľností s následným vytvorením systému riadenia bezpečnosti. Sústreďuje sa hlavne na odstrašenie, zamedzenie, zdržanie a detekciu narušenia. Aj s pomocou odkazov na iné technické normy skúma široký rozsah aspektov bezpečnosti - návrh verejného priestoru, okolité budovy, tvar terénu, ochrana perimetru a plášťa budovy, stavebná línia, osvetlenie, možnosť vniknutia s využitím zariadení pre základné služby[5] a podobne. Taktiež odporúča konkrétne triedy odolnosti pre prvky ako dvere, okná, vložky, či elektronické zabezpečovacie systémy a kamerový systém. Okrajovo sa spomína aj fyzická ochrana výpočtovej techniky a vedenia.

5. Výťahové šachty, ventilácia a pod.

Norma trestné činy rozdeľuje na profesionálne vlámania a príležitostné lúpeže, pričom počíta s tým, že väčšina z nich spadá do druhej kategórie. Preto sa vo veľkej miere venuje aj obmedzeniu týchto náhodných činov návrhom verejného priestoru. Odporúča napr. oživenie priestoru prítomnosťou väčšieho množstva osôb, čo môže byť podľa môjho názoru kontraproduktívne pri ochrane od profesionálnych vlámaní - skúsený a motivovaný páchateľ môže ruch prostredia využiť.

Každopádne, norma je pre prácu aj vodítkom k ostatným normám, ktoré sa venujú jednotlivým prvkom fyzického zabezpečenia.

## 2.6 Zdroje informácií o známych bezpečnostných chybách a zraniteľnostiach

Z vlastnej skúsenosti viem, že firmy v oblasti IT málokedy testujú používané zariadenia na bezpečnostné riziká a spoliehajú sa na marketing, alebo certifikovaný bezpečnostný stupeň. Bezpečnostné chyby v informačných systémoch, ale aj iných zariadeniach však môžu byť dôležitou súčasťou trestných činov či už náhodných, alebo motivovaných. Lenže aj samotné spoločnosti poskytujúce zabezpečovacie riešenia sa k bezpečnosti samotných zariadení často stavajú laxne až bizarne. Preto je dôležité investovať čas do skúmania podrobností o zakúpenom riešení a zisťovania možností, ktoré potenciálny útočník má.

Najzákladnejším zdrojom sú určite verejné databázy zraniteľností *CVE*[6]. Pri kúpe zariadenia je veľmi dôležité overiť si, či verzia nainštalovaného softvéru netrpí zraniteľnosťou využiteľnou útočníkom. K mnohým z nich totiž existujú exploity, ktoré sú extrémne jednoducho použiteľné aj amatérmi. Asi najpoužívanejšou je databáza[17] spravovaná spoločnosťou *Offsec Services Ltd.*

Ďalším užitočným zdrojom je znalostná báza *MITRE ATT&CK*[18]. Ide o unikátnu štrukturovanú maticu známych techník útokov zasadených do štádia, v ktorom sú nasadzované. To umožňuje postupné vytváranie vrstiev bezpečnosti odolných voči daným technikám.

Skvelým príkladom sú aj konferencie ako *Black Hat Briefings, DEF CON, Hacktivity, Wild West Hackin' Fest* a pod. Na tých sú predvádzané zraniteľnosti zneužiteľné v mnohých oblastiach, pričom veľká časť z

6. Common Vulnerabilities and Exposures

nich sa niekedy nedostane ani do databázy *CVE*. Na videá z podobných konferencií sa budem odkazovať často, keďže informácie v nich obsiahnuté zväčša nie sú nikde zhrnuté vo forme akademického, či vedeckého textu. Podľa môjho názoru by sa mal človek zodpovedný za vytváranie bezpečnostnej politiky vzdelávať aj na tomto poli.

Nemenej dôležité sú aj čisto mechanické prvky ako zámky. Pri výbere je podstatné sa pozerať nie len na marketing a certifikovanú triedu odolnosti, ktorá hovorí o odolnosti voči násilným formám vlámania. Lockpicking[7] je obľúbenou zábavou mnohých etických hackerov, ale aj páchateľov. Preto je dobré všímať si informácie od profesionálov aj v tomto obore.

Tu však zoznam z ďaleka nekončí. Navyše, aj najlepší zámok, prístupový systém či iné elektronické zabezpečovacie zariadenie je bezcenné, ak samotná implementácia umožňuje ich obídenie, alebo dokonca zneužitie.

7. Nenásilná a nedeštruktívna metóda otvárania zámkov

# 3 Hrozby a výzvy pri zabezpečovaní firmy

Návrh správnej bezpečnostnej politiky by mal podľa väčšiny štandardov a frameworkov začínať identifikáciou dôležitých aktív a následne odhadom súvisiacich hrozieb, ich pravdepodobností a možných dopadov. Tento postup predpokladá znalosť možných hrozieb, čo môže byť problém a preto som sa rozhodol niektoré z nich opísať. Táto kapitola prevedie ukážkou malej časti možných spôsobov narušenia bezpečnosti vrámci vybraných aspektov a to z pohľadu podobne motivovaného útočníka, ktorý sa snaží čo najlepšie využiť okolnosti, ktoré mu úroveň zabezpečenia jeho cieľa poskytuje - aj takto chcem zdôvodniť na prvý pohľad možno prehnanú úroveň princípov, ktoré opisujem v následujúcej kapitole.

## 3.1 Fyzická bezpečnosť

V prípade menších firiem a organizácií zabezpečenie ďaleko zaostáva za ukážkovými príkladmi ako sú dátové centrá *Microsoft Azure*[19], alebo budova Národného úradu pre kybernetickú a informačnú bezpečnosť na ulici Mučednická v Brne[1]. Naopak, často úplne chýba akékoľvek riešenie mimo jednoduchého zámku vo dverách, či nanajvýš základného zabezpečovacieho systému v podobe niekoľkých pohybových senzorov, pričom sa jedná o najsilnejšie články. Preto som názoru, že fyzická bezpečnosť je najčastejšie prehliadanou a podceňovanou.

### 3.1.1 Neoprávnený prienik do objektu a oblastí

Motivovaný útočník ako jednu z prvých zvažuje možnosť preniknúť do priestorov, v ktorých sa hľadané aktíva fyzicky nachádzajú. To je mimochodom potrebné riešiť aj pre prevenciu náhodných krádeží, keďže techniky spomínané nižšie sú jednoduché na použitie.

V prípade neverejnej budovy sa útočník najprv presvedčí, či je možné sa cez perimeter dostať k jej plášťu. Vzhľadom na nízky pomer malých a stredných IT firiem sídliacich v podobných priestoroch, ne-

1. Z viditeľných prvkov má budova napr. kamerami pokrytý celý perimeter s veľkou mierou redundancie.

budem sa prieniku cez perimeter podrobne venovať, idem teda opísať časté chyby, ktoré umožňujú neautorizovaný vstup za ním.

**Nechránený plášť** Pozornosť pri zabezpečovaní sa často uberá len na hlavný vchod. Vedľajšie vchody, okná, balkóny, strešné otvory a pod. sa však dajú pre vstup použiť tiež. Prípadné ozdobné a technické prvky na plášti budovy to, samozrejme, uľahčujú.

Napríklad Okná typu *Tilt & Turn*[2] otvorené náklonom je veľmi jednoduché z vonku otvoriť tak, aby bol vstup možný. Aj pri úplne zatvorenom okne existuje primitívna cesta ako ho otvoriť - vyvŕtaním menšej diery, cez ktorú sa vmestí nástroj, ktorý pohne kľučkou. Zásah je síce čiastočne deštruktívny, ale pomerne dobre maskovateľný. Navyše, v norme *EN 1627*[20] (a súvisiacich), z ktorej sa určuje u nás používaná klasifikácia odolnosti nie je o podobnom útoku ani zmienka. Pritom je možné si kúpiť špecializovaný nástroj[3] pre tento účel. Zraniteľnosť sa týka aj balkónových dverí, keďže v našich končinách fungujú na rovnakom princípe. Balkón navyše útočníkovi ponúka väčší komfort v podobe zákrytu.

Využiť sa dajú aj ostatné otvory ako sú šachty, ventilácia, či garážové dvere. Pri starších budovách môže útočník zvažovať aj dvierka pre uhlie, výťah, miestnosť s kontajnermi, prípadne núdzové východy a výlezy z krytu. Všetky bývajú zabezpečené maximálne tak jednoduchým visiacim zámkom a čo je horšie - z vonkajšej strany. Navyše doba detekcie deštruktívneho narušenia je vzhľadom na frekventovanosť týchto miest podstatne predĺžená.

**Zabezpečenie vstupu** To, že väčšina vložiek zámkov je premožiteľná som už naznačil. Lockpicking, ale aj jednoduchšie odvŕtanie umožňuje útočníkovi dostať sa cez podobnú prekážku s menšou námahou, pričom v prvom prípade tiež neexistuje používaná norma, ktorá by ho riešila. Lenže nepodarená inštalácia, niektoré prvky návrhu a zlé návyky ponúkajú iné možnosti prieniku aj za predpokladu, že by bola vložka dokonalá.

---

2. Druh okien, ktoré sa dajú otvoriť aj náklonom ("vetračka") aj otočením ("dokorán") - rozšírený hlavne v Európe
3. Nástroj je možné nájsť pod názvom *WOPER* napr. na shop.multipick.com

Jedným z častých zvykov, ktoré si všímam je združovanie kľúčov na jednom mieste so zabezpečením slabším, ako majú priestory ktoré majú byť príslušnými zámkami chránené. Často ide o presklenné[4] skrinky vo verejných priestoroch, vrátnice, alebo zázemie pre upratovaciu službu, ktorá máva k dispozícii generálny kľúč k viacerým častiam objektu.

Dôsledkom zlého návrhu sú napr. škáry medzi dverami a rámom umožňujúce takzvané útoky pod dvere a nad dvere - primitívnymi nástrojmi je bez väčšej námahy možné pohnúť kľučkou, či nárazovou lištou na druhej strane, rafinovanejšími aj otočiť olivou[5] vložky. Známejším príkladom je obyčajné vypáčenie jazýčka, ktoré je umožnené hlavne zlou inštaláciou dverí - vtedy nepomôže ani pokročilý zapadací systém[22].

**Elektronické prístupové systémy** Sú osobitnou kategóriou s viacerými slabinami. Jednou z nich je *REX*[6] v kombinácii s nedostatočným utesnením a nesprávnym nastavením. Infračervené *REX* senzory je možné spustiť studeným oblakom média z aerosólových sprejov, zatiaľ čo u nás populárnejším mikrovlnným radarom stačí kus odrazivého materiálu[23].

Ďalším častým problémom je jednoducho prístupná elektronika systému[22] - sama je nedostatočne zabezpečená proti fyzickému útoku. Okrem priamej manipulácie je možné napríklad implantovať zariadenie zachytávajúce autentifikačné údaje z bezkontaktného čipu. K tomu môže pomôcť aj použitá technológia - napr. čipy založené na 125 kHz technológiách ako *EM4100*, alebo *HID Prox* je extrémne jednoduché skopírovať a zároveň sú veľmi populárne.

### 3.1.2 Monitorovanie priestorov - detekcia narušenia

Ak útočník úspešne prenikne do oblasti, prácu mu môžu narušiť elektronické zabezpečovacie systémy (ďalej EZS). Tie pozostávajú z viacerých zaužívaných technológií, z ktorých najpoužívanejšie tiež majú svoje slabiny.

---

4. Vo veľa prípadoch stačí na vytvorenie funkčnej kópie kľúča jeho fotografia[21]
5. Rukoväť na vnútornej strane niektorých vložiek
6. Request-to-exit - systém, ktorý umožňuje automatické otváranie dverí na základe pohybu

**Magnetické detektory** Používajú sa na prvotnú detekciu narušenia - výstup jazýčkového spínača z magnetického poľa spôsobí prerušenie obvodu, čo vyústi v alarm. Detektory bez, alebo s nízkym stupňom certifikácie podľa EN 50131-2-2 môžu byť náchylné na rušenie externým magnetickým poľom a teda ich efektívne blokovanie.

**Detektory pohybu** Podobne, ako pri REX systémoch sú asi najpoužívanejšími technológiami pasívny infračervený snímač (*PIR*) a mikrovlnný radar (*MW*), prípadne ich kombinácia. Známou technikou proti *PIR* je tepelné maskovanie, pričom útočník musí dbať na to, aby maskovanie vyžarovalo rovnakú intenzitu infračerveného svetla (malo rovnakú teplotu) ako pozadie, cez ktoré prechádza. Najčastejším spôsobom je práve využitie prostredia. Ďalšou možnosťou je zakrytie senzoru, či zníženie detekčného rozsahu.

*MW* radar detekuje dopplerov efekt, rovnako ako staršie ultrazvukové radary, ktoré je možné prekonať obyčajnou textíliou pohlcujúcou vyššie frekvencie zvuku. Podobne existujú špecializované a zároveň dostatočne flexibilné materiály schopné pohltiť *MW* žiarenie. Navyše radar pochopiteľne nedeteguje pohyb, pri ktorom sa vzdialenosť od neho nemení. Techniky sú dokonca známe aj medzi verejnosťou, za čo môže aj popularizácia seriálom *MythBusters*[24].

Kombinácia technológií má zväčša zabrániť falošným poplachom, takže na spustenie alarmu musí prebehnúť detekcia v oboch naraz. Útočníkovi teda stačí oklamať jeden z nich. Častým problémom je taktiež nesprávna inštalácia umožňujúca preplazenie mimo rozsahu detektoru.

**Centrálne jednotky - ústredne** Ich úlohou je spracovať udalosť z detektorov a následne informovať autorizovanú osobu, či pult centrálnej ochrany. Základné ústredne však tiež majú slabiny, a to hlavne v externom pripojení, kedy je detekcia sabotáže negatívne ovplyvnená absenciou záložného napájania, či použitou technológiou[21]:

**Pripojenie pevnou linkou** Zastaralý spôsob - ústredňa, resp. komunikátor ako detekciu sabotáže využíva meranie napätia v pripojenej telefónnej sieti, zatiaľ čo pult centrálnej ochrany vo väčších časových intervaloch kontroluje, či je zariadenie pripojené.

Útočník tak môže prepojiť ústredňu na externý zdroj a pokojne vyvolať poplach.

**Pripojenie cez *GPRS*[7]** Slabinou je známy komunikačný protokol v kombinácii s absenciou šifrovania a IMSI Catcherom[8] Útočník môže kontrolovať komunikáciu a zabrániť odoslaniu udalosti do pultu centrálnej ochrany.

***CCTV* - kamerové systémy** Sú dobrým príkladom prieniku so zabezpečením infraštruktúry, keďže po prístupe do siete, v ktorej sa kamery nachádzajú sa útočníkovi otvárajú zraniteľnosti, ktorými veľká časť IP kamier, ale aj nahrávacích systémov trpí[25]. Z príkladov môžem spomenúť zvyk výrobcov vkladať zadné vrátka s preddefinovanými prístupovými údajmi, ktoré je možné vyčítať z firmvéru zariadenia, alebo možnosť priam až filmového podvrhnutia živého obrazu.

### 3.1.3 Odpočúvanie

Ide o skvelý spôsob, akým sa dajú získať či už prvotné aktíva, ktoré útočníka zaujímajú, alebo údaje, ktoré ho k ním dostanú. Možností je viacero - zachytávanie zvuku, obrazu, bezdrôtových technológií (*GSM*, *Wi-Fi*, bezdrôtové klávesnice a myši), vysielačiek a pod. Pokročilejšia metóda je tzv. Van Eck phreaking, čo je zachytávanie nezámerných elektromagnetických emisií zo zariadení a ich následná rekonštrukcia v pôvodné dáta. Najznámejším príkladom sú staré *CRT*[10] obrazovky. Ale úspešné útoky už boli referované[26] aj pre kryptografický hardvér, klávesnice, čipové karty, mikroprocesory a iné zariadenia, pričom bolo možné informácie získať z niekoľkých metrov aj pri ochrane výrazným elektromagnetickým tienením. Niektoré z týchto útokov boli uskutočnené vďaka skúmaniu zmeny napätia pri napájaní zariadení.

---

8. Zariadenie schopné *MiTM*[9] útoku pre GSM siete. Navzdory všeobecnému presvedčeniu je jeho postavenie záležitosťou nízkych desiatok tisícov korún.
10. Cathode ray tube - technológia využívajúca pulzujúci lúč elektrónov pre vybudenie fosforových pixelov vykresľujúcich obraz

### 3.1.4 Prepojenie s personálnou a infraštruktúrnou bezpečnosťou

Personál z pravidla disponuje kľúčom (vo všeobecnom slova zmysle) k objektu. Mnohé z nich je jednoduché skopírovať - či už fyzické kľúče[27], alebo už spomínané bezkontaktné čipy. Je možné sa k ním dostať viacerými spôsobmi - či už vlámaním do obydlia zamestnanca, sledovaním[11], využitím nepozornosti a pod. Pri iných technológiách sa dajú použiť aj pokročilejšie útoky diaľkovým prenosom komunikácie[29]. Alebo môže stačiť sociálnym inžinierstvom presvedčiť personál, aby útočníkovi prístup poskytol sám. Aj odpočúvanie personálu je pre útočníka jednoduchšie mimo zabezpečené priestory organizácie.

Súvislosťou s dátovou infraštruktúrou môže byť sprístupnenie vnútornej siete cez fyzicky prístupnú elektroniku a rovnako je možné po prvotnom prístupe do siete niektoré elektronické prístupové systémy zneužiť bez fyzického prístupu k nim[30]

Mimochodom, ak hovoríme o fyzickej bezpečnosti, musíme brať do úvahy aj podporné služby a kritickú infraštruktúru - pripojenie do elektrickej siete, vodu, či plyn. Útočník môže zvažovať sabotáž ako spôsob vyhnutia sa detekcie neoprávneného prieniku, zničenia dôkazov, alebo priameho poškodenia organizácie.

## 3.2 Zabezpečenie dátovej infraštruktúry

Podľa môjho názoru sa tiež jedná o súčasť organizácie, ktorej riziká nemajú dostatočné povedomie nielen medzi manažmentom IT firiem. Stretávam sa skôr s názorom, podľa ktorého by mal byť k rozvodom a koncovým bodom čo najjednoduchší prístup, aby sa mohli napr. opravy vykonávať bez zdržania, ktoré manažéri označujú za zbytočné. To však môže mať veľmi nepríjemné dopady.

V sekcii sa dátovej infraštruktúre venujem hlavne z pohľadu možného úniku dát, alebo jej zneužitia. Ako som však spomenul pri fyzickej bezpečnosti, zničenie je tiež možnosť a absencia záložných spôsobov komunikácie medzi zariadeniami môže spoločnosť poškodiť.

---

11. S bezkontaktnými čipmi je v kombinácii s výkonnými čítačkami[28] možné komunikovať aj na vzdialenosť 1 m, dajú sa skopírovať od okoloidúceho človeka bez toho, aby si to všimol

### 3.2.1 Rozvody a embedded zariadenia

Zabezpečenie rozvodov hlboko súvisí s fyzickou bezpečnosťou - ťažko si predstaviť závažnejšiu hrozbu, ako priamy prístup k nim. A preto je veľa zraniteľností spôsobených absenciou dodatočnej vrstvy fyzickej ochrany vrámci zabezpečenej oblasti, alebo aj mimo nej. Tento problém je často v starších budovách, pri ktorých stavbe nepočítalo s umiestnením väčšieho množstva káblov. Útočník môže svoje zariadenie napojiť priamo na kabeláž v rozvodoch, rozvodových skriniach a miestnostiach, alebo v koncových bodoch a z bezpečnej vzdialenosti postupovať v zamýšľanom útoku.

Problémom sú taktiež zásadné chyby v embedded zariadeniach ako sú ovládacie panely klimatizácie, interkomy, komunikátory a ústredne EZS a pod.

Ako príklad zneužitia vstavaného zariadenia môžem uviesť vlastný etický útok[30] vrámci internátu univerzity, ktorého vstupným vektorom bol veľmi zle zabezpečený *elektronický mincovník* určený pre platby za pranie. Po ovládnutí zariadenia som na diaľku skúmal sieť, v ktorej operuje a zistil, že sú na nej aj zabezpečovacie systémy budovy vrátane prístupového systému, ktorý nešifrovane posielal holé čísla kariet priložených k čítačke. K tým som následne mohol priradiť identitu vďaka rozhraniu `Úschovňa` v informačnom systéme univerzity. Keďže vstupy do budov a aj niektorých oblastí sú vrámci univerzity založené na týchto kartách a ľudia bývajúci na danom internáte môžu mať prístupové práva aj do iných, umožňuje mi to získať tam prístup tiež. Taktiež je to využiteľné na sledovanie pohybu osôb. Nemenej podstatná je aj možnosť využiť prvé spomínané zariadenie pre vlastnú útočnú činnosť vzhľadom na jeho neobmedzený prístup do internetu. Navyše, kvôli absencii sond na tejto sieti a jednoducho možnému vymazaniu dôkazov zo zariadenia by sa po odhalení zneužitia veľmi ťažko pri forenznej analýze zisťoval vstupný vektor. Ide o dobrý príklad zlyhania viacerých aspektov bezpečnosti na viacerých úrovniach.

Zaujímavým je aj fakt, že dané prístupové zariadenie[12] je na zozname certifikovaných technických prostriedkov Národného Bezpečnostného Úradu[31]. Samozrejme, záleží na konkrétnej implementácii, avšak dodávateľ sa v tomto prípade de facto spolieha na dokonalé zabezpečenie samotnej siete.

12. Honeywell NetAXS-123

Ak sú sieťové rozvody a zariadenia dostatočne fyzicky chránené pred priamym napojením a manipuláciou, stále by mohli byť hypoteticky cieľom spomínaného Van Eck phreakingu, aj keď som v dostupných zdrojoch nenašiel zmienku o úspešnom rekonštruovaní sieťovej komunikácie z elektromagnetických emisií.

### 3.2.2 Prístup na sieť

V súvislosti s predchádzajúcou podkapitolou je jasné, že nechávať odhalené fyzické sieťové prvky nie je dobrý nápad. Ak takáto sieť nie je chránená autentifikáciou a vzájomnou izoláciou klientov, útočníka od kompromitácie informácií delí len zabezpečenie vzdialených služieb na konkrétnych strojoch a bez ochrany proti podvrhnutiu *DHCP*[13] a *ARP*[14] môže útočník pohodlne prevádzkovať *MiTM* útok.

Rovnako vďačným cieľom sú siete *Wi-Fi*. Zatiaľ čo prevádzka nezabezpečenej bezdrôtovej siete, alebo využitie zastaralých protokolov ako je *WEP*[15] je v dnešnej dobe samozrejmá nezodpovednosť, dôležité slabiny majú aj vo veľkom používané algoritmy *WPA2*[16].

V prípade *WPA2-Personal* existuje technika[33], ktorá útočníkovi v špecifických (ale za to častých) prípadoch umožňuje čiastočný *MiTM* útok bez znalosti hesla.

WPA2-Enterprise v kombinácii s autentifikačnými protokolmi *EAP-LEAP* a *MS-CHAPv2* dokonca umožňuje[34] úplné odhalenie[17] údajov potrebných pre autentifikáciu. Vzhľadom na predvolené nastavenie väčšiny klientov[18] nepomôže ani *EAP-TLS* - túto kombináciu využíva napríklad služba *eduroam*.

---

13. Dynamic Host Configuration Protocol - protokol, ktorý priraďuje IP adresy pripojeným klientom. V prípade, že switche nefiltrujú DHCP odpovede z klientských portov, sieť je náchylná na ich podvrhnutie.
14. Address Resolution Protocol - protokol, ktorý prekladá IP adresy na MAC adresy. Keďže dotazy a odpovede nie sú nijako previazané, sú jednoducho podvrhnuteľné.
15. Wired Equivalent Privacy - zabezpečovací algoritmus pre bezdrôtové siete. Je preukázateľne slabý[32] a zastaralý.
16. Wi-Fi Protected Access II - protokol zabezpečenie Wi-Fi, náhrada za *WEP*. Skladá sa z troch protokolov pre distribúciu kľúčov označovaných ako Personal, Enterprise a WPS.
17. V prednáške spomínaná služba umožňujúca z tokenu získaného nástrojom chapcrack zistiť akýkoľvek MD4 hash hesla z MS-CHAPv2 v priebehu jedného dňa aktuálne beží na adrese `https://crack.sh`
18. Nevyžadovanie a neoverovanie certifikátu

Keďže získať prístup na niektorú zo sietí môže byť pomerne jednoduché, používanie jednej, ale aj viacerých (avšak fyzicky prepojených) sietí vrámci celej organizácie so sebou nesie určité riziká v podobe viacerých techník[35] postupného prieniku.

## 3.3 Personálna bezpečnosť

Ľudský faktor je mnohokrát spomínaný ako najslabší článok bezpečnosti organizácie. Je podrobne skúmaný a jeho vplyv je do veľkej miery známy. Že by sa z týchto nespočetných výskumov firmy poučili sa však povedať nedá. V prieskume[36] Ponemon Institute až 78% organizácií uviedlo, že sa u nich za posledné dva roky vyskytol únik dát zavinením zamestnanca, alebo spolupracovníka (ďalej budem používať spoločné označenie personál). Pritom iba 8% uviedlo, že hlavnou príčinou únikov za rovnaké obdobie bol externý kyberútok. Oveľa častejšími boli uvádzané straty zariadení, zle zaobchádzanie s dátami, či úmyselné konanie. Navyše, iba 19% únikov bolo nahlásených priamo zodpovedným personálom. Organizácie si pritom tento problém uvedomujú - až 60% priznalo, že ich bezpečnostné procedúry nie sú dostatočné pre zastavenie úniku dát či už z nedbalosti, alebo úmyselnej činnosti personálu.

Ak aj organizácia má zavedené bezpečnostné procedúry, zamestnanci majú tendenciu niektoré z nich výraze podceňovať. Špeciálne ma v tomto prieskume zaujali dve pozorovania: Aj keď veľkosť organizácie ovplyvňuje nebezpečné správanie sa zamestnancov, rozdiel je minimálny a až 41% z nich uviedlo, že niektorí zamestnanci vôbec nerozumejú zavedenej bezpečnostnej politike.

Nebezpečné správanie môžeme na vyššej úrovni rozdeliť do dvoch základných kategórií: neúmyselné - spôsobené nedbanlivosťou alebo nevedomosťou a úmyselné - také, ktoré predpokladá nejaký druh motivácie pre záškodnícku činnosť.

### 3.3.1 Neúmyselné narušenie

Nejakú formu neúmyselného narušenia podľa spomínaného prieskumu citovalo najviac organizácií ako hlavný dôvod úniku informácií. Vyberám niektoré z častých alebo závažných príkladov nebezpečného

správania sa, pričom vychádzam zo spomínaného prieskumu, prednášok[22][21][37] a vlastných skúseností:

**Zbytočné prenášanie a ponechávanie dát** Straty USB flash diskov obsahujúcich citlivé informácie si personál často nevšimne, ani nenahlási. Problémom je aj samotné prenášanie dát (akýmikoľvek prostriedkami) mimo priestory organizácie keď sa to nevyžaduje, ich držanie doma, či ponechávanie na zariadeniach keď už nie sú potrebné pre prácu. Útočník tak môže pri dlhodobejšom sledovaní zamestnanca nájsť spôsob, ako tieto dáta ukradnúť. Možnosťou je aj vlámanie sa do jeho obydlia a skopírovanie údajov, pričom si to nikto nikdy nemusí všimnúť.

**Zlá práca s prihlasovacími údajmi** Členovia personálu vytvárajú slabé heslá, používajú rovnaké vo viacerých systémoch, nemenia ich dostatočne často, alebo ich držia v nezabezpečenej podobe. Veľká časť heslá dokonca zdieľa so spolupracovníkmi. Útočníkovi rovnaké prihlasovacie údaje na viacerých miestach veľmi nahrávajú pri postupnom prieniku sieťou.

**Ponechávanie informácií prístupnými na pracovisku** Personál citlivé dokumenty ponecháva bez dozoru na stole a na iných miestach a nezamyká počítače s prístupom k dátam. Útočník, ktorý nejakým spôsobom dostal do priestorov tak môže využiť nepozornosť. Zaujímavé informácie sa môžu nachádzať aj napr. v tlačiarni - fyzicky, alebo v podobe tlačovej fronty.

**Používanie súkromných zariadení na prácu, alebo v práci** To zvyšuje riziko najmä za predpokladu, že pracovné zariadenia podliehajú prísnej kontrole a zvýšeným bezpečnostným pravidlám. Súkromné zariadenia môžu byť napadnuté, čo sa môže prejaviť nielen priamym únikom dát, ale aj zneužitím siete. Taktiež na nich môžu ostávať citlivé údaje, o ktorých nemá personál vedomosť. S tým súvisí aj samotné zvýšené riziko, že sa neznalý používateľ stane obeťou malvéru. Ak útočník vie o takejto činnosti zamestnanca, môže zariadenie využiť ako skratku.

**Používanie zariadení na nezabezpečenej sieti** Personál sa tým vystavuje riziku MiTM útoku, alebo využitia zraniteľnosti zariadenia.

**Používanie sociálnych sietí a verejných služieb pre pracovné účely** Zvyšuje sa tak možný povrch pre útoky, ktoré vyústia v kompromitáciu informácií. Útočník môže preniknúť na účet niektorého zo zamestnancov veľa spôsobmi - napr. aj využitím iného zariadenia prepojeného so sociálnou alebo cloudovou službou, ktoré nie je pod dohľadom.

**Podľahnutie sociálnemu inžinierstvu, neoverovanie identity** Nedostatočné bezpečnostné pravidlá a osveta dávajú za vznik situáciám, kedy sa personál rozhodne dôverovať útočníkovi vydávajúcemu sa za autorizovanú osobu a poskytnúť mu elektronický, alebo fyzický prístup k dátam, alebo zariadeniam. Vystupovanie napr. za servisného pracovníka za účelom fyzického prieniku do oblastí je obľúbenou a často úspešnou stratégiou profesionálnych pentesterov, alebo ľudí ktorí sa s dobrými úmyslami potrebujú urýchlene dostať do objektu[19]. A s rovnakou eleganciou to môže využiť aj profesionálny útočník.

**Nenahlasovanie a neoverovanie podozrivých aktivít** Podozrivou aktivitou môže byť napr. pohyb neznámych osôb bez sprievodu, či neohlásené konštrukčné a stavebné práce. To všetko môžu profesionálni útočníci využiť ako pokus splynutia s prostredím. Aj zvláštne správanie sa personálu môže byť kľúčové pri odhaľovaní úmyselného narušenia.

### 3.3.2 Úmyselné narušenie

Podľa výskumu založenom na ohlásených zločinoch vrámci americkej FBI[38] sa personál dopúšťa širokého spektra zločinov voči svojim zamestnávateľom: ničenie majetku, finančné podvody, sprenevera, krádež intelektuálneho aj fyzického majetku a pod. V prípadoch úmyselnej aktivity vyúsťujúcej k narušeniu bezpečnosti informácií musíme brať do úvahy motiváciu, ktorá za takýmto konaním je a zároveň chyby v bezpečnostnej politike a procesy, ktoré mu to umožňujú.

**Motivácia** Pri skúmaní motívu pracovníka so zlým úmyslom ho môžeme rozdeliť na nedobrovoľný a dobrovoľný. V prvom prípade hovoríme o motíve, s ktorým potenciálny páchateľ nie je plne stotožnený a teda o náchylnosti k ovplyvneniu nátlakom, vydieraním, zastrašovaním a pod. K tejto náchylnosti môže prispieť napr. zadĺženie, psychické problémy, či aféry.

Motívom, s ktorým je páchateľ stotožnený môže byť napr. vidina zárobku, vernosť konkurenčnej firme, alebo inej krajine - dosadenie personálu špeciálne pre účely špionáže, alebo vlastný záujem poškodiť spoločnosť, povedzme z pomsty alebo kvôli nespokojnosti v práci. Spomínaný výskum ako možné motívy spomína aj dobrodružnú povahu, deštruktívne správanie sa, alebo aj túžbu potešiť niekoho, kto by mal z takého konania prospech. Netreba podceňovať ani ideológiu, či pocit príslušnosti k skupine s nejakými záujmami.

Dôležitým faktorom je aj perspektíva daného zamestnanca o tom, aké jednoduché je zločin vykonať a ako jednoducho môže uniknúť jeho zisteniu a prípadnému trestu[2].

### Praktiky a situácie umožňujúce úmyselné narušenie

**Chýbajúce, alebo nedostatočné pravidlá** Problémom je hlavne absencia pravidiel týkajúcich sa nakladania s citlivými informáciami ako napr. ich označovanie, pohyb po objekte a kontroly pri jeho opúšťaní, resp. opatrenia proti všetkým vyššie spomenutým rizikám správania sa zamestnancov. K tomu patria aj pravidlá pre neštandardné situácie. Zamestnancovi so zlými úmyslami hrá do karát aj samotný prístup k informáciám, ktoré vôbec nepotrebuje pre svoju prácu.

**Nedostatok povedomia, tréningu a motivácie** Analýzy[39] prípadov priemyselnej špionáže poskytujú príklady zamestnancov, ktorí až po zatknutí a vypočúvaní prezradili, že si všimli podozrivého správania sa spolupracovníkov, ale nepovažovali to za dostatočne významné pre nahlásenie, alebo nechceli byť pred spolupracovníkmi za donášača. Tak to vyzerá, keď bezpečnostná politika spoločnosti nezahŕňa dostatočné školenie a vytváranie povedomia o možných hrozbách zo strany personálu. Riziko nebezpečného zaobchádzania s aktívami sa zvyšuje aj ak zamestnanci nie sú plne stotožnení so sa-

motnou potrebou bezpečnostných pravidiel, alebo nie sú motivovaní k ich dodržiavaniu.

**Dočasný chaos, alebo nátlak** Určitou hrozbou sú aj situácie, ktoré vznikajú v dôsledku zmien vedenia, alebo inej reštrukturalizácie organizácie, ktoré zaneprázdňujú manažment. Taktiež sa môže v dôsledku podobných zmien stať, že zamestnanci dostanú vyššie privilégiá, ako potrebujú[2]. Podobné dočasné vákuum v zabezpečení môže nastať aj pri časovom strese zamestnancov, ktorí tak nemajú potrebný komfort pre dodržiavanie bezpečnostných pravidiel, čo v konečnom dôsledku spôsobí ich nedodržanie či už vedome, alebo nevedome.

# 4 Princípy zabezpečovania

Bezpečnostná politika by mala byť na mieru nastavená pre každú organizáciu. Z požiadaviek v normách plných podmieňovacích spôsobov, či zákonov a vyhlášok s bodovacími systémami sa však často nedá vychádzať samostatne - poskytujú príliš veľkú slobodu. Preto v tejto kapitole vytváram nižšiu úroveň abstrakcie, na ktorej sú princípy z viacerých zdrojov skombinované a špecifikované špeciálne pre účely spoločnosti vyvíjajúcej softvér a vyžadujúcej ich vysoký štandard.*Väčšina základov pre tieto princípy je založená na zdrojoch, ktoré boli uvedené, alebo odkazované v predchádzajúcich kapitolách.*

Princípy sú síce rozdelené do kategórií, avšak pri ich vytváraní bol braný výrazný ohľad na vzájomné prepojenie. Je potrebné upozorniť, že princípy sú stále na relatívne vysokej úrovni abstrakcie a procedúry určujúce konkrétne postupy pri plnení politiky sa už naozaj musia vytvárať na mieru. K tomu je nutné pridať kategóriu všeobecných požiadaviek pri vytváraní projektu bezpečnosti, ktorá rozoberá kto a akým spôsobom má tieto procedúry vytvárať a ako docieliť, aby boli vôbec efektívne.

Taktiež považujem za potrebné ešte raz upozorniť, že práca nerozoberá všetko. Nedostávam sa napríklad na detailnú úroveň softvérového zabezpečenia vrámci informačného systému, či protipožiarneho zabezpečenia. Pri vytváraní komplexnej politiky je však potrebné uvažovať aj to - prepojenie všetkých aspektov nikdy nemôže byť dostatočne zdôraznené.

## 4.1 Všeobecné požiadavky pre projekt bezpečnosti

Samotné vytváranie a implementácia a udržiavanie politiky a procedúr majú svoje špecifiká, ktoré je potrebné adresovať. Medzi tie patrí vytvorenie tímu, klasifikácia informácií, kontrola dodržiavania pravidiel a pod.

### 4.1.1 Bezpečnostný tím

Tím, ktorý má na starosti zavádzanie a udržiavanie bezpečnostnej politiky a procedúr je tým najdôležitejším prvkom pri vytváraní a implementácii projektu bezpečnosti. Tento tím:

- je plne stotožnený s potrebou riešiť zabezpečenie,
- má lídra, ktorý zadáva jasné ciele a kontroluje celý proces,
- pozostáva z profesionálov vo viacerých oblastiach, ktorí vyhľadávajú a vyhodnocujú aktuálne informácie o možných hrozbách, porovnávajú ich s aktuálnym zabezpečením a podnikajú kroky k náprave,
- identifikuje a klasifikuje informácie a iné aktíva podľa najhoršieho možného dopadu pre spoločnosť po narušení ich bezpečnosti,
- vytvára politiku a procedúry a to úplne presne, tak, aby nevznikla žiadna pochybnosť o zamýšľanom význame,
- vytvára politiku a procedúry aj pre krízové a špeciálne situácie ako sú prírodné katastrofy, či podozrenie na únik informácií,
- určuje a kontroluje technickú realizáciu zabezpečenia vrátane identifikácie osôb a aktív, či riadenia prístupu (fyzického, či logického)
- určuje kto, kedy a ako vykonáva kontroly fyzického zabezpečenia, infraštruktúry a iných,
- určuje, kto, kedy a ako získava, resp. stráca prístup k informáciám (vrátane konkrétnych procedúr), alebo lokalitám,
- školí a preškoľuje manažment a personál o politike a procedúrach, motivuje ich k dodržiavaniu týchto pokynov a overuje, či ich naozaj plne chápu a dodržiavajú,
- indoktrinuje manažment a personál povedomím o rizikách, potrebou riešiť zabezpečenie a ostražitosťou,

- prispôsobuje svoj prístup k zamestnancom rôznym štýlom učenia sa, ktoré sa medzi odborníkmi v rôznych oblastiach líšia,
- tajne spolupracuje s personálom mimo bezpečnostného tímu a využíva ich vlastností ako je prirodzená ostražitosť[1], či prirodzený rešpekt k zefektívneniu bezpečnostnej politiky.

Konkrétnejší spôsob niektorých z týchto činností uvádzam v nasledujúcich statiach.

### 4.1.2 Klasifikácia informácií

Klasifikácia informácií implikuje stupeň ich utajenia. Rôzne stupne môžeme vidieť napríklad pri legislatíve o ochrane utajovaných skutočností, avšak tie sú zadefinované pre potreby štátu. Softvérová firma je hlavne komerčná organizácia, ktorej záujmom je udržať sa na trhu a mať dobrú povesť. Použiteľný príklad klasifikácie, ktorý dopĺňam o príklady v kontexte opisovanej firmy ponúka norma ISO 27002 v časti *8.2.1 - Klasifikácia informácií*:

**I Prezradenie informácie nemôže spôsobiť žiadne škody.** Napr. všeobecné informácie o činnosti a produktoch firmy potrebné pre jej propagáciu, reklamu, či uzavretie obchodu.

**II Prezradenie informácie môže spôsobiť menšie nepríjemnosti, alebo prevádzkové problémy.** Tu môžu spadať napr. informácie o inžinierskych sieťach, či dodávateľoch základných služieb.

**III Prezradenie informácie môže spôsobiť významný krátkodobý dopad na prevádzkové činnosti, či krátkodobé taktické ciele.** Napr. informácie o významných zákazníkoch, či zamestnancoch, ktoré by mohla zneužiť konkurencia. Taktiež tu môžu byť známe chyby vytváraného softvéru.

**IV Prezradenie informácie môže mať vážny dopad na dlhodobé strategické ciele, či riziko nepokračovania spoločnosti v činnosti.** Tu patria spravidla zdrojové kódy, interná dokumentácia zachytávajúca know-how a princípy fungovania produktov a pod.

---

1. všímanie si a nahlasovanie podozrivej aktivity

Osobne som názoru, že minimálne stupne III a IV si zaslúžia ochranu na rovnakej - čo najvyššej úrovni, ktorej sa v práci venujem. Užitočnou môže byť rozdielna klasifikácia pri určovaní kto má k takýmto informáciám prístup, od čoho sa môže odvíjať rozloženie a určenie jednotlivých zabezpečených oblastí.

### 4.1.3 Analýza a adresovanie zraniteľností a hrozieb

Podklady pre analýzu som uviedol v predchádzajúcich kapitolách - členovia bezpečnostného tímu sa musia v týchto oblastiach neustále vzdelávať.

Skvelým spôsobom ako udržať kontinuum a aktuálnosť politiky je vytvoriť tabuľku s možnými hrozbami (v prípade komplexnej politiky skombinovať ju s *ATT&CK*[18]) a priradiť ku každej z nich spôsoby (prostriedky, procedúry, zariadenia...), ktoré ju zmiernia - odstrašením, zabránením, odhalením, alebo nápravou. Hrozby a príslušné spôsoby zmiernenia je potrebné pravidelne kontrolovať a aktualizovať. Uvedomovať si možné zraniteľnosti (myslieť ako útočník) je teda základom efektívne implementovanej politiky.

Riešiť pravdepodobnosť zneužitia nejakej zraniteľnosti, či uplatnenia známej hrozby je podľa mňa irelevantné hlavne kvôli nedostupnosti informácií na určenie tejto pravdepodobnosti pri väčšine z nich. Často sa nedá určiť, ktorú zraniteľnosť bude motivovaný útočník preferovať. Ku každej zraniteľnosti by sa malo ideálne pristupovať rovnako. Výnimkou je postupné zavádzanie politiky - niekedy je nevyhnutné urýchliť proces návrhu a implementácie niektorých častí politiky práve z dôvodu preukázateľne vyššej pravdepodobnosti zneužitia niektorých zo zraniteľností. Takýto prístup nemôže byť dlhodobý a vo finálnej verzii politiky sa musí urýchlená časť opäť zrevidovať vzhľadom na celok.

Dôležité však je sledovať tých, ktorí by mohli mať záujem spoločnosť ohroziť. Užitočné je vytvoriť si zoznam nepriateľov (konkurencia, ich zákazníci a pod.) a monitorovať ich aktivity. Taktiež monitorovať dianie vo svete ako sú teroristické útoky, či politika môže mať opodstatnenie.

Ako už bolo v práci spomenuté, určité hrozby so sebou nesú aj externí dodávatelia systémov a služieb. Firma si preto musí v zmluve vynútiť právo na audit takýchto produktov.

### 4.1.4 Identifikácia

Pri všetkých aspektoch bezpečnosti sa musí riešiť spoľahlivý systém riadenia prístupu a manipulácie s aktívami, čo implikuje spoľahlivý systém identifikácie osôb, zabezpečených oblastí, zariadení, či iného majetku spoločnosti.

Navrhovaný systém identifikácie osôb:

- pozostáva z databázy obsahujúcej identitu osoby a s ňou spojených skrytých autentifikačných dát zabezpečených na úrovni utajovanej informácie. Tieto dáta pozostávajú z:
  - jednoznačných a bezpečne prístupných dát spoľahlivej NFC technológie[2],
  - bezpečného hešu číselného hesla známeho len danej osobe,
  - biometrického údaju - ideálne obrazu sietnice, alternatívne odtlačku prsta,
- taktiež pozostáva z odznaku v podobe karty s kompatibilnou NFC technológiou následujúcimi viditeľnými údajmi:
  - meno a priezvisko osoby,
  - určenie a príslušnosť osoby vrámci spoločnosti vyjadrená textom aj farebným kódom,
- rozdeľuje určenie a príslušnosť na:
  - vlastných zamestnancov s prístupom k utajovaným informáciám a zabezpečeným oblastiam, pričom je vhodné rozdeľovať oddelenia, ktorých zamestnanci nepotrebujú prístup k informáciám iných oddelení,
  - vlastných zamestnancov bez takéhoto prístupu,
  - externých spolupracovníkov
  - verifikovaných zamestnancov externých dodávateľov
  - stráž

2. Technológia, ktorá nemá známe bezpečnostné chyby, ktoré by umožňovali jednoduché kopírovanie. Aktuálne napr. *MIFARE Ultralight EV1*

– návštevy

Identifikácia lokalít je implikovaná použitím prístupového zariadenia opísaného nižšie. Identifikácia fyzických aktív (zariadení, dokumentov v holej podobe a pod.) by tiež mala byť formou bezpečnej NFC technológie v kombinácii s čítačkou s veľkým rozsahom na rozhraniach oblastí pre ich jednoduchšie sledovanie.

### 4.1.5 Riadeniu prístupu

Riadeniu prístupu sa špecificky venujem pri fyzickej, infraštruktúrnej aj personálnej bezpečnosti. Avšak vždy platí všeobecná zásada *need-to-know* - každá osoba má mať prístup len k takej informácii, zariadeniu, či oblasti, ktorú nutne potrebuje pre výkon svojej činnosti a zároveň má príslušný stupeň oprávnenia k nim. Laxnejšia kontrola prístupu síce môže urýchľovať vývoj, ale pre nás sú riziká spojené s takýmto prístupom neprípustné.

### 4.1.6 Všeobecné požiadavky pre uchovávanie a spracovávanie informácií viacerých organizácií

Legislatíva zaoberajúca sa ochranou utajovaných skutočností nehovorí nič o fyzickom, alebo logickom oddeľovaní skutočností, ktoré spadajú pod rôzne odvetvia štátu. Vytváranie, spracovávanie a uchovávanie všetkých utajovaných skutočností rovnakého stupňa tak môže z jej pohľadu prebiehať v jednej zabezpečenej oblasti.

Ak však firma pracuje na takýchto zákazkách nepriamo, alebo na iných zákazkách cez, resp. pre iných komerčných zákazníkov, pričom vznikajú informácie citlivé pre týchto zákazníkov, oddeľovanie by sa riešiť malo. A to hlavne ak o to zákazníci explicitne žiadajú. Navyše, ak chceme aj vrámci jednej organizácie čo najprísnejšie dodržiavať zásadu *need do know*, takéto oddelenie je žiadúce.

Podľa *ISO 27002* by sa malo fyzické zabezpečenie špeciálne zvážiť v prípade, že budova hosťuje viacero organizácií. Avšak žiadne konkrétne požiadavky nie sú uvedené tam, ani som ich nenašiel v iných zdrojoch.

Ak chceme takéto oddelenie medzi rôznymi zabezpečenými oblasťami riešiť tak, aby to malo zmysel, je zrejme najdôležitejšie, aby

narušenie bezpečnosti jednej z nich neovplyvnilo bezpečnosť iných. Mnou navrhovaný spôsob oddelenia spĺňa, že:

- každý zákazník má vo svojich oblastiach nezávislé EZS aj systém pre kontrolu vstupu (jeho databáza sa fyzicky nachádza inde a je pripojená na inú sieť) vrátane zdroja neprerušovaného napájania,
- vložky zámkov týchto oblastí majú nezávislý systém - nie sú súčasťou systému centrálneho kľúča spoločného pre celú budovu,
- každá oblasť má vlastnú ochranu pred elektromagnetickými emisiami a napájacími emisiami,
- siete a iné dátové, resp. komunikačné spojenia nie sú medzi oblasťami rôznych zákazníkov logicky, ani fyzicky prepojené s výnimkou sietí určených pre internetovú komunikáciu - tie však musia byť označené, špeciálne tienené vnútri oblasti a ich spojenie je až na úrovni prvku, ktorý zabezpečuje spojenie s poskytovateľom služby,
- systém identifikácie osôb v celej budove je upravený tak, aby pri v ňom nevznikali kolízie - napr. použitím dvojitého farebného kódovania, kde jedna farba označuje úroveň a druhá príslušnosť k organizácii. Ak má jedna osoba prístup do viacerých oblastí, má k tomu dve rôzne karty a ideálne aj rôzny číselný kód, či biometrický údaj (iná sieťovka, iný palec..)
- personál je špeciálne poučený o tom, aby nekomunikoval utajované informácie pred personálom s inou príslušnosťou a neprenášal elektronické zariadenia medzi týmito oblasťami.

## 4.2 Fyzická bezpečnosť

Pri uvažovaní o fyzickej bezpečnosti je najprv potrebné skúmať podmienky, ktoré sú k dispozícii, najmä kvôli určeniu vrstvy, na ktorej firma môže začať vlastnú zabezpečovaciu činnosť. Touto úrovňou môže byť hranica pozemku celého zariadenia, plášť budovy, alebo hranice oblasti vrámci budovy. Ako už bolo spomenuté, väčšina malých

a stredných softvérových firiem nemá k dispozícii celý pozemok nejakého zariadenia, resp. nie sú oprávnené ho zabezpečovať. Navyše, o zabezpečení perimetru by sa dala napísať samostatná kapitola, keďže výber technológií je obrovský[3] a návrh záleží od veľmi špecifických činiteľov. Práca teda začína u plášťa budovy.

V sekcii definujem všeobecné požiadavky a následne niektoré z nich špecifikujem detailnejšie.

### 4.2.1 Všeobecné požiadavky pre budovu a oblasti

Budova musí byť navrhnutá, alebo upravená tak, aby lokalita a okolie nemali vplyv na jej zabezpečenie - je potrebné čo najviac odbúrať, alebo zabezpečiť prvky, ktoré zjednodušujú prístup, zmenšujú možnosti pozorovania a pod. Zabezpečená budova:

- musí mať jednoznačné určenie seba a svojich oblastí, prevádzkový poriadok a plán zabezpečenia v krízových situáciách,
- zároveň musí pre okolie a personál, ktorý to nepotrebuje vedieť budiť čo najmenší náznak o svojom účele a s každou informáciou, ktorá by mohla odhaľovať umiestnenie a účel oblastí a budov sa musí zachádzať ako s utajovanou,
- preto musí mať priestory upravené tak, aby boli hranice zabezpečených oblastí jasné a predišlo sa tak zbytočným konfliktom,
- musí mať hladkú, ničím nerušenú stavebnú líniu,
- musí mať kompletne zabezpečený plášť - všetky možné otvory, vrátane zariadení pre základné služby musia podliehať minimálne mechanickej kontrole prístupu a EZS a musia sa testovať na odolnosť a pravidelne kontrolovať,
- musí mať prevádzkový poriadok navrhnutý tak, aby za normálnych podmienok osoby do budovy a pracovných oblastí prechádzali len elektronickým prístupovým systémom,
- musí byť navrhnutá, alebo upravená tak, aby sa do nej nikto nedostal nepozorovaný, to platí aj o oblastiach,

3. Pozornosť môžem upriamiť napríklad na radarový sledovací systém[40]

- sama, ale aj jej oblasti musia spĺňať úroveň zabezpečenia 5 podľa *EN 14383-4* - tá okrem určenia triedy dverí, okien, okeníc, zasklenia, cylindrických vložiek a EZS implikuje aj povinnosť mať zosilnené kryty, prístupový systém a kamerový systém,
- má zabezpečené oblasti chránené pred rôznymi formami odpočúvania,
- musí byť navrhnutá, alebo upravená tak, aby výpadok napájania, alebo iných základných služieb nemal významný vplyv na zabezpečenie - zabezpečovacie systémy sú pripojené na zdroj neprerušovaného napájania,
- musí mať všetky bezpečnostné prvky správne nainštalované tak, aby sa nezmenila zamýšľaná funkčnosť a aby inštalácia neumožňovala nezamýšľaný spôsob použitia.

Znovu zopakujem, že pri inštalácii, alebo funkčnosti bezpečnostných prvkov sa netreba spoliehať na dodávateľov - produkty pred aj po zakúpení musia prejsť dôkladným skúmaním bezpečnostného tímu, prípadne s externou výpomocou na možnosti narušenia. Napríklad dvere musia byť správne osadené tak, aby nemali pri zatvorenom stave škáry, ktoré sa dajú zneužiť na manipuláciu napr. s vnútornou kľučkou.

### 4.2.2 Požiadavky pre zabezpečenie a kontrolu vstupu

Riadenie prístupu na mechanickej úrovni implikuje predchádzajúca stať. Je jasné, že nezabezpečený vchod či už zamýšľaný, alebo nezamýšľaný je neprípustným rizikom. Rozobrať však môžeme požiadavku pre triedy odolnosti dverí, okien, vložiek, zasklenia a okeníc podľa *EN 1627*, ktoré *EN 14383-4* úrovne 5 určuje medzi 4-6, pričom trieda 6 je najvyššia možná.

Tu je potrebné si problematiku poriadne naštudovať, keďže napr. pri cylindrických vložkách sú triedy 4-6 de iure ekvivalentné. K vložkám zopakujem, že je podstatné si všímať neoficiálnych referencií na odolnosť voči lockpickingu[4].

4. Na základe mnou známych informácií môže byť aktuálne vyhovujúcou vložkou napr. *TOKOZ PRO 400*, alebo bezp. vložky s jadrom *ABLOY PROTEC 2*. Túto problematiku mimochodom interne rieši aj NBÚ[41]

Svoje triedy bezpečnosti majú aj prvky ako zámky, či zapadacie plechy, pričom sa jednotlivo rieši odolnosť proti odvŕtaniu, korózii, elektromagnetickému rušeniu a pod. U dverí môžeme v iných normách zas nájsť aj odolnosť voči priestrelu, či explózii (podľa *EN 1522, EN 1523, EN 13123-2*) - o tom je tiež potrebné uvažovať, aj keď vlámania touto formou sú štatisticky minimálne. Pre extrémne citlivé informácie, či peniaze je možné zvažovať aj bezpečnostné úschovné systémy (*EN 1143-1*).

Špeciálnu požiadavku môžem uviesť pre okná - okná s jednoduchým prístupom z vonku, balkónové dvere a okná zabezpečených oblastí by mali mať na svojej kľučke zámok - predíde sa tak útoku spomínanom v časti *3.1.1 - Neoprávnený prienik do objektu a oblastí*.

**Elektronický prístupový systém** je ďalšou kategóriou. Na tú nemáme platnú normu, avšak špecifikujem ju aj vzhľadom na vlastnú skúsenosť. Navrhovaný systém:

- pozostáva na každom vstupe z:
  - dverí, zámku a elektromechanického zapadacieho plechu požadovanej (čo najvyššej) triedy odolnosti,
  - užívateľského zariadenia pozostávajúceho z číselnej klávesnice, čítačky NFC technológie a biometrického systému kompatibilných s definovaným identifikačným systémom,
  - kontrolného zariadenia ovládajúceho zapadací plech - to musí byť vnútri oblasti zabezpečovanej systémom,
- taktiež pri viacerých vstupoch do oblastí rovnakej kategórie pozostáva zo serveru, ktorý obsahuje databázu identifikačného systému a na základe nej rozhoduje o povolení vstupu - ten musí taktiež byť vnútri niektorých z oblastí rovnakej kategórie, ktoré zabezpečuje,
- je navrhnutý a inštalovaný tak, že komunikácia medzi prvkami prebieha po fyzicky oddelenej a zabezpečenej sieti (môže byť aj zabezpečená vnútorná sieť danej oblasti), v prípade komunikácie medzi kontrolným panelom a užívateľským zariadením môže ísť aj o zabezpečenú komunikáciu sériovým protokolom,

- pre prechod oboma smermi vyžaduje kartu a biometrický údaj, vo výnimočných prípadoch miesto biometrického údaju číselný kód,
- zaznamenáva všetky pokusy o prístup a to na dobu neurčitú,
- v prípade požiaru odblokuje zapadací plech.

**Stráž** tvorí dôležitú a povinnú súčasť kontroly prístupu pri ochrane utajovaných skutočností štátu úrovne tajné a prísne tajné[3]. V prípade čisto komerčných záležitostí ju môžem len odporučiť. Avšak je potrebné venovať zvýšenú pozornosť jeho pozadiu a zaškoľovaniu, ktoré musí byť na úrovni interného zamestnanca. Takáto osoba totiž môže aj zvýšiť povrch možného útoku.

### 4.2.3 Požiadavky pre elektronickú zabezpečovaciu signalizáciu

EZS do veľkej miery rozoberajú spomenuté normy. Zadefinované všeobecné požiadavky pre budovu a oblasti implikujú stupeň zabezpečenia 4 podľa *EN 50131-1*. Vysoký stupeň zabezpečenia je vitálny, pretože kladie na EZS a jeho prvky požiadavky ako je ochrana pred sabotážou, zakrytím, znížením detekčného rozsahu, odolnosť voči magnetickému rušeniu a pod. Elektronická zabezpečovacia signalizácia spĺňa, že:

- oddelené systémy zabezpečujú zabezpečené oblasti a priestory mimo zabezpečených oblastí,
- má komunikátor, resp. ústredňu umiestnenú v niektorej z oblastí, ktoré zabezpečuje a na pult centrálnej ochrany je pripojený cez IP sieť - vzhľadom na tienenie nemôžeme využiť bezdrôtovú sieť a kvôli bezpečnosti nemôžeme využiť telefónnu sieť,
- jeden systém kontroluje len oblasti rovnakej kategórie, avšak rozdelených do rôznych podsystémov,
- má detektory inštalované tak, aby bolo čo najzložitejšie sa vyhnúť detekcii nimi - tomu zodpovedá aj vysoká miera redundancie a potreba správneho usporiadania nábytku a iných predmetov,

- magnetickými detektormi sa strážia všetky dvere plášťa budovy, okná a otvory plášťa prístupné z vonku a všetky dvere, okná a otvory zabezpečených oblastí,
- detektormi rozbíjania skla sa strážia všetky okná plášťa prístupné z vonku a všetky okná zabezpečených oblastí,
- kombinovanými (*PIR+MW*) detektormi sa strážia všetky priestory a tie najkritickejšie nekombinovanými *PIR*.

### 4.2.4 Požiadavky pre kamerový systém

Kamerové systémy technicky podrobne špecifikujú normy rodiny *EN 62676*. A to vrátane zabezpečenia prenosu videa. Pri kamerovom systéme je potrebné si dávať pozor hlavne na informatické chyby, ktoré som opísal v stati *3.1.2 - CCTV - kamerové systémy*. Preto by mala sieť, na ktorej tento systém operuje byť oddelená od ostatných a to minimálne logicky s izoláciou jednotlivých klientov na druhej vrstve (podrobnosti v ďalšej sekcii).

Kamerovým systémom by mal byť pokrytý celý perimeter budovy, ale aj všetky priestory vrámci budovy, ktoré nespadajú do zabezpečených oblastí. Nahrávacie zariadenie by malo byť v nejakej (ideálne špeciálne na to určenej) zabezpečenej oblasti, ktorá by mala byť tiež pokrytá.

Čo sa týka pokrytia ostatných zabezpečených oblastí, stojí za dôkladné zváženie, či umiestniť kamerové systémy aj v nich. Záznamy síce môžu výrazne pomôcť pri overovaní incidentov, avšak vzniká hrozba, že sa do nich dostanú nejaké časti utajovaných informácií, čo zväčšuje povrch možných útokov. Ideálne by mala každá oblasť mať vlastný uzavrený okruh, s ktorého nahrávkami sa nakladá ako s utajovanými informáciami.

### 4.2.5 Oddelenie prostredí vývoja, testovania a prevádzky

*ISO 27002* zavádza zaujímavú požiadavku - oddelenie fyzického prostredia vývoja, testovania a prevádzky. V zásade ide o to, že do systémov pre testovanie a prevádzku sa za žiadnych okolností nesmú dostať citlivé informácie a k vývojovým systémom nesmú mať prístup neoprávnení užívatelia. Rovnaký výsledok síce implikujú zvyšné

princípy v tejto práci, avšak do politiky by sme mali explicitne pridať aj nutnosť vytvoriť komplexné procedúry pre prenos softvéru medzi týmito oblasťami a systémami.

### 4.2.6 Požiadavky pre ochranu pred odpočúvaním - *TEMPEST*

Najlepšou fyzickou obranou proti odpočúvaniu je tieniaca komora, ktorú vyhláška[10] definuje ako priestor, ktorý zabraňuje šíreniu elektromagnetického, optického aj akustického vyžarovania mimo tento priestor. Explicitne to v legislatíve vyjadrené nie je, ale metodické pokyny NBÚ[42] naznačujú, že tieto komory musia filtrovať aj napájanie.

Podrobné bezpečnostné štandardy sú však utajovanou skutočnosťou stupňa Dôverné[41], čo sťažuje verejnú dostupnosť takýchto prostriedkov na rovnakej úrovni. Ostáva len využiť komerčne dostupné prostriedky, resp. si navrhnúť, vyrobiť a testovať vlastné.

Pre vysokú technickú aj expertíznu náročnosť Van Eck phreakingu pri moderných technológiách je však potrebné zamyslieť sa, či takáto ochrana stojí za to. Pre odpočúvanie sa však dajú využiť nielen nechcené elektromagnetické emisie - určite treba zvážiť obmedzenie používania elektroniky, ktorá bezdrôtovo komunikuje účelne - myši, klávesnice, slúchadlá a pod.

Ak hovoríme o odpočúvaní v širšom zmysle, je potrebné myslieť aj na vynášanie dokumentov a informačných systémov - všetky musia byť pred vynesením zo zabezpečenej oblasti, alebo iným úkonom umožňujúcim prístup inej, ako oprávnenej osoby bezpečne skartované, resp. v prípade úložných zariadení (vrátane RAM) prepísané neutajovanými informáciami. Vitálnymi sú aj pokyny pre personál, ktorým sa v práci tiež venujem.

## 4.3 Bezpečnosť infraštruktúry

V tejto sekcii navrhujem zabezpečenie dátovej, napájacej a signalizačnej infraštruktúry. Niektoré požiadavky som načrtol už aj v predchádzajúcich statiach.

### 4.3.1 Vedenie kabeláže

Najdôležitejším je zabránenie fyzického prístupu. Kabeláž je vedená a udržiavaná tak, že:

- káble majú čo najhoršiu dostupnosť, čo znamená, že:
  - ich umiestnenie nie je nijakým spôsobom naznačené,
  - sú vedené v podzemí, resp. pod podlahou všade, kde to je možné,
  - sú vedené v pancierových chráničkách,
  - rozvodové skrine a miestnosti majú kontrolovaný prístup - minimálne zámkom s vložkou rovnakej úrovne, ktorá sa používa pri vstupoch, pričom by jednotlivé kľúče nemali spadať pod existujúci systém centrálneho kľúča,
  - rozvodové skrine a miestnosti sú pod dozorom kamerového systému, ideálne aj kontrolované magnetickými detektormi, ktoré tvoria oddelený podsystém EZS,
- napájacie, dátové a signalizačné (EZS) káble sú oddelené, taktiež sú oddelené dátové káble interných komunikačných systémov od externých (napojených na internet),
- pred údržbou alebo inou manipuláciou rozvodov od nich musia byť zariadenia s citlivými informáciami odpojené,
- prebiehajú pravidelné prehliadky na neoprávnene pripojené zariadenia,
- sú vedené podrobné záznamy o poruchách, podozreniach na poruchy, pokusoch o opravu a pod.

V súvislosti s ochranou pred odpočúvaním navrhujem využitie vysokofrekvenčných filtrov[5] napájania na rozhraní oblastí s tienením a využívať rôzne fázy v zabezpečených oblastiach a zvýšku budovy. Taktiež treba brať ohľad na to, že sieťová kabeláž vedúca mimo oblasť (internetové pripojenie) môže byť vrámci oblasti použitá ako anténa. Tieto teda musia byť špeciálne tienené a v oblasti používané len ak to je nutné a aj to s vysokou mierou obozretnosti.

5. Jednoduchým (avšak nie dokonalým) filtrom môže byť napr. 1:1 transformátor

### 4.3.2 Požiadavky na návrh sietí

Už som na viacerých miestach zdôrazňoval fyzické aj logické oddeľovanie. Tento princíp v prvom rade zabraňuje postupnému prieniku sieťou a navyše obmedzuje možnosti pre zneužitie nežiadúcich emisií. Keďže prípady, v ktorých je požadované úplné fyzické oddelenie sú z predchádzajúcich statí jasné, budem sa venovať hlavne tomu logickému.

Logickou izoláciou na *L2* pre tieto potreby rozumieme využitie rôznych *bridge* a *VLAN* na rôznych prípojkách fyzicky pripojených k smerovaču. Logickou izoláciou na *L3* rozumieme, že je zároveň zakázané smerovanie medzi nimi.

Siete môžu byť fyzicky prepojené, ak:

- ide o siete, ktoré poskytujú prístup k internetu ak zároveň:
  - fyzické prepojenie je až na smerovači, ktorý zabezpečuje priame pripojenie na sieť poskytovateľa služby,
  - sú rôzne oblasti, resp. oblasti rôznych kategórií od seba logicky oddelené na *L2* aj *L3*,
- ide o siete pre EZS a CCTV vrámci jednej oblasti ak zároveň:
  - všetky jednotlivé prvky sú medzi sebou logicky oddelené na *L2* a všetky prvky, ktoré nepotrebujú medzi sebou komunikovať sú oddelené na *L3*,
- ide o spôsob prepojenia externej siete (napr. internetu) s nejakou internou sieťou ak zároveň:
  - existuje významný dôvod pre takéto prepojenie aj po zvážení všetkých možných rizík a minimalizácii možného dopadu pri kompromitácii,
  - ide o využitie maximálne zabezpečeného prvku a technológie[6].

6. Napr. plnohodnotný linuxový počítač s dvoma sieťovými kartami s využitím *OpenVPN* v kombinácii s tvrdými požiadavkami na prihlasovacie údaje, certifikáty a prístup k nim. Zvážiť treba aj ďalšiu vrstvu ochrany, napr. *Shibboleth*

  - prístup k tomuto prepojeniu je riadený, kontrolovaný a zaznamenávaný,

- všetky prvky, na ktorých sa siete fyzicky prepájajú sú pravidelne aktualizované a kontrolované na známe bezpečnostné chyby,

Samozrejmosťou sú aj požiadavky na siete Wi-Fi:

- Wi-Fi považujeme za externú sieť - žiaden z prvkov vytvárajúcich Wi-Fi nesmie byť fyzicky spojený s internými sieťami oblastí s výnimkou prípadov uvedených vyššie,

- prevádzka Wi-Fi sietí vrámci zabezpečených oblastí by mala byť zakázaná - pre takéto konanie musí tiež byť významný dôvod[7] a v danej oblasti minimalizovaný výskyt ostatných utajovaných informácií,

- pri zabezpečovaní siete bezpečnostnými protokolmi vyžadujeme také, ktoré umožňujú jednoznačné priradenie identity k pripojeniu, pričom je potrebné brať zreteľ na ich vlastnosti vrátane nedostatkov:

  - v blízkej budúcnosti preferovať *WPA3-Enterprise 192-bit Mode*, ktorého rozšírenie je zatiaľ minimálne,
  - alternatívne použiť *WPA2-Enterprise PEAP/MS-CHAPv2*, ktorý má síce rozšírenú podporu, avšak je potrebné uvedomovať si slabé šifrovanie a školiť užívateľov pre správne zaobchádzanie - vynucovanie certifikátu vydaného organizáciou,
  - alternatívne použiť *WPA2-Personal AES* s veľmi silným heslom, avšak pridať dodatočnú ochranu - napr. autentifikáciu cez *Shibboleth* a pre tú vynucovať použitie organizáciou vydaného certifikátu.

súvis

7. Napr. vývoj zariadenia pracujúceho s Wi-Fi.

### 4.3.3 Požiadavky pre užívateľské zariadenia na sieti

Medzi užívateľské zariadenia nepatria len používané osobné počítače. Je to všetko, s čím môže užívateľ nejakým spôsobom interagovať - panely pre ovládanie klimatizácie, zabezpečovacie zariadenia a pod. Ako som už veľakrát v práci spomenul, dôležité je vlastné testovanie týchto zariadení - fyzický pentesting a vyhľadávanie bezpečnostných chýb. To sa viac pre špecifickosť takýchto zariadení opísať nedá.

Na chvíľu však odbočím aj k osobným počítačom: úplné šifrovanie úložísk pracovných strojov a kombinovanú (smartcard, heslo, biometrika) autentifikáciu k nim považujem za samozrejmosť. Menej rozšíreným je presvedčenie, že antivírusové systémy v poslednej dobe len zbytočne zvyšujú možný povrch pre útoky, pretože samé mávajú závažné bezpečnostné chyby a za účelom kontroly prenášaných dát narúšajú zabezpečenie samotného systému[43]. Nad tým by sa správcovia IT v organizácii mali zamyslieť.

## 4.4 Prenos informácií mimo zabezpečených oblastí a infraštruktúry

Prenos informácií je z pohľadu legislatívy o utajovaných skutočnostiach pomerne zaujímavý. Rozhodnutie Rady EÚ[12] explicitne uvádza, že prenos utajovaných informácií mimo zabezpečených oblastí všeobecne prebieha elektronicky, alebo na dátových nosičoch, v oboch prípadoch s ochranou certifikovaným kryptografickým prostriedkom. Ak sú informácie prenášané v nezašifrovanej, alebo holej podobe, musia sa využívať špeciálne opatrenia - tie sú však v prípade prenosu na šifrovaných dátových nosičoch nepovinné.

Česká legislatíva[3][44][45] naopak nikde explicitne neuvádza všeobecnú potrebu prenášať utajované informácie s využitím kryptografického prostriedku s výnimkou taktickej informácie[8]. Avšak pri prenose kryptografického materiálu vyžaduje rovnako tvrdé kritériá, ako pri prenose v holej podobe.

Keďže prístup k zoznamu certifikovaných kryptografických prostriedkov nemám, musím vychádzať z verejne dostupných informácií. Po zohľadnení možností a inšpirácii uvedenou legislatívou navrhujem

8. Informácia s krátkou dobou dôvodu pre utajovanie

následujúce podmienky prenosu utajovaných informácií, pri ktorých je podľa mňa minimálne riziko zlyhania:

- informácie sa prenášajú fyzicky a to na úložnom médiu (flash pamäť, externý disk a pod.) za splnenia týchto podmienok:
  - samotné súbory sa zašifrujú algoritmom *AES* s dĺžkou kľúča aspoň 256-bit, ideálne s využitím archivačného nástroja s otvoreným kódom,
  - na médiu sa softvérom *VeraCrypt* vytvorí hosťovský šifrovaný zväzok a skrytý šifrovaný zväzok,
  - zašifrované súbory sa umiestnia na tento skrytý zväzok[9],
  - pri používaní softvéru *VeraCrypt* sa používa aspoň algoritmus *AES*, prípadne (ak výkon nehrá rolu) kaskádový algoritmus *AES-Twofish-Serpent*,
  - heslá pre šifrovanie súborov, hosťovského zväzku a skrytého zväzku sú rozdielne,
  - médium je zabezpečené v obale, ktorý zabraňuje neoprávnenej manipulácii napr. zámkom - ten sa zatvorí v oblasti, z ktorej informácie pochádzajú a otvorí až na mieste určenia,
  - médium je prenášané osobou, ktorá je v identifikačnom systéme spoločnosti, je oprávnená manipulovať s informáciou danej úrovne, médium má počas celej cesty pri sebe a nemá vedomosť o heslách a ideálne ani o obsahu média,
- informácie sa taktiež môžu prenášať elektronicky - cez internet, alebo ideálne zabezpečenú organizačnú sieť pri splnení týchto podmienok:
  - samotné súbory sa rovnako ako v prvom prípade zašifrujú algoritmom *AES* s dĺžkou kľúča aspoň 256-bit, avšak minimálne dvakrát s použitím rozdielnych hesiel,

9. Tento postup, ak je správne vykonaný, pridáva okrem ďalšej úrovne šifrovania aj možnosť hodnoverného poprenia existencie zväzku na médiu

  - pre prenos cez sieť sa využije priameho spojenia *SSH* tunelom medzi odosielacím a prijímacím zariadením - ak priame spojenie nie je možné, môžu sa nad ním vytvoriť ďalšie *SSH* tunely, resp. *OpenVPN* pripojenia so sprostredkujúcim zariadením, ktoré je na to určené,
  - celý proces podlieha prísnej certifikačnej politike - certifikáty všetkých strojov musia byť všetkým stranám vopred známe,

- všetky heslá použité pri vyššie opísaných procesoch musia byť dostatočne komplexné a dlhé a každé z nich sa medzi odosielateľom a prijímateľom komunikuje zabezpečeným kanálom, ktorý je iný ako ten, ktorým prebieha prenos samotnej utajovanej informácie, ideálne iný pre každé heslo - napr. osobným stretnutím, alebo komunikáciou cez aplikáciu *Signal*,

- prenášanie dokumentu v holej podobe je povolené len, ak to je vyslovene nutné, pričom musia byť splnené tieto podmienky:

  - dokument je prenášaný osobou, ktorá je v identifikačnom systéme spoločnosti, je oprávnená manipulovať s informáciou danej úrovne a minimálne jednou ďalšou doprovodnou osobou, ktorá je na to poverená a zaškolená,
  - dokument je chránený spevneným obalom, ktorý znemožňuje nahliadnutie, alebo manipuláciu s ním neautorizovanej osobe:
  - tento obal je fyzicky spevnený a opatrený kvalitným zámkom s číselným kódom,
  - osoba, ktorá obal s dokumentom prenáša nedisponuje kľúčom - ten musí byť taktiež komunikovaný iným kanálom.

## 4.5 Personálna bezpečnosť

Zabezpečenie ľudských zdrojov je asi najkomplexnejšie a najhoršie riešiteľné, keďže ponúka ohromný priestor pre chyby. V prípade, že tieto opatrenia nie sú dostatočné, alebo nie sú dodržiavané, všetky ostatné vrstvy bezpečnosti ničomu nepomôžu. Avšak kombinácia šťastného

zamestnanca, ktorého práva neboli nijako porušené a bezpečnostných opatrení na vysokej úrovni sa zdá byť na prvý pohľad nemožná.

V tejto sekcii sa o to pokúšam návrhom viacerých politík pre celé spektrum personálu vrátane manažmentu ľudských zdrojov.

### 4.5.1 Výberové konanie a nástup do zamestnania

Rozsah bezpečnostnej politiky by mal siahať až na prvý kontakt s potenciálnym zamestnancom - životopis a pracovný pohovor. Okrem samotnej odbornej kvalifikácie a zručností je potrebné riešiť aj možné bezpečnostné riziko. Ak sa opäť pozrieme na politiku v legislatíve o ochrane utajovaných skutočností, vidíme, že vlastnosti požadované pre osvedčenie fyzickej osoby pre vyššie stupne utajenia sú označené ako osobnostná spôsobilosť a bezpečnostná spoľahlivosť[3], resp. lojalita, dôveryhodnosť a spoľahlivosť[12], pričom konkrétne požiadavky sú pomerne presne dané a nižšie ich mierne pozmenené používam.

Požiadavky sa pri ochrane utajovaných skutočností overujú počas tzv. bezpečnostného konania, pričom Úrad, ktorý vedie toto konanie je obmedzovaný de iure len požiadavkou zachovania osobnej cti a dôstojnosti účastníka. Ináč vynucuje zbavenie mlčanlivosti osôb zúčastnených na správe daní, využíva svedkov[10], políciu, alebo dokonca (v prípade konania pre stupeň Prísne tajné) spravodajskú službu.

Súkromná firma však podobné legálne možnosti pre vlastné konanie nemá a musí si vystačiť s informáciami, ktoré im účastník poskytol, sú verejne dostupné[11], alebo vyplývajú z jeho správania sa na pohovore. Užitočným môže byť aj psychologické vyšetrenie zamerané na bezpečné a zodpovedné správanie sa, čo sa však v ČR vynútiť nedá. Spôsob výberu pri konaní navyše nesmie mať diskriminačný charakter. Personálny manažment v spolupráci s bezpečnostným tímom by mal aj tak urobiť čo je v jeho silách a zákonných možnostiach na to, aby zistil skutočný stav vecí. Základnou požiadavkou je, že organizácia by nemala zobrať do pracovného pomeru niekoho kto predstavuje bezpečnostné riziko.

Osoba môže predstavovať zvýšené riziko pre bezpečnosť organizácie ak:

---

10. Svedkom môže byť skoro každá fyzická osoba, pričom za nedostavenie sa, alebo úmyselne zlú výpoveď jej hrozí pokuta až 100 000 Kč.
11. V dnešnej dobe tomu napomáhajú hlavne sociálne siete

- bola právoplatne odsúdená za trestný čin,
- je výrazne zadĺžená, alebo má iné finančné problémy,
- je členom, alebo stúpencom organizácie v hocijakej forme, ktorá verejne prejavuje extrémne názory, alebo je nimi známa,
- má styky, alebo iné napojenie na konkurenciu, či jej zákazníkov, hlavne ak sa tá už v minulosti pokúsila o nekalú súťaž,
- skreslila alebo sfalšovala poskytnuté informácie, či klamala,
- je závislá na alkohole, alebo inej omamnej látke, resp. pravidelne užíva nedovolené omamné látky,
- jej činy, prejavy, správanie sa a hypotetické[12] správanie sa:
  - je príliš riadené emóciami, ktoré nezvláda,
  - ukazuje, že by mohla podľahnúť vydieraniu, nátlaku, alebo inej činnosti, ktorá by v konečnom dôsledku mohla mať vplyv na jej schopnosť utajovať informáciu,
  - ukázali, že osoba je nečestná, nespoľahlivá, nedôveryhodná, alebo nelojálna,

Ak sa spoločnosť pre nejakého zamestnanca rozhodne, musí zabezpečiť, že v prípade ním spôsobeného narušenia bezpečnosti ho môže legálne postihnúť. Zmluva by tak mala obsahovať:

- dohodu o mlčanlivosti,
- požiadavku dodržiavania bezpečnostnej politiky, pravidiel a procedúr,
- postihy za nedodržanie týchto požiadaviek a to vrátane možného vyvodenia právnej zodpovednosti.

Istá forma bezpečnostného konania a zmluvnej dohody s uvedenými parametrami by mala prebiehať aj v prípade externých spolupracovníkov, zamestnancov od zmluvných poskytovateľov služieb a častých návštev.

12. Hypotetické správanie sa môže byť odhadnuté na základe dobre formulovaných otázok o postupe pri potenciálnych situáciách

### 4.5.2 Riadenie oprávnení a prístupu

Ďalším dôležitým článkom v bezpečnostnej politike je priraďovanie a vykonávanie oprávnení osôb k oblastiam, zariadeniam a informáciám. Na to k všeobecným podmienkam zadefinovaným v *4.1.4 a 4.1.5* navyše potrebujeme tieto personálne opatrenia:

- Všetky osoby, ktoré sa vrámci organizácie pohybujú do nejakej miery samostatne musia byť registrované v popísanom identifikačnom systéme - to teda platí aj o externých pracovníkoch, alebo pracovníkoch údržby.

- Registrovaní v identifikačnom systéme by mali byť aj častí návštevníci ako napr. zákazníci.

- Zmeny prístupových práv navrhuje manažment príslušného oddelenia a schvaľuje a nastavuje člen bezpečnostného tímu na to určený, ktorý predtým overí podmienku *need-to-know*.

- Všetky osoby, ktoré sa pohybujú vrámci organizácie musia mať svoj identifikačný odznak celý čas na jasne viditeľnom mieste. Návštevy, ktoré nie sú v identifikačnom systéme musia byť tiež viditeľne označené.

- Pred vstupom externého pracovníka, zmluvného pracovníka údržby, alebo návštevy do zabezpečených oblastí, či iných firemných priestorov musí byť takáto požiadavka manažmentom a bezpečnostným tímom vopred posúdená, schválená a oznámená osobám, ktorí s nimi prídu do styku.

- Návštevy a údržbu by mali pracovníci stráže preveriť na identitu aj keď sa nachádzajú v identifikačnom systéme.

- Všetky návštevy a údržba sú celý čas sprevádzané dozorom, v zabezpečených oblastiach to podľa potreby platí aj pre externých spolupracovníkov.

- Prístupové práva sú pravidelne preskúmavané a aktualizované.

### 4.5.3 Politika pre dohľad

Mimo všeobecných pokynov pre personál by mala byť vytvorená aj politika špeciálne pre dohľad nad dodržiavaním bezpečnostných pravidiel a odhaľovanie hrozieb plynúcich z dynamiky prostredia. Táto by nemala byť dostupná celému personálu. Jej účelom je monitorovať a aktívne zvyšovať efektivitu zvyšku zavedenej politiky. Uvádzané aktivity by mala vykonávať osoba na to určená - najlepšie člen bezpečnostného tímu, alebo člen manažmentu v spolupráci s bezpečnostným tímom. Táto osoba:

- dohliada na správne dodržiavanie konkrétnych procedúr,
- monitoruje a ak to je možné aj reguluje osobné vzťahy medzi personálom z rôznych oblastí a hlavne medzi personálom a častými návštevníkmi,
- monitoruje personál, ktorý vykazuje vyššie známky ostražitosti (nahlasuje podozrivú aktivitu), motivuje ho a v prípade prehnaných reakcií poučuje, pričom je potrebné myslieť na diskrétnosť - nikto nemusí vedieť, akým spôsobom sa na bezpečnosti podieľa,
- motivuje[13] personál, ktorý vykazuje väčšie nadšenie pre bezpečnosť a dodržiavanie politiky a má v tomto ohľade dobrý vplyv na spolupracovníkov,
- informuje stráž a prípadne iný personál o bývalom zamestnancovi, ktorý bol vyhodený nedobrovoľne a mohol by spôsobovať problémy,
- dokumentuje zvláštne správanie sa personálu - sem môžu patriť:
  - pokusy sa o prístup tam, kde na to nemajú právo,
  - žiadosti o prístupové práva, ktoré pre svoju prácu nepotrebujú,

13. Medzi možné spôsoby je nechať mu navrhnúť súčasť nejakej politiky, alebo ho pravidelne prizývať na jej revidovanie.

- rozhovory s kolegami o utajovaných informáciách, ktoré nepotrebujú riešiť, alebo vedieť,
- bezdôvodné trvanie na práci osamote - bez dozoru,

### 4.5.4 Politika pre celý personál

Nakoniec predstavujem hlavnú politiku pre personálnu bezpečnosť - ide o pravidlá pre správanie sa zamestnancov a zároveň je svojim spôsobom vyvrcholením všetkých predchádzajúcich statí, ktoré v podstate budovali základ pre to, aby vôbec mohla táto politika fungovať.

Pre personál platia následujúce požiadavky:

- Všetky osoby, ktoré sú v identifikačnom systéme musia pri prechádzaní medzi miestnosťami použiť prístupový systém a nesmú pri tom cez takto zabezpečený vstup púšťať iné osoby - všetky prístupy musia byť zaznamenané.
- Všetci sú povinní mať svoje prístupové karty, prípadne kľúče vždy pod dohľadom, alebo bezpečne ukryté. To platí aj pri pohybe mimo firemné priestory, či doma. Kľúče musia byť ukryté vždy, keď sa nepoužívajú - nesmú byť viditeľné napr. na stole, na nástenke a pod.
- Uchovávajú sa všetky prístupy k citlivým informáciám či už ide o klonovanie repozitárov, alebo sprístupnenie fyzického dokumentu.
- Zamestnanec je povinný vymazať zo svojho (samozrejme, pracovného) stroja všetky citlivé informácie, ktoré už nepotrebuje a to presne podľa zavedenej procedúry, pričom musí toto počínanie zdokumentovať,
- Citlivé informácie nesmú byť personálom bez pádneho dôvodu a povolenia kopírované a reprodukované či už fyzicky, alebo elektronicky na súkromné zariadenia,
- Vynášať dokumenty, zariadenia, alebo médiá s citlivými informáciami je prísne zakázané s výnimkou schváleného prenosu podľa bodu *4.4*.

- Ak personál citlivé informácie produkoval, alebo kopíroval, presvedčí sa, že v prostriedku, ktorý na to využil sa tieto informácie už nenachádzajú - na to sa tiež vytvoria špeciálne procedúry.

- Súkromné zariadenia nesmú byť používané na internej sieti a ideálne by sa ani nemali fyzicky nachádzať v zabezpečenej oblasti,

- Svoje prístupové heslá personál vytvára bezpečné a s nikým ich nezdieľa.

- Práca z domu je povolená len v mimoriadnych prípadoch, pričom musí pracovník použiť vysoko zabezpečený pracovný stroj, musí byť preškolený o jeho správnom používaní a nesmie sa na ňom nachádzať žiadna iná citlivá informácia ako sú tie, ktoré pre prácu nutne potrebuje.

- Rozprávanie sa o utajovaných informáciách je povolené iba v zabezpečených oblastiach a miestnostiach na to určených, taktiež elektronická komunikácia musí byť vykonávaná tiež s prostriedkami na to určenými - nesmú sa dostať na sociálne siete, či iné služby pre verejnosť.

- Rozprávanie sa o utajovaných informáciách je možné len v prítomnosti osôb z rovnakého oddelenia - s príslušnými farebnými kódmi na ich odznakoch.

- Ak sa v miestnosti nachádza návšteva, externý spolupracovník, stráž, alebo údržba, zamestnanci zvýšia svoju ostražitosť a prispôsobia svoje správanie sa tak, aby minimalizovali riziko vyzradenia citlivej informácie. Je potrebné si dať pozor na obsah verbálnej komunikácie, ale aj odhalený obsah monitorov, stolov a pod. Podobne sa postupuje aj ak ide o osobu s vyhovujúcim farebným kódom, avšak zamestnanec ju vidí prvýkrát - vtedy je potrebné sa opýtať spolupracovníkov a následne upovedomiť manažment, alebo bezpečnostný tím. Taktiež je potrebné nahlásiť zvláštne správanie sa týchto ľudí.

- Zamestnanci prísne dodržiavajú zásadu prázdneho stola a prázdnej obrazovky - v ich neprítomnosti na ich pracovisku nesmú byť dokumenty obsahujúce citlivé informácie a ich pracovný stroj musí byť zamknutý a na obrazovke sa nesmie nachádzať žiadna časť citlivej informácie.
- Zamestnanci, ktorí pracujú na jednom projekte majú k dispozícii otvorený priestor tak, aby bol možný vzájomný dohľad.
- Vytvorí sa zoznam kódových slov, ktoré poznajú len zamestnanci a použijú ich v prípade podozrivej aktivity, pri ktorej nechcú jej vykonávateľa vyrušiť, alebo v prípade, že je potrebná okamžitá pomoc.

# 5 Konkrétna Firma - Návrh zabezpečenia

*Konkrétna spoločnosť z bezpečnostných dôvodov nie je v práci uvedená.* Na posúdenie zabezpečenia som dostal plán menšej firmy, ktorý ukazuje rozloženie miestností s ich určením a obsahom. Ide o malú spoločnosť, ktorá pozostáva z 9-13 zamestnancov a zaberá 50-70 $m^2$ prenajatého priestoru vrámci budovy, ktorá podlieha určitej forme stráženia. Na chodbu, ktorá je na vyššom poschodí sa však môže teoreticky dostať hocikto, bez toho, aby bol zastavený. Firma aktuálne nepracuje s utajovanými informáciami a výhľadovo sa počíta maximálne so stupňom *Vyhradené*, kde sú požiadavky minimálne. Spoločnosť zároveň nezávisle na tejto práci rieši manažment riadenia bezpečnosti informácií podľa *ISO 27001* a navyše som dostal explicitnú požiadavku neriešiť *TEMPEST* - ochranu pred elektromagnetickými emisiami.

Keďže princípy pre personálne zabezpečenie sú z minulej kapitoly jasné a neviem si okrem procedúr predstaviť konkrétnejšie návrhy, môžem v tejto kapitole akurát tak navrhnúť konkrétne technické opatrenia - vrámci možností aj s využitím produktov existujúcich na trhu vrátane cenového odhadu. Vzhľadom na vyššie uvedené okolnosti a iné, ktoré sa objavili pri rešerši dostupných riešení musím pri svojom návrhu mierne poľaviť od technických princípov, ktoré som v predošlej kapitole zaviedol.

## 5.1 Fyzická bezpečnosť

Tieto kancelárske priestory aktuálne nemajú skoro žiadne zabezpečovacie systémy, takže začínam s čistým návrhom fyzických prvkov bezpečnosti. Poďme sa však najprv pozrieť na rozvrhnutie priestoru.

Priestory[1] sú tvorené troma susediacimi miestnosťami s vlastným vstupom, pričom stredná je v polovici predelená na dve časti. Časť miestnosti v strede, ktorá má vlastný vstup je úplne izolovaná od zvyšku priestorov a slúži čisto pre návštevy. Druhá časť (pri okne), ktorú používajú analytici dvoma dverami spája zvyšné dve miestnosti. Tie zas majú každá rôzne určenie - vývojová a administratívna.

1. Viď plánik v prílohe A

Samotné rozloženie sa mi pozdáva a spĺňa požiadavku rozloženia miestností podľa účelu.

Avšak dvere prepájajúce analytické a vývojové priestory mi prídu nadbytočné. Síce chápem, že častejší styk vývojárov a analytikov urýchľuje vývoj, lenže všetky tri časti by nemali byť prepojené a radšej oddelíme vývoj, kde sú z tohoto hľadiska najcennejšie informácie. Týmto krokom môžeme nahrávacie zariadenie kamerového systému a kontrolér prístupového systému strategicky umiestniť tak, aby na nich nemali fyzický dosah ľudia, ktorí by ich so svojimi vedomosťami mohli sabotovať jednoduchšie, ako zvyšok personálu. V ideálnom prípade by mali byť všetky prvky rozmiestnené tak, aby k nim mal prístup len ten, kto je za ich správu zodpovedný. Tu však musíme počítať s obmedzeným priestorom a kumulácii aktív a bezpečnostných prvkov na jednom mieste je teda potrebné zabrániť.

### 5.1.1 Mechanické prvky

Ako prvé je potrebné vyriešiť dvere a zámky. Aj napriek tomu, že riešime chodbu budovy, v ktorej je do nejakej miery kontrolovaný prístup, nasadil by som všetky tri chodbové dvere triedy bezpečnosti 4 podľa *EN 1627*. Oproti 3. triede nie je relatívny cenový rozdiel markantný, avšak je tam veľký skok v odolnosti a aj v dojme pre potenciálneho útočníka. Vnútorným dverám teoreticky stačí 2. bezpečnostná trieda, keďže v prípadoch, v ktorých si viem predstaviť útočníka v administratívnej oblasti bez toho, aby vyvolal alarm aj tak najskôr nepomôžu.

Pri dverách je potrebné upozorniť na kontrolu pevnosti stien a zárubní. Ak požadovanej pevnosti nezodpovedajú, bezpečnostné dvere nemajú zmysel. Taktiež je potrebné pri inštalácii zamedziť nedbalostiam ako sú škáry, cez ktoré sa vmestí aj najmenšie teleso, alebo pánty z vonkajšej strany.

Vložky do všetkých dverí by určite mali byť 4. bezpečnostnej triedy. Aktuálne je na českom trhu výhodná vložka *TOKOZ PRO 400*, ktorá spĺňa požiadavky tejto triedy, jej jadro je veľmi rezistentné pre lockpicking[2] a jej cena je pritom zanedbateľná. Kľúče by mali byť rozdelené následovne:

2. Ide de facto o napodobeninu jadra ASSA ABLOY Potec 2, ktoré majú problém prekonať aj profesionálni zámočníci.

- Všetky kľúče má len najvyšší predstaviteľ manažmentu, ktorý za bezpečnosť zodpovedá.
- Kľúč od miestnosti pre návrh a analýzu majú navyše aj ľudia pracujúci v tomto priestore,
- Kľúče od miestnosti pre návštevníkov a jednanie môžu mať laxnejšiu správu,
- Zámky od dverí, ktoré riadi prístupový systém sa nechávajú počas pracovnej doby odomknuté. Pre zvýšenie bezpečnosti a samotné využitie bezpečnostných prvkov vyššej kategórie dverí by sa mali zamykať vždy, keď sa v priestoroch nikto nenachádza. Tieto zámky však operuje len najvyšší predstaviteľ manažmentu, v prípade jeho neprítomnosti jeden jeho zástupca.

Ďalším podstatným prvkom sú okná. Vyššie poschodie je síce veľmi dobrá voľba, profil konkrétnej budovy nie je úplne hladký a hypoteticky by sa dal zneužiť. Záleží na zvážení rizika na mieste (konkrétnu polohu vrámci budovy nepoznám) a možností, či chceme okná meniť. Ale najskôr asi nie.

### 5.1.2 Prístupový systém

Pri vyberaní prístupového systému som bol veľmi nemilo prekvapený ponukou na trhu. V celom odvetví existuje jediný otvorený štandard s cieľom bezpečnej komunikácie medzi prvkami - *OSDP*[3] v kombinácii s *SCP*[4]. Avšak skoro všetky podporujúce prvky zároveň ako legacy podporujú aj desiatky rokov starý *Wiegand*[5], ktorý je jednoduché odpočúvať a útočník by ich mohol teoreticky využiť.

Lákavé sú aj bezdrôtové prvky, ktoré výrazne zjednodušujú inštaláciu. Tie často využívajú protokol *ZigBee*[6], ktorý však má niektoré návrhové vzory zle a samotné implementácie v produktoch nevyužívajú

3. Open Supervised Device Protocol - protokol pre bezpečnú drôtovú komunikáciu medzi prvkami fyzickej bezpečnosti použiteľný na TCP/IP sieti, ale aj na sériovej zbernici - najlepšie RS485.
4. Secure Channel Protocol - šifrovacia nadstavba OSDP.
5. De facto úplne prvý štandard pre bezkontaktné (pasívne) karty hojne využívaný v odvetví elektronickej kontroly prístupu.
6. Bezdrôtový protokol postavený na *IEEE 802.15.4* - ten umožňuje životnosť zariadenia vytiahnuť až na niekoľko rokov na jednu batériu.

ani odporúčané postupy[46], čo vyúsťuje v jednoducho vykonateľné útoky. Napr. *Aperio* od *ASSA ABLOY* má zrejme vlastný proprietárny protokol na podobnej bázi, avšak v dokumentácii sa pri bezpečnosti bezdrôtového spojenia uvádza len *AES-128*, čo samo o sebe o bezpečnosti nič nehovorí. Podobné technológie vyzerajú sľubne, avšak prístup *security through obscurity* by zákazník brať nemal, hlavne pri bezdrôtových technológiách.

K tomu všetkému je zabezpečovacia technika veľmi rozdrobená - aj keď sa väčšinou používa len pár protokolov, výrobcov prvkov je veľké množstvo. Len na českom trhu existuje minimálne 10 rôznych riadiacich prvkov pre kontrolu vstupu, ktoré si integrátori vyvíjajú sami. Zákazník by mal pri výbere požadovať konkrétnejšie informácie ako napr. využitie knižnice *liblogicalaccess*[7], ktoré znižuje riziko že pri vlastnom vývoji zanedbali implementáciu *OSDP*. Keďže ja pri vyhľadávaní produktov takéto informácie nemám, uvediem len príklady produktov, ktoré minimálne na papieri vyzerajú dobre:

- Možné zabezpečovacie systémy:
  - *Axis A1001*
  - *CEM eDCM 350*
- elektromechanické zapadacie plechy podľa zárubne, dverí a zámku,
- Možné čítačky:
  - *ICLASS R40*
  - *Rosslare AYH-6255*
- Možné technológie kariet: (*Pozn.: Je potrebné využívať zabezpečené bloky kariet a nie ich samotnú identifikáciu*)
  - *MIFARE DESFire EV2*
  - *MIFARE Ultralight EV1*

7. `https://github.com/islog/liblogicalaccess`

### 5.1.3 Elektronická zabezpečovacia signalizácia

Pri zabezpečovacej signalizácii sú podstatné umiestnenie a technológia prvkov, rozloženie podoblastí a bezpečnostná úroveň podľa *EN 50131-3*. Čo sa týka bezpečnostnej úrovne, určite preferujem úroveň 4, avšak na trhu sú oveľa dostupnejšie prvky úrovne 3, ktorá by mohla plne postačovať.

Priestory by som rozdelil na dve oblasti - do prvej by spadala miestnosť pre manažment a analytikov, do druhej zas priestory pre vývoj. Návštevné priestory by ostali nezabezpečené, prípadne by mohli spadať do prvej oblasti. Každý z týchto oblastí má vlastnú ústredňu, aby sa predišlo zbytočnému prístupu do cudzích miestností.

Ako prvé je potrebné vyriešiť umiestnenie ústrední - najlepšie umiestnenie je vedľa okna. Je potrebné zabrániť, aby ich mohol niekto pozorovať a čítať kódy jednotlivých užívateľov. To platí o pozorovaní cez okno, ale aj kamerou. Svojim osobným kódom by mal disponovať každý, kto má oprávnenie zapínať a vypínať stráženie danej oblasti. A podľa v predchádzajúcej kapitole zadefinovaných princípov by takýchto ľudí malo byť minimum.

Pohybové senzory považujem za nutnosť. Použijeme v každej miestnosti jeden *PIR* senzor inštalovaný v rohu pri okne, pričom ho môžeme vrámci princípu redundancie doplniť vo väčších miestnostiach kombinovaným *MW+PIR* detektorom v rohu pri dverách. Technológie a umiestnenia sú navrhnuté tak, aby bola detekcia čo najcitlivejšia a zároveň aby sa zabránilo nechceným falošným poplachom. Taktiež nie je dobrý nápad používať viacero mikrovlnných radarov proti sebe.

Chodbové dvere do zabezpečených oblastí by mali byť vybavené magnetickým detektorom otvorenia umiestnenom v bode, kde sú dvere mechanicky najslabšie (medzera medzi zámkami je najväčšia). Prípadného zlodeja tak alarm vyruší už počas otváraní dverí.

Pre ochranu okien by sa mali vybaviť priestory detektorom rozbíjania skla - zvukovým a to kvôli ich veľkosti a členitosti. Ideálne by bolo nainštalovať aj detektor otvorenia, avšak prvkov, ktoré sa otvárajú je priveľa.

Výber konkrétnej ústredne záleží hlavne na ústredni používanej centrálnym pultom, ktorý chce firma použiť. V tomto sa bohužiaľ viac určiť nedá, aj keď môžem odporúčať kombináciu aspoň dvoch nezávislých technológií komunikácie s ústredňou a navyše zasielanie

správ na telefón najvyššieho manažéra. Taktiež sa hodí mať podporu pre protipožiarne prvky. Konkrétne zariadenia vyberám len kvôli približnému cenovému ohodnoteniu.

Možnými použiteľnými prvkami sú:

- Ústredne:
  - *DIGIPLEX EVO192*
  - *KELCOM Power NEO*
- Pohybové senzory:
  - *Siemens PDM-I12T, PDM-IXD12T*
  - *BOSCH ISC-PDL1-WA18G*
- Magnetické senzory:
  - Techfors DC148
- Detektory rozbíjania skla:
  - *Jablotron JA-110B*

### 5.1.4 Kamerový systém

Rozloženie kamerového systému navrhujem tak, aby boli pod dohľadom všetky dvere vrámci zabezpečených oblastí (prípadne jednu kameru navyše umiestniť aj na chodbu, ak je to možné) a zariadenia uchovávajúce dôležité dáta, s ktorými by mohlo byť fyzicky manipulované.

Čo sa týka bezpečnosti, je potrebné si pred objednaním zistiť, či kamery, alebo nahrávacie zariadenia nemajú závažné bezpečnostné chyby. Osobne som sa totiž nestretol so značkou, ktorá by to robila správne, v čom súhlasím s výskumníkom Craigom Heffnerom, na ktorého prednášku [25] som sa viackrát odkazoval. Preto nechcem navrhovať konkrétne produkty. Craig v prednáške spomína väčšie spoločnosti, ktoré zas idú cestou *Security through obscurity* - nezverejňujú aktualizácie firmvérov, čo určite nie je dobrá cesta. Môžem spomenúť kamery značky *Wonderex*, ku ktorým sa mi počas spopmíaného

etického útoku[30] ani po dlhých hodinách skúmania firmvéru nepodaril zistiť spôsob resetu hesla, ktorý tam však očividne je. To však môže hovoriť aj o mojich schopnostiach. Pri cenotvorbe teda použijem priemernú cenu kamier z danej oblasti.

Je potrebné myslieť aj na možnosť sabotáže, preto by mali byť všetky kamery nahrávané redundantne na dvoch miestach. V prílohe A ukazujem možnosť umiestnenia záložného systému v priestoroch pre manažment, avšak ekvivalentným, možno v určitom hľadisku lepším miestom by boli priestory pre vývoj.

### 5.1.5 Infraštruktúra

Pri inštalácií sietí pre spomínané zariadenia, ale aj firemné servery by sme sa mali riadiť pokynmi, ktoré som navrhol v predchádzajúcej kapitole. Bude potrebné vybudovať infraštruktúru tak, aby k nej nebol jednoduchý prístup a hlavne zabezpečiť napájanie zabezpečovacích systémov zdrojom neprerušovaného napájania.

Keďže kamerové systémy trpia známymi problémami, mal by sa princíp oddelenia sietí uplatňovať hlavne tam.

Taktiež je dôležité pripomenúť, že všetky tieto zariadenia vrátane firemných serverov, ku ktorým nie je potrebný pravidelný fyzický prístup by mali byť fyzicky chránené skriňou so zámkom aj keď sú dobre rozložené.

## 5.2 Ochrana utajovaných informácií stupňa Vyhradené

Firma chce do budúcnosti prenajať ďalší priestor (ktorý rozlohou tvorí tretinu aktuálnych priestorov) a niektorý z týchto priestorov prideliť vývoju pre tento stupeň. Využiť by sa mohol práve tento nový priestor, keďže nie je fyzicky blízko zvyšku - ostatní zákazníci, ani niektorí zamestnanci vôbec nemusia vedieť, kde sa nachádza.

Čo sa týka zabezpečenia vrámci tohoto priestoru, je potrebné ako konkrétne prvky použiť niektoré z prostriedkov[8] certifikovaných NBÚ.

8. https://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/

Pre získanie bodového ohodnotenia pre stupeň Dôverné plne stačí redundancia a rozloženie navrhované pre zvyšok priestorov.

# 6 Záver

V práci som opísal problémy a hrozby, ktoré existujú pri zabezpečovaní IT organizácií. Základný problém som uviedol v prvej kapitole a tu by som ho možno zhrnul ako paradoxný nedostatok informatického prístupu pri komplexnom navrhovaní zabezpečenia - zabezpečovacie prvky nie sú dostatočne otvorené, využíva sa prístup *Security through obscurity* a zastaralé technológie. Celému problému napomáha aj to, že vývojári sa spravidla nezaujímajú o tieto fyzické prvky, ale ani o personálne záležitosti, či štruktúry medziľudských vzťahov.

Tieto problémy som sa pokúsil vyriešiť komplexným návrhom zabezpečenia s aspektami, ktoré sa najviac podieľajú na zabezpečení toho (po ľudskom živote) najcennejšieho - aktív spoločnosti. Skombinoval som pri tom informácie z mnohých zdrojov vrátane princípov, ktoré sa uplatňujú pri zabezpečovaní utajovaných skutočností. Na tomto pomerne naddimenzovanom návrhu sa dajú jednoducho stavať procedúry použiteľné v každej IT spoločnosti, ale aj v iných organizáciách, ktoré svoje citlivé údaje spracúvajú vrámci informačných systémov. A Keďže návrh fyzického zabezpečenia sa dá jednoducho konkretizovať na základe poskytnutého rozloženia priestorov, demonštroval som tieto princípy na príklade menšej spoločnosti.

Práce v tejto oblasti je však ešte veľa a niekedy to vyzerá, ako by sme sa vôbec neposúvali vpred. Odvetvie zabezpečovania nutne potrebuje viac *open source* prístup - auditu návrhov, možnosti aktualizácie pre prípad nájdenia bezpečnostnej chyby atď. Z pochopiteľných dôvodov však nikto nechce riskovať závratný nárast konkurencie na trhu. Preto dúfam, že sa toho rovnako, ako svojho času softvéru a hardvérových štandardov chytí oveľa širšia komunita a tým sa zvýši agresivita vo vývoji. A aj keď netuším, ako to docieliť, manažéri si potrebujú viac uvedomovať potrebu bezpečnosti aj keď sa nechcú len blysnúť certifikátom *ISO 27001* a taktiež si uvedomovať nebezpečenstvo *ad-hoc* prístupu, ktorý nerieši bezpečnosť komplexne.

Preto sa tomuto odvetviu chcem venovať aj v profesionálnej praxi a čo najviac rozvíriť ustálené postupy.

# A Orientačný plán priestorov firmy s navrhovaným rozložením bezpečnostných prvkov

# A. Orientačný plán priestorov firmy s navrhovaným rozložením bezpečnostných prvkov

# B Hrubý cenový odhad navrhovaného zabezpečenia

Cenový odhad je približný a pre istotu mierne nadhodnotený, keďže nie všetky produkty majú, pochopiteľne zverejnenú cenu.

- Fyzické prvky:
  - Bezpečnostné dvere kat. 4: 3x 40 000 Kč
  - Bezpečnostné dvere kat. 2: 15 000 Kč
  - Vložka TOKOZ PRO 400: 4x 1500 Kč
- Prístupový systém:
  - Prístupový systém (ICLASS R40 alebo Rosslare AYH-6255): 20 000 Kč
  - Zapadací plech: 2x 5000 Kč
  - Čítačka: 2x 10 000 Kč
  - Náklady na jednu kartu: do 500 Kč
- Elektronická zabezpečovacia signalizácia
  - Ústredňa s klávesnicou (*DIGIPLEX EVO192* alebo *KELCOM Power Neo*): 2x 8 000 Kč
  - Pohybové senzory (*Siemens, alebo BOSCH*: 5x 3 000 Kč
  - Magnetické senzory (*Techfors DC148*: 2x 1000 Kč, prípadne viac aj na okná
  - Akustický detektor rozbitia skla (*JA-110B*): 3x 1 000Kč
- Kamerový systém
  - Kamera (z dôvodov uvedených v práci nešpecifikovaná): 3x 5 000 Kč
  - Nahrávací systém: (2x) 8 000 Kč
- UPS - zdroj neprerušovaného napájania (napr. *CyberPower OLS1000E)*: 10 000 Kč

- Výsledná cena prostriedkov: cca 280 000 Kč
- Zvyšné náklady práce, integračnej marže a budovania infraštruktúry veľmi hrubo odhadujem na ďalších 50 000 Kč
- Náklady na zabezpečenie ďalšieho priestoru: do 150 000 Kč

# Bibliografia


1. *Hackers Are Using Leaked NSA Backdoors to Hack Tens of Thousands of Vulnerable Windows PCs* [online]. Washington (D.C.): WCCF PTE LTD, 2017 [cit. 2017-12-09]. Dostupné z: https://wccftech.com/windows-nsa-backdoor-shadow-brokers/.
2. ERBSCHLOE. *Walling Out the Insiders: Controlling Access to Improve Organizational Security*. 1st ed. Boca Raton: CRC Press, 2017. ISBN 978-1-13-803160-9.
3. *Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti (412/2005)*. Parlament České Republiky, 2005. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/1089-zakon-c-4122005/.
4. GATES, Johnson. *Purple Teaming Cyber Kill Chain* [online]. 2017 [cit. 2018-10-21]. Dostupné z: https://sector.ca/wp-content/uploads/presentations16/Gates%20Johnson%20Purple%20Teaming%20Cyber%20Kill%20Chain%20Final.pdf.
5. *Zákon o kybernetické bezpečnosti (181/2014)*. Parlament České Republiky, 2014. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/1091-zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/.
6. *Vyhláška o kybernetické bezpečnosti (316/2014)*. Parlament České Republiky, 2014. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1081-provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/.
7. *Vyhláška o významných informačních systémech (317/2014)*. Parlament České Republiky, 2014. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1081-provadeci-pravni-predpisy-k-zakonu-c-1812014-sb-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu/.

8. *Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)* [online]. Národní úřad pro kybernetickou a informační bezpečnost, 2014 [cit. 2018-05-01]. Dostupné z: https://www.govcert.cz/download/kii-vis/container-nodeid-663/2schemakii-cz.pdf.

9. *Vyhláška o fyzické bezpečnosti a certifikaci technických prostředků (528/2005)*. Parlament České Republiky, 2005. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1085-vyhlaska-c-5232005/.

10. *Vyhláška o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor (523/2005)*. Parlament České Republiky, 2005. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1087-vyhlaska-c-5282005/.

11. *Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznam utajovaných informací, ve znění pozdějších předpisů*. Parlament České Republiky, 2005. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1080-narizeni-vlady-c-5222005/.

12. *ROZHODNUTÍ RADY o bezpečnostních pravidlech na ochranu utajovaných informací EU (2013/488/EU)*. Úřední věstník Evropské unie, 2013. Dostupné tiež z: https://www.nbu.cz/download/pravni-predpisy-eu/container-nodeid-722/l27420131015cs00010050.pdf.

13. *ČSN EN ISO/IEC 27000 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník*. Standard. Český normalizační institut.

14. *ČSN EN ISO/IEC 27002 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací*. Standard. Český normalizační institut.

15. *ČSN ISO/IEC 27033-1 Informační technologie - Bezpečnostní techniky - Bezpečnost sítě - Část 1: Přehled a pojmy*. Standard. Český normalizační institut.

16. *ČSN P CEN/TS 14383-4 Prevence kriminality - Plánování městské výstavby a navrhování budov - Část 4: Obchodní a administrativní budovy*. Standard. Český normalizační institut.

17. *Exploit database* [online]. Offensive Security Ltd., 2018 [cit. 2018-10-21]. Dostupné z: `https://www.exploit-db.com/`.

18. *ATT&ck knowledge base* [online]. MITRE, 2018 [cit. 2018-05-01]. Dostupné z: `https://attack.mitre.org/`.

19. PIKUS, Miroslav. *tajné dátové centrum Azure ma prekvapilo enormnou škálou, bezpečnostnými procesmi a jednoduchými riešeniami* [online]. 2018 [cit. 2018-11-26]. Dostupné z: `http://blog.hysteria.sk/bol-som-v-dc-azure/`.

20. *ČSN EN 1627 Dveře, okna, lehké obvodové pláště, mříže a okenice - Odolnost proti vloupání - Požadavky a klasifikace*. Standard. Český normalizační institut.

21. OLLAM, Deviant. *Copying Keys from Photos, Molds & More* [online]. 2018 [cit. 2018-11-28]. Dostupné z: `https://www.youtube.com/watch?v=AayXf5aRFTI`.

22. OLLAM, Deviant. *I'll Let Myself In: Tactics of Physical Pen Testers* [online]. 2017 [cit. 2018-11-01]. Dostupné z: `https://www.youtube.com/watch?v=rnmcRTnTNC8`.

23. ŠANTA, Marek. *Targeting microwave request-to-exit sensor from the outsides* [online]. 2018 [cit. 2018-11-01]. Dostupné z: `https://www.youtube.com/watch?v=oaOJCwdPZmM`.

24. *MythBusters: Crimes and Myth-Demeanors 2*. 2006. Č. 59.

25. HEFFNER, Craig. *Black Hat 2013 - Exploiting Network Surveillance Cameras Like a Hollywood Hacker* [online]. 2013 [cit. 2018-11-01]. Dostupné z: `https://www.youtube.com/watch?v=B8DjTcANBx0`.

26. ROBERT CALLAN, Alenka Zajic; PRVULOVIC, Milos. *A Practical Methodology for Measuring the Side-Channel Signal Available to the Attacker for Instruction-Level Events*. 2014. Dostupné tiež z: `https://www.cc.gatech.edu/home/milos/Papers/2014_MICRO_SAVAT.pdf`. Georgia Institute of Technology.

27. *Casting Key Copies - Demo* [online]. MrAnybody, 2015 [cit. 2018-11-01]. Dostupné z: `https://www.youtube.com/watch?v=bWUhav3relw`.

28. *Tastic RFID Thief* [online]. Bishop Fox, 2013 [cit. 2018-10-21]. Dostupné z: https://www.bishopfox.com/resources/tools/rfid-hacking/attack-tools/.

29. ROMAN SILBERSCHNEIDER, Thomas Korak; HUTTER, Michael. *Access Without Permission: A Practical RFID Relay Attack*. 2013. Dostupné tiež z: https://www.researchgate.net/publication/263314494_Access_Without_Permission_A_Practical_RFID_Relay_Attack. Graz University of Technology.

30. ŠANTA, Marek. *Challenges of Securing a Custom Embedded System* [online]. 2018 [cit. 2018-11-26]. Dostupné z: https://santomet.eu/2018/11/26/challenges-of-securing-a-custom-embedded-system/.

31. *Seznam certifikovaných technických prostředků - Elektrická zámková zařízení a systémy pro kontrolu vstupů*. Národní Bezpečnostní Úřad ČR, 2018. Dostupné tiež z: https://www.nbu.cz/cs/informacni-centrum/seznamy/seznam-certifikovanych-technickych-prostredku/923-elektricka-zamkova-zarizeni-a-systemy-pro-kontrolu-vstupu/.

32. SCOTT FLUHRER, Itsik Mantin; SHAMIR, Adi. *Weaknesses in the Key Scheduling Algorithm of RC4*. 2004. Dostupné tiež z: http://www.mattblaze.org/papers/others/rc4_ksaproc.pdf. Cisco Systems, Inc. a Computer Science department, The Weizmann institute.

33. MATHY VANHOEF, Frank Piessens. *Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2*. 2017. Dostupné tiež z: https://papers.mathyvanhoef.com/ccs2017.pdf. imec-DistriNet, KU Leuven.

34. MARLINSPIKE, Moxie; HULTON, David. *Defeating PPTP VPNs and WPA2 Enterprise with MS-CHAPv2* [online]. DEF CON, 2012 [cit. 2018-11-01]. Dostupné z: https://www.youtube.com/watch?v=gkPvZDcrLFk.

35. *ATT&ck knowledge base - Lateral Movement Techniques* [online]. MITRE, 2018 [cit. 2018-11-01]. Dostupné z: https://attack.mitre.org/tactics/TA0008/.

36. *The Human Factor in Data Protection*. 2012. Dostupné tiež z: https://www.ponemon.org/local/upload/file/The_Human_Factor_in_data_Protection_WP_FINAL.pdf. Ponemon Institute LLC.

37. OLLAM, Deviant; PAYNE, Howard. *Elevator Hacking - From the Pit to the Penthouse*. 2015. Dostupné tiež z: https://www.youtube.com/watch?v=srt3c38jhHcI.

38. *The Insider Threat: An Introduction to Detecting and Deterring an Insider Spy*. United States Department of Justice, Federal Bureau of Investigation, 2012. Dostupné tiež z: https://www.fbi.gov/file-repository/insider_threat_brochure.pdf.

39. *Insider Thread Guide: A Compendium of Best Practices to Accompany the National Insider Thread Minimum Standards*. Office of the Director of National Intelligence, The National Counterintelligence a Security Center, National Insider Thread Task Force, 2017. Dostupné tiež z: https://www.dni.gov/files/NCSC/documents/nittf/NITTF_InsiderThreatGuide2017_022818.pdf.

40. *PSR-500 perimeter surveillance radar system* [online]. Rockwell Collins, 2017 [cit. 2018-11-28]. Dostupné z: https://www.youtube.com/watch?v=oHf1vD5_b5I.

41. *Věstník Národního bezpečnostního úřadu*. Národní bezpečnostní úřad, 1/2011. Dostupné tiež z: https://www.nbu.cz/download/vestnik/container-nodeid-570/0238-11.pdf.

42. *Kompromitující vyzařování - Metodické pokyny* [online]. Národní bezpečnostní úřad [cit. 2018-12-01]. Dostupné z: https://www.nbu.cz/cs/ochrana-utajovanych-informaci/bezpecnost-informacnich-systemu/kompromitujici-vyzarovani/999-metodicke-pokyny/.

43. JOXEAN KORNET, COSEINC. *Breaking antivirus software* [online]. SYSCAN 360 [cit. 2018-12-01]. Dostupné z: http://www.syscan360.org/slides/2014_EN_BreakingAVSoftware_JoxeanKoret.pdf.

44. *Vyhláška o zajištění kryptografické ochrany utajovaných informací (432/2011)*. Parlament České Republiky, 2011. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1084-vyhlaska-c-4322011/.

45. *o administrativní bezpečnosti a o registrech utajovaných informací (529/2005)*. Parlament České Republiky, 2005. Dostupné tiež z: https://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/1088-vyhlaska-c-5292005/.

46. ZILLNER, Tobias; STROBL, Sebastian. *ZigBee Exploited: The Good, The Bad, And The Ugly* [online]. Black Hat, 2015 [cit. 2018-11-01]. Dostupné z: `https://www.youtube.com/watch?v=bWUhav3relw`.