Univerzita Pardubice

Fakulta ekonomicko-správní

Informační a monitorovací systémy při ochraně bezpečnosti a detektivní - zpravodajské činnosti v malých a středních firmách

Pavel Knap

Bakalářská práce

2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Pavel KNAP**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Informační a monitorovací systémy při ochraně bezpečnosti a detektivní - zpravodajské činnosti v malých a středních firmách**

Zásady pro vypracování:

Identifikace osob
Sledování pohybu osob a vozidel
Ochrana citlivých dat a informací
Ochrana počítačových sítí

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

BRABEC, František. OCHRANA BEZPEČNOSTI PODNIKU. Praha : EUROUNION, 1996. 203s.
KAMENÍK, Jiří, BRABEC, František, MUSIL, Rudolf. KOMERČNÍ BEZPEČNOST. Praha : Aspi, 2007. 300s.

Vedoucí bakalářské práce: **doc. Ing. Pavel Petr, Ph.D.**
Ústav systémového inženýrství a informatiky

Konzultant bakalářské práce: **JUDr. František Brabec**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **6. října 2008**

Termín odevzdání bakalářské práce: **1. května 2009**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:
Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univezita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřené příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 24.8.2009

Pavel Knap

Děkuji vedoucímu bakalářské práce doc. Ing. Pavlu Petrovi Ph.D. za cenné rady a pomoc při psaní této práce.

Anotace

Předkládaná bakalářská práce se zabývá bezpečnostními systémy v ochraně vlastnictví malých a stredních firem. Je založena na rozboru existujících zabezpečovacích systémů; jednotlivě pojednává o součástech těchto systémů. Vývoj elektronických zabezpečovacích systémů je neoddělitelně propojen s vývojem informačních technologií. V závěrečné části práce autor konstatuje zásadní závislost zabezpečovacích systémů na obecném vývoji technologií, který podmiňuje jejich vysokou variabilitu.

Klíčová slova

identifikace, bezpečnostní systémy, biometrie, detektory, trezory

Title

Information and monitoring systems in the security and detection policies of small and middle-sized companies

Annotation

This bachelor thesis concerns the role of security systems in the protection of the property of small and middle-sized companies. It is based on a detailed analysis of the security systems used today and considers the functional parts of these systems separately. The electronic security systems are integrally connected with the development of information technologies – in the final part of this thesis, the author states therefore that the progress of the security systems depends on the technological development as a whole, and it is highly variable.

Keywords

identification, monitoring systems, biometrics, safes

Obsah

1. Úvod

Stejně tak jako manažeři věnují svůj čas výběru vhodného počítače, měli by věnovat čas i ochraně majetku firmy. Počty krádeží každým rokem rostou a stačí jediná noc a firma může přijít o velmi drahé vybavení. Mnohdy jde o majetek, jež firma nemusí být schopna nahradit.

Ceny elektronických zabezpečovacích systémů stále klesají. Vybudování vhodného bezpečnostního systému stojí zlomek hodnoty, než majetek který pomáhá chránit. Bezpečnostní systém, ale není jen malá plastová krabička krčící se u stropu v rohu místnosti. Jedná se o komplexní záležitost.

V dnešní době rozvoje internetu je třeba chránit i data a informace. Zabezpečit firmu nejen před útoky zlodějů vkrádajícími se rozbitým oknem, ale také před zloději, vkrádajícími se do firemních databank pomocí počítačů. Dobře nastavený bezpečnostní systém nebude firmu omezovat, naopak ji může pomocí svých dodatečných funkcí usnadnit například evidenci zaměstnanců a jejich příchodů a odchodů do zaměstnání.

Bezpečnostní a informační systémy ale dokážou mnohem více. Mohou se starat o klimatizaci, hlídat osvětlení, kontrolovat požární detektory a řídit protipožární systém. Mohou být využity jako vnitropodnikový videotelefon. K tomu všemu ani nebude třeba tahat úplně nové vedení, protože stačí použít již existují počítačové rozvody. V případě nutnosti se lze obejít i bez nich. Cílem této práce je prozkoumat možnosti zabezpečovací techniky a vybrat, které prostředky by byly nejvhodnější pro středně velkou firmu. Vše začíná u vstupních dveří.

2. Identifikace osob

Podle vyhlášky 523/2005 Sb. [1] se autentizací subjektu myslí proces ověření jeho identity splňující požadovanou míru záruky. Subjektem může být nejen osoba, ale například i stroj či program. Subjekt se během autentizace může prokázat:

a) znalostí,
b) předmětem,
c) vlastností.

Znalostí myslíme například znalost příslušného hesla. Předmětem pak může být klíč k zámku, identifikační karta nebo i obyčejná pozvánka. Vlastností subjektu jsou jeho biometrické údaje v případě osob a správná reakce na vyslaný signál v případě strojů či programů [2, strana 48].

Proces autentizace lze dále dělit podle spolupráce subjektu na kooperativní a nekooperativní, a to podle doby, kdy je autentizace prováděna na statickou a průběžnou, podle nároků na autentizovaný subjekt na obvyklou a neobvyklou. Samozřejmě lze autentizaci provádět zjevně i skrytě tak, aby subjekt netušil, že je kontrolován. Autentizaci může provádět buď osoba, vrátný či člen ochranky objektu, ale stále častěji, tak jak jsou tyto systémy zdokonalovány, je autentizace prováděna pouze k tomu určeným strojem bez nutnosti lidské přítomnosti.

2.1 Identifikace znalostí

Tato metoda představuje jeden z nejrozšířenějších prostředků autentizace. Osoba se v tomto případě prokazuje znalostí, kterou by měla znát pouze ona [2, strana 88]. Touto znalostí je nejčastěji heslo nebo číselný kód. Heslo či kód je snadno přenositelné a jeho používání je celkem pohodlné. Pohodlí je ale vyváženo řadou nevýhod a rizik. V současnosti jsou hesla považována za slabý prostředek zabezpečení.

Hesla mají různé podoby jména, iniciál a názvů z okolí uživatele. Běžná jsou data narození přímo uživatele či jeho blízkého příbuzného. Testy dokazují, že v 50 % případů lze heslo odhalit během deseti pokusů.

Uživatelé vždy volí hesla tak, aby si je mohli zapamatovat, což samozřejmě usnadňuje jejich uhodnutí. Nemají rádi hesla dlouhá a složitá. Přitom všichni někdy slyšeli o případu, kdy neoprávněně nainstalovaná kamera snímala osobní identifikační číslo (PIN) vkládané z klávesnice bankomatu. Kamera ani není nutností. Stačí opodál postávající člověk nenápadně sledující zadávání kódu.

Běžným problémem je také zapomnětlivost. Mnoho uživatelů tento problém řeší zapsáním hesla na malý lístek, který pak klidně nosí s bankovní kartou v jedné peněžence (v případě PINu) nebo jej přilepí na spodní stranu klávesnice či podložky pod myš.

Zvýšení bezpečnosti hesel by pomohlo tvoření hesel kombinací velkých i malých písmen abecedy, číslic a speciálních znaků (pokud jsou přípustné). Hesla by měla být dostatečně dlouhá a neměla by tvořit žádné známé slovo ani jejich kombinaci. Hesla je vhodné pravidelně měnit, zamezit zadávání stále stejného hesla či pouhé střídání hesel. Pokud je to možné, využíváme hesel jednorázových s časově omezenou platností. Vyplatí se i kontrola, zda uživatel neužívá stejné heslo v několika systémech současně.

2.2 Identifikace předmětem

Identifikace přemětem je asi nejstarším způsobem identifikace [2, strana 48]. Jako úplně nejjednodušší identifikační předmět můžeme asi považovat obyčejnou pozvánku nebo například lístek do kina. Stačí tento malý předmět, nejčastěji vyrobený z papíru, ukázat u vchodu a obsluha nás pustí dovnitř. Výhodou je snadná přenositelnost (pokud není pozvánka na jméno) a levná výroba. Většina vstupenek a pozvánek má jasně vyznačenou platnost a je tedy pouze jednorázová. Pro zvýšení spolehlivosti vám obsluha odrhne či odstřihne menší část vstupenky.

Nejběžnějším způsobem identifikace je klíč [3]. Klíče mají nejrůznější tvary a velikosti a umožňují nám odemknout zámek na vratech, v domovních dveřích nebo nastartovat auto. Klíče a zámky jsou všude kolem nás.

Mechanické zařízení fungující jako zámek znali již staří Egypťané. Jejich dřevěné závory obsahovaly sadu západek, které byly vlivem gravitace ve své spodní

klidové poloze, čímž bránily otevření dveří.

Pouze člověk vlastnící klíč mohl odsunout závoru. Klíč vypadal jako dřevěná tyč opatřená na jedné straně kolíčky, jež přesně zapadaly do příslušných dírek. Kolíčky posunuly západky vzhůru do jedné roviny a bylo otevřeno.

Již v dobách velkého Říma existovaly kovové zámky, jež vypadaly jako ty, které známe z chalup našich babiček. Přesvědčily nás o tom archeologické vykopávky v popelu pohřbených Pompejích. Kovové zámky se nacházeli na vnitřní straně dveří a obsluhovali se klíčem zvenku. V té době bylo velkou módou zakomponování klíče do různých šperků.

V současné době je nejrozšířenější zámek cylindrický. Vynalezl jej v roce 1847 američan Linus Yale. Tehdejší zámky mu nepřipadaly příliš bezpečné a tak změnil tvar zámku ve válcovou vložku a použil ploché klíče se zářezy.

Klíč po vložení do zámku nadzdvihne odpružené kolíčky, a to právě o tolik, aby se jejich modrá část ocitla mimo otočný válec, zatímco jejich červená část zůstala v něm. Tak je možno klíčem otočit a odsunout západku. Princip je velmi podobný již výše uvedenému Egyptskému zámku. Linus Yale při konstrukci zámku přišel s geniálním nápadem. Zámek se již nemontuje po jedné straně dveří, ale prochází napříč dveřmi. Samozřejmě existuje způsob jak tento zámek, stejně jako všechny ostatní, otevřít i bez příslušného klíče. Proto jsou zámky a jejich klíče stále vylepšovány. Základní princip ale zůstává stejný až do dnes.

Identifikační kartu si lze představit jako vstupenku na více použití [2, stana 71][4]. Pro větší odolnost jsou většinou vyrobeny z plastu či papíru zataveného do plastu a navíc opatřeny ochrannými prvky proti duplikování. Identifikační karty nejčastěji označují příslušnost ke státu, společnosti apod.

V řadě států je vydávána identifikační karta jako všeobecně povinný doklad. V České republice jsou to občanský průkaz, řidičský průkaz a průkaz pojištěnce zdravotní pojišťovny.

Všechny identifikační karty mají stejný účel. Přiřazují jedinci jednoznačný identifikační kód, pomocí kterého jsou pak v centrálním registru obyvatel vyhledávány další údaje. Karta velikosti bankovní karty obsahuje řadu osobních informací o jeho držiteli - jméno a příjmení, pohlaví, datum narození, adresu bydliště, občanství a

podobně. Informace o vydavateli karty, číslo karty a datum platnosti jsou na kartě často uvedeny reliéfním písmem (tzv. embosované karty). Častá je také fotografie majitele. Množství osobních údajů je většinou nepřímo úměrné důležitosti karty. Stačí si vedle sebe položit například řidičský průkaz a kartu, která nám umožňuje vstup do místní knihovny.

Plastová karta s magnetickým páskem je nejvíce rozšířena v bankovnictví. Velikost karty 85,6x54,0x0,76 mm je stanovena mezinárodní normou ISO 3554. Zápis údajů se provádí na magnetický proužek na spodní straně karty.

Proužek je tvořen velkým množstvím malých permanentních magnetů. Pro změnu zaznamenaných dat musíme působit silnou magnetickou indukcí přímo na jeden magnet. Pokud se odchýlíme, ovlivníme i některý ze sousedních magnetů a tím znehodnotíme zapisovaná data.

Životnost samotné karty je velmi vysoká, stejně tak spolehlivost na ní uložených dat. Možnost měnit již jednou zapsaná data je na jednu stranu velkou výhodou, ale na stranu druhou nevýhodou zároveň.

Výhodou je možnost aktualizovat údaje bez nutnosti výroby nové karty. Bohužel z toho samého důvodu nelze považovat kartu za zcela důvěryhodnou. Kdokoliv může pomocí vhodného zařízení kartu upravit či duplikovat. Současně se nedoporučuje nosit karty s magnetickým proužkem pohromadě s mobilním telefonem, protože dlouhodobé působení vyzařovaných vln z antény telefonu může data uložená na magnetickém pásku poškodit.

Ve standardu ISO pro magnetické karty jsou definovány 3 stopy záznamu, které mohou být v jednom magnetickém proužku.

Na 1. stopu lze uložit v numerické nebo alfanumerické podobě 79 Bytů informací. Na 2. a 3. stopu lze již ukládat pouze znaky numerické. Na 2. stopu 40 Bytů a na 3. stopu 107 Bytů. Od této technologie se však postupně ustupuje.

Čipová karta je téměř stejná jako karta s magnetickým páskem, jen jako nosič informací je místo magnetického pásku použit integrovaný čip. Nejjednoduší čipy si pouze pamatují uložené údaje. Takový čip nalezneme například na telefonních kartách. Informace lze nejen přečíst, ale také měnit. Funkce takové karty se příliš neliší od obyčejné karty s magnetickým proužkem. Čipové karty sloužící k identifikaci

osoby využívají tzv. „chytrých“ čipů. V praxi to znamená, že čip na kartě neobsahuje jen paměť, ale také procesor. Procesor slouží ke zpracování aplikací uložených v paměti a obsluhuje rozhraní sloužící ke komunikaci s okolním prostředím. Většina této komunikace je šifrovaná.

Další výhodou je, že čipová karta může pro každou operaci vyžadovat tzv. PIN (z angličtiny Personal Identification Number). PIN je číselný kód, jež identifikuje oprávněného majitele karty a tím ještě snižujeme riziko zneužití karty.

Karta vybavená Radiofrekvenčním identifikačním čipem (RFID čip) funguje i bez nutnosti vkládání karty do přístroje [5]. Stačí se jen přiblížit s kartou dostatečně blízko. Čipy využívají ke komunikaci převážně nosnou frekvenci 125 kHz, 134 kHz a 13,56 MHz.

RFID čipy se dělí do dvou základních skupin - pasivní a aktivní.

Pasivní čipy se dnes nejčastěji v podobě malé nálepky přidávají obchodech na prodávané zboží. U vstupu do obchodu jsou „rámy“ vysílající pulsy s dosahem do 30 cm. Pokud se do jejich dosahu dostane pasivní RFID čip, využije energii signálu k nabití kapacitoru a k následnému odvysílání odpovědi. Odpověď zpětně vyhodnotí přijímač, který je také umístěný v „rámu“. Pokud není zboží zaplaceno u pokladny, kde je z něho čip odstraněn, spustí poplach.

Aktivní čipy jsou dražší a složitější na výrobu. Obsahují navíc zdroj sloužící k neustálému napájení čipu. Přítomnost baterie značně omezuje životnost čipu. Nejčastěji se využívají k aktivní lokalizaci.

Využití technologie automatického sběru informací a identifikace pomocí čipu ovládaného rádiovou frekvencí v současné době velmi roste. Umožňuje totiž sledovat předměty, zvířata a osoby na dálku bez jejich vědomí. Tyto čipy se v současné době dávají i do pasů občanů ČR.

Problémem však zůstává, jak zabránit neoprávněnému čtení údajů z čipu. Navíc s příchodem nových generací čipů se očekává prodloužení čtecí vzdálenosti z 20 cm až na 10 m. Rizik je hned několik. Díky všesměrovému vysílání nelze zabránit tajnému odposlechu komunikace mezi čipem a čtečkou. Nelze zneplatnit či pozměnit údaje v čipu. Stále je možné čipy klonovat. Do budoucna proto očekáváme snížení bezpečnosti a zvýšení rizika krádeže identity.

Zčásti tento problém řeší aplikace komunikačního standardu EAC (Extened Access Control). V praxi to znamená, že čip smí povolit přístup k datům na něm uložených pouze čtečce, která se prokáže validním certifikátem.

Technologie NFC (near field comunication) je zatím ve fázi testování. Cílem je možnost využívat k identifikaci a placení pomocí mobilního telefonu. Při placení jednoduše přiložíte ke čtecímu zařízení mobilní telefon a čip umístěný uvnitř přístroje vyřídí vše za vás.

2.3 Biometrická identifikace

Biometrická identifikace je metoda založená na rozpoznávání fyzických charakteristik osob [2, strana 103]. Nejznámějším takovým biometrickým prvkem jsou asi otisky prstů. Při použití biometrik pro identifikaci nebo autorizaci osoby jsou porovnávány dva vzorky. První vzorek, tzv. „živá data“, získáme přímo od osoby, jejíž totožnost chceme zjistit. Druhý vzorek, tzv. „referenční data“, jsou vzorky získané například při přijímání osoby na pracovní místo a nyní uložené v podnikové databázi. Referenční data mohou být také uložena na čipu identifikační karty. Pak ověřujeme, zda identifikační karta opravdu patří osobě, která se touto kartou prokazuje.

Referenční data nejsou klasicky uložena jako například obrázky otisků prstů, ale převádějí se do elektronické podoby, což je dlouhý kód přepočítaný z podstatných znaků sledovaného atributu. Například kód popisující otisk jednoho prstu má velikost kolem 100 kB.

Pokud se rozhodneme využít biometrické údaje při kontrole vstupu do našeho objektu, je třeba se dobře rozmyslet, kterou z metod zvolíme. Metody se velmi liší v ekonomické, technické i časové náročnosti.

Největší nevýhodou biometriky je, že nikdy nelze na 100% potvrdit či vyvrátit platnost. Heslo můžeme zapsat buď správně nebo špatně, ale biometrika má vždy jisté procento (lišící se podle použité technologie) chybně identifikovaných [7][8]. Jako příklad lze použít například podpis. Nikdy se vám nepodaří se dvakrát podepsat úplně stejně.

Oproti tomu je hlavní výhodou biometriky její jednoduchost. Nemůže se vám

stát, že zapomenete heslo nebo ztratíte klíče. Při identifikaci stačí jen například přiložit na snímač prst.

Biometrické údaje se velmi špatně falšují. Jsou známé drastické případy, (useknuté prsty) i nedrastické případy pokusů ošálit čtečku otisků prstů (pomocí želatiny vyrobený falešný prst) Pravý otisk prstu stačí sejmout například ze sklenice. Kvalitní systémy jsou proti takovýmto praktikám odolné, protože kontrolují i sekundární znaky jako je srdeční tep, teplota kůže nebo elektrický odpor kůže [2,strana 603].

Dalším problémem biometriky je, že ne každý je schopen či ochoten svoji totožnost prokázat. Důvody nemusí být jen náboženské či etické. Těžko můžeme chtít otisk prstu po bezrukém člověku, vlas na test DNA od holohlavého a ani neidentifikujete podle oční duhovky člověka, který přišel o oči. Samozřejmě se jedná o extrémní případy, ale pokud chceme, aby byl náš systém kvalitní, musíme s těmito případy počítat.

Výše zmíněný etický problém může nastat například při identifikaci pomocí testu DNA. Nejenom, že pomocí testu zjistíme spoustu informací o zdravotním stavu osoby (dědičné choroby), ale hlavně lze tímto způsobem sledovat příbuzenské vztahy.

Další nevýhodou biometrie je její pomalost. Pokud pouze ověřujeme identitu majitele předloženého identifikačního průkazu, máme výsledek okamžitě. Horší situace nastane, máme-li v databázi 46 milionů sad otisků prstů jako třeba americká FBI. I kdyby vaše firma neměla tolik zaměstnanců, chtělo by se vám každé ráno čekat u vchodových dveří třeba jen 1 minutu, než systém vše ověří a dveře otevře?

Přes všechny nevýhody nám biometrika každý den pomáhá. Ověřuje vlastnictví předmětů, identifikuje ztracené děti a nalezená mrtvá těla či určuje otcovství.

Téměř 50% všech přístrojů ověřujících biometrické údaje jsou snímače otisků prstů. Na světě nejsou dva lidé se stejným vzorem papilárních linií (kresbou prstů). Místa, jež nás na otisku zajímají, se nazývají markanty. Markant je jakákoliv změna v průběhu papilárních linií. Každý kompletní otisk prstu obsahuje 100 - 200 těchto bodů. Pro spolehlivou shodu stačí najít 12 shodných bodů. Testy ukázali, že při

identifikaci při použití jednoho prstu je výsledná přesnost 98,6 %, u porovnání charakteristických bodů v křivkách otisku dvou prstů je přesnost 99,6% a u více prstů pak tato přesnost dosahuje 99,9%.

Při porovnávání otisků prstů se využívají dvě základní metody [2, strana 212].

První metodou je porovnávání globálního vzoru. V jednoduchosti lze říci, že rozložíme obraz na jednotlivé oblasti a poté srovnáváme jednotlivé linie. Na tuto metodu stačí čtečka s rozlišením 250 dpi a metoda je spolehlivá i při drobných poraněních.

Druhá metoda testuje otisk daleko podrobněji. Po naskenování otisku je obrázek upraven tak, že se jednotlivé linie ztenčí na šířku jednoho pixelu. Na vytvořeném zjednodušeném modelu sledujeme typ, pozici a orientaci znaků na otisku. Tato metoda je přesnější, ale je vyžadována čtečka o citlivosti nejméně 500 dpi.

V současné době se nejčastěji používají optické a kapacitní snímače otisků prstů.

Optický snímač funguje přibližně jako klasický skener. Nejprve se prst nasvítí, aby se linie zvýraznili a následně je obraz převeden do datové podoby.

U kapacitních snímačů je snímač tvořen destičkou tvořenou velkým množstvím křemíkových polovodičů. Přiložením prstu dochází ke změnám odporu v místech, kde se papilární linie dotýkají destičky, čímž vzniká obraz otisku prstu [9].

Bohužel u všech systémů snímajících otisky prstů je velmi důležitá poloha prstu na snímací ploše. Stačí malá odchylka a systém identifikaci zamítne. Nepřesnosti mohou také vytvářet příliš suché nebo příliš vlhké ruce. Je třeba dávat pozor i na nečistoty, jež by mohly ulpět na zařízení.

Další možností porovnávání biometrie je obrys ruky [2, strana 265]. Je dokázáno, že tvar ruky se u člověka s věkem nemění. Nevýhodou této metody je velká chybovost. Lze pracovat jen s omezeným počtem osob, a proto je metoda vhodná spíše k verifikaci. Výhodou je, že na rozdíl od otisků, jež po nás zůstávají na všem čeho se dotkneme, lze rozměry naší ruky těžko získat bez našeho vědomí. Tato technologie se používá již více než 30 let.

Technologie otisku dlaně je stejná jako u otisků prstů. Vzhledem k větší ploše

dlaně využívá daleko více srovnávacích bodů než při identifikaci podle otisků prstů a proto je také mnohem přesnější. Nevýhodou je nutnost většího čtecího zařízení. Větší čtečka zabere daleko více prostoru a její cena mnohonásobně převyšuje cenu čteček otisků prstů.

Hlavním rozpoznávacím znakem člověka je jeho obličej [7]. Všichni tak poznáváme své blízké. Zatímco mozek pracuje s obličejem jako celkem, počítače se zatím musí soustředit spíše na detaily jako jsou oči (sítnice, duhovka), uši nebo nos. Alespoň do té doby, než přijdeme na to, jakým způsobem to dělá náš mozek.

Identifikace podle oční duhovky patří mezi nejpřesnější identifikace. V průběhu života se nemění. Nemá na ni vliv ani většina očních operací. Protože se pracuje s černobílým obrázkem oka, neovlivníte identifikaci, ani když si aplikujete barevné čočky. Výhodou také je, že při využití kvalitní kamery funguje tato metoda i na několika metrovou vzdálenost. Její přesnost a spolehlivost je bohužel také vyvážena vysokou cenou zařízení.

Při identifikaci podle oční sítnice se pomocí infračerveného paprsku skenuje okolí slepé skvrny našeho oka. Metoda je drahá, náročná a mezi lidmi neoblíbená. Oproti identifikaci podle oční duhovky u této metody vadí při skenování brýle i čočky a trvá dvakrát déle. Dalším problémem je strach lidí ze skenování oka infračerveným světlem. Navíc není na 100% jisté, zda se sítnice oka s věkem nemění.

Při vyhodnocování identity můžeme využít nejen tvaru ušního boltce, ale lze i využít technologii, která pomocí ozvěny studuje tvar ušního kanálku. Můžeme tak ověřit identitu osoby z druhé strany telefonní linky.

Na rozpoznávání lidí pomocí obličeje pracují vědci již dlouhé roky. Do dnešní doby totiž stačilo, aby se člověk nedíval přímo do kamery a systém ho již nedokázal rozeznat. Proto se neukládají data o obličeji jako fotografie, ale jako vzdálenosti mezi jednotlivými částmi obličeje (nos, ústa, oči a uši).

I přesto, že 99,99% DNA všech lidí je stejná, ještě pořád lze naleznout mezi dvěma nepříbuznými lidmi více než 10 000 000 rozdílů [7][2, strana 543]. Stačí vzít na porovnání jedinou buňku s jádrem. Například bílou krvinku. Tato metoda je sice velmi spolehlivá, ale zároveň je drahá a náročná na čas. Laboratoř vám totiž vrátí výsledky až za několik dní. Odebírání vzorků také není příjemné. Navíc test vašeho

DNA vás nejen identifikuje, ale prozradí na vás i další informace týkající se vašeho zdravotního stavu. Problém do této identifikace přináší i dnešní medicína, zejména čím dál běžnější transplantace orgánů.

Výhodou této techniky je možnost výroby umělé DNA a následně s touto DNA „značkovat“ například umělecká díla.

2.4 Verifikace hlasu

Vzhledem k tvaru hlasivek, ústní dutiny, jazyka i zubů zní hlas různých osob natolik odlišně, že jej bylo možno použít k identifikaci [11]. Zpravidla se k identifikaci používá celých vět. Samostatná slova jsou často příliš krátká a neobsahují dostatek akustických informací. Navíc větu použitou k identifikaci zná obvykle pouze osoba, která ji k identifikaci používá. Tím se spolehlivost metody ještě zvyšuje . Testy prokázali spolehlivost až 99%.

Kladem identifikace pomocí hlasu je jeho přijatelnost mezi uživateli. Nevýhodou pak jsou změny hlasu člověka. Ty nastávají například v období nemoci. U některých lidí navíc dochází ke změnám hlasu v závislosti na citovém rozpoložení.

2.5 Identifikace podle chůze

Teprve až rozvoj výpočetní techniky v posledních letech umožnil využití rozpoznávání osob podle chůze [10]. Důvodem je velká náročnost tohoto postupu při digitálním zpracování obrazových dat. Na druhou stranu tato metoda přináší výhodu, která předčí všechny ostatní způsoby identifikace. Významným přínosem je vzdálenost, na kterou lze tuto metodu použít. Nejlépe je možno tohoto vědeckého postupu využít v případě, kdy máme identifikovat osoby procházející prostorem, například uvnitř hlídaného areálu budov. Pohybující se osoby přecházejí zornými poli různých kamer, systém si automaticky předává jejich identifikaci na obraze a výrazně tak usnadňuje práci obsluze. Automatické biometrické rozpoznávání člověka se podle použitých analytických metod dělí na přístup modelově orientovaný a přístup orientovaný na

vyhodnocování siluety pohybujícího se člověka [12].

Modelově orientovaný přístup nahrazuje postavu člověka např. modelem tvořeným dráty. Systém pak při sledování pohybující se postavy vyhodnocuje délku jednotlivých částí a úhly mezi těmito částmi. Kromě drátěného modelu jsou využívány modely cylindrické a oválné. Jednotlivé konce jsou spojeny v kloubech. Nejjednodušší model využívá 6 základních částí: hlava, trup, 2x ruce, 2x nohy.

Přístupy orientované na vyhodnocování siluety pohybujícího se člověka zjednodušeně pracují tak, že z obrazu vyčlení siluetu člověka a její rozměry pak převedou na graf. Výsledný graf sice není zcela unikátní pro každého člověka, ale stejně jako lidský podpis obsahuje znaky jedinečnosti.

2.6 Vyhodnocování biometrik

V případě identifikace znalostí nebo předmětem je vyhodnocení jednoduché. Buď identifikační prvek se vzorem souhlasí nebo nesouhlasí. K chybě může dojít jen v případě, kdy se nám například podaří nešťasnou náhodou ohnout klíč.

Při vyhodnocování biometrik je situace složitější. Stačí například položit prst na snímač trochu jinak než při vytváření vzoru a výsledkem bude jiný snímek. Proto musí systém, při vyhodnocování biometrických údajů, pracovat s určitou mírou tolerance.

Míra tolerance či nepřesnosti vyhodnocování biometrik se určuje pomocí dvou základních parametrů [2, strana 135 a dál] . Prvním je FAR (False Acceptance Rate) a vyjadřuje procentualní pravděpodobnost, že bude přijat neplatný prvek. Oproti tomu FRR (False Reject Rate) označuje procentuální pravděpodobnost, že bude odmítnut platný identifikační prvek. V praxi se snažíme o co nejnižší FAR aby nám do budovy nepronikali neoprávněné osoby, zatímco rozumná výška FRR (<5%) tolik nevadí. Obě křivky jsou vzájemně provázané. Pokud zpřísníme vyhodnocování, dojde sice k poklesu FAR, ale zároveň stoupne FRR.

Pravděpodobnost FAR ani FRR nelze teoreticky vypočítat. Hodnoty lze zjistit jedině tak, že provedeme sadu pokusů a z výsledků vypočteme pravděpodobnosti.

FAR = A / B

Kde **A** je počet chybných přijetí a

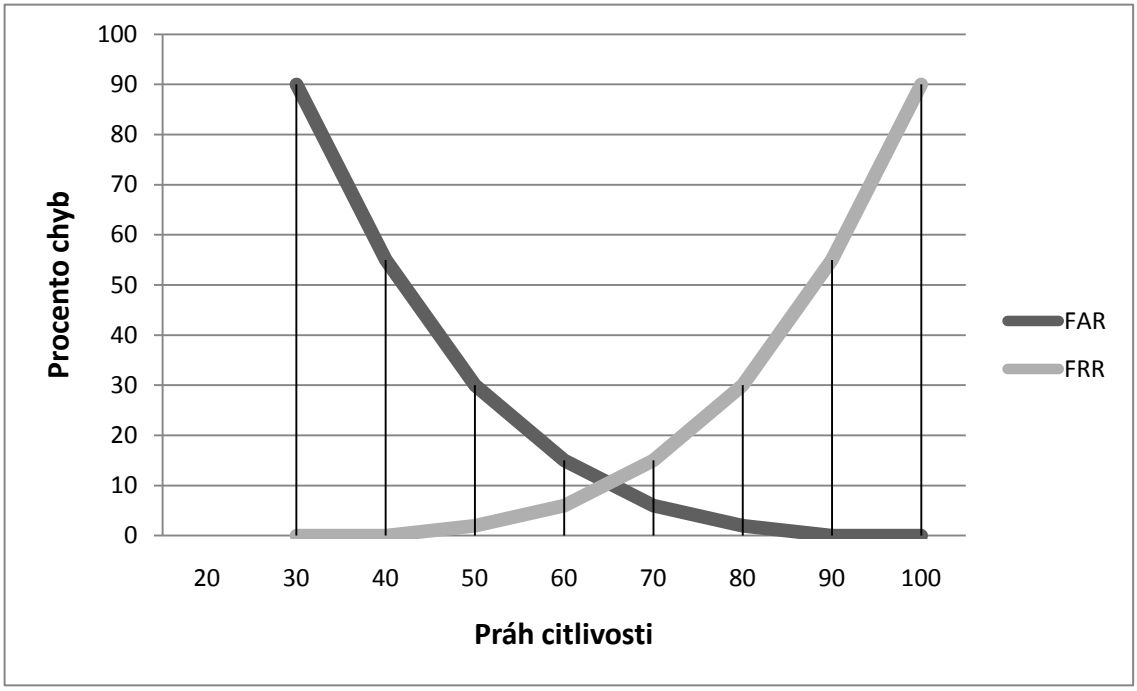
B je počet pokusů neoprávněných osob.

FRR = C / D

Kde **C** je počet chybných zamítnutí a

D je počet pokusů oprávněných osob.

EER (Equal Error Rate) je zkratka označující průsečík křivek FAR a FRR. V češtině jej označujeme jako míru rovné chyby.



Obr. 1: Průběh křivek FAR a FRR

Pro dobré zabezpečení objektu firmy je nejlepší bezpečnostní prvky vhodně kombinovat. Osvědčenou variantou je například instalace ovládacího terminálu alarmu těsně za dveřmi. Osoba, která první ráno odemkne budovu, má předem stanovenou dobu na zadání bezpečnostního kódu do malé klávesnice, čímž se bezpečnostní systém přepne na denní režim. Tímto způsobem se ověří, zda odemyká pověřená osoba. Každý zaměstnanec dostane svůj přívěsek na klíče nebo jmenovku vybavenou pasivním čipem. Můžeme použít kontakní, kdy se každý při příchodu či odchodu zaregistruje u senzoru například na stole recepční, nebo použít bezkontaktní, které jsou sice dražší, ale detektory se pak mohou skrytě zamontovat například do dveřních rámů. Senzor otisku prstu nebo dlaně naistalujeme před

místnost s trezorem. Čímž zajistíme, že bude muset být při otvírání trezoru fyzicky přítomna odpovědná osoba. Také není špatné kupovat pouze notebooky se senzorem na otisku prstu. Senzor otisku prstu společně s heslem vhodně doplní zajištění firemního počítače, aby s ním pracovala jen oprávněná osoba.

3 Sledování pohybu osob a vozidel

První co člověka napadne při zmínce o sledování pohybu osob a vozidel jsou většinou kamerové systémy.

3.1 Kamerové systémy

Dříve než se rozhodneme zakoupit kamerový systém, je třeba si uvědomit, že povinností každého provozovatele je dodržovat zákon o ochraně osobních údajů. Záznam kamerového systému je podle českého právního řádu osobním údajem ve smyslu ustanovení § 4 písmene a) zákona číslo 101/2000 Sb. [13], o ochraně osobních údajů. Základní zákonné povinnosti správce kamerového systému jsou stanoveny § 5.:

„*Správce je povinen*

a) stanovit účel, k němuž mají být osobní údaje zpracovány,

b) stanovit prostředky a způsob zpracování osobních údajů,

c) zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje. Zjistí-li správce, že jím zpracované osobní údaje nejsou s ohledem na stanovený účel přesné, provede bez zbytečného odkladu přiměřená opatření, zejména zpracování blokuje a osobní údaje opraví nebo doplní, jinak osobní údaje zlikviduje. Nepřesné osobní údaje lze zpracovat pouze v mezích uvedených v § 3 odst. 6. 11) Nepřesné osobní údaje se musí označit. Informaci o blokování, opravě, doplnění nebo likvidaci osobních údajů je správce povinen bez zbytečného odkladu předat všem příjemcům,

d) shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,

e) uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do

soukromého a osobního života subjektu údajů a osobní údaje anonymizovat, jakmile je to možné,

f) zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

g) shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

h) nesdružovat osobní údaje, které byly získány k rozdílným účelům.“

V odstavci 2 téhož paragrafu jsou pak stanoveny případy kdy lze zpracovávat osobní údaje bez souhlasu sledovaného subjektu:

„*Správce může zpracovávat osobní údaje pouze se souhlasem subjektu údajů. Bez tohoto souhlasu je může zpracovávat,*

a) jestliže provádí zpracování nezbytné pro dodržení právní povinnosti správce,

b) jestliže je zpracování nezbytné pro plnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro jednání o uzavření nebo změně smlouvy uskutečněné na návrh subjektu údajů,

c) pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,

d) jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem. Tím však není dotčeno právo na ochranu soukromého a osobního života subjektu údajů,

e) pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby; takové zpracování osobních údajů však nesmí být v rozporu s právem subjektu údajů na ochranu jeho soukromého a osobního života,

f) pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti, o

jeho funkčním nebo pracovním zařazení, nebo,

g) jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona.“

Při stanovování účelu provozu kamerového systému je doporučeno stanovit tento účel u každé kamery zvlášť. V důsledku těchto nařízení nelze záznamy z kamery určené k ochraně majetku použít například jako důkaz nevěry při rozvodovém řízení.

Druhým úskalím je pak doba ukládání záznamů. U systémů se stálým dozorem je povolováno ukládání na dobu 24 hodin. Doba uchovávání záznamů nesmí přesáhnout dobu nutnou ke zpracování informací. U systémů bez stálého dozoru lze záznam uchovat maximálně po dobu deseti kalendářních dnů.

Významný je také § 10 zákona číslo 101/2000 Sb.: „*Při zpracování osobních údajů správce a zpracovatel dbá, aby subjekt údajů neutrpěl újmu na svých právech, zejména na právu na zachování lidské důstojnosti, a také dbá na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů.“*

§ 11 zákona číslo 101/2000 Sb. nařizuje správci povinnost informovat subjekt (sledovanou osobu) o tom, že jeho osobní údaje, v našem případě kamerový záznam, budou zpracovány. Musí být stanoveno kdo a jakým způsobem bude údaje zpracovávat a komu mohou být tato data zpřístupněna. Klíčovou částí § 11 je odstavec 1: *„Správce je při shromažďování osobních údajů povinen subjekt údajů informovat o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje zpřístupněny, nejsou-li subjektu údajů tyto informace již známy. Správce musí subjekt údajů informovat o jeho právu přístupu k osobním údajům, právu na opravu osobních údajů, jakož i o dalších právech stanovených v § 21.“*

§ 13 téhož zákona ukládá správci, přijetí takových opatření, která zabrání neoprávněnému nakládání s osobními údaji. Odstavce 1 a 2 § 13 ukládají: „*(1) Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému*

zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů.

(2) Správce nebo zpracovatel je povinen zpracovat a dokumentovat přijatá a provedená technicko-organizační opatření k zajištění ochrany osobních údajů v souladu se zákonem a jinými právními předpisy.“

Z tohoto zákona vyplývá, že nahrávací mechanizmus kamer rozhodně nemůže být uložen na veřejně přístupné chodbě, kde z něj může kdokoliv vzít nahrávané medium, či jinak ovlivnit nahrávaná data.

Poslední z výčtu nejdůležitějších zákonů pro instalaci kamerového systému je § 16. Stanovuje povinnost budoucího správce oznámit ještě před zahájením zpracovávání údajů tento úmysl Úřadu na ochranu osobních údajů. V odstavci 2 pak jsou uvedeny informace, které musí oznámení obsahovat.

Zkratka CCTV je odvozena od anglického výrazu „Closed Circuit Television“, v češtině mající význam: „uzavřený televizní okruh“ [14]. Což znamená, že televizní obraz není veřejný, ale je přístupný pouze těm, kteří jsou připojeni do CCTV okruhu. Starší ale stále používaný český pojem pro označení CCTV je „průmyslová televize“. Tento název vychází z původního využití kamer pro sledování výrobních procesů. Postupně se kamerové systémy rozšířily i do dalších oblastí. V současnosti jsou kamery nejvíce využívány právě při zabezpečování objektů. Na bezpečnostní kamery narazíme téměř na každém kroku - v bance, muzeu, galerii, či obchodě, na letištích a nádražích, u benzínových pump, na parkovištích i jinde. Soukromé subjekty a firmy si pomocí těchto kamer doplňují své zabezpečovací systémy střežící jejich majetek. Policie využívá kamer při sledování provozu na silnicích, či hlídání a monitoringu města.

OCTV je označení pro „Open Circuit Television“, neboli v češtině „otevřený televizní okruh“. Tyto televizní okruhy využívají k přenosu signálu internetu. Každý se tak může ze svého počítače podívat na dopravu, či sněhové zpravodajství ze zimních středisek. Pro OCTV se využívají tzv. webové kamery.

Webové kamery, nebo též IP kamery obsahují kromě vlastní videokamery i videoserver, jež upravuje signál do podoby vhodné k přenosu datovou sítí [19].

Digitalizuje analogový videosignál a komprimuje jej. Právě tímto se webová kamera liší od web-kamer, které koupíme v každé prodejně elektroniky či počítačů. Web-kamera musí být pro svůj provoz připojena k počítači vybavenému patřičným softwarem pomocí USB rozhraní nebo videokarty.

První, co při pohledu na kameru zaujme uživatele, bude nejspíš objektiv [15]. Objektiv se skládá ze soustavy čoček. Ty obraz podle potřeby obraz zmenšují, zvětšují, zaostřují a potlačují různé optické vady. Většina objektivů kamer má zabudovanou clonu, která reguluje množství světla procházející objektivem stejně jako oční duhovka. Clona je buď pevně nastavená, či automaticky řízená podle údajů vyhodnocených systémem kamery anebo může být řízena dálkově.

Některé typy kamer mají objektivy pevně připojené již od své výroby, jiné lze libovolně obměňovat. Kamery s výměnným objektivem jsou opatřeny závitem C nebo CS, které se liší ve vzdálenosti mezi snímacím prvkem (čipem) od zadní čočky objektivu. C objektivy mají tuto vzdálenost 17,52 mm, CS objektivy pak 12,526 mm. Součástí balení CS objektivu bývá kroužek s tloušťkou 5mm umožňující použití CS objektivů do kamer s C závitem. C objektivy nelze použít v CS kamerách.

Důležitým údajem o objektivu je jeho světelnost [F]. Čím menší je tato hodnota, tím lépe kamera pracuje za zhoršených světelných podmínek.

Kamery vybavené objektivy s pevným ohniskem neumožňují ostření a jsou určeny k hlídání omezeného prostoru ve stanovené vzdálenosti. Objektivy s proměnlivým ohniskem umožňují zaostření obrazu během instalace.

Nejsložitějším tipem objektivu jsou objektivy vybavené motorovým pohonem umožňujícím nejen dálkové nastavení ohniskové vzdálenosti a tím zaostření, ale i přiblížení nebo oddálení sledovaného objektu. Tato technologie bývá označena jako optický zoom. Čím jednoduší je systém nastavení ohniskové vzdálenosti, tím horší je, v porovnání s objektivy pevné ohniskové vzdálenosti, kvalita obrazu. Druhou možností je zoom digitální provedený pomocí čipu kamery či následně pomocí softwaru v počítači. Při přepočtu však dochází k výraznému zhoršení obrazu.

Po průchodu světla přes objektiv dopadá obraz na snímací čip. U analogových kamer se dříve používala snímací elektronka. Ta byla později

nahrazena čipem označovaným jako CMOS (Complementary Metal–Oxide–Semiconductor) [16]. V dnešní době většina kamer místo CMOS čipů používá kvalitnější CCD (Charge Coupled Device) čipy [17]. Lineární a černobílá verze CCD čipů se používají např. v čtečkách čárových kódů. CCD čipy používané v současnosti v kamerách a fotoaparátech mají rozlišení od 1 do 8 Mpx. Svůj malý CCD čip mají například optické myši. Naopak příklad velmi velkého CCD čipu nalezneme na palubě Hublova teleskopu.

Před výběrem vhodné kamery, je třeba popřemýšlet, proč si ji chceme pořídit a co od ní vyžadujeme. Barevný obraz je jistě hezčí a lépe podle něj identifikujeme neznámého člověka, ale barevná kamera je mnohem méně citlivá a má i menší rozlišení než kamera černobílá. Nejvíce je rozdíl vidět v noci. Pokud chceme vysokou kvalitu obrazu, musíme samozřejmě počítat s většími náklady, a to nejen za samotnou kameru. Abychom docílili co nejlepšího výsledku, musí být kromě toho kvalitnější i další prvky kamerového systému.

Kamery den/noc jsou speciální kamery, jejichž čip během dne pracuje v barevném režimu. Při poklesu osvětlení pod stanovenou úroveň se přepne do režimu černobílého. Tento systém je obzvláště vhodný pro sledování venkovních prostor. Druhou možností, jak řešit nedostatek světla, je použití infračervených diod na přisvícení. Kamera vybavená infračerveným přisvícením dokáže snímat i za naprosté tmy. Nevýhodou je zkrácení dosahu kamery. Diody dosvítí jen asi na 40 metrů. Další nevýhodou je zkreslení barev.

3.2 Detektory

Ne vždy lze kamerový systém použít. I na pracovišti má člověk právo na soukromí a pokud nepracuje například v bance či jiném vysoce střeženém prostředí, smíme jej sledovat, ale nesmíme nahrávat. Navíc kamery jsou drahé. Chceme-li naši firmu zabezpečit proti zlodějům přicházejícím v noci či o víkendu, může nám stačit několik detektorů, čímž se vyhneme drahé investici do kamerového systému a nutnosti vyplňovat formuláře pro Úřad na ochranu osobních údajů.

Nejjednodušším typem detektoru je prostý magnetický kontakt [20]. Snadno

s ním zastřežíme dveře či okna. Detektor se skládá ze dvou částí: permanentního magnetu a jazýčkového relé. Jazýčkové relé je přesně nastaveno na permanentní magnet, a proto jej dokáže přerušit i přiložení cizího magnetu.

Obzvláště důležitý je tento magnet na vstupních dveřích, neboť příchod neznámého člověka často spouští odpočet, během něhož je třeba u příslušného terminálu zabezpečení vypnout. Stejně tak při odchodu posledního člověka alarm čeká na uzavření hlavních dveří než se plně aktivuje.

Nejčastěji používané detektory pohybu jsou pasivní infračervené detektory. Pasivní infračervené detektory reagují na teplo, jež každé těleso vysílá do okolí. Detektor zaznamenává změny a pokud změna překročí nastavenou hranici, senzor spustí poplach. Přístroj by neměl být zaměřený na skla, okna, zrcadla či jiné lesklé plochy. Stejně tak by neměl by neměl být umístněn poblíž zdrojů tepla či zdrojů vodních nebo olejových par, které by jej mohli „oslepit“ či zmást. Nedoporučuje se jej dávat ani do míst, kam dopadá přímé nebo odražené sluneční světlo.

Detektor lépe zachycuje předměty či osoby pohybují se napříč jeho zorným polem než ty, které se pohybují od něj či k němu.

Ultrazvukový detektor funguje podobně jako radar. Do svého zorného pole vysílá signál o určité frekvenci a následně vyhodnocuje jeho odraz. Pokud dojde k odchylce překračující povolenou mez, spustí poplach. Ultrazvukový detektor patří do kategorie aktivních detektorů. Pracuje se signálem pro nás, na rozdíl od některých zvířat, neslyšitelným.

Přístroj se nedoporučuje instalovat do blízkosti zdrojů hluku s širokým kmitočtový spektrem (například telefon), za závěsy či nad topná tělesa.

Mikrovlnný detektor patří stejně jako detektor ultrazvukový mezi detektory aktivní. Do svého zorného pole vysílá v pásmu od 1 do 10 GHz. Výhodou tohoto detektoru je, že mikrovlny jsou schopné proniknout sklem a tenkými stěnami, takže může zaznamenat narušitele ještě dříve, než si jej on všimne.

Detektor rozbití skla pracuje tak, že pomocí mikrofonu vyhodnocuje dvě různé frekvence zvuku. Pro náraz na okenní tabuli je charakteristická nízká frekvence. Pro následné tříštění skla frekvence vysoká. Samozřejmě není vhodné tento přístroj používat v hlučném prostředí. Přístroj je třeba nastavit podle druhu použitých oken,

protože okna potažená např. bezpečnostní folií vydávají při rozbíjení jiný zvuk než okna obyčejná.

Kombinované detektory jsou vlastně dva detektory v jednom zařízení. Například pasivní infračervený detektor kombinovaný s detektorem mikrovlnným. Cílem je snížit počet falešných poplachů. Další možností je doplnění senzoru o fotoaparát s bleskem. V případě poplachu přístroj provede v rychlém sledu několik fotografií. Zabudovaný blesk má za úkol scénu nasvítit, připoutat pozornost narušitele a nakonec snímky odeslat do ústředny, která poplach vyhodnotí.

Infrazávora se skládá z vysílače infračerveného paprsku a přijímače [21]. Při přerušení paprsku vyšle zařízení signál do ústředny. Infrazávory jsou například mezi sloupky u vstupu do metra. Jejich úkolem je počítat cestující.

Laserový skener nám umožňuje bezkontaktně změřit vzdálenosti velkého množství bodů v okolí 270 stupňů až do vzdálenosti 8 metrů od hlavy skeneru. Přístroj vytvoří 3D mapu okolí složenou z velkého množství bodů. Každému bodu je přiřazena jeho vzdálenost od přístroje a v případě lepších skenerů i odrazivost skenovaného povrchu. Měření probíhá rychlostí statisíců bodů za sekundu. Podle použité technologie se laserové skenery dělí do dvou kategorií.

První kategorií jsou skenery založené na měření délek. Nejčastěji využívají buď impulzní dálkoměr meřící vzdálenost podle času mezi vysláním paprsku a přijetím jeho odrazu zpět nebo dálkoměr pracující s fázovým posunem odraženého světla. Tento typ přístroje je méně náročný na kvalitu odraženého světla a pracuje i na větší vzdálenosti.

Drouhou kategorií jsou triangulační skenery. V tomto případě je přijímací zařízení (CCD kamera) umístněné jinde než zdroj paprsku. Vzdálenost cíle, na který paprsek dopadá, se pak vypočte vyřešením trojúhelníka. Přesnost výpočtu hodně závisí na vzdálenosti cíle od detektoru.

Podzemní potrubí nebo kabely lze chránit pomocí optických vláken [22]. Stačí položit do země nad potrubí optické vlákno. V případě vedení optického kabele, rezervovat dvě z vláken na zabezpečení. Systém využívá kontinuálního laseru vysílaného do obou kontrolních vláken. Senzor na konci vláken vyhodnocuje příchozí světlo s obou vláken a pokud se vzájemně neliší, je vše v pořádku. V případě, že

dojde někde podél vedení ke změně, dojde i ke změně procházející paprsku. Vlákna jsou citlivá nejen na přerušení, ale i na pohyb, či vibrace způsobené například zvukem. Systém pomocí speciálního programu vyhodnotí, se spolehlivostí větší než 95%, zda se jedná o falešný poplach či skutečné narušení a určí polohu narušení s přesností na 150 metrů při délce jedneho segmentu až 40 kilometrů. Optická vlákna se nemusí umístňovat jen pod zem, mohou být připojena i k plotům. Navíc jsou optická vlákna imuní vůči elektromagnetickému rušení, bleskům nebo elektřině.

Při výběru vhodného detekčního zařízení se budeme nadále řídit zásadou o vhodné kombinaci. Nad příjezdová vrata umístníme černobílou kameru bez záznamového zařízení. Vyjde levněji a bude lépe pracovat i v zimě za šera. Obrazovku i spínač otvírání vrat bude ovládat recepční rovnou od svého stolku. Na okenní i dveřní rámy necháme přidělat magnetické kontakty. Ty nám zároveň pomohou večer zjistit, jestli některý ze zaměstnanců nezapoměl zavřít okno. Za vstupní dveře a do důležitých místností instalujeme detektory pohybu a detektory tříštěného skla.

4 Ochrana citlivých dat a informací

Informace a znalosti byly, jsou a budou tím nejdražším co firmy vlastní. V dnešní době nám prudký rozvoj internetu umožňuje velmi snadný přístup k velkému množství informací. Tento přístup ale funguje všemi směry a jsou informace, které bychom raději se světem nesdíleli, například pokud jde o naši soukromou poštu či novou firemní obchodní strategii. Když chceme, aby nám byla data i nadále přístupná, ať již jsme doma, v práci nebo někde na cestách musíme je před cizím zrakem chránit. Jednou z možností ochrany je šifrování.

4.1 Kryptografie

Nejstarším způsobem šifrování je metoda symetrická [23]. Při využití této metody je náš text zašifrován pomocí určitého klíče a jedině s tímto klíčem může být znovu obnoven do původní podoby. Odolnost šifrovaného textu proti útoku, kdy postupně zkoušíme všechny možné klíče, je dána délkou našeho klíče. Délka se uvádí v počtu bitů binárního čísla. Šifra s klíčem o síle 4 bity znamená 2^4, tedy celkem 16 možných klíčů. Výkon současných počítačů pak způsobil, že současné šifry používají klíče o síle 128 bitů. Rozluštit takovou šifru pomocí hrubé síly, tedy zkoušení každého klíče, by zabralo několik desítek let. Bohužel má symetrické šifrování jednu závažnou slabinu kterou nelze přehlédnout. Aby mohl náš text přečíst i někdo jiný než my, musíme mu předat klíč. Ale jak zašifrovat klíč, aby jej nemohl použít někdo, komu nebyl určen?

Asymetrické šifrování vymyšlené v 70. letech 20. století pracuje se dvěma různými klíči. Jedním klíčem, takzvaným veřejným, se zpráva zašifruje a druhým, soukromým, se rozšifruje. První klíč může použít každý, kdo si přeje zprávu zašifrovat. Druhý klíč si jeho majitel drží v tajnosti.

Asymetrické šifrování většinou používá čísla se speciálními vlastnostmi, jako jsou třeba prvočísla. Tato skutečnost sice zjednodušuje útok hrubou silou, neboť stačí zkoušet jen tato čísla. Dnešním standardem je využití délky klíče o 2048 bitech. Nejznámější asymetrickou šifrou je RSA.

RSA pracuje s myšlenkou, že je velmi snadné dvě čísla vynásobit, ale rozložit číslo zpět na prvočinitele je časově velmi náročné. Obvzláště u hodně velkých čísel.

Postup tvorby šifry je následující: Vybereme si dvě velká prvočísla **p** a **q**. Jejich součin označíme **n:=p*q**. Podle malé Fermatovy věty, vyjde

$$\mathbf{m^{(f(n)+1)} \bmod n=m}$$

pro libovolné číslo **m** v intervalu 1,2,...,n-1, kde funkce **f(n)** dává počet čísel mezi 1,2,...,n-1 nesoudělných s **n** (Eulerova funkce), **mod** je zbytek po celočíselném dělení.

Pomocí indukce pak lze dokázat, že také

$$\mathbf{m^{(k*f(n)+1)} \bmod n=m}$$

pro libovolné přirozené číslo **k**, protože

$$\mathbf{m^{(k*f(n)+1)} \bmod n=m^{f(n)}*m^{((k-1)*f(n)+1)} \bmod n.}$$

Podle indukčního předpokladu

$$\mathbf{m^{f(n)}*m \bmod n=m^{(f(n)+1)} \bmod n=m}.$$

V našem případě

$$\mathbf{f(n)=f(p*q)=(p-1)*(q-1)},$$

proto najdeme dvojici čísel **e, d** takových, že

$$\mathbf{e*d=1 \bmod (p-1)*(q-1)}.$$

Dvojice **(e,n)** tím utoří veřejný klíč a dvojice **(d,n)** vytvoří soukromou část klíče.

Zprávu **m** (maximální délky **n<m**) zašifrujeme pomocí

$$\mathbf{c=m^e \bmod n.}$$

Zašifrovanou zprávu **c** odešleme adresátovi, který k rozšifrování použije funkci

$$\mathbf{m:=c^d \bmod n}.$$

Algoritmus lze ověřit:

$$\mathbf{e*d=k*f(n)+1}$$

pro nějaké číslo **k**, a tedy

$$\mathbf{m^{(e*d)} \bmod n=m^{(k*f(n)+1)} \bmod n=m}.$$

Šifru s klíčem o velikosti 384 bitů 100 spolupracujících počítačů lámalo několik měsíců reálného času.

Elektronickým podpisem se dle zákona 227/2000 Sb. [24], rozumí: „*údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě*.“ To může být jméno, adresa nebo rodné číslo připojené na konec textu a zaručuje identifikaci autora. Nás ale daleko více zajímá tzv. zaručený elektronický podpis, což je: *„elektronický podpis, který splňuje následující požadavky*

1. je jednoznačně spojen s podepisující osobou,

2. umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,

3. byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,

4. je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat,“

Rozdíl mezi dopisem s elektronickým podpisem a dopisem se zaručeným elektronickým podpisem je jako mezi dokumenty s notářsky ověřeným a neověřeným podpisem.

Účelem je, aby byla zajištěna identita autora dopisu a že po podepsání nedošlo k žádné úmyslné či neúmyslé změně dokumentu.

Na rozdíl od šifrování, kdy se pro zašifrování používá veřejný klíč příjemce, se v případě zaručeného elektronického podpisu pro zašifrování používá tajný klíč autora. Tím se ověří jeho totožnost. Podpis pak může kdokoliv ověřit pomocí veřejného klíče.

To, že dokument nebyl během přenosu pozměněn, se ověřuje pomocí kontroly jeho otisku. Otisk dokumentu (hash) se zašifruje autorovým klíčem a po dešifrování se dále ověří nezávislým výpočtem.

Hash funkce je taková funkce, která převádí vstupní libovolně dlouhou posloupnost na posloupnost pevné délky. I malá změna vstupních dat způsobí výraznou změnu výsledku funkce.

4.2 Zálohování

Nikdy nic nefunguje úplně na 100%. Snad jen Murphyho zákony. Počítače jsou již dnes většinou spolehlivé. Mnohdy spolehlivější než člověk. Zachraňuje nás záložní kopie, nebo-li backup [25].

Obvykle se záložní kopie ukládá na jiné médium, než na kterém jsou uložena původní data. Například vypálíme zálohu na dvd disk. Firmy zálohující pravidelně velké množství dat využívají speciální zařízení s magnetickými páskami s kapacitou až několik gigabytů.

Programů pro vytváření záloh je dnes spousta. Nabízejí nám mnoho dodatečných nastavení, od komprese archivovaných dat, přes filtry pro výběr zálohovaných souborů, po možnosti nastavení času, kdy se bude archivace spouštět.

Zálohy se dělí do tří základních druhů:

1) Záloha úplná – provede se úplná kopie všech souborů.
2) Záloha diferenciální – okopíruje jen soubory, jež se od poslední úplné zálohy změnily
3) Záloha incrementální – okopíruje jen soubory, jež se změnili od poslední inkrementální zálohy.

Například v naší firmě se úplná záloha z důvodu časové náročnosti prování jednou týdně o víkendu.

Rozdíl mezi jednotlivými druhy záloh je nejvíce vidět při obnovování. V případě úplné zálohy stačí data pouze okopírovat. Pokud je naše poslední záloha diferenciální, nahrajeme nejprve poslední úplnou zálohu a poté poslední diferenciální zálohu. V případě, že je naše poslední záloha icrementální, nahrajeme nejprve poslední úplnou zálohu a pak postupně nahráváme zálohy incrementální až do současnoti.

Podle frekvence a doby nutné k obnovení dělíme zálohování do tří základních kategorií.

První je elektronické překlenutí, kdy se data na záložní server ukládají dávkovým způsobem, například jednou za den. Obnova je nejpomalejší a dochází

k největší ztrátě dat. Výhodou pak je malá náročnost na podnikový systém, protože záholování může běžet v noci kdy je jinak systém nevyužit.

Další možností je žurnálování. Opět se data ukládají na záložní systém dávkovým způsobem, ale tentokrát ve velmi častých intervalech (jednou za méně než hodinu). Výhodou je menší ztráta dat při obnově, nevýhodou vyšší náročnost na firemní systém.

Nejnáročnější formou zálohování je zrcadlení. Jak už z názvu vyplývá, jsou všechna data průběžně ukládána na dva různé počítače.

Pro zvýšení bezpečnosti zálohování je vhodné, aby záložní stroj či místo, kam zálohy ukládáme, byli pokud možno jinde než originály. Zabráníme tím společnému zničení, například při požáru budovy. Můžeme využít firem, které pronajímají prostor na jejich serverech nebo umístnit náš server do jejich serverové místnosti.

4.3 Trezory

Ne vše může být uloženo na disku či jiném médiu. Média s citlivým obsahem, jako jsou smlouvy, tajné dokumenty, cennosti, zbraně, prototypy a jiné důležité předměty potřebují také být někde bezpečně uloženy. Zde přicházejí ke slovu trezory a trezorové místnosti [26].

Bezpečnost trezorů a trezorových dveří se stanovuje podle Evropské normy EN 1143-1. Podle této normy je každý trezor podroben skupině testů, jejichž cílem je násilné otevření trezoru. Podle použitých nástrojů a nejkratší doby nutné k proražení trezoru či vyvrácení dveří se stanovuje jednotka odporu (RU – resistance unit). Před pořízením trezoru je třeba myslet na skutečnost, že námi pořízený trezor nás téměř určitě přežije. Je proto velmi důležité pečlivě zvážit jeho velikost a bezpečnostní třídu.Doporučené maximální ceny uložených cenností jsou stanoveny podle nejvyšší částky, na kterou jsou pojišťovny ochotny pojistit trezor v dané třídě. Tyto částky jsou ovšem pouze orientační. Lze je zvýšit dodatečným zajištěním budovy (mříže, čidla, ostraha). Navíc každá pojišťovna nabízí stejný nebo obdobný druh pojištění za různou cenu.

Dalším důležitým kritériem pro výběr vhodného trezoru je stupeň utajení ukládaných informací. Pokud je trezor umístěn v zabezpečené oblasti (dům chráněný bezpečnostním systémem), je minimální třída pro uložení dokumentů s následujícím označením:

Stupeň utajení	Minimální bezp. třída
Přísně tajné	II
Tajné	I
Důvěrné	0
Vyhrazené	Z1

Tabulka 1: Minimální bezpečnostní třída trezoru pro uskladnění utajených dokumentů

Norma stanovuje tyto bezpečnostní třídy trezorů:

1) Nezjištěná konstrukce – univerzální třída, do které se řadí všechny trezory, které nemají žádný certifikát.

2) Bezpečnostní třída Z1 – Nejnižší forma zabezpečení. Odporové jednotky RU(10/10). Trezor musí obsahovat alespoň jeden zámek třídy A. Tato třída se používá například na uložení zbraní.

3) Bezpečnostní třída Z2 – Odporové jednotky RU(15/20). Podmínkou je alespoň jeden trezorový zámek třídy A. Nejčastěji se tyto trezory montují do skříní či se používají v archivech. Vhodné jsou také pro uložení zbraní nebo jedů. Doporučená maximální hotovost je do 30 000 Kč.

4) Bezpečnostní třída Z3 - Odporové jednotky RU(20/25). Alespoň jeden trezorový zámek třídy A. Trezory s dvouplášťovou konstrukcí. Doporučuje se ukládat zbraně do deseti kusů či hotovost do 50 000 Kč.

5) Bezpečnostní třída 0 – Odporové jednotky RU(30/30). Alespoň jeden zámek třídy A. Trezor je vhodný pro uschování důvěrných dokumentů, šperků a cenností do hodnoty 100 000 Kč.

6) Bezpečnostní třída I – Odporové jednotky RU(30/50). Alespoň jeden zámek třídy A. Doporučená maximální hodnota uložených věcí do 300 000 Kč. Tato třída je nejčastější volbou menších firem na uložení denní hotovosti.

7) Bezpečnostní třída II – Odporové jednotky RU(50/80). Alespoň

jeden zámek třídy A. Vhodný pro uložení cenností do 500 000 Kč. Nejčastěji používaný ve středních firmách a zlatnictvích. Lze jej použít pro dokumenty do stupně utajení „Přísně tajné“

8) Bezpečnostní třída III – Odporové jednotky RU(80/120). Alespoň jeden zámek třídy B. Doporučená maximální hodnota uložených ceností je 5 000 000 Kč. Nejčastěji tuto třídu využívají velké podniky a lidé chránící přeměty větší hodnoty.

9) Bezpečnostní třída IV – Odporové jednotky RU(120/180). Alespoň dva trezorové zámky třídy B. Třída určená pro bankovní a finanční instituce. Vhodné pro uložení ceností do 6 000 000 Kč.

10) Bezpečnostní třída V – Odporové jednotky RU(180/270). Alespoň dva trezorové zámky třídy B. Doporučená maximální hodnota cenností je 16 000 000 Kč.

Trezorové zámky se dělí do tří základních kategorií. Jsou to zámky klíčové, mechanické a elektronické. Podle stupně odolnosti proti násilnému otevření se dále podle normy EN 1300 dělí do bezpečnostních tříd A – D, plus třída NK pro zámky necertifikované.

4.4 Řízení přístupu

Dokud má naše firma jen několik málo zaměstnanců, kteří se vzájemně znají a v případě, že místo kanceláře používá prázdnou garáž u babičky, nebudeme si zřejmě informační a zabezpečovací systém pořizovat. Ale i zde můžeme vidět řízení přístupu. Nebo snad mají všichni zaměstnanci klíče od hlavních vrat či od pokladny s hotovostí?

Řízení přístupu je součástí bezpečnostní politiky každé firmy. Účelem je zabránit aktivitám, ať už chtěným či nechtěným, které by mohli způsobit nějaké škody. Řízení přístupu se dělí na tři základní kategorie [27].

První kategorii nazýváme administrativní. Sem patří výběr vhodných zaměstnanců a jejich proškolování v používání nových technologií a postupů.

Druhá kategorie se nazývá logicko-technická. Patří do ní hardware a sofware jako jsou firewall, router, zabezpečení heslem, dále pak použití čipu či biometriky.

Poslední kategorii označujeme jako fyzickou. Do této kategorie patří dveře, ploty, detektory pohybu, zámky, alarmy, ochranka.

V okamžiku, kdy se při vstupu do firmy identifikujeme, nám jsou přiděleny pravomoce. Rozsah těchto pravomocí záleží na technice řízení přístupu, kterou naše firma používá.

Při využití techniky přenechání volnému uvážení si tvůrce či vlastník stanovuje pravomoce jednotlivě každému uživateli. Tento způsob řízení přístupu je nejdynamičtější. Při větším počtu uživatelů je ale velmi náročný. Ze všech přístupů k rozdělování pravomocí je nejméně bezpečný.

Při využívání techniky nepřenechání volnému uváže se udělování pravomocí řídí systémem pravidel. Tato pravidla určují, na co vše má uživatel právo a kam má přístup.

Jednou z možností jak přidělovat pravomoce je mandátní technika. Každý uživatel dostane oprávnění podle stupně prověření. Stejně tak všechny systémy, dokumenty a prostory jsou označeny podle stupně utajení (např.:„veřejné až přísně tajné“) . Uživatel pak může používat systémy a navštěvovat jen místa se stejnou nebo nižší mírou utajení.

Rozšířením mandátní techniky řízení přístupu je technika založená na potřebě, při které musíme znát uživatelovu pracovní náplň a jeho pravomoce. Uživatel tehdy může přistupovat k datům se stejným a nižším stupněm prověření pouze v případě, pokud to potřebuje k plnění svých pracovních povinností. Chemik ke své práci nepotřebuje znát výsledky hospodaření za poslední měsíc a podobně.

Další možností, jak přistupovat k řízení přístupových práv, je technika založená na roli. Tento přístup je vhodný hlavě pro místa, kde se často střídá personál. Uživateli jsou přidělena práva podle práce, kterou vykonává (např. brigádník). Práva se dále individuálně neupravují.

Technika založená na úkolu je velmi podobná technice založené na roli. Cílem této techniky řízení přístupu je například rozdělit přístupová práva zaměstnanců v chemické laboratoři podle úkolu, na kterém pracují a zabranit tak například neúmyslnému přemazání výsledků meření někoho jiného.

Administrátor firemního systému by měl být vybírán s maximální pečlivostí,

neboť má ze všech uživatelů ty největší pravomoce. Jeho úkolem je vytvářet nové (nebo rušit staré) uživatelské účty, upravovat práva již existujících účtů a zaznamenávat aktivity uživatelů. Způsobem, jak zabránit jednomu administrátorovi narušit nějakým způsobem, ať již úmyslně či neúmyslně, bezpečnost systému, je rozdělení povinností a odpovědnosti mezi více lidmi.

Veškeré úpravy uživatelských účtů je třeba přesně evidovat. Vždy musí být dodrženy administrativní postupy návrhu a schválení každé žádosti o jakoukoliv změnu.

Pravidelně je třeba provádět kontroly uživatelských účtů za účelem odhalení chyb, jako jsou nadměrná práva a účty, jež nikdo nevyužívá.

Všechna citlivá data uložená na přenosných počítačích a záložních mediích by měla být šifrována. Ochráníme tak data před zneužitím, pokud si některý ze zaměstnanců odnese nějaká data mimo budovu. I v případě kdy by se někdo pokusil poslat firemní data emailem, budou mimo firemní počítače nečitelná. Všechny systémy je třeba zálohovat. Nejlépe mimo budovu, nebo alespoň v serveru se samostatnou místností a zdrojem energie. Bezpečnostní třídu trezoru zvolíme podle plánované hodnoty ukládaných věcí a pak raději ještě jednu třídu přidáme, protože trezor je velmi trvanlivé zařízení a s největší pravděpodobností jej budou používat ještě naši nástupci za pár desítek let. Pro stanovení pravidel řízení přístupu a bezpečnostní politiky firmy vybereme pracovní tým skládající se ze zástupců jednotlivých odborů [28].

5 Ochrana počítačových sítí

Sestavit malou počítačovou síť není v dnešní době žádná velká věda. Většinou stačí jen zasunout konektor do správné zdířky (spletete se jen těžko, protože většinou se tvarově hodně liší) a počkat až se váš systém automaticky připojí. U bezdrátových sítí je systém ještě o něco jednodušší. Stačí jen mít ve vašem počítači wi-fi a část s připojováním kabele se zjednoduší na kliknutí na ikonu „připojit k síti“.

Dnes nejčastěji používaným kabelem ve světě počítačových sítí je kabel typu Cat5, který umožňuje teoretickou propustnost 12,5 MB/s. Pokud jej rozříznete, zjistíte, že se skládá ze čtyř párů kroucených vodičů. Poptávka po vyšší rychlosti připojení stále roste a proto je kabel typu Cat5 postupně nahrazován vylepšenými kabely Cat5e nebo Cat6. Takové sítě jsou pak označovány jako Gigabit Ethernet.

Počítačové sítě jsou typicky uspořádány do „hvězdy“ či „stromu“. Kořen, nebo střed hvězdy, většinou tvoří přepínač (Switch) nebo směrovač (Router).

5.1 Síťová zařízení

Základním síťovým zařízením pro stavbu počítačové sítě je síťová karta [24]. V dnešní době je součástí většiny základních desek počítačů. Pokud snad v některém chybí, je zakoupení nové síťové karty otázka přibližně 200 Kč. Pokud spojíte pouze dva počítače bez přítomnosti jiného zařízení mezi nimi, je třeba použít speciálního, takzvaného „kříženého“ kabele. Většinou ale spojujeme více než dva počítače a pak použijeme kabel přímý, nekřížený.

Přepínač, nebo-li Switch je zařízení zapojené uprostřed naší hvězdy. Stará se o to, aby data odeslaná z našeho počítače pokračovala k počítači, jemuž jsou určena.

Směrovač (Router) slouží k připojení naší sítě k internetu nebo jiné síti. Často obsahují i jednouchý firewall, který chrání naši síť.

Funkce Switche v počítačových sítích dříve nahrazovali opakovače (Huby). Na rozdíl od Switche došlý signál pouze zopakovali a rozeslali jej všem počítačům připojeným do sítě. Tím se síť zbytečně zatěžovala a zpomalovala. Dnes se již nepoužívají.

5.2 Veřejná / Neveřejná adresa

Dva počítače spolu přes počítačovou síť komunikují pomocí protokolu označovaného zkratkou TCP/IP. Aby se počítače během komunikace poznali, označují se vzájemně pomocí IP adres. IP adresa se skládá ze 4 čísel od 1 do 255 oddělených od sebe tečkou (např: 192.168.5.3). Protože ale kombinací čísel není nekonečné množství a počítačů připojených do internetu je stále více a více, došlo k zavedení privátních sítí. Privátní síť je síť, jež s okolním světem komunikuje pomocí Brány (Gateway) a navenek se tváří jako jediný počítač. Bránou je vždy nějaký router. IP adresy lokálních sítí začínají 192.168.aaa.bbb. IP adresy jsou na lokální straně sítě jedinečné, ale lokálních sítí jsou po celém světě miliony.

Pokud připojujeme do sítě nový počítač, neměl by dostat novou adresu automaticky. Naopak by adresa měla být přidělena dle pevných pravidel a manuálně administrátorem sítě. Jinak riskujeme, že si například zaměstnanec připojí do sítě svůj z domova přinesený počítač, čímž se do naší sítě může dostat například virus.

Komunikace našeho počítače s internetem pak probíhá přibližně takto: Náš počítač pošle požadavek na zobrazení například určité internetové stránky bráně a ta jej předá serveru požadovaných stránek. A protože si naše brána pamatuje od kterého počítače požadavek vzešel, předá nám došlou odpověď a nám se na monitoru zobrazí stránky, jež jsme požadovali.

Výhodou tohoto uspořádání je větší zabezpečení a menší cena za připojení.

Problém avšak nastane, pokud se chceme na náš domácí počítač připojit například z práce nebo na něm provozovat web či herní server. Tehdy potřebujeme, aby náš počítač měl takzvanou veřejnou IP adresu. S veřejnou IP adresou se náš počítač stane přímo přístupným z internetu. Nevýhodou jsou vyšší náklady na připojení a větší riziko napadení počítače.

Pro naší firmu by tedy bylo vhodné si pořídit jedno nebo dvě veřejná IP. Předtím než si veřejnou adresu pořídíme, je třeba se zamyslet, protože jestli ji budeme potřebovat pouze na webové stránky, bude jednodušší a nejspíš i levnější umístit je na server u firmy pronajímající prostor na svých serverech.

5.3 Zabezpečení sítě

Nejvíce nebezpečí podnikové síti vždy hrozilo a hrozit bude od vlastních zaměstnanců. Jediným způsobem, naši firmu účinně bránit, jsou pravidelná školení, důsledné uplatňování bezpečnostní politiky a udržovaní našeho softwaru aktualizovaného. Aktualizace probíhají většinou automaticky nebo po zobrazení dotazu na obrazovce uživatele, v případě antivirových programů běžně každý den, někdy i víckrát za den.

Útoky na počítačové sítě „zvenčí“ sice nejsou příliš časté, ale i s nimi je třeba počítat. Firewall je zjednodušeně filtr, který má za úkol propustit do vnitřní sítě pouze data, o která máme zájem a ostatní nechat venku za zdí [30]. Firewallem může být router nebo počítač vybavený patřičným programem. Pokročilejší zařízení nekontrolují jen adresy, odkud a kam data míří. Studují i obsahy dat, což jim pomáhá určit, které aplikaci data patří a tím odhalovat některé z rafinovanějších druhů útoku. Rozhodně bychom neměli pořizovat do naší firmy software načerno stažený z internetu. Trocha ušetřených peněz nikdy nezaplatí škody, jež by naší firmě mohli vzniknout používáním takového softwaru.

Demilitarizovaná zóna, jak již název napovídá, je prostor mezi dvěma válčícími stranami, v našem případě zastoupenými vnitřní (LAN) a vnější (WAN) sítí. Funguje to tak, že obě strany vidí demilitarizovanou zónu, ale již nevidí, co je za ní, protože všechna data jsou vždy nasměrována do této zóny, kde se skupina specializovaných programů rozhodne, co s nimi udělá. Do demilitarizované zóny se umísťují počítače, na kterých běží například aplikace jako web, FTP, poštovní server. Můžeme si to také představit jako první nádvoří hradu, kde probíhá trh. Hlídač u první brány pouští na tržiště jen osoby, které přijíždějí obchodovat. Žebráci a jiní podezřelí musí zůstat venku. Hlídač u brány mezi prvním nádvořím s tržištěm a vnitřkem hradu pak pustí dovnitř a ven jen osoby, které v hradu bydlí.

Virtuální soukromá síť (Virtual Private Network) je prostředek, jak spojit dvě různé sítě, například dvě pobočky naší firmy, pomocí nezabezpečené sítě, jako je internet. Často těchto služeb využívají zaměstnanci, když pomocí notebooku vyřizují

například firemní poštu. Celá komunikace přitom probíhá šifrovaně.

Na začátku uživatel prostřednictvím svého notebooku pošle požadavek na vytvoření VPN na VPN koncentrátor podnikové sítě. Pokud dojde k úspěšnému ověření důvěryhodnosti uživatele, požádá koncentrátor firewall o vytvoření VPN a tím získá uživatel přístup například k pracovní poště. Je výhodné, když naše firemní síť bude VPN umět. Zaměstnanci vybavení notebookem se pak mohou věnovat své práci i během cesty na konferenci.

5.4 Bezdrátové sítě

Nejtypičtějším příkladem bezdrátových sítí je Wifi [31]. V dnešní době má wifi kartu zabudovanou většina notebooků a čím dál více i mobilních telefonů. Pomocí Wifi se spolu mohou spojit dvě zařízení nebo se pomocí přístupového bodu (AP) připojí zařízení do sítě. Přístupový bod (AP) je zařízení vysílající do svého okolí své SSID. SSID je kód, podle nějž se zařízení identifikuje svému okolí. Pokud má naše podniková síť více přístupových bodů, vysílají všechny stejné SSID. Díky tomu náš notebook pozná, ke kterému přístupovému bodu se připojit.

Problémem bezpečnosti bezdrátových sítí je hlavně všesměrové šíření signálu. Většinou jej nezastaví ani zeď a případnému narušiteli stačí mít směrovou anténu a zachytí veškerou komunikaci naší firmy i na velkou vzdálenost.

Jednou z možností, jak chránit své soukromí, je použití VPN a šifrování komunikace. Další možností, sice porušující standard, ale velmi jednoduchou na provedení, je skrytí vysílání SSID u firemního wifi. Bezdrátová síť pak umožní připojení jen tomu, kdo zná její SSID z jiného zdroje. Bohužel je ale při započetí komunikace SSID vysíláno veřejně a může tak dojít k jeho odposlechnutí. Jinou možností, jak zamezit připojení neautorizovaného zařízení, je MAC adresa zařízení. Každá síťová karta má výrobcem danou unikátní MAC adresu. Přístupový bod při pokusu o připojení provede kontrolu této adresy a pokud nebude souhlasit, připojení zakáže. Všechna zařízení používající wifi v naší firmě by měla mít své MAC adresy zaregistrované a jinému zařízení by neměl být povolen přístup.

5.5 Cloud computing

Cloud computing je sdílení hardwarových i softwarových prostředků pomocí internetu [32]. Vychází z teorie, že pořídit si výkonný server, nakoupit pro něj programové vybavení a zaměstnat techniky, jež se o zařízení budou starat, je velmi drahé. Daleko levnější může být pronajmutí podobného zařízení. Ke všemu se pak připojujeme přes internet a pokud potřebujeme určitý speciální software, můžeme si jej místo zakoupení jen na čas pronajmout. Za služby ovšem neplatíme jen penězi. Přicházíme i o kousek firemního soukromí, kdy svěřujeme všechna svá data třetí straně, která je může prodávat naší konkurenci.

Správa počítačové sítě je úzce specializovanou oblastí. Pokud naše firma nemá v tomto oboru vhodného odborníka, existují i firmy, jež nám vhodného specialistu dočasně pronajmou. Jejich bohaté zkušenosti v oboru pomohou mnohem snáze překonat jakýkoliv zádrhel pří výstavbě či správě podnikové sítě.

6 Závěr

V současné době je zabezpečovací technika v každé organizaci nutností, ať jde o sféru veřejnoprávní nebo podnikatelskou. Vzhledem k široké nabídce a hlavně různorodosti takových produktů doporučujeme menší firmě, která zpravidla nezaměstnává špičkového odborníka v tomto oboru, obrátit se na fundovanou společnost, jež pomůže s výběrem vhodného zabezpečovacího systému.

Při výběru zabezpečovací techniky musíme brát v potaz nejen pořizovací cenu produktů, jejich životnost a hodnotu majetku, který je třeba zajistit, ale i v případě poruchy zařízení dostupnost servisu, náhradních dílů a součástek.

V době internetu je vhodné přečíst si odborné recenze a případné stížnosti zákazníků . Častá poruchovost nejen navyšuje pořizovací cenu systému, v případě ochrany fyzického majetku navíc zvyšuje možnost útoku zlodějů nebo v případě počítačového softwaru útoku hackerů.

Proti neoprávněnému vniknutí cizích osob do budovy organizace se můžeme bránit identifikací našich zaměstnanců.

U hlavního vchodu často uplatňujeme čipové karty, které jsou snadno dostupné, jednoduché na použití a na rozdíl od karet s magnetickým páskem nehrozí poškození magnetem (například od zapínání dámské kabelky) či mobilním telefonem.

Vstup do kanceláří a oddělení, kde se nachází trezor chránící majetek firmy či dokumenty podléhající vysokému stupni utajení, doplňujeme o znalostní autentizaci, například ovládacím panelem pro vyťukání číselného kódu pracovníkem, který má pravomoc do takové místnosti či oddělení vstoupit.

Identifikaci pomocí biometriky zatím mnoho firem nevyužívá. Jedním z důvodů je i neochota zaměstnanců poskytnout své biometrické údaje pro firemní účely, další pak jistá nepohodlnost při ověřování.

Na ochranu fyzického majetku firmy s oblibou instalují kamerové systémy. Ty ale přinášejí problémy ohledně ochrany osobních dat pracovníků, a proto se využívají hlavně v noci a ve dnech pracovního klidu. V pracovní době suplují kamery detektory pohybu.

Kromě fyzického majetku musíme chránit i citlivá data a informace. Většinu jich

máme uloženu v elektronické podobě. Ztráta takových dat by mohla způsobit i krach společnosti, proto jejich kopie uchováváme na záložním serveru.

Elektronická data dále zajišťujeme pravidelnou aktualizací počítačového softwaru a instalací antivirového programu a firewallu.

Své zaměstnance poučíme o nebezpečnosti stahování dat z internetu a svévolného instalování softwaru či používání z domova přinesených médií.

Pokud to nebrání plnění pracovních povinností zaměstnanců, povolíme nakládání se softwarovým vybavením pouze správcům počítačové síťě.

Svět informačních a monitorovacích systémů prochází podobně jako celý svět výpočetní techniky, na němž je bytostně závislý, překotným vývojem. Co je dnes takřka nemyslitelné a technicky nemožné, je zítra skutečností a pozítří všední realitou.

V budoucnosti budeme jistě běžně využívat různé technologie a zařízení, které dnes známe pouze z televizních vědecko-fantastických filmů a dosud používané systémy budou jen historickou vzpomínkou.

Příloha 1

Biometrická metoda	Metoda snímání	Časová stálost	Jednoznačnost	Přijatelnost
Otisk prstu	Optická, kapacitní	Velmi dobrá	1:1 000 000	Dobrá
Geometrie ruky	Optická	Dobrá	1:10 000	Velmi dobrá
Tvář	Optická	Dobrá	Neznámá	Dobrá
Oční sítnice	Optická – laser	Velmi dobrá	1:1 000 000	Malá
Oční duhovka	Optická	Velmi dobrá	1:6 000 000	Malá
Hlas	Elektroakustická	Malá	1:10 000	Dobrá
Chůze	Optická	Malá	1:10 000	Velmi dobrá

Tabulka 2: Základní biometrické metody a jejich charakteristiky

Seznam literatury

[1] *Vyhláška č. 523/2005 Sb. o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor* [online]. Národní bezpečnostní úřad, [2005] [cit. 2008-12-03]. Dostupný z WWW: <http://www.nbu.cz/cs/pravni-predpisy/provadeci-pravni-predpisy/vyhlaska-c-5232005/>.

[2] RAK, Roman, et al. *Biometrie a Identita člověka ve forenzních a komerčních aplikacích*. [s.l.] : [s.n.], 2008. 664 s. ISBN 978-80-247-2365-5.

[3] KASÍK, Pavel. *Klíče zapomínáme už 4000 let. Od dřevěných zámků k čtečkám otisků prstů* [online]. c1999-2009 [cit. 2009-04-18]. Dostupný z WWW: <http://technet.idnes.cz/klice-zapominame-uz-4000-let-od-drevenych-zamku-k-cteckam-otisku-prstu-1gj-/tec_technika.asp?c=A080307_153542_tec_technika_pka>.

[4] MORAVEC, Ondřej. *Čipové karty a vše o nich* [online]. 30.5.2006 [cit. 2009-01-03]. Dostupný z WWW: <http://www.finexpert.cz/Autori/Cipove-karty-a-vse-o-nich/sc-48-sr-1-a-16871/default.aspx>.

[5] *RFID* [online]. 8.7.2009 [cit. 2009-08-01]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/RFID>.

[6] ZEZULA, Radek. *Přístupové systémy k identifikaci osob* [online]. 16.11.2002 [cit. 2008-10-05]. Dostupný z WWW: <http://www.elektrorevue.cz/clanky/02054/index.html>.

[7] PŘIBYL, Tomáš. *Výhody a nevýhody biometrických systémů (1)* [online]. 28.5.2008 [cit. 2008-11-04]. Dostupný z WWW: <http://scienceworld.cz/technologie/vyhody-a-nevyhody-biometrickych-systemu-1-515>.

[8] PŘIBYL, Tomáš. *Výhody a nevýhody biometrických systémů (2)* [online]. 29.5.2008 [cit. 2008-11-04]. Dostupný z WWW: <http://scienceworld.cz/technologie/vyhody-a-nevyhody-biometrickych-systemu-2-512>.

[9] ZOUZALÍK, Marek. *Jak pracuje kapacitní snímač otisků prstů* [online]. 21.1.2005 [cit. 2008-11-25]. Dostupný z WWW: <http://www.21stoleti.cz/view.php?cisloclanku=2005012120>.

[10] RAK, Roman, et al. Lidská chůze a její počítačové využití při rozpoznávání identity člověka. *Magazín Security*. 1.1.2008, roč. 15, č. 84, s. 62-64.

[11] JANEČEK, T. *Biometrika : Verifikace Hlasu* [online]. c2004-2009 [cit. 2009-07-06]. Dostupný z WWW: <http://www.nula.wz.cz/biometrika/hlas.html>.

[12] KOUKAL, Martin. *Nejnovější světový objev českých odborníků: Pachatele prozradí chůze!* [online]. 19.3.2007 [cit. 2008-08-22]. Dostupný z WWW: <http://www.21stoleti.cz/view.php?cisloclanku=2007031915>.

[13] *Zákon č.101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů* [online]. Ministerstvo vnitra, c2003-2009 [cit. 2009-04-28]. Dostupný z WWW: <http://portal.gov.cz/wps/portal/_s.155/701/.cmd/ad/.c/313/.ce/10821/.p/8411/_s.155/701?PC_8411_number1=101/2000&PC_8411_l=101/2000&PC_8411_ps=50#10821>.

[14] *Bezpečnostní kamery, kamerové systémy, zabezpečení, CCTV, webové IP-kamery* [online]. c2009 [cit. 2008-10-28]. Dostupný z WWW: <http://www.escadtrade.cz/>.

[15] *Objektiv* [online]. 21.3.2009 [cit. 2009-04-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Objektiv>.

[16] *CMOS* [online]. 25.3.2009 [cit. 2009-04-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CMOS>.

[17] *CCD* [online]. 24.3.2009 [cit. 2009-04-05]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/CCD>.

[18] HOUSER, Pavel. *Budovy s detektory pohybu namísto kamer* [online]. 11.4.2008 [cit. 2008-10-18]. Dostupný z WWW: <http://securityworld.cz/securityworld/budovy-s-detektory-pohybu-namisto-kamer-672>.

[19] ČÁKA, Jan. IP kamerové systémy Bosh. *Magazín Security*. 1.1.2007, č. 80, s. 29.

[20] JAROŠ, Miroslav. *Základní informace o detektorech* [online]. [2005] [cit. 2008-09-16]. Dostupný z WWW: <http://www.acces.cz/acces/poradna/detektory-pohybu.asp>.

[21] PELIKÁN, Filip. *Použití bezpečnostního laserového skeneru pro ochranu nebezpečného prostoru* [online]. 2009 [cit. 2009-07-01]. Dostupný z WWW: <http://www.hadyna.cz/smartwelding/motoman/pdf/Skener_S3000_%C4%8Dl%C3%A1nek.pdf>.

[22] *FTP Secure Solutions - Perimeter Security* [online]. c2007 [cit. 2009-08-05]. Dostupný z WWW: <http://www.ftpemea.com/index.htm>.

[23] *Jak PGP pracuje* [online]. c2009 [cit. 2009-03-18]. Dostupný z WWW: <http://www.pgp.cz/index.php?l=cz&p=7&r=6>.

[24] *Zákon č. 227/2000 Sb. o elektronickém podpisu* [online]. Ministerstvo vnitra, c2003-2009 [cit. 2009-05-21]. Dostupný z WWW: <http://portal.gov.cz/wps/portal/_s.155/701?number1=227%2F2000&number2=&name=&text=>.

[25] PETERKA, Jiří. *Backup* [online]. 1993 [cit. 2008-12-28]. Dostupný z WWW: <http://www.earchiv.cz/a93/a330c120.php3>.

[26] *Bezpečnostní třídy trezorů* [online]. c1995-2009 [cit. 2009-05-04]. Dostupný z WWW: <http://www.jinova.cz/bezpecnostni-tridy-trezoru.php>.

[27] HUB, Miloslav. *Účtovatelnost a řízení přístupu* [online]. 3.10.2007 [cit. 2009-04-16]. Dostupný z WWW: <http://files.it-enclave.webnode.cz/200000022-305b931551/1_Uctovatelnost_a_rizeni_pristupu.pdf>.

[28] KAMENÍK, Jiří, et al. *Komerční bezpečnost : Soukromá bezpečnostní činnost detektivních kanceláří a bezpečnostních agentur*. 1. vyd. Praha : Aspi, 2007. 340 s. ISBN 978-80-7357-309-6.

[29] *Počítačové sítě snadno a rychle* [online]. 18.9.2006 [cit. 2009-06-05]. Dostupný z WWW: <http://pctuning.tyden.cz/navody/zaklady-stavba-pc/7543-zaklady_pc-pocitacove_site_snadno_a_rychle?start=2>.

[30] PETERKA, Jiří. *Jak fungují firewally?* [online]. 2003 [cit. 2009-06-29]. Dostupný z WWW: <http://www.earchiv.cz/b03/b0800001.php3>.

[31] *Wi-Fi* [online]. 2.8.2009 [cit. 2009-08-06]. Dostupný z WWW: <http://cs.wikipedia.org/wiki/Wifi>.

[32] SCHWARTZ , Ephraim. *Cloud computing skrývá řadu nebezpečí* [online]. 26.7.2009 [cit. 2009-07-27]. Dostupný z WWW: <http://computerworld.cz/technologie/nebezpeci-cloud-computingu-4405>.