ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA

Provozně ekonomická fakulta

Katedra informačních technologií

DIPLOMOVÁ PRÁCE

Psychologie a bezpečnostní politika organizace

Michaela Filingerová

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Akademický rok 2010/2011

ZADÁNÍ DIPLOMOVÉ PRÁCE

Michaela Filingerová

obor Informatika

Vedoucí katedry Vám ve smyslu Studijního a zkušebního řádu ČZU v Praze čl. 17 odst. 2 určuje tuto diplomovou práci.

Název práce: **Psychologie a bezpečnostní politika organizace**

Osnova diplomové práce:

1. Úvod
2. Cíl práce a metodika
3. Přehled řešené problematiky
4. Vlastní řešení
5. Zhodnocení výsledků a doporučení
6. Závěr
7. Seznam použitých zdrojů
8. Přílohy

Rozsah hlavní textové části: 60 - 80 stran

Doporučené zdroje:

HARRIS, S., HARPER, A., EAGLE, CH. Manuál hackera. Praha : Grada, 2008. 400 s. ISBN 978-80-247-1346-5.
JÍROVSKÝ, V. Kybernetická kriminalita. Praha : Grada, 2007. 288 s. ISBN 978-80-247-1561-2.
MCCLURE, S., SCAMBRAY, J., KURTZ, G. Hacking bez záhad. 5. vyd. Praha : Grada, 2007. 520 s. ISBN 978-80-247-1502-5.
MITNICK, K., SIMON, W. Umění klamu. Polsko : Helion S.A., 2003. 348 s. ISBN 83-7361-210-6.

Vedoucí diplomové práce: **Ing. Čestmír Halbich, CSc.**

Termín odevzdání diplomové práce: duben 2011

L.S.

....

Vedoucí katedry Děkan

V Praze dne: 7. 2. 2011

Evidováno děkanátem PEF pod č.j.: KIT-177-10D

ČESTNÉ PROHLÁŠENÍ

Prohlašuji, že jsem tuto diplomovou práci vypracovala samostatně a s využitím uvedených zdrojů a literatury, které v práci řádně cituji.

V Žatci 29. listopadu 2011 Michaela Filingerová

PODĚKOVÁNÍ

Na tomto místě bych ráda poděkovala všem, kteří napomohli vzniku této diplomové práce. Především děkuji svému vedoucímu Ing. Čestmíru Halbichovi, CSc. za jeho vedení, cenné připomínky a rady při zpracování práce.

PSYCHOLOGIE A BEZPEČNOSTNÍ POLITIKA ORGANIZACE

V diplomové práci „Psychologie a bezpečnostní politika organizace“ je představena problematika bezpečnosti aktiv organizace ve vztahu k managementu a práci manažerů nejen na poli bezpečnosti organizace obecně, ale zejména tvorby bezpečnostní politiky a motivace jednotlivých pracovníků.

Přehledným a stručným způsobem podává alespoň základní rozbor obecných požadavků na fyzickou, informační, personální, administrativní a internetovou bezpečnost organizace, principy bezpečnostních incidentů a prostředků, které napomáhají při jejich detekci, zábraně, či zotavení organizace z útoku.

Podrobněji se zaměřuje na podceňování lidského faktoru v oblasti bezpečnosti aktiv organizace, rozbor nejčastějších chyb a prací manažerů při motivaci dodržování základních bezpečnostních zásad všemi pracovníky organizace.

KLÍČOVÁ SLOVA

bezpečnost, bezpečnostní politika, informace, data, ochrana informací a dat, útok, bezpečnostní rizika a hrozby, bezpečnostní mechanismy

PSYCHOLOGY AND SECURITY POLICY OF ORGANISATION

The thesis „Psychology and security policy of organisation“ introduce issues of organisation security assets in relation to management and managers in the field of security organisation in general, especially security policy-making and motivation of individual employees.

Clear manner provides a basic analysis of the general requirements for organisation physical, information, personnel, administrative and Internet security, principles of security incidents and resources to assist in their detection, inhibition and recovery organisation from attack.

Detail focuses on the underestimate of the human factor in security of the assets the organisation, analysis of the most common mistakes and work managers in motivating compliance with basic safety principles by all employees of the organisation.

KEY WORDS

security, security policy, information, data, protection of information and data, attack, safety risks and threats, safety mechanism

OBSAH

1 ÚVOD

V současné době hrají informační a komunikační technologie důležitou roli ve všech sférách života. Stále více dat je předáváno v digitální podobě a stále více významných a důležitých dat v organizacích je ukládáno do informačního systému.

Tento trend s sebou přináší řadu výhod (možnost přenosu nejen textových dokumentů, ale i obrazových a zvukových informací, zkrácení lhůt pro přenos dokumentů, snížení nákladů na administrativu a archivaci), ale též jisté nevýhody (ochrana a zabezpečení citlivých dat a informací, které mají pro organizace nepostradatelnou a životně důležitou hodnotu, kdy jejich ztráta může omezit nebo úplně zastavit činnost organizace).

Je proto potřeba věnovat náležitou pozornost ochraně a zabezpečení takovýchto informací a dat před jejich neúmyslným poškozením (tzn. například před živelnými pohromami, různými poruchami, chybami při přenosu dat, nedbalostí osoby, která s daty nakládá aj.) nebo před úmyslným a záměrným poškozením (tj. neoprávněným přístupem, zničením, odcizením, zneužitím, vyzrazením konkurenci aj.).

K tomu, aby bylo možné data a informace zabezpečit, je nutné znát jednak slabá místa systému organizace, jež má být chráněn, a jednak způsoby, jimiž mohou útočníci těchto slabých míst využít ve svůj prospěch. Nejvíce ohroženou oblastí úniku a ztráty informací a dat jsou samotné informační a komunikační technologie a pak lidský faktor, který dané technologie v organizaci užívá.

Nezbytným předpokladem pro zajištění bezpečnosti informací a dat je vyhotovení písemného dokumentu, takzvané bezpečnostní politiky organizace, který bude závazný pro celou organizaci a platný pro všechny pracovníky.

Stejně tak velkou pozornost je nutné věnovat personální bezpečnosti, neboť bezpečnost informací a dat zajišťují právě lidé. Tuto problematiku má na starosti management organizace, který je zodpovědný za výběr vhodných pracovníků, jejich kvalifikaci, vhodnou motivaci a stimulaci správným směrem.

1.1 VÝKLAD ZÁKLADNÍCH POJMŮ

K porozumění a pochopení problematiky „Psychologie a bezpečnostní politiky organizace“ je důležité vymezit a objasnit výklad některých pojmů, které budou dále v práci často používány.

Informace

Pojmy informace a data jsou v praxi velmi často zaměňovány nebo slučovány. Ve skutečnosti má každý z těchto pojmů jiný význam.

Informace je sdělení o nějaké události, jevu či procesu, které snižuje nebo částečně odstraňuje neznalost o této události. Je možné z něj získat něco nového, co o něm nebylo dříve známo, nebyl znám jeho obsah.

Rozdíl mezi informacemi a daty je tedy ten, že informaci z dat lze získat tím, že umíme data interpretovat, rozumíme tomu, co nám sdělují a sdělí nám něco nového. [1]

Informacemi v organizaci tak mohou být například interní informace o organizaci a jejích pracovnících, její strategické záměry a plány, know-how, databáze zákazníků, nebo informace získané z volně dostupných zdrojů. [2]

Data

Pojem data (jednotné číslo údaj) vyjadřuje jakoukoliv skutečnost odrážející stav reality v určitém okamžiku získanou čtením, pozorováním, měřením a podobně, která je schopná přenosu, uchování, zpracování či interpretace.

Data mají zpravidla textovou, číselnou, grafickou, znakovou či jinou symbolickou formu. Pro jejich přenos, uchování, zpracování či interpretaci je nutný technický prostředek, který slouží jako nosič dat.

Informační systém (IS)

Informační systém je možné definovat jako soubor hardwaru, softwaru, dat a lidských zdrojů, který zabezpečuje systematickou a účelnou správu svých informací.

Informační a komunikační technologie (ICT)

Informační a komunikační technologie zahrnují veškeré hardwarové a softwarové prostředky sloužící pro přenos, uchování, zpracování a distribuci dat, které umožňují komunikaci a práci s informacemi.

Bezpečnost

Bezpečnost je vlastnost nějakého objektu či subjektu, která určuje stupeň jeho ochrany před nebezpečím a před hrozbami. Je zajišťována bezpečnostními opatřeními, takzvanými bezpečnostními mechanismy. [3]

Bezpečnostní politika

Bezpečnostní politika je označení pro základní a klíčový bezpečnostní dokument schválený vedením organizace, který je závazný pro celou organizaci a všechny její pracovníky. Jejím cílem je deklarování základních cílů organizace v oblasti ochrany informací, stanovení toho, co má být chráněno a jak toho má být dosaženo, a definování příslušných zodpovědností a kompetencí. [17]

Hrozba

Bezpečnostní hrozba je jakákoliv událost působící na zranitelné místo v organizaci, která může způsobit potenciální škodu, poškození nebo zničení hodnoty citlivých dat.

Riziko

Bezpečnostní riziko je pravděpodobnost zničení a poškození hodnoty citlivých dat organizace vyplývající z působení bezpečnostní hrozby na její slabou stránku. [3]

Zranitelnost

Zranitelnost je nedostatek nebo slabina bezpečnostního systému, která může být zneužita bezpečnostní hrozbou tak, že dojde k poškození či zničení hodnoty citlivých dat.

Útok (bezpečnostní incident)

Útokem se rozumí úmyslné využití zranitelného místa nebo neúmyslné uskutečnění akce, které mají za následek způsobení škody nebo ztráty na aktivech organizace.

2 CÍL PRÁCE A METODIKA

Cílem této práce je prohloubení vědomostí a znalostí o problematice bezpečnosti informací v organizaci v souvislosti s činnostmi managementu a prací manažerů na poli bezpečnosti organizace a dále pak bezpečnostní politikou, jakožto základním dokumentem každé organizace v oblasti bezpečnosti.

Obsah práce je koncipován tak, aby nejdříve podal rozbor obecných požadavků kladených na bezpečnost organizace jako takové, následně je zaměřen na lidský faktor jako podceňovaného činitele bezpečnosti informačního systému organizace. V další části bude rozpracována problematika bezpečnosti ve vztahu k managementu a vývoji bezpečnostní politiky organizace. Nakonec budou nastíněny možnosti ke zlepšení bezpečnosti z hlediska motivace a stimulace uživatelů a správců informačního systému organizace. Závěr práce bude souhrnem poznatků a přínosů v oblasti bezpečnosti. V příloze č. 1 bude zpracována případová studie na analýzu rizik konkrétní organizace, jejímž cílem bude identifikovat klíčové rizikové oblasti organizace, na jejichž základě budou navrženy doporučení pro jejich eliminaci.

Oblast bezpečnosti organizace je velmi široká, stále se měnící a díky tomu také problematická. Proto nemůže být podán vyčerpávající rozbor ochrany a zabezpečení, ale bude teoreticky zpracován s poznatky z běžné praxe do stručného přehledu.

3 OBECNÉ POŽADAVKY NA BEZPEČNOST

Jedna z mnoha definic obecné bezpečnosti, a to definice Ministerstva vnitra České republiky, zní následovně: *„Bezpečnost je stav, kdy je systém schopen odolávat známým a předvídatelným vnějším a vnitřním hrozbám, které mohou negativně působit proti jednotlivým prvkům (případně celému systému) tak, aby byla zachována struktura systému, jeho stabilita, spolehlivost a chování v souladu s cílovostí.“* [18]

Hlavním důvodem zavádění bezpečnosti je především zajištění ochrany veškerých aktiv organizace před všemi hrozbami a minimalizace případných škod. Aktiva představují veškeré hmotné i nehmotné statky, které mají pro organizaci nějakou hodnotu. Nejcennější aktiva jsou peníze, majetek, pracovníci firmy a především data a informace, jejichž ztrátou, zneužitím či modifikací by organizace utrpěla škodu.

Důsledkem nedostatečné bezpečnosti může být částečné nebo úplné znehodnocení dat a informací, krádež, neoprávněné zneužití, dočasná nebo trvalá ztráta dat a citlivých informací, vyzrazení obchodních záměrů nebo ztráta dobrého jména organizace. [3]

Řešení bezpečnosti musí zajišťovat celkovou bezpečnost *organizace*, která zahrnuje bezpečnost *dat*, *médií*, na kterých se data nacházejí, *hardware*, který je potřeba pro práci s médii, *software*, který je na hardware nainstalován, *sítě*, prostřednictvím které přistupuje k datům více uživatelů, *prostor*, ve kterých je vše umístěno, a *lidí*, kteří se starají o celý systém a kteří jej používají (viz. obrázek č. 3). Zavedení bezpečnosti přináší finanční náklady, ale nepřináší okamžitý výsledek v podobě přínosů či zisku. Redukuje však možnost ztráty či zneužití nejdůležitějších aktiv organizace, na nichž je závislá její činnost.

Při zavádění ochrany aktiv by se měla brát v úvahu cena ochranných mechanismů a nákladů v poměru k jejich bezpečnostnímu efektu nebo nároky na jejich provoz a údržbu. Náklady by neměly přesáhnout případnou škodu. Proto je někdy výhodnější počítat s určitými riziky, která ohrožují aktiva, než je nákladným způsobem eliminovat.

Pro zajištění bezpečnosti jednotlivých oblastí organizace se předpokládá vypracovat bezpečnostní strategii organizace, provést analýzu rizik organizace, stanovit opatření a zásady ochrany aktiv organizace a zpracovat bezpečnostní politiku organizace a postup implementace bezpečnostního systému organizace. [2]

3.1 BEZPEČNOST ORGANIZACE

3.1.1 Fyzická bezpečnost

Na prvním místě stojí bezpečnost organizace, tedy zajištění bezpečnosti objektů, majetku a zařízeních organizace, ve kterých se nachází hardware a software, média s daty a lidé. Primárním cílem je *zamezit přístupu nepovolaných osob* do budovy organizace. Pokud totiž získá útočník přístup k počítači, který je připojen k informačnímu systému organizace, má mnohem více možností ke zničení, odcizení či modifikaci dat. Řada objektů má proto k dispozici bezpečnostní mechanismy, ke kterým lze zařadit například automatický dveřní systém založený na principu identifikačních čipových karet, biometrické systémy, snímače pohybu chránící okna a dveře, rozmístěné bezpečnostní kamery po objektu, kniha návštěv zaznamenávající dobou příchodu a odchodu návštěvy. Kombinace více bezpečnostních mechanismů v organizaci najednou poskytuje dostatečnou ochranu v případě selhání jednoho z nich.

Sekundárním cílem je *odrazování, ztěžování a detekování nežádoucích aktivit ze strany pracovníků* organizace. Na vybrané dveře jsou instalovány čtečky identifikačních čipových karet, které slouží pro kontrolu pohybu pracovníků po budově. [3]

Do oblasti fyzické bezpečnosti spadá i *ochrana proti zásahům „vyšší moci“*, tj. proti živelným pohromám jako je požár, zemětřesení, záplavy či klima. Ochrana před živelnými katastrofami spočívá v instalaci samočinných požárních hlásičů a komplexních systémů pro hašení vzniklých požárů, kvalitním upevnění disků a skříní s počítači, aby se zabránilo nežádoucím pádům a nárazům, vybavení místností kvalitní klimatizací, aj. Proti všem přírodním katastrofám se lze bránit duplikací důležitých částí systému a pravidelným zálohováním dat. [4]

Proti *neočekávaným výpadkům napájení* se lze chránit používáním záložních zdrojů napájení, která dokáží zajistit stabilitu dodávaného proudu i ochranu před neočekávanými špičkami či výpadky. V případě, že je potřeba zabezpečit napájení v době delšího výpadku napájení, které nedokáže záložní zdroj zajistit, je třeba zvážit využití záložního generátoru. *Napájení, telekomunikační a síťové kabely* nesoucí data nebo informace o podpůrných službách je třeba *chránit před poškozením nebo odposlechem*.

Na obrázku č. 1 jsou ilustrovány možnosti fyzického zabezpečení organizace.

Obrázek 1 - Fyzická bezpečnost organizace

Zdroj: archiv autora

3.1.2 Informační bezpečnost

Jak již bylo zmíněno v úvodu, informace pro každou organizaci hrají velkou, často až nepostradatelnou a životně důležitou roli. Schopnost s těmito informacemi pracovat představuje významnou konkurenční výhodu. V případě, že organizace nedokáže tyto informace uchránit, může dojít ke ztrátě konkurenční výhody, ztrátě dobrého jména organizace, neplnění zákonných povinností nebo k ukončení celé její činnosti. [17]

Důvody k zajištění bezpečnosti informací jsou povinnosti vyplývající z platné legislativy České republiky, závazky organizace vůči svým klientům a spolupracujícím společnostem, které plynou z podmínek uzavřených dohod a smluv, a zejména vlastní obchodní zájmy organizace.

Informační bezpečnost zajišťuje *ochranu dat a informací* tak, aby k nim měly přístup pouze oprávněné osoby, aby se zpracovávaly neporušené, byly dostupné v době, kdy jsou potřebné, dalo se zjistit, kdo je vytvořil, upravil či odstranil, a aby nebyly nekontrolovaným způsobem vyzrazeny.

Dále zajišťuje *zabezpečení dat a informací*, čímž je myšleno zajištění jejich důvěrnosti, integrity a dostupnosti. Důvěrnost je zajištění bezpečnosti vlastního obsahu dat a informací, integrita je zaručení celistvosti a neporušenosti obsahu informací a dostupnost je obnova přístupu k informacím. K těmto třem klasickým hlediskům se dnes připojují ještě autenticita, prokazatelnost odpovědnosti, nepopiratelnost odpovědnosti a spolehlivost. Autenticitou se rozumí proces ověřování identity uživatele (ujištění, že konkrétní uživatel je skutečně ten, za koho se prohlašuje), prokazatelností odpovědnosti získání záruky, že lze učinit uživatele zodpovědného za jeho aktivity, nepopiratelností odpovědnosti nemožnost popřít účast uživatele na transakci a spolehlivostí konzistence zamýšleného a výsledného chování informací a služeb informačních technologií. [19]

Nutné je starat se nejen o ochranu a zabezpečení dat a informací, ale zároveň o *dodržování oprávněnosti přístupu* k nim. Tento požadavek zajišťují zásady bezpečné práce s informacemi, a to například zásady skartace materiálů, zásady pro poskytování informací novinářům, způsob zpracování, uložení a správy archivu či zásady nakládání s informacemi během jejich transportu na jiná místa. [3] Metody zajištění informační bezpečnosti znázorňuje obrázek č. 2.

Obrázek 2 - Informační bezpečnost organizace

Zdroj: http://www.designplus.cz/uvodni-stranka/nase-reseni/dp-netservice/systemova-a-aplikacni-infrastruktura-sai/informacni-bezpecnost (dne: 2011-11-20)

3.1.3 Personální a administrativní bezpečnost

Organizace si může najmout tu nejlepší firmu na noční ostrahu objektů, pořídit ty nejlepší a nejdražší bezpečnostní technologie, nainstalovat všechny nejnovější produkty zabezpečující ochranu, a přesto bude stále zranitelná. Jedním z neproblematičtějších míst zabezpečení je lidský faktor.

Cílem bezpečnostních opatření personální bezpečnosti je *minimalizovat rizika lidských omylů a chyb, špatného používání informačního systému, krádeží a podvodů*. [2]

Oblast personální a administrativní bezpečnosti by se měla promítnout *do všech procesů, směrnic a nařízení organizace*, které se týkají personalistiky, počínaje přijetím nového zaměstnance do pracovního poměru, bezpečnostním školením, definováním odpovědností a povinností zaměstnance v oblasti bezpečnosti, písemným prohlášením zaměstnance o dodržování zásad nakládání s informacemi a rozvázáním pracovního poměru konče.

Aby bylo možné v organizaci zavádět, prosazovat a úspěšně řídit bezpečnost, je nezbytné *definovat potřebné pozice, role, odpovědnosti, rozhodovací pravomoci a stanovit procesy*, prostřednictvím nichž budou bezpečnostní principy a opatření realizovány. Každé sdělení tisku, rozhlasu a televizi by měl prověřit pracovník odpovědný za bezpečnost organizace.

O zabezpečení informačního systému a počítačů se budou starat zaměstnanci oddělení IT, o rozhodování a odpovědnosti za bezpečnost organizace by se měl starat pracovník, který je vybaven dostatečnými manažerskými schopnostmi, znalostmi v oblasti bezpečnosti informačních technologií a neměla by mu chybět znalost vnitropodnikových procesů a struktury organizace. Zaměstnanci spravující a udržující informační systém mají rozsáhlé pravomoci, proto je nutné vybírat je s velkou opatrností. [3]

Ve větších organizacích je ustanovena pozice bezpečnostní manažer, kterému podléhá vlastní pracovní tým bezpečnosti. Posláním bezpečnostního týmu je příprava materiálů a podkladů pro potřeby bezpečnostního manažera a prosazování jeho rozhodnutí. U malých organizací může být tato funkce přidělena některé z vedoucích pozic organizace nebo řešena najmutím externího poskytovatele, takzvaného outsourcingu.

3.1.4 Internetová bezpečnost

Ačkoliv mezi tradiční dělení bezpečnosti prozatím autoři v literatuře internetovou bezpečnost neuvádějí, v dnešní době je více než vhodné brát ji v potaz. Internetu jako takovému totiž chybí bezpečnostní mechanismus, který by jakkoliv chránil přenášená data.

Usnadnění komunikace prostřednictvím Internetu přináší organizaci řadu výhod. Využívají jej k nejrůznějším obchodním transakcím, získávání informací, ke styku s úřady a korespondenci s dalšími organizacemi, k on-line nakupování včetně placení a mnoha dalším činnostem, jejichž spektrum se neustále rozšiřuje.

Takovéto využívání Internetu s sebou nese samozřejmě i jistá rizika, s kterými musí uživatel a organizace počítat. Těmi nejvíce rozšířenými riziky je napadení počítače viry nebo jinými uživateli Internetu, ztráta identity, odcizení osobních údajů a hesel.

Řešení internetové bezpečnosti je důležitým problémem jak pro běžné uživatele, tak pro správce rozsáhlých sítí. Cílem je *zavedení opatření*, která znemožní nebo maximálně znesnadní útočníkovi získat soukromá či neveřejná data, obsah komunikace, zamezí převzít nadvládu nad počítačem, zabrání útoku s pokusem vyřadit z provozu server.

Jako ochrana proti útokům ze sítě Internet se používají *technická zařízení* (firewall, proxy server) a *programová vybavení* (antivirové programy, antispyware, aj.).

Asi největší hrozbou však zůstává stále uživatel, a proto je důležité, aby udržoval aktuální operační systém a používané aplikace, neotvíral neznámé či podezřelé soubory, programy nebo přílohy zpráv z e-mailů a instant messengerů (Icq, Qip, Jabber, Skype apod.), nezveřejňoval osobní citlivé údaje a informace „zevnitř“ organizace na sociálních sítích (Facebook, Twitter, Google+, aj.).

Obrázek 3 - Bezpečnostní správa organizace

Zdroj: archiv autora

3.2 LEGISLATIVA ŘEŠÍCÍ BEZPEČNOST

V České republice dosud neexistuje zákon, který by komplexně řešil bezpečnost v prostředí elektronického zpracování informací. Existuje však mnoho zákonů a vyhlášek, které se vztahují alespoň částečně k problematice informační bezpečnosti (viz. příloha č. 2). Mezi ty nejdůležitější lze jmenovat následující zákony.

Obchodní zákoník

Zákon č. 513/1991 Sb., ustanovení § 17 až § 20 obchodního zákoníku, ve znění pozdějších předpisů, řeší otázky spojené s obchodním tajemstvím. Obchodním tajemstvím jsou veškeré skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu, nejsou v příslušných obchodních kruzích běžně dostupné, mají být podle vůle podnikatele utajeny a podnikatel odpovídajícím způsobem jejich utajení zajišťuje. Podnikatel provozující podnik, na který se obchodní tajemství vztahuje, má výlučné právo tímto tajemstvím nakládat, zejména udělit svolení k jeho užití a stanovit podmínky takového užití. [20]

Zákon o ochraně osobních údajů

Zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, upravuje mimo jiné práva a povinnosti při zpracování osobních údajů. Vztahuje se na osobní údaje, které zpracovávají státní orgány, jiné orgány veřejné moci, nebo fyzické a právnické osoby, ať již ke zpracování dochází automatizovaně nebo jinými prostředky.

Osobní údaj je zákonem vymezen jako jakákoliv informace týkající se určeného nebo určitelného subjektu údajů, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu.

Zpracování osobních údajů je jakákoliv operace nebo soustava operací, které správce nebo zpracovatel systematicky provádějí s osobními údaji, a to automatizovaně nebo jinými prostředky. Jedná se zejména o shromažďování, ukládání na nosiče informací, zpřístupňování, úprava nebo pozměňování, vyhledávání, používání, předávání, šíření, zveřejňování, uchovávání, výměna, třídění nebo kombinování, blokování a likvidace. [21]

Zákon o ochraně utajovaných informací

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů, upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.

Zákon vymezuje utajovanou informaci jako informaci v jakékoliv podobě, která je zaznamenaná na jakémkoliv nosiči a označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací (§ 139). Utajované informace se klasifikují stupněm utajení. Mohou být přísně tajné, důvěrné nebo vyhrazené. [22]

Zákon o elektronickém podpisu

Zákon č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů, upravuje používání elektronického podpisu a značky, poskytování certifikačních služeb a souvisejících služeb poskytovateli usazenými na území České republiky, kontrolu povinností stanovených tímto zákonem a sankce za porušení povinností stanovených tímto zákonem.

Elektronický podpis je zákonem vymezen jako údaje v elektronické podobě, které jsou připojeny 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.

Poskytovatelem certifikačních služeb je fyzická osoba, právnická osoba nebo organizační složka státu, která vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy. [23]

3.3 BEZPEČNOSTNÍ INCIDENTY

Bezpečnostní incident, někdy též nazývaný útok, představuje narušení bezpečnosti informačního systému nebo informačních technologií v důsledku selhání bezpečnostních opatření nebo porušení bezpečnostní politiky organizace. Řešení bezpečnostních incidentů znázorňuje obrázek č. 4.

Obrázek 4 - Řešení bezpečnostních incidentů

Zdroj: http://www.systemonline.cz/clanky/prevence-a-zvladani-bezpecnostnich-incidentu.htm (dne: 2011-11-20)

3.3.1 Útočníci na bezpečnost

Důležité je uvědomit si, kdo může útok provést. Útočníky můžeme rozdělit do tří skupin, podle toho v jakém jsou postavení k organizaci. Největší skupinou, která může napáchat nejvíce neúmyslných škod, jsou *náhodní vnitřní útočníci*. Jde o nové zaměstnance organizace, nezkušené uživatele aplikací a systému, správce systému nebo vývojáře softwaru. Druhou skupinou jsou *záludní vnitřní útočníci*, což mohou být nespokojení a zlomyslní zaměstnanci, obchodní partneři, případně trpěliví specialisté, kterým se podařilo nepozorovaně dostat se do organizace. Poslední skupinou jsou *vnější útočníci*, kteří provádějí svůj útok zvnějšku systému organizace.

Útočníci mohou přesvědčit nebo přinutit oprávněného uživatele, aby útok provedl za ně, mohou zaútočit na aplikace změnou nebo záměnou jejich skutečného kódu či mohou provést přímý útok na aplikaci prostřednictvím jejich skrytých nebo nedokonalých funkcí.

Některé útočníky zajímá pouze osobní uspokojení, kterého dosáhnou pokořením systému zabezpečení, jiné otestování a dokázání svých dovedností prostřednictvím změny nějakých veřejně dostupných informací (zpravidla na internetových stránkách), případně pomsta zaměstnavateli po propuštění ze zaměstnání. [5]

3.3.2 Útoky na bezpečnost

Na jednotlivé incidenty lze nahlížet z několika pohledů. Prvním takovým pohledem je charakter útoku, tedy zda byl útok proveden úmyslně, nebo neúmyslně nedbalostí, neznalostí nebo nevědomostí uživatele. Druhým pohledem je cíl útoku, který lze rozdělit na aktivní (např. přerušení dostupnosti) a pasivní útok (odposlech). Dalším pohledem je dopad, jaký útok způsobí. Hodnota dopadu může být nízká, střední, vysoká či kritická.

Následuje stručný přehled nejběžnějších forem útoku.

Hacking

Hacking je metoda odborně velmi zdatných uživatelů Internetu (hackerů), kteří dokáží využít zranitelných míst informačního systému organizace k průniku do systému organizace pro pobavení, potěšení z řešení problémů, překonávání limitu, důkaz svých schopností a získání nových zkušeností. Základním principem hackingu není způsobit organizaci škodu či ztrátu, nýbrž upozornit správce systému na jeho zranitelná místa.

Cracking

Cracking je metoda k odstraňování ochranných prvků komerčních programů za účelem možnosti používání bez nutnosti jeho zakoupení. Ochrannými prvky mohou být registrační čísla, ochrany před kopírováním, hardwarové klíče, ochrany s funkčním nebo časovým omezením. Osobám odstraňující softwarové ochrany se říká crackeři.

Backdoors

Backdoors (v překladu zadní vrátka) je metoda umožňující obejít běžnou autentizaci uživatele, která za normálních okolností uživateli brání v neoprávněném vstupu do programu nebo systému. Jsou součástí zdrojového kódu programu. Mohou být využívána pro servisní přístup, ale často jsou zneužívána ke způsobení škod či ztrát.

Phishing

Phishing je podvodné jednání používané na Internetu s cílem vylákat z uživatele citlivé údaje jako jsou hesla, čísla kreditních karet a podobně. S podvody tohoto typu je možné se setkat v e-mailových zprávách, které se tváří jako oficiální žádosti bankovních institucí, sociálních sítí atd. a vyzývají uživatele k zadání jeho údajů na falešné stránky.

Pharming

Pharming je podvodná technika, jejímž principem je napadení systému překladu doménových jmen a přepsání IP adresy, které způsobí přesměrování specifického odkazu na falešné stránky útočníka.

Social Engineering

Sociální inženýrství je metoda pro přesvědčování a manipulaci s lidmi. Účelem je provedení určité akce nebo získání určité informace. Ve většině případů útočník nepřichází do osobního kontaktu s obětí. Používanou technikou je mimo jiné např. phishing.

Sniffing

Odposlech je pasivní útok na utajení. Útočník zachytává všechna data, která se pohybují po síti, odposlouchává komunikaci nebo nedovoleně kopíruje data.

Denial of Service (DoS)

Denial of Service (v překladu odepření služby) je technika útoku, při níž dochází k přehlcení požadavky, pádu, nefunkčnosti nebo nedostupnosti určité služby, systému nebo dokonce celé sítě pro ostatní uživatele. Druhou možností jsou distribuované DoS útoky, kterých se účastní více počítačů.

Port scanning

Skenování portů je průzkumná technika na Internetu, která bývá velmi často zneužívána hackery jako prostředek pro pokus o prolomení systému. Cílem je identifikovat běžící služby, zjistit typ operačního systému a provozovaných aplikací. Pomocí nich je možné využít znalosti bezpečnostních chyb a děr systému.

Malware

Malware je souhrnné označení pro zákeřné počítačové programy, které jsou určeny ke vniknutí nebo poškození počítačového systému. Nejčastěji to může být počítačový vir, červ, trojský kůň nebo stále častěji spyware.

Počítačový vir je program, který se instaluje na počítač a sám se dokáže šířit bez jasného vědomí a svolení uživatele. Počítačový červ oproti viru navíc schopen šířit sám sebe prostřednictvím sítě na další počítače. Trojský kůň je program, který vykonává funkce, které ohrožují bezpečnost uživatelova počítače.

Spyware je používán jako marketingový nástroj, který odesílá data z počítače bez vědomí jeho uživatele. Odcizována jsou data, která zaznamenávají přehled uživatelem navštívených internetových stránek či nainstalovaných programů.

3.4 BEZPEČNOSTNÍ MECHANISMY

Bezpečnostním incidentům lze předejít implementací bezpečnostních opatření, tzv. bezpečnostních mechanismů. Vztah mezi bezpečnostními hrozbami a bezpečnostními opatřeními ilustruje obr. č. 5. Bezpečnostní mechanismy jsou navrženy tak, aby detekovaly útoky, zabraňovaly jim, eventuelně pomáhaly ze zotavení systému z útoků. Je jich mnoho a mohou mít charakter softwarových (logických) nástrojů, technických zařízení, fyzických opatření nebo administrativních akcí. [19]

Ne vždy je možné veškerým incidentům předejít. Pokud dojde ke zjištění incidentu, je třeba vyřešit jeho příčinu, podrobně analyzovat situaci s cílem zjistit zdroje infiltrace a uvést informační systém do původního a důvěryhodného stavu. Současně s odstraněním důsledků je třeba uskutečnit i opatření zamezující možnosti opakování tohoto incidentu.

Obrázek 5 - Bezpečnostní hrozby a opatření organizace

Zdroj: http://www.tsoft.cz/bezpecnost (dne: 2011-11-20)

3.4.1 Softwarové mechanismy

Softwarové mechanismy (též označované jako logické bezpečnostní mechanismy) jsou založeny na principu řízení přístupu v daném operačním systému, kryptografie, standardů pro návrh, kódování, testování, údržbu programů nebo ochranných nástrojů v operačních systémech a aplikačních programech.

Přístupová hesla

Hesla slouží k ochraně přístupu k nejrůznějším systémům a informacím, do kterých by se neměl dostat nikdo nepovolaný.

Heslo by mělo být bezpečné, to znamená takové, které je často obměňované a není snadno zjistitelné, odhadnutelné nebo jinak zneužitelné. Mělo by mít alespoň osm znaků, které spolu dohromady netvoří žádné slovníkové slovo. Řetězec by měl obsahovat malá a velká písmena, číslice, případně speciální symboly. Nemělo by vzniknout z nějakého osobního údaje o uživateli či jeho okolí (například z vlastního jména či někoho z rodiny, jména domácího mazlíčka, data narození, adresy, čísla domu, apod.).

Jakkoliv těžké heslo však není bezpečné, pokud ho uživatel komukoliv prozradí, napíše si ho na papírek, na harddisk nebo uloží heslo do programu, který dokáže při dalším přihlašování zadat údaje za uživatele.

Antivir, antispyware

Antivirové programy slouží k identifikaci, odstraňování a eliminaci počítačových virů a jiných škodlivých programů. Dnešní antivirové programy bojují i proti spyware. Účinnost zachycení nežádoucích virů a spyware závisí na schopnostech antivirového programu a aktuálnosti jeho virové databáze.

Antispyware jsou speciální programy sloužící k odstraňování a blokování spyware, který se bez vědomí uživatele stáhl do jeho počítače.

Logování

Logování poskytuje správci systému užitečné informace pro diagnostiku událostí. Operační systémy, některé programy či služby vytvářejí soubory záznamů, takzvané logy, do kterých ukládají informace o své činnosti a běhu. Ty slouží jako informace o tom, jak a kým byla daná aplikace či služba využívána, nebo jako detekce a analýza bezpečnostních incidentů. V praxi se nejčastěji sledují úspěšné a neúspěšné pokusy o přihlášení a odhlášení k systému, neúspěšné pokusy o přístup k jakékoliv funkci aplikací, ukončení aplikací apod.

Autentizace a autorizace

Autentizace je proces sloužící k ověřování identity uživatele, který přistupuje k informačnímu systému. Cílem je zajistit, aby systém přesně věděl, s jakým uživatelem komunikuje, a že jím skutečně je. Ověření identity je možné provést na základě toho, že uživatel *něco zná* (heslo), *něco má* (čipová karta), nebo *někdo je* (otisk prstu).

Autorizace je proces, který slouží k ověřování přístupových práv uživatele, který přistupuje k informačnímu systému. Probíhá na základě správné autentizace uživatele. Její podstatou je ověřit, zda daný uživatel má oprávnění provést příslušnou akci.

Elektronický podpis

Elektronický podpis je technika ověření identity uživatele, která zpravidla kryptografickými metodami zaručuje integritu dokumentu a autentizaci podepsaného uživatele na Internetu. Může navíc obsahovat časové razítko, které prokazuje datum a čas podepsání dokumentu. V současné době je využíván pro komunikaci organizace s orgány veřejné správy.

3.4.2 Hardwarové mechanismy

Hardwarové bezpečnostní mechanismy jsou založeny na principu technických bezpečnostních funkcí, jako jsou identifikační karty pro řízení autentizace a přístupu, šifrovače dat, autentizační kalkulátory, firewally aj.

Router

Routery, neboli směrovače, jsou aktivní síťová zařízení, která propojují dvě a více sítí a přenáší mezi nimi data. Všechny počítače za routerem nejsou z Internetu viditelné. Obsahují firewall, který zachycuje případné pokusy o průnik do vnitřní sítě.

Firewall

Hardwarový firewall je zařízení, které vytváří ochrannou zeď mezi počítačem uživatele a potenciálně škodlivým obsahem na Internetu. Plní funkci jednoho z nástrojů komplexní bezpečnosti. Umožňuje nastavení povolených služeb poskytovaných lokálním a vzdáleným uživatelům, požadavky na filtrování provozu, případně také požadovanou autentizaci uživatelů. Navíc poskytují funkce, které nesouvisí přímo se zabezpečením vnitřní sítě, podporují například vnitropodnikový přístup do sítě pro vzdálené připojení uživatelů (VPN), nebo podporu tunelování pro propojení více sítí.

Biometrické systémy

Nejmodernější způsob ověřování identity uživatele jsou biometrické systémy. Jejich síla není v utajení informací používaných pro autentizaci, ale v jedinečnosti těchto informací. Výhodou je možnost kombinace s dalšími metodami autentizace (např. s hesly) nebo odolnost vůči krádežím. Naopak nevýhodou je náročnost na prostředky a složitost implementace. Biometrické systémy jsou založeny na fyziologických charakteristikách (otisk prstu, geometrie ruky, snímání sítnice nebo duhovky, obličejové znaky, aj.), nebo na charakteristikách chování (charakteristiky hlasu, dynamiky podpisu, dynamiky psaní na klávesnici, atd.).

Hardwarové klíče

Hardwarový klíč je zařízení, které se připojuje k počítači vložením do paralelního portu, zasunutím do PCMCIA slotu nebo připojením do USB portu. Používá se pro ověření platnosti licence používané aplikace a omezení možnosti jejího nelegálního používání. Slouží jako ochrana u drahých a specializovaných programů.

Autentizační karty

Autentizační karty slouží pro identifikaci a autentizaci uživatelů do počítačů, sítí nebo aplikací organizace, při vstupu do objektů, zabezpečení elektronické pošty formou digitálního podpisu nebo šifrování, bezpečné uložení citlivých dat, při platebních a jiných transakcích a mnoho dalších funkcí. Karty mohou obsahovat magnetický proužek nebo čip, který může být proveden jako kontaktní nebo bezkontaktní. Přístup k autentizačním údajům bývá chráněn PIN kódem a k autentizaci je navíc nutné čtecí zařízení.

3.4.3 Administrativní mechanismy

Personální a administrativní bezpečnostní mechanismy jsou založeny na principu ochrany organizace před vnitřními útočníky kontrolou přístupu k datům či zodpovědností za dodržování pravidel určených bezpečnostní politikou.

Výběr důvěryhodných osob

Vedení organizace by mělo zaměstnávat takové loajální pracovníky, kteří budou pracovat s nadšením, vnášet kreativitu a přispívat k prosperitě organizace. Do pozice bezpečnostního manažera a oddělení správy informačních technologií musejí být vybrány důvěryhodné osoby. Ti totiž zajišťují bezpečnost organizace, citlivých dat v informačním systémů a řízení přístupových práv k těmto datům.

Řízení vstupu a přístupu

Systém řízení vstupu a přístupu určuje, kdo a kam smí vstoupit. Všichni pracovníci musejí být autorizováni pro vstup do organizace a k činnostem v informačním systému. Každý pracovník má jiné potřeby a je jinak autorizován pro vstup do vymezených prostor organizace, či k určitým datům v informačním systému. Vzniká potřeba definovat

individuální přístupová oprávnění. Takové řízení vstupu a přístupu mají na starosti správci informačních technologií na základě přidělených přístupových práv konkrétnímu pracovníkovi organizace. Při změně jeho role nebo při zániku jeho určení musí správci přístupová oprávnění pozměnit.

Filtrování webu

Filtrování webu je založeno na analýze potřeb jednotlivých skupin uživatelů. Vede k efektivnímu využívání zdrojů, nižším nákladům a především vyšší bezpečnosti. Cílem je zakázat uživatelům přístup k různým obsahům webu, u kterých hrozí snížení produktivity práce, narušení bezpečnosti nebo porušení zákona. Oblasti, které může naprostá většina organizací bez rozmyslu zakázat, jsou servery a sítě nabízející nelegální software, hudbu, filmy, erotický obsah, aukční nebo inzertní servery.

Školení pracovníků

Smyslem školení pracovníků organizace je rozvíjení jejich znalostí bezpečnostních pravidel a konkrétních odpovědností, zvyšování bezpečnostního povědomí a dodržování opatření stanovených v bezpečnostní politice. Součástí každého školení je kontrola, zda problematice bezpečnosti pracovníci porozuměli, a závěrečný test sloužící k prověření nabytých znalostí.

Uvedené bezpečnostní hrozby jsou jen zlomkem všech možných hrozeb, kterým organizace a uživatelé musí v praxi čelit v závislosti na oblasti a situaci, ve které se právě nachází. Obecně nejvyšším rizikem je v současné době sociální inženýrství, kterému se lze velmi těžko bránit, neboť útočníci úspěšně obcházejí technická bezpečnostní opatření a využívají přílišné důvěry lidského faktoru. K zabezpečení organizace před různými útoky existuje opět celá řada bezpečnostních mechanismů. Jejich nasazení a kombinace závisí na požadavcích na bezpečnost každé konkrétní organizace.

4 LIDSKÝ FAKTOR – PODCEŇOVANÝ ČINITEL BEZPEČNOSTI IS

Při hodnocení úniků nebo zneužití informací se ukazuje, že nejslabším článkem a nejčastěji opomíjenou oblastí v celém systému zabezpečení je lidský faktor. Většina profesionálních útočníků ví, že je snazší přesvědčit někoho s příslušným oprávněním, aby provedl útok za něj, než se někam vloupat a útok provést sám. Navíc překonání „lidské bariéry“ je mnohem snazší, vyžaduje často méně nákladů a při dobrém skrývání útočníka je téměř nemožné jej vystopovat. Pokud lze pracovníky oklamat nebo jimi manipulovat, aby sdělili důvěrné informace, pak neexistuje žádná technologie, která by mohla organizaci jakkoliv ochránit.

V rámci systému zabezpečení organizace není tedy možné zapomenout na lidský faktor, díky kterému vzniká mnoho bezpečnostních problémů. Je důležité definovat konkrétní personální pravidla, zejména pak přesně stanovenou odpovědnost jednotlivých uživatelů systému včetně jejich oprávnění pro přístup do systému a postupy schvalování mimořádných požadavků a událostí. Součástí přijatých pravidel musí být také postupy, jak případným útokům a porušením bezpečnostních pravidel aktivně přecházet.

Porušení bezpečnosti organizace a následné úniky dat, finanční ztráty či jiné škody mohou být způsobeny úmyslným jednáním či neúmyslnými chybami pracovníků z důvodu nedbalosti, neznalosti, nevědomosti a podcenění situace. A právě lidských selhání budou s vývojem dokonalejších bezpečnostních technologií, které znesnadňují útok na zranitelná místa v informačním systému, stále častěji využívat útočníci.

4.1 ŽIVOTNÍ CYKLUS ZAMĚSTNANCE

Každý pracovník projde během své kariéry v organizaci několika fázemi, které lze souhrnně nazvat životním cyklem zaměstnance. Z hlediska bezpečnosti začíná jeho cesta přijetím do pracovního poměru, pokračuje běžnými pracovními činnostmi spojenými s užíváním informačního systému organizace a končí rozvázáním pracovního poměru. Životní cyklus pracovníka zobrazuje obrázek č. 6.

Obrázek 6 - Životní cyklus pracovníka

Zdroj: archiv autora

Přijetí zaměstnance

Při přijetí do pracovního poměru se zaměstnanci přiděluje osobní počítač, který je nakonfigurován v souladu s předpisy a přístupovými právy do informačního systému, tak aby měl umožněn přístup jen k těm informacím, které pro výkon své práce bude nezbytně potřebovat. Zaměstnanec je řádně proškolen v oblasti směrnic týkajících se bezpečnosti.

Běžný život zaměstnance

Během řádného zaměstnání nejsou potřeba žádné zvláštní zásahy bezpečnostního oddělení. K zásahům dochází pouze tehdy, pokud je zaměstnanec přeřazen na jinou pozici či povýšen. S tím souvisí potřeba úpravy v jeho přidělených oprávněních.

Školení zaměstnanců

Zaměstnanci jsou většinou školeni především při přijetí do pracovního poměru. Měli by být seznámeni nejen se všemi směrnicemi, které se týkají jejich odpovědnosti za bezpečné používání informačního systému, ale také se základy principů bezpečnostního chování obecně. Je velice vhodné vysvětlit na konkrétních případech, proč je po nich požadováno určité chování a k čemu může dojít, pokud nebudou tato pravidla dodržovat.

Všechny směrnice a nařízení týkající se bezpečnosti mají být přístupné všem zaměstnancům, kteří je při své práci mohou využít. Zaměstnanci by měli vědět, kde tyto směrnice naleznou a na koho se mají v případě nejasností obrátit.

Kontroly zaměstnanců

Neustálá kontrola bezpečnostních opatření je důležitá ze dvou důvodů. Za prvé potřebuje organizace vědět, zda se podařilo implementovat navržená bezpečnostní opatření (zda fungují, za je zaměstnanci respektují a řídí se jimi, zda jsou celkově účinná apod.). Za druhé je potřeba také průběžně ověřovat úroveň bezpečnostního povědomí uživatelů, funkčnosti stěžejních bezpečnostních procesů.

Pro tyto kontroly lze využít simulace útoků metodami sociálního inženýrství, simulace vybraných situací vzhledem k ověření funkčnosti souvisejících procesů (např. v oblasti havarijního plánování), či prověrky znalostí konkrétních uživatelů informačního systému formou dotazování co byste dělal(a), kdyby ... Provádění kontrol na sociální inženýrství je vhodné jak v rámci komplexních testů bezpečnosti organizace, tak ověření správných návyků uživatelů, například po bezpečnostním školení.

Zákoník práce opravňuje organizaci přiměřeným způsobem kontrolovat užívání výrobních a pracovních prostředků organizace zaměstnanci pro svou osobní potřebu bez souhlasu organizace. Kontroly činností zaměstnanců jsou dobré pro odhalení nepoctivých zaměstnanců, udržování určitého stupně produktivity a pracovní kázně nebo identifikaci nepracovních činností.

Monitorování může odhalit, že se zaměstnanci během své pracovní doby věnují například hraní her, chatování, brouzdání po Internetu a sociálních sítích, sledování videí, osobní poštou nebo zkrátka jsou jen neaktivní.

Odchod zaměstnance

Z bezpečnostního hlediska je odchod zaměstnance nejproblematičtější záležitostí. K rozvázání pracovního poměru může dojít jak ze strany zaměstnance, tak ze strany organizace. Důležité je uvědomit si, jakým způsobem zaměstnanec odchází. Jestliže zaměstnanec rozvázal pracovní poměr bez jakýchkoliv problémů, je možné vyloučit pokus o poškození organizace. V případě, že zaměstnanec neopustil organizaci „přátelsky“, je dobré očekávat pokus o pomstu či poškození organizace. Pokud byl zaměstnanec po svém odchodu přetáhnut ke konkurenci, lze očekávat, že může použít informace, které měl možnost při své práci (a i po odchodu) v organizaci získat.

Odchod zaměstnance z organizace s sebou nese řadu činností, které by měly být oddělením informačních technologií provedeny. Kromě fyzického odebrání počítače a jeho případné reinstalace pro nového zaměstnance, je třeba zrušit přístup do informačního systému, zrušit e-mailový účet, změnit případná sdílená hesla, ke kterým měl zaměstnanec přístup a vyřadit adresu jeho notebooku z firemní sítě. [4]

4.2 NEJČASTĚJŠÍ CHYBY ZAMĚSTNANCŮ

Lidské chyby mohou mít různé příčiny a může k nim docházet na různých místech v organizaci. Vždy však budou doprovázeny slabinami v organizaci a jejím řízení nebo v nedostatku chápání principů bezpečnosti ze strany pracovníků.

Nejčastějšími chybami, kterých se dopouštějí zaměstnanci a které vedou k porušení bezpečnostních principů organizace, jsou:

- prozrazování hesel a jiných autentizačních údajů,
- přílišná důvěra k informacím od nedůvěryhodných zdrojů,
- náchylnost k podlehnutí sociálním technikám,
- podcenění nebezpečí z Internetu a surfování po podezřelých stránkách,
- zasílání důvěrných údajů e-mailem,
- ukládání důvěrných údajů mimo bezpečná úložiště,
- vynášení nezabezpečených informací,
- zneužívání prostředků zaměstnavatele pro soukromé účely,
- nezabezpečení nebo zrušení zabezpečení prostředků informačních technologií,

4.3 ZÁKLADNÍ BEZPEČNOSTNÍ ZÁSADY

Aby pracovníci organizace dodržovali určité bezpečnostní zásady, měla by je organizace sepsat tak, aby byly naprosto srozumitelné, snadno zapamatovatelné a mohli se jimi skutečně řídit. Následující zásady by měl dodržovat každý pracovník, bez ohledu na to, v jaké organizaci a pozici pracuje.

Komunikace

Každý pracovník při své práci přijde do styku s informacemi, které mohou být předmětem obchodního tajemství, může se jednat o osobní údaje a podobně. V případě, že se takové informace dostanou k osobě, která není oprávněna se s nimi seznamovat, může pracovník organizaci způsobit značnou škodu. Vždy by proto měl vědět, s kým komunikuje, co může komu sdělit a jakou formou.

Přístup do systému

Přístup k informacím je obvykle řízen na základě přidělených oprávnění pro přihlášení do informačního systému. Přihlášení nejčastěji spočívá v zadání uživatelského jména a hesla. Pokud někdo zneužije pracovníkovo přístupu do systému, bude to právě pracovník, kdo bude hnán k odpovědnosti.

Zacházení s informacemi

Citlivé informace, se kterými pracovník může přijít do styku, mohou být nejen v elektronické, ale také v papírové podobě. Proto by pracovník neměl nechávat citlivé dokumenty na stole či na monitoru počítače, nevyhazovat je do koše, při tisku kontrolovat kompletnost dokumentu.

Internet

Při brouzdání Internetem po sobě pracovník zanechává stopy, na jejichž základě je administrátor (a někdy i ostatní návštěvníci daných stránek) schopen podle IP adresy rozpoznat, z které organizace k přístupu na stránky došlo. Svým jednáním a nevhodným chováním může snadno pracovník poškodit dobré jméno organizace.

Vzdálený přístup

Není vhodné se přihlašovat do informačního systému organizace nebo k službám, které se nacházejí na Internetu, prostřednictvím nezabezpečených Wi-Fi sítí. Je důležité zkontrolovat správnost adresy stránek, certifikát apod.

Hlášení nestandardních stavů

Jakékoliv nestandardní chování operačního systému nebo aplikačních programů by měl pracovník oznámit správcům informačních technologií. [25]

4.4 NESPOKOJENÍ ZAMĚSTNANCI

Nespokojený zaměstnanec je pro organizaci v mnoha ohledech nebezpečnější než profesionální útočník zvenku. Má dobré vědomosti o chodu organizace, které nashromáždil během své pracovní činnosti, a mnohdy znalosti klíčových informací o zabezpečení. Současný či bývalý zaměstnanec, který prošel bezpečnostním školením, zná slabá místa systému, která cizí útočník musí před zahájením útoku identifikovat. Další jeho výhodou jsou znalosti přihlašovacích jmen a hesel, a to i v případě, že již ukončil pracovní poměr, a správce bezpečnosti informačních technologií tyto údaje nezměnil.

Spokojenost zaměstnance v organizaci je ovlivněna celou řadou faktorů, ale výše částky na výplatní pásce je pro většinu zaměstnanců zásadní. Mnoho útoků proti organizaci však není jen z důvodu finančního obohacení, ale zaměstnance (často již bývalého) k útoku vedou jiné lidské pohnutky. Pro propuštěného pracovníka to může být touha po pomstě, demonstrace vlastních schopností, kdy chce zklamaný jedinec bývalému zaměstnavateli ukázat, jak dobrého zaměstnance ztratil.

Každý pracovník, každá profese a každá pozice v organizaci přináší své možnosti při získávání informací důležitých k provedení útoku.

Správce informačního systému

Pracovní náplň správce informačního systému ho staví do role nejvýše postaveného kontrolora provozu dat v organizaci. Dostává se tím do výhodné pozice k neoprávněné manipulaci s daty, aniž by byl výrazně ohrožen odhalením.

Manažer, vedoucí pracovník

Vedoucí pracovník nese největší část zodpovědnosti za provedená rozhodnutí. Ze své pozice má přístup k většině důležitých informací včetně těch s nejvyšším stupněm utajení. Pro vysoce postaveného pracovníka není problém informace získat (okopírovat pro svoji potřebu nebo pro prodej konkurenci), změnit (ve svůj prospěch nebo prospěch třetí strany), nebo dokonce zničit.

Účetní / právní oddělení

Pracovník účetního oddělení může záměrně vytvořit účetní chyby, které poslouží k vlastnímu obohacení nebo které při případné kontrole či auditu poškodí organizaci. Podobného provinění se může dopustit i pracovník právního oddělení. Ten může svého zaměstnavatele poškodit zejména vypracováním nevýhodné či zcela chybné smlouvy.

Vrátný organizace

Samotný vrátný objektu obvykle nemá k záměrnému ohrožení citlivých informací dostatečnou kvalifikaci. Významnější riziko představuje selhání fyzických bezpečnostních opatření. Vrátný může v důsledku nedbalosti při kontrole vstupujících osob poskytnout příležitost jiné osobě pro spáchání trestné činnosti. [6]

4.5 SOCIÁLNÍ INŽENÝRSTVÍ

Sociální inženýrství (nebo také sociotechnika) je soubor psychologických technik, jejichž cílem je vytvořit v člověku nějakým způsobem dojem, že situace je jiná, než jaká je ve skutečnosti. Na základě uměle navozených situací a předem zjištěných informací se oběť domnívá, že komunikuje s někým úplně jiným (důvěryhodným).

Sociotechnici využívají k realizaci svých útoků především telefon, e-mail a sociální sítě a těží ze svých znalostí v oblasti počítačových a telefonních systémů. Zkušenější útočníci provádějí své útoky i „tváří v tvář“. Dovedou být zdvořilí, okouzlující a je snadné si je oblíbit. Využívají běžných lidských vlastností, jako je důvěra k druhým, občasná lenost, přehlížení drobných odlišností, ochota pomoci druhým a strach před tím, aby se nedostali do problémů. Proto si velmi často vybírají za oběť osoby s nízkým postavením v organizaci. Těmito pracovníky je snadné manipulovat, neuvědomují si význam některých

informací a důsledky některých činností. Kromě toho jsou proti sociotechnickým metodám méně odolné, neboť volající má autoritu, zdá se milý a přátelský, dělá dojem, že zná různé lidi v organizaci, a věc, o kterou žádá, velmi spěchá.

O významu informací v organizaci a správném zacházení s nimi je proto potřeba seznámit všechny pracovníky formou teoretického i praktického školení. Prvním krokem k úspěšné ochraně informací je mít vyškolené, informované a svědomité pracovníky. Druhým krokem je pak stálé připomínání bezpečnostních opatření.

Průnik do zabezpečené firmy často začíná od získání informace či dokumentu, který je zdánlivě bezvýznamný, obecně dostupný a nepříliš důležitý. Většina pracovníků organizace tedy nepokládá jejich ochranu za nezbytnou. Po získání základních informací dochází k samotnému útoku. Úspěch je jen otázkou času, trpělivosti, osobnosti a úsilí. [7]

4.5.1 Využívání lidských vlastností

Základní princip manipulace sociotechniků je založen na šesti vlastnostech lidské povahy, které se projevují při pokusu podřídit někoho vůli sociotechnika. Těmi je autorita, sympatie, vzájemnost, důslednost, společenský souhlas a vzácná příležitost.

Autorita

Lidé obecně mají přirozenou tendenci podřídit se osobě s vyšší funkcí, vedoucí pozicí ve firmě, ve škole a podobně. Vydává-li se sociotechnik např. za asistenta ředitele, jeho slova mají vzhledem k průměrnému pracovníkovi vyšší váhu.

Sympatie

Lidé velmi rádi vyhoví požadavkům těch, ke kterým mají jisté sympatie. Ty si lze získat různými způsoby, např. díky stejným názorům na problém, zájmům apod.

Vzájemnost

Pokud se bude cítit být potenciální oběť útočníkovi za něco zavázána, je velmi pravděpodobné, že bude se sociotechnikem spolupracovat a snáze podlehne jeho žádosti.

Například nainstaluje nějaký program, který bude pro sociotechnika užitečný k útoku (program pro přístup ke vzdálené ploše uživatele nebo spyware).

Důslednost

Součástí lidského charakteru je tendence podřídit se, pokud předtím veřejně vyhlásili podporu a angažovanost v určité záležitosti. Pokud už jednou slíbili, že něco udělají, nechtějí vypadat nedůvěryhodně a postupují podle jejich dřívějších prohlášení a slibů.

Společenský souhlas

Společenský souhlas funguje tak, že sociotechnik oznámí oběti, že potřebuje něco vyplnit s tím, že všichni ostatní už to vyplnili. Když to tedy udělali ostatní, proč ne oběť? Pak již záleží na útočníkovi, jaké otázky oběti předloží.

Poukázání na zvláštní příležitost, akční nabídku apod.

Šikovný sociotechnik může například operovat s tím, že prvních sto registrovaných uživatelů dostane nějaký dárek. Registraci odkáže na uměle vytvořenou stránku, která získá od uživatelů hesla, osobní údaje atp. a spoléhá na to, že uživatel používá univerzální heslo. Podobným způsobem probíhá i phishing. [7]

4.5.2 Sociotechnické útoky

Sociotechnické útoky představují způsob, jak mohou útočníci získat přístup k počítači oběti. Cílem takových útoků obvykle bývá instalace škodlivého softwaru nebo snaha přesvědčit oběť k poskytnutí hesel a jiných finančních či osobních informací.

Přímý útok

Nejjednodušší a velmi často účinná sociotechnická metoda je přímý útok. Útočník svou oběť o informace prostě požádá. Lidé od přírody důvěřují jiným, zejména když je žádost odůvodněna.

Phreaking

Phreaking představuje pronikání do telefonních sítí díky využívání pracovníků telefonních služeb a znalostí fungování sítě za účelem volat kamkoliv zdarma, surfovat zdarma po internetu či odposlouchávat cizí telefonní hovory.

Díky této metodě se sociotechnici mohou dozvědět, jak fungují různá oddělení organizace, naučit se žargon a procedury, které jejich pracovníci používají. Takto získané informace používají dále při budování důvěry u svých obětí.

Trashing

Trashing znamená prolézání obchodních nebo osobních odpadků za účelem získání cenných informací jako jsou dokumenty spojené s výpisy z účtů, telefonních karet a jiné cennosti. Řada velkých organizací má kontejnery umístěny v nestřeženém okolí svých budov, stávají se tak snadno dostupné pro útočníka.

Phishing

Phishing (do češtiny někdy překládáno jako rhybaření) je podvodná technika, která se používá na Internetu k získávání citlivých údajů (hesel, čísel kreditních karet apod.) od obětí útoku. Jejím principem je rozesílání e-mailových zpráv, které se tváří např. jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku, která však vede někam jinam. Uživatel do nich zadá své přihlašovací údaje, čímž je prozradí útočníkovi, který je poté schopen oběti z účtu vykrást peníze.

Návnada

Cílem této metody je zanechání návnady útočníkem na vhodném místě. Jako vhodná návnada je například CD odložené tak, aby vypadalo jako zapomenuté, s patřičným popiskem (např. „Tajné – výplaty duben 2011“). To jistě nezůstane dlouho na svém místě. Ze souboru „vyplaty_duben11.xls“ se však dostane pomocí makra do počítače nežádoucí program. [7]

4.5.3 Obrana proti sociotechnickým útokům

Obrana před sociotechnickými útoky není jednoduchá, neboť směřuje na nejméně spolehlivý a přitom nejsložitější bezpečnostní prvek celého systému – lidský faktor. Útok může přijít odkudkoliv a útočník bývá velmi dobře připravený.

Základem každé úspěšné obrany je dobře zpracovaná bezpečnostní politika, která vymezuje oblasti organizace, které vyžadují vysoký stupeň ochrany dat a informací. Oblasti, které bývají nejčastějším cílem sociotechnického útoku, jsou především pracovníci sekretariátu, vrátnice, recepce a telefonních ústředen. Tyto pracovníky je nutné seznámit s tím, která data mají jaký stupeň utajení a co mohou nebo nemohou říci jiným osobám. Dále je třeba, aby zvládli alespoň základní techniky ověřování totožnosti při kontaktu s jinými lidmi po telefonu. [25]

5 MANAGEMENT A BEZPEČNOSTNÍ POLITIKA ORGANIZACE

Rozhodnutí řešit bezpečnost citlivých informací organizace musí být podpořeno nejvyšším vedením organizace, které určí pracovníka a tým, jenž bude zodpovědný za budování systému řízení bezpečnosti organizace. Problematika řešení bezpečnosti představuje poměrně rozsáhlou oblast, která ve větších organizacích často zaměstnává celá specializovaná oddělení.

Tímto pracovníkem zpravidla bývá manažer informační bezpečnosti, který by měl být přímo podřízený řediteli organizace. Ve střední nebo menší organizaci dbá manažer informační bezpečnosti na to, aby byla její rizika řízena do té míry, že se dokáží v rámci organizace identifikovat, dokumentovat a organizace o nich měla přiměřeně aktuální vědomí. Ve větší organizaci manažer informační bezpečnosti zajišťuje ve vlastní odpovědnosti vybudování, implementaci a neustálé zlepšování systému řízení informační bezpečnosti (ISMS – Information Security Management System) a funguje jako rozhraní mezi nejvyšším vedením a operativními úseky organizace.

Systém řízení informační bezpečnosti je nezbytný pro řízení bezchybného provozu a rozvoje každé organizace. Musí být prováděn výhradně pracovníky organizace, nicméně je vhodné provádět ho za odborné konzultační a poradenské pomoci specializované firmy.

5.1 MANAGEMENT BEZPEČNOSTI

Bezpečnostní management se zabývá tvorbou, udržením a obnovením optimální bezpečnostní situace organizace. Představuje činnosti, procesy a funkce, kterými manažeři bezpečnosti čelí hrozbám, jejich odvracení, zmírnění a eliminaci.

Práce každého manažera bezpečnosti představuje komplexní činnosti, které mají technické, technologické, ekonomické, organizační, sociální a psychologické aspekty. Měl by být vybaven dostatečnými manažerskými schopnostmi (řídí tým pracovníků v běžných

i krizových situacích), znalostmi v oblasti informačních technologií i jejich bezpečnosti. Neměla by mu chybět znalost vnitropodnikových procesů a struktury organizace obecně. Je hodnocen nejen na základě vlastní práce, ale i na základě výsledků svého týmu. Úspěšně vést a řídit může jen ten manažer, který zná potřeby a názor svých spolupracovníků, který je dokáže vhodně ovlivňovat a který dokáže propojovat jejich zájmy a cíle se zájmy a cíli organizace.

Funkce manažera informační bezpečnosti je často v praxi nazývána jako CISO – Chief Information Security Officer. Jeho hlavním posláním je analyzovat současný stav bezpečnosti informací v organizaci a navrhnout jeho zlepšení. Za tímto účelem vytváří strategie informační bezpečnosti organizace, řídí práce podřízených pracovníků, zajišťuje celkovou bezpečnosti organizace (jak fyzickou, tak digitální) a zpracovává bezpečnostní politiku. Podle měnících se požadavků zaměstnanců a vedení organizace zajišťuje průběžnou aktualizaci bezpečnostní politiky. [26]

Každý bezpečnostní tým by měl mít svou kontrolní a výkonnou složku. *Kontrolní složka* sleduje dodržování bezpečnostních požadavků definovaných v bezpečnostních dokumentech, řeší a vyhodnocuje krizové stavy. Úkolem *výkonné složky* je aplikace bezpečnosti v denním provozu systému. [8]

5.1.1 Motivy managementu bezpečnosti

Motivy k řešení problematiky managementu bezpečnosti informací lze shrnout do tří základních bodů:

- *organizace si je vědoma* závislosti na svých informacích a snaží se jim poskytnout náležitou ochranu,
- *vedení organizace si je vědomé* své odpovědnosti, většinou vyplývající ze zákona, vůči zajištění dostatečné ochrany informací své organizace a chce zavést takový systém bezpečnostních opatření, který by nejenom minimalizoval pravděpodobnost vzniku bezpečnostního incidentu, ale v případě jeho výskytu by také nezvratně prokázal, že došlo k selhání jednotlivce a nikoli k systémové chybě,
- *organizace chce deklarovat* svou spolehlivost v oblasti bezpečnosti informací vůči svým pracovníkům, zákazníkům a obchodním partnerům.

5.1.2 Přínosy managementu bezpečnosti

Přínosem zavedení systému řízení bezpečnosti informací jsou *přiměřené náklady* na bezpečnost v poměru k hodnotě chráněných aktiv organizace, *zavedení systému pravidelné aktualizace* všech bezpečnostních dokumentací a s tím souvisejících bezpečnostních procesů, *zvýšení bezpečnostního povědomí* zaměstnanců jasným definováním působností a povinností jednotlivých rolí v organizaci, *soulad s legislativou* (zejména se zákonem č. 101/2000 Sb., o ochraně osobních údajů), *snížení rizik* souvisejících s únikem či ztrátou citlivých informací a dat nebo *konkurenční výhoda* aj.

5.1.3 Oblasti působnosti bezpečnostního manažera

Manažer informační bezpečnosti působí primárně v řízení operativních problémů a úkolů, nicméně se ukazuje potřeba řídit informační technologii na vyšší úrovni, včetně řízení bezpečnosti a strategie, která by orientovala organizaci do budoucnosti.

Reprezentace organizace z hlediska bezpečnosti

Argumentuje nejvyššímu vedení organizace ve smyslu prosazení důležitosti řešení bezpečnosti, účastní se tvorby strategie organizace, má možnost prosadit takové investice, které budou pokrývat nejen udržitelný stav informačních technologií, ale mohou směrovat i pro jejich budoucí rozvoj a potřeby. Poskytuje rady a doporučení nejvyššímu vedení.

Bezpečnostní hodnocení software

Hodnotí všechny hardwarové a softwarové komponenty z hlediska možných dopadů na informační bezpečnost, sleduje a zajišťuje jejich modifikaci, autorizuje jejich nákup a použití v organizaci.

Posuzování rizik, vyšetřování bezpečnostních incidentů

Vede odhady rizik a připravuje zprávy, které sdělují výsledky odhadů nejvyššímu vedení organizace. Navrhuje a realizuje protiopatření ke zvládání bezpečnostních rizik, přijímá preventivní opatření k zamezení nebo minimalizaci rizik.

Řízení přístupu a technický software řízení přístupu

Řídí a úkoluje správce bezpečnostního systému organizace, poskytuje jim manažerské zázemí, potřebné pravomoci k ochraně dat a informací.

Obnova po havárii

Koordinuje zpracování plánů kritických situací a zajišťuje rychlou obnovu systému organizace podle vypracovaného havarijního plánu a plánu obnovy.

Tvorba a správa bezpečnostní politiky

Vypracovává bezpečnostní politiku a rozpracovává jí do dalších bezpečnostních dokumentů. Prosazuje dodržování bezpečnostních zásad stanovených v politice.

Zvyšování bezpečnostního uvědomění

Připravuje a realizuje školení pro manažery, správce a uživatele informačního systému organizace, je zdrojem informací poskytovaných různými médii o bezpečnosti.

Testování a hodnocení informační bezpečnosti

Plánuje a vede provádění bezpečnostních testů a hodnocení bezpečnosti všech systémů s cílem zajistit, aby se tyto systémy provozovaly podle vydaných bezpečnostních předpisů.

Vykonávání dozoru

Vykonává dozor nad vypracováním přehledu bezpečnostních funkcí a je nejvyšším manažerem při vyšetřování bezpečnostních incidentů a odpovídá za rychlou obnovu systému v organizaci. Monitoruje plnění přijatých preventivních opatření pro minimalizaci či zamezení rizik organizace. [3]

5.2 TVORBA BEZPEČNOSTNÍ POLITIKY

Každá organizace musí bez ohledu na svou velikost a předmět podnikání dodržovat určité bezpečnostní zásady, které bývají nejčastěji formulovány v bezpečnostní politice organizace. Současná legislativa České republiky ukládá povinnost zpracovat bezpečnostní politiku pouze v případech, které jsou řešeny zákonem č. 412/2005 Sb., o ochraně utajovaných informací a zákonem č. 56/2006 Sb., o prevenci závažných havárií. Uvedené zákony však neřeší komplexní bezpečnost, ale pouze část chráněných zájmů.

Proces k dosažení požadované úrovně zabezpečení se skládá ze šesti základních kroků (podle normy ISO/IEC 17799 - Soubor postupů pro management bezpečnosti informací). Jednotlivé fáze na sebe navazují a postupuje se shora dolů. Na počátku stojí rozhodnutí zabývat se bezpečností a vytvořit předpoklady pro její řešení. Pokračuje se analýzou rizik a oceňováním aktiv, na jejímž základě se určí, jaká aktiva se budou chránit a jak. Nalezené řešení se formalizuje do vnitropodnikových dokumentů (zejména do bezpečnostní politiky, postupů a směrnic), určí se jejich závaznost a sankce za jejich porušení. Po implementaci zvolených opatření se jejich stav průběžné monitoruje a periodicky ověřuje. [3] Celý proces řízení systému bezpečnosti popisuje obrázek č. 8.

Další normy řešící řízení bezpečnosti informačních technologií jsou vyjmenovány v příloze č. 3.

5.2.1 Cíle a strategie řešení bezpečnosti

Bezpečností studie je základní dokument, ze kterého bude vycházet management při řešení bezpečnosti organizace. Zpracování bezpečnostní studie má význam pro všechny typy organizací. Vychází zejména z posouzení současného stavu bezpečnosti v organizaci, který vytyčuje hlavní směry dalšího postupu.

Jde o fázi, která zahrnuje definici základních cílů organizace v oblasti požadavků na analyzovaný systém a strategií řešení jeho bezpečnosti.

5.2.2 Analýza rizik

Podnikatelské riziko je definováno jako nebezpečí, že určitá událost nebo akce negativně ovlivní schopnost organizace dosahovat svých cílů a naplnit svoji strategii. Aby organizace přežila, musí určitá rizika přijmout a do jisté míry je řídit. Ke zjištění, jakým rizikům a hrozbám organizace čelí, je třeba provést analýzu rizik.

Existují různé přístupy k provádění analýzy rizik. Dle normy ISO/IEC TR 13335 - Řízení zabezpečení informačních a komunikačních technologií jsou rozlišovány přístupy základní, neformální, kombinovaný a podrobná analýza rizik. Ty se liší rozsahem analýzy, jejich rychlostí a finanční náročností.

Cílem každé analýzy je přinést odpověď na otázky: jakému působení hrozeb je organizace vystavena, jak moc jsou její aktiva vůči těmto hrozbám zranitelná, jak vysoká je pravděpodobnost, že hrozba zneužije určitou zranitelnost a jaký dopad by to mohlo mít na organizaci. Skládá se ze tří fází: identifikace a ohodnocení aktiv, identifikace hrozeb a zranitelností a stanovení výsledného rizika (viz. obrázek č. 7). Na základě analýzy rizik a pravděpodobnosti zneužití rizika je vedoucími pracovníky provedeno rozhodnutí, která rizika budou řízena bezpečnostními opatřeními v bezpečnostní politice a která budou pro organizaci přijatelná a akceptovaná. Na základě dobře provedené analýzy rizik lze sestavit kvalitní bezpečnostní politiku organizace.

Typickým výstupem je dokument obsahující popis systému a výsledky analýzy. Výsledky analýzy jsou velice citlivým dokumentem, protože obsahuje podrobné informace o „kritických místech“ v organizaci. Proto je tento dokument určen úzkému okruhu lidí v managementu, a v rámci organizace je klasifikován nejvyšším stupněm utajení.

Vzhledem k neustálému vývoji jak informačního systému, tak prostředí, v kterém pracuje, je nutné analýzy rizik aktualizovat. Obvykle se aktualizují její jednotlivé části při každé významné změně informačního systému nebo při zjištění nové hrozby. [3]

Identifikace a ohodnocení aktiv

Identifikace aktiv má za úkol zjistit, jaká aktiva se v organizaci vyskytují a jakou pro ni mají hodnotu. Zahrnuje aktiva ve formě budov a místností organizace, hardware (servery, pracovní stanice, tiskárny, směrovače, kabely, atd.), software (operační systém, aplikační programy) a informací (databáze, sestavy dat, dokumenty, aj.).

Po vytvoření seznamu všech aktiv organizace se musí vyčíslit jejich hodnota pro organizaci, přičemž je potřeba brát vždy tu nejvyšší cenu. Ohodnocení fyzických aktiv se určuje na základě pořizovací ceny nového aktiva s přibližně stejnými parametry, jaké má oceňované aktivum. Obtížněji se stanovuje cena informací. Každá informace je hodnocena z hlediska důvěrnosti, integrity a dostupnosti. Jeden z možných přístupů je, že je informační jednotka ohodnocena na principu nejhoršího možného dopadu pro organizaci v případě, že nastane vyzrazení, zneužití, modifikace, nedostupnost či zničení informace.

Identifikace hrozeb a zranitelností

Identifikace hrozeb a zranitelností je mnohem složitější, neboť možné hrozby se poměrně rychle vyvíjí. Existuje několik způsobů identifikace hrozeb, které mohou využít zranitelnosti jednotlivých aktiv. Jedním z nich je identifikace pečlivým přemýšlením nad všemi situacemi, které mohou v organizaci nastat. Je velmi pravděpodobné, že se při takovém přístupu na něco zapomene. Druhým způsobem je inspirace jinými seznamy rizik, které byly vytvořeny pro obdobné prostředí, ve kterém se nachází analyzovaná organizace, a optimalizace dle vlastních požadavků. Posledním způsobem je najmutí bezpečnostního experta, který na základě podrobných dotazníků zjišťuje, v jakém stavu se analyzovaná organizace a její systém nachází. [9]

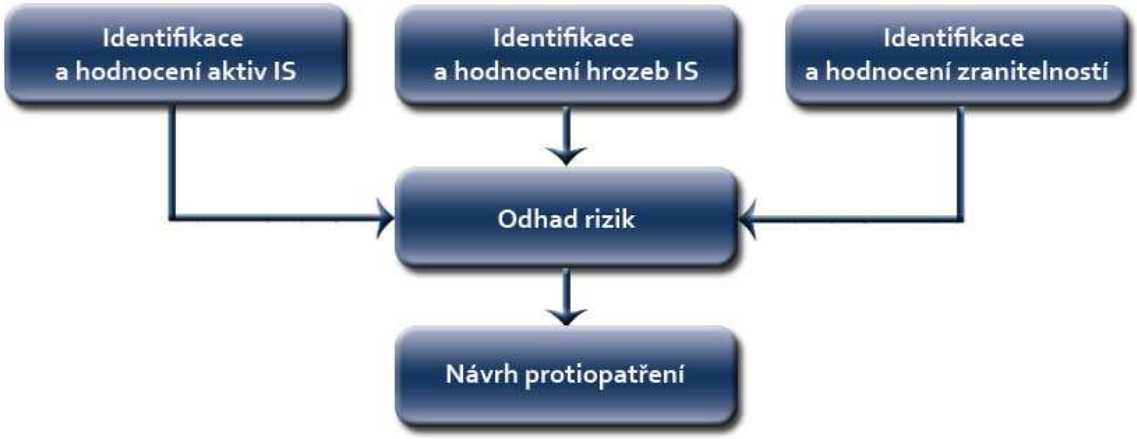
Vlastní analýza rizik

Úkolem vlastní analýzy rizik je stanovit, jaká rizika konkrétním aktivům hrozí. Postupně se prochází jednotlivá aktiva a rozhoduje se, která rizika se na dané aktivum vztahují. Za účelem zjednodušení se obvykle provádí slučování aktiv do skupin, kdy se do jedné skupiny zahrnou aktiva stejných vlastností a sloužící v informačním systému ke stejným účelům. Aktivům, začleněným do společné skupiny, se přiřadí konkrétní rizika. Každé konkrétní skupině aktiv lze navíc přiřadit pravděpodobnost, s jakou ke konkrétnímu riziku dané skupiny aktiv může dojít. Na základě pravděpodobností je pak možné určit priority z pohledu dopadu a pravděpodobnosti výskytu a zaměřit se na klíčové rizikové oblasti. [4]

Závěrečná zpráva o provedení analýzy rizik

Závěrečná zpráva by měla být rozdělena do dvou částí. První část je určena pro vedení organizace. Ta by měla být stručná a měla by obsahovat hlavní záměry vyplývající z provedené analýzy rizik a navržená opatření k eliminaci bezpečnostních rizik. Jejím hlavním cílem je základní seznámení vedení s aktuálním stavem bezpečnosti. Druhá část, určená pro odborné pracovníky, by měla obsahovat podrobný popis existujících rizik v organizaci a navržené postupy pro jejich odstranění. Tento dokument může být rozsáhlý a měl by řešit problematiku včetně všech detailů. [2]

Obrázek 7 - Analýza rizik organizace



Zdroj: http://www.cleverlance.cz/cz/Produkty-a-reseni/Bezpecnost/Stranky/Rizeni-informacnich-rizik.aspx (dne: 2011-11-20)

5.2.3 Bezpečnostní politika organizace

Bezpečnostní politika organizace je klíčový *písemný* bezpečnostní dokument, který je *schválený* nejvyšším vedením a který je *známý a závazný* pro všechny pracovníky organizace i pracovníky externích společností využívající informační systém organizace. Pokud není v písemné podobě, každý pracovník si může politiku vysvětlovat po svém, vznikají nebezpečné mezery, nejasnosti, chybí jasné postupy a důkazní materiál pro postih pracovníka.

Organizace v ní deklaruje účel, své základní cíle a záměr vedení organizace v oblasti informační bezpečnosti. Řeší otázky typu co, kde, jak a proč se bude chránit, jak bude ověřeno, že je to opravdu chráněno, kdo za to nese odpovědnost, jak bude dodržování bezpečnostní politiky vynuceno a kontrolováno a jak se bude postupovat v případě, že někdo bude jednat v rozporu s politikou a bude porušovat zásady v ní uvedené.

Bezpečnostní politika, která je rozpracována do *obecných principů* je trvalejšího charakteru s delší dobou platnosti bez potřeby časté aktualizace. Detailní rozpracování konkrétních částí informačního systému je provedeno v návazných *bezpečnostních předpisech*. Při formulaci obecného obsahu bezpečnostní politiky může docházet ke špatné interpretaci bezpečnostních principů, kdy si pracovníci nedokáží představit jejich konkrétní obsah. Pokud je bezpečnostní politika *rozsáhlejší a detailněji řeší bezpečnost informačních systémů*, může být často pro management nepřehledná a pro jednotlivé pracovníky jsou určeny pouze některé části. Rozsáhlejší politika je obvykle dělena na více částí, podle jednotlivých oblastí bezpečnosti. Takový dokument je navíc nutné často aktualizovat a jeho opakované schvalování nejvyšším vedením může být problematické.

Podle toho, co bezpečnostní politika povoluje, či zakazuje, je možno ji rozdělit do čtyř typů. *Promiskuitní bezpečnostní politika* vše dovoluje a bezpečnost se řeší mimo oblast informačních technologií. *Liberální bezpečnostní politika* dovoluje pracovníkům dělat vše, až na věci explicitně zakázané. *Opatrná (racionální) bezpečnostní politika* naopak zakazuje dělat vše, co není explicitně povoleno. *Paranoidní bezpečnostní politika* zakazuje dělat vše i potenciálně nebezpečné.

Jednotlivé oblasti řešené v bezpečnostní politice (obvykle vztahy s třetími stranami, zajištění bezpečnosti informací v rámci organizace, dodržování dokumentovaných postupů, zabezpečení práv, řízení přístupu a komunikací, vzdálený přístup, soulad s požadavky, personální procesy, fyzická bezpečnost, plány obnovy, aj.) by měly být pro přehlednost rozpracovány do více dokumentů, aby se každý pracovník mohl seznámit především s tím, co se ho přímo týká. Samotné dělení závisí na struktuře a velikosti dané organizace.

Vyhotovení bezpečnostní politiky vede k jejímu schválení, přijetí a seznámení s ní pracovníky prostřednictvím bezpečnostního vzdělávání nebo školení. [3]

Havarijní plán

Havárie nebo krizový stav nastává tehdy, kdy se stane cokoliv nepředvídatelného, dojde k selhání bezpečnostních opatření a podobně. Celý proces obnovy systému začíná odstraněním akutního nebezpečí, pokračuje obnovením důležitých částí systému, obnovením poškozených dat, zprovozněním systému v celém rozsahu a končí zavedením příslušných protiopatření (viz. obrázek č. 8).

Havarijní plán popisuje činnosti, které je potřeba začít provádět bezprostředně po zjištění krizové události, na kterou je havarijní plán sestaven. Stanovuje, kdo je za krizové řízení zodpovědný a jaké má pravomoci. Měl by obsahovat i hierarchii pracovníků, kteří mají právo vydávat dočasně platná nařízení, a musí být schválen vedením organizace jako závazná vnitropodniková směrnice.

Havarijní plán bývá součástí bezpečnostní politiky a alespoň jedna kopie musí být od bezpečnostní politiky uložena odděleně, na dostatečně bezpečném a dostupném místě.

Obrázek 8 – Havarijní řízení

Zdroj: archiv autora

5.2.4 Bezpečnostní projekt

Bezpečnostní projekty, někdy též strategie, standardy nebo postupy, jsou taktické dokumenty, které rozpracovávají hlavní oblasti a obecné principy informační bezpečnosti definované v obecné bezpečnostní politice do detailní podoby. Zatímco bezpečnostní politika je relativně neměnným dokumentem, u bezpečnostních projektů se předpokládá častější frekvence úprav. Musejí s ní být seznámeni všichni pracovníci organizace, a proto musí být volně dostupná, nejlépe v sekci interních dokumentů v intranetu organizace.

Nejdůležitějším prvkem bezpečnostní strategie je stanovení rozsahu chráněných informací a majetku, důvod jejich ochrany a jasné určení zodpovědnosti. Výstup z projektu popisuje, jak jsou realizovány a implementovány bezpečnostní požadavky z příslušných bezpečnostních politik a jaké podpůrné procedury jsou vytvořeny k jejich prosazení. [3]

Plán obnovy funkčnosti informačního systému organizace

Plán obnovy slouží pracovníkům informačních a komunikačních technologií k zajištění obnovy provozu informačního systému v co nejkratších lhůtách, aniž by to mělo negativní dopad na plnění legislativních a interních požadavků, smluvních povinností vůči zákazníkům, obchodním partnerům či akcionářům.

Definuje pracovní postupy a činnosti, kterými lze zajistit provoz informačního systému organizace v omezené míře do té doby, než bude obnoven tak, aby dopad na chod organizace byl minimální. Dále stanovuje alternativní postupy, kterými lze po stanovenou dobu provádět kritické činnosti bez informačních a komunikačních technologií. [10]

5.2.5 Implementace bezpečnostní politiky

Zpracovaný bezpečnostní projekt, který realizuje bezpečnostní politiku, je třeba zavést do každodenního fungování organizace. Implementace je snad nejdůležitější krok, který uvádí bezpečnostní politiku do praxe.

Celý proces představuje rozsáhlou komplexní činnost, která znatelně zasahuje do běžného každodenního fungování organizace a která musí být dobře manažersky vedená a koordinovaná. Správně implementovaná bezpečnostní politika znamená pro organizaci účelné využití stávajících prostředků a nástrojů bezpečnosti a jejich rozvoj na základě nově definovaných požadavků. Proces implementace zahrnuje i školení správců a ostatních pracovníků tak, aby celkové bezpečnostní povědomí přispělo k pochopení, osvojení a vědomé podpoře implementovaných opatření co nejširšího okruhu pracovníků.

Vlastní implementace končí provedením uznávacích bezpečnostních testů, které mají za úkol přesvědčit a dokumentovat, že požadovaná opatření byla implementována správně, v požadovaném rozsahu a plně v souladu s bezpečnostní dokumentací.

Penetrační testy

Penetrační testy umožňují získat přehled slabých míst v zabezpečení organizace, které pomáhají lépe se připravit na reálné. V průběhu testů jsou používány techniky a nástroje běžně používané v praxi za účelem co nejvěrnější simulace pravděpodobného postupu útočníka při pokusu o průnik do různých částí informačního systému zvenčí či zevnitř. Testy je vhodné provádět kvalifikovanými odborníky a pravidelně opakovat.

V případě vnějšího testu je simulován útok z Internetu, který vychází především z běžně dostupných informací veřejnosti a jejich následným využitím při sociotechnickém útoku. Při interním testu jsou simulovány činnosti běžného uživatele systému organizace, připojeného do vnitřní sítě organizace, který se snaží o neoprávněný přístup k důvěrným informacím organizace. [11]

5.2.6 Provoz, kontrola a vyhodnocení

Do provozu předaný bezpečnostní systém je podřízen periodické kontrole, zda implementovaná a realizovaná opatření bezpečnostní politiky pracují efektivně a v souladu s tím, jak bylo zamýšleno. Sledování a hodnocení systému je nedílnou součástí procesu řízení informační bezpečnosti. Je třeba určit kritéria, podle kterých bude hodnocení probíhat. Postupně jsou procházeny jednotlivé oblasti řešené v bezpečnostní politice. Případné odchylky jsou dokumentovány a odstraňovány nápravnými akcemi.

Průběžné hodnocení stavu bezpečnosti ve větší organizaci vykonává bezpečnostní management nebo interní útvar auditu.

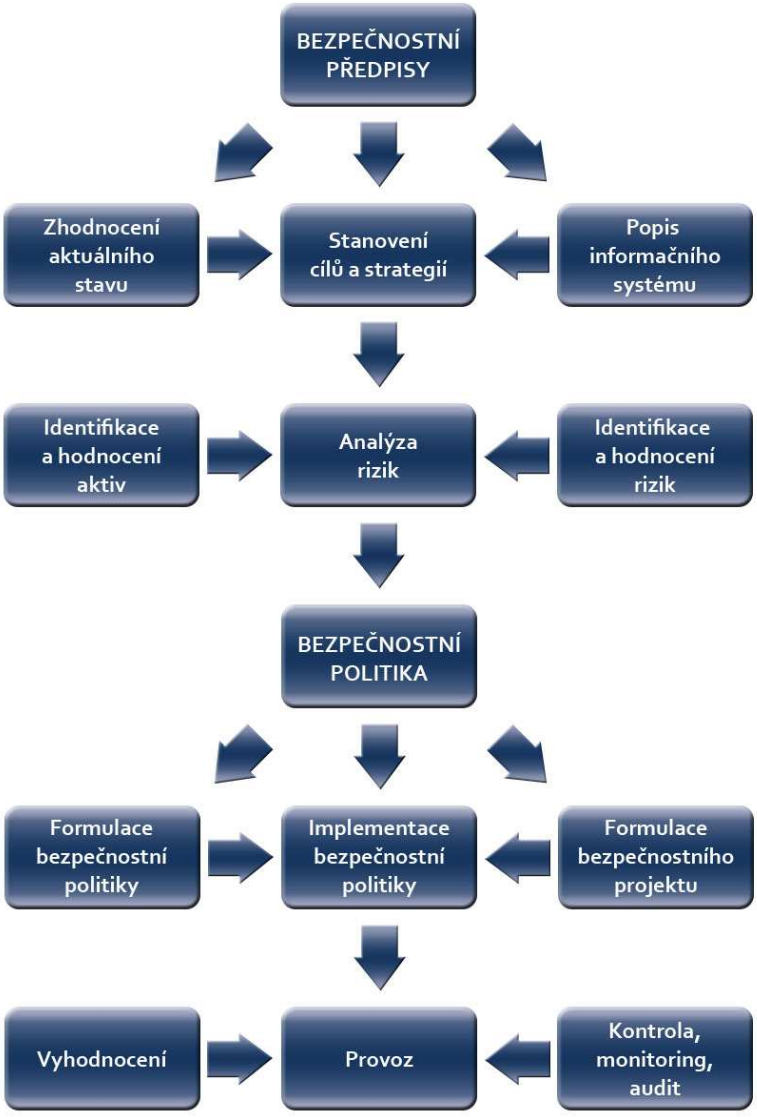
5.2.7 Monitoring a audit

Monitoring, tj. nepřetržitý dohled nad provozem informačního systému organizace, se provádí pro ověření toho, zda pracovníci organizace bezpečnostní politice rozumí a dodržují zásady v ní uvedené, zda bezpečnostní mechanismy odpovídají dané situaci a jsou dobře nastaveny a zda se nezměnily podmínky tak, že již nevyhovují. Monitoring by měl být primárně zaměřen na oblasti s nejvyšším rizikem a další klíčové oblasti činnosti organizace. Zpravidla bývá zaměřen na server a jednotlivé stanice pracovníků, provoz na síti, elektronickou poštu, detekci virů, výpadek jakýchkoliv zařízení, připojených do sítě, nebo průnik do vnitřní sítě. V případě chyby nebo potenciálního problému bude správce informačního systému organizace automaticky informován.

Audit je jednorázové hodnocení, které provádí analýzu požadavků, analýzu rizik, potvrzení správného nastavení bezpečnostních mechanismů a hodnocení současného stavu zabezpečení informačního systému organizace. Závěrečný dokument (auditní záznam

či log) uchovává informace o všech z bezpečnostního hlediska zajímavých událostech, ke kterým v informačním systému docházelo. Součástí každého záznamu v logu je přesný čas akce, jméno programu, který akci provedl, a co nejpodrobnější popis důvodu, který k záznamu vedl. Výsledkem auditu může být rozhodnutí: vyhovuje, vyhovuje s výhradami nebo nevyhovuje a dále pak popis problémových oblastí včetně opatření pro odstranění bezpečnostních rizik. Obvykle jej provádí nezávislá specializovaná firma. [3]

Obrázek 9 - Systém řízení bezpečnosti



Zdroj: archiv autora

5.3 PROBLÉMY A CHYBY PŘI FORMULACI A IMPLEMENTACI BEZPEČNOSTNÍ POLITIKY

Prvním problémem může být *nízká úroveň přípravy a kvality analýzy rizik*, která předchází formulaci bezpečnostní politiky organizace.

Při stanovení a zavádění bezpečnostní politiky může dojít k *velkému množství kompromisů*, kdy po procesu schvalování z původní verze bezpečnostní politiky zůstane jen část a problematické pasáže jsou vypuštěny nebo přepsány, pravomoci a zodpovědnosti jsou zredukovány na nezbytné minimum.

Nereálná bezpečnostní politika může být přísná a organizaci téměř v žádném bodě nebude vyhovovat. Bude potřeba definovat přechodné období s postupným procesem implementace.

Příliš rozsáhlá politika znemožňuje managementu seznámit se dostatečně podrobně s celým dokumentem a pochopit význam jednotlivých opatření.

Bude-li implementovaná bezpečnostní politika *nedostatečně propagována*, dojde u zaměstnanců k její ignoraci, neakceptování a zapomnění.

Pokud se organizace při tvorbě bezpečnostní politiky inspiruje jinými politikami, které nepřepracuje do obrazu svého, hrozí zde riziko, že může *přebrat nevhodný vzor* a implementovat tak neadekvátní bezpečnostní opatření.

6 MOTIVACE UŽIVATELŮ A SPRÁVCŮ IS

Jedním z mnoha způsobů, jak přispět k prosperitě jak organizace, tak pracovníka, je *psychologie* a přiměřená aplikace jejích poznatků v manažerské praxi. *Psychologie organizace* staví do centra svého zájmu pracovníka, jakožto člena organizačních systémů a vztahy mezi jednotlivcem a tímto organizačním systémem. *Sociální psychologie práce* je aplikovaným oborem, který se zabývá člověkem v pracovním procesu z hlediska jeho kontaktů a vztahů s druhými lidmi.

Psychika reguluje a řídí veškerou činnost člověka (prožívání, chování) na základě přijímání, zpracování a vyhodnocování informací z jeho vnějšího i vnitřního prostředí. Schopnosti člověka (včetně jeho vědomostí, dovedností a zkušeností) nejsou samy o sobě postačující zárukou uplatnění člověka a jeho úspěšnosti v práci. Ani vynikající schopnosti nemusí člověk umět či chtít využít v plné míře, zejména pokud mu budou chybět další potřebné vlastnosti. Patří mezi ně především vlastnosti stimulační a motivační.

6.1 STIMULACE

Stimulace je vnější působení na psychiku pracovníka, na jeho prožívání a jednání, v jehož důsledku dochází k ovlivňování a usměrňování jeho motivace. Stimulem může být jakýkoliv podnět, který vyvolá změny v motivaci člověka.

Může být využita k posílení perspektivy úspěchu (stimulace kladným hodnocením či odměnou), nebo ke zvýraznění hrozby neúspěchu a z něj vyplývajících nepříznivých důsledků (stimulace záporným hodnocením, sankcí, trestem). Žádoucí účinek má však jen taková stimulace, kdy užívané stimuly budou v souladu s motivací pracovníka.

Základním předpokladem účinného stimulování je uplatňování stimulačních podnětů manažerem ve shodě s potřebami a celkovým motivačním profilem daného pracovníka. [8]

6.2 MOTIVACE

Motivace je souborem činitelů představující vnitřní hnací síly činnosti pracovníka. Jejím smyslem je nenásilné vytvoření pozitivního přístupu k nějakému výkonu, k určitému chování nebo jednání.

Vnitřním podnětem může být příležitost využívat své znalosti a dovednosti při práci nebo pocit uspokojení z dobře vykonané práce, vnějším podnětem pak peněžitá odměna, sociální výhody nebo možnost kariérního růstu. Pokud je člověk navíc k nějaké činnosti nebo ke konkrétnímu výkonu *nedostatečně* motivován, bývá výsledek málo uspokojivý. Podobně tomu bývá i v případě, kdy je naopak motivován příliš *nadměrně*. K optimální úrovni výkonu vede motivace *přiměřená*. [8]

6.2.1 Motivační činitelé

Pokud chce manažer docílit určitého výkonu, chování či jednání pracovníků (konkrétně pak dodržování bezpečnostní politiky a bezpečnostních předpisů), musí umět uplatňovat široký soubor motivačních a stimulačních činitelů, vhodně je kombinovat a na každého svého pracovníka použít právě takové činitele, které na něj platí nejvíce. Aby pracovník podal požadovaný výkon, je nutné, aby k tomu měl osobní předpoklady a aby mu organizace zajistila potřebné podmínky. Manažer může přecenit schopnosti či znalosti pracovníka, nebo může dojít k tomu, že nebyly dostatečně zajištěny podmínky pro plnění (pracovník nemá potřebné vybavení, informace, aj.).

Činiteli, které se v praxi nejvíce osvědčili, jsou cíle, náplň práce, zpětná vazba, pravomoc a odpovědnost, styl vedení, osobnost manažera, osobní rozvoj, sociální program a vedlejší výhody, vztahy na pracovišti, systém odměňování a jistota pracovního místa.

6.2.2 Role manažera v motivaci

Cílem bezpečnostního manažera je motivovat uživatele informačního systému tak, aby se sami chtěli účastnit procesu ochrany aktiv organizace. Dobrou motivací je v tomto případě popis prospěchu pro organizaci i samotné pracovníky, které vyplývají z takového

postoje. Protože organizace má kromě pracovních informací také část osobních informací každého pracovníka, přispívání pracovníkem k ochraně dat organizace znamená rovněž příspěvek k ochraně jeho vlastních osobních údajů.

Je třeba vyjadřovat uznání pracovníkům, kteří se zasloužili o úspěch informačního bezpečnostního programu nebo odhalili sociotechnický útok a zabránili mu.

Existence systému odměn by měla být oznamována pracovníkům na všech akcích, které se týkají bezpečnosti, a všechny případy porušení bezpečnostních zásad by měly být v organizaci široce publikovány. Pracovníci si musejí být vědomi důsledků plynoucích z nepřizpůsobení se bezpečnostním postupům. Každý se někdy může dopustit chyby, ale opakující se případy porušování bezpečnostních pravidel nemohou být tolerovány. [8]

6.2.3 Chyby v motivaci

Podcenění významu a potřeby motivace pracovníků organizace nebo nepochopení motivačních nástrojů vede k přímé ztrátě produktivity. Stejný dopad má i manažerské jednání, které pracovníky demotivuje. Ještě větší ztráty může vyvolat nesprávné zaměření motivace vedoucí pracovníka k jednání, které není v zájmu organizace.

Nedostatečné povzbuzování motivace

Z praxe je dobře známo, že ani relativně vysoký základní plat není zárukou trvale vysokého pracovního nasazení. Motivaci pracovníků je třeba *trvale povzbuzovat*, nejlépe předem jasně stanovené osobní odměny ve vazbě na dosažené výsledky, případně způsob či kvalitu provedené práce v oblasti ochrany aktiv organizace.

Podceňování nefinanční motivace

Finanční odměna je pro pracovníky sice důležitá, ale většina pracovníků spíše ocení, mají-li možnost v práci získat uznání a být respektováni, vykonávat smysluplnou práci a být na ni, na své pracovní výsledky i svou organizaci hrdý, a udržovat přátelské vztahy s dalšími pracovníky v organizaci.

Nedostatek pochvaly a ocenění

Nejdůležitějším nástrojem okamžité motivace pracovníků je pochvala za práci, kterou odvedli. Její význam spočívá v tom, že podporuje výkon či chování, kterého se týká nebo na které upozorňuje. Pochvalu by měl pracovník dostat především tehdy, pokud se zachoval způsobem, který chce manažer podpořit. Pochvala zvyšuje pravděpodobnost, že se daný pracovník v budoucnu zachová podobně.

Jednání, které demotivuje

Největší vliv na motivaci, ale i nespokojenost či demotivaci pracovníka, má jednání přímých nadřízených. K nejčastějším faktorům zbytečné demotivace patří nedostatek pochvaly a ocenění, nespravedlivé hodnocení a projevy nedůvěry. Dalšími příčinami může být poskytování nezasloužených odměn, opomíjení zpětné vazby, podceňování osobních schopností, nedostatečná pozornost věnovaná názorům či podnětům pracovníka aj.

Nespravedlivé hodnocení

Druhým nejdůležitějším faktorem vyvolávajícím zbytečnou ztrátu motivace je nespravedlivé hodnocení. Nejčastější příčinou je stejné hodnocení pracovníků podávajících nestejný výkon. Na pocit nespravedlivého hodnocení, finančního i slovního, pracovníci reagují většinou velmi citlivě. [12]

6.3 VÝKONNOST

Důležitým předpokladem bezpečnosti informací organizace je optimální výkonnost pracovníků. Výkonnost pracovníka je determinována nejen jeho pracovní způsobilostí (schopnostmi, dovednostmi), ale také jeho ochotou, tj. pracovní motivací. V pracovní výkonnosti se příznivě či nepříznivě odráží míra pracovní spokojenosti pracovníků.

Při zkoumání úrovně pracovní spokojenosti pracovníků bývá obvykle pozornost věnována skutečnostem jako je obsah a charakter práce, mzdové ohodnocení či pracovní perspektivy. Nepříznivé sociální podmínky zvyšují citlivost pracovníků na vše, co ruší jejich pracovní pohodu, naopak příznivé sociální podmínky v pracovní skupině podstatně zvyšují celkovou pracovní spokojenost. [8]

7 ZÁVĚR

Zpracování diplomové práce na téma „Psychologie a bezpečnostní politika organizace“ si kladlo za cíl prohloubení vědomostí a znalostí o problematice bezpečnosti informací v organizaci v souvislosti s činnostmi managementu a prací manažerů na poli bezpečnosti organizace a dále pak s bezpečnostní politikou.

Za tímto účelem byly využity zejména logické metody, metody analýzy a syntézy shromážděných informací o této problematice z dostupné odborné a vědecké literatury, osobní zkušenosti a vědomosti z oboru informatiky. Dalším zdrojem poznání byly konzultace s odborníky v oblasti počítačové bezpečnosti.

Každý informační systém je specifický a každý slouží pro jiné účely, proto jsou na každý informační systém kladeny jiné specifické požadavky na bezpečnost. Bezpečnost je navíc neustávající proces, neboť se objevují stále nové hrozby a rozvíjí se technologie. Vzhledem k tomuto faktu, byly v práci představeny požadavky na fyzickou, informační, personální a internetovou bezpečnost organizace na obecné úrovni.

Zvláštní pozornost byla zaměřena na lidský faktor a jeho úlohu v bezpečnostním systému. Byly rozebrány nejčastější chyby, kterých se pracovníci organizace dopouštějí, základní bezpečnostní zásady, které by měli dodržovat všichni pracovníci bez ohledu na to, v jaké pozici se nacházejí, a motivační faktory, které ovlivňují jednání pracovníků.

Část zaměřená na management řeší motivy a přínosy systému řízení bezpečnosti informací, oblasti působení manažera bezpečnosti informací a různé pohledy na styl řízení podřízených pracovníků manažery. Problematika bezpečnostní politiky organizace rozebírá jednotlivé kroky při stanovení cílů a strategií, tvorbě, implementaci, provozu a monitoringu bezpečnostní politiky.

Na závěr byla zpracována případová studie, která posloužila jako nástroj pro ověření získaných teoretických znalostí v praxi. Pro konkrétní organizaci byla vypracována analýza rizik. Vyhodnocení stávajícího stavu a analýza rizik poukázala na riziková místa dané organizace v oblasti bezpečnosti informací a dat, na jejichž základě byla navržena konkrétní doporučení a nastíněna řešení, která by přispěla k jejich eliminaci a předcházení.

8 SEZNAM POUŽITÝCH ZDROJŮ

[1] VANÍČEK, Jiří, a kol. *Teoretické základy informatiky*. 1. vyd. Praha: Kernberg Publishing, 2007. 436 s. ISBN 978-80-903962-4-1.

[2] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. 1. vyd. Brno: Computer Press, 2007. 154 s. ISBN 978-80-251-1511-4.

[3] POŽÁR, Josef. *Informační bezpečnost*. Plzeň : Vydavatelství a nakladatelství Aleš Čeněk, 2005. 309 s. ISBN 80-86898-38-5.

[4] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. 1. vyd. Brno : Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[5] TAILOR, Art. *Hacking bez tajemství : Java J2EE.* 1. vyd. Brno : Computer Press, 2003. 409 s. ISBN 80-7226-868-6.

[6] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. 1. vyd. Praha : Grada, 2007. 284 s. ISBN 978-80-247-1561-2

[7] MITNICK, Kevin. *Umění klamu.* Gliwice : Nakladatelství HELION S.A., 2003. 348 s. ISBN 83-7361-210-6.

[8] PAUKNEROVÁ, Daniela. *Psychologie pro ekonomy a manažery*. 1. vyd. Praha : Grada Publishing, 2006. 254 s. ISBN 80-247-1706-9.

[9] ČERMÁK, Miroslav. *Řízení informačních rizik v praxi*. 1. vyd. Brno : Tribun EU, 2009. 138 s. ISBN 978-80-7399-731-1.

[10] ZUZÁK, Roman; KÖNIGOVÁ, Martina. *Krizové řízení podniku.* 2., aktualiz. a rozš. vyd. Praha : Grada, 2009. 253 s. ISBN 978-80-247-3156-8.

[11] HARRIS, Shon; et al. *Hacking: manuál hackera.* 1. vyd. Praha : Grada, 2009. 339 s. ISBN 978-80-247-1346-5.

[12] URBAN, Jan. *10 nejdražších manažerských chyb.* 1. vyd. Praha : Grada, 2010. 166 s. ISBN 978-80-247-3176-6.

[13] MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ, George. *Hacking bez tajemství.* 3. aktualiz. vyd. Brno : Computer Press, 2003. 612 s. ISBN 80-7226-948-8.

[14] GÁLA, Libor; POUR Jan; TOMAN Prokop. *Podniková informatika.* Praha : Grada, 2006. 484 s. ISBN 80-247-1278-4

[15] LIDINSKÝ, Vít; et al. *Egovernment bezpečně.* 1. vyd. Praha : Grada, 2008. 145 s. ISBN 978-80-247-2462-1

[16] PLAMÍNEK, Jiří. *Tajemství motivace : jak zařídit, aby pro vás lidé rádi pracovali.* 2. dopl. vyd. Praha : Grada, 2010. 127 s. ISBN 978-80-247-3447-7.

[17] CCB, spol. s r.o. *System OnLine : S přehledem ve světě informačních technologií* [online]. c2001 - 2011 [cit. 2011-09-22]. Dostupné z WWW: <http://www.systemonline.cz/>. ISSN 1802-615X.

[18] *Ministerstvo vnitra České republiky* [online]. c2010 [cit. 2011-09-18]. Bezpečnost. Dostupné z WWW: <http://www.mvcr.cz/clanek/pojmy-bezpecnost.aspx>.

[19] HANÁČEK, Petr; STAUDEK, Jan (zprac.). *Bezpečnost informačních systémů : Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií* [online]. Úřad pro státní informační systém, 2000 [cit. 2011-10-02] (PDF). Dostupné z WWW: <http://aplikace.mvcr.cz/archiv2008/micr/files/479/uvis_bezpecnost_20000701.pdf >.

[20] ČERMÁK, Miroslav. *Clever and Smart : ICT management* [online]. c2008 - 2011 [cit. 2011-10-03]. Dostupné z WWW: <http://www.cleverandsmart.cz/>.

[21] Obchodní zákoník (Zákon č. 513/1991 Sb.). Dostupné on-line na http://business.center.cz/business/pravo/zakony/obchzak/cast1.aspx [cit. 2011-10-12].

[22] Zákon o ochraně osobních údajů (Zákon č. 101/2000 Sb.). Dostupné on-line na http://business.center.cz/business/pravo/zakony/oou/cast1h1.aspx [cit. 2011-10-12].

[23] Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti (Zákon č. 412/2005 Sb.). Dostupné on-line na http://www.nbu.cz/cs/pravni-predpisy/zakon-c-4122005/uplne-zneni-zakona-c-4122005/ [cit. 2011-10-12].

[24] Zákon o elektronickém podpisu (Zákon č. 227/2000 Sb.). Dostupné on-line na http://business.center.cz/business/pravo/zakony/epodpis/cast1.aspx [cit. 2011-10-12].

[25] CSO magazine. *CSO Online : Security and Risk* [online]. c1994 - 2011 [cit. 2011-10-22]. Dostupné z WWW: <http://www.csoonline.com/>.

[26] ZANDL, Petr, et al. *Lupa.cz : server o českém Internetu* [online]. c1998 – 2011 [cit. 2011-11-22]. Dostupné z WWW: <http://www.lupa.cz>. ISSN 1213-0702.

Seznam obrázků

Seznam tabulek

9 PŘÍLOHY

9.1 PŘÍLOHA Č. 1 - PŘÍPADOVÁ STUDIE

9.1.1 Úvod

Cílem případové studie je analýza rizik konkrétní firmy a navržení bezpečnostních opatření k eliminaci bezpečnostních hrozeb z pohledu jejich dopadu na bezpečnost organizace.

K tomu, aby bylo možné navrhnout bezpečnostní opatření, je nutné identifikovat a ohodnotit všechna aktiva organizace, identifikovat hrozby a zranitelnosti organizace, jednotlivým aktivům přiřadit možná rizika a pravděpodobnosti, s jakou ke konkrétnímu riziku dané skupiny aktiv může dojít, díky nimž se určí klíčové rizikové oblasti.

Vzhledem k faktu, že otázka bezpečnosti organizace je velice citlivým tématem a analýza rizik odkrývá zranitelnosti firmy, není název firmy jmenován.

9.1.2 Popis systému

Firma se zabývá výrobou reklamních předmětů, digitálních fotografií a videí. Má vlastní prostory, ve kterých pracuje majitel a tři zaměstnanci. Firma má navíc zaměstnané dva externí pracovníky, kteří se vzdáleně připojují do informačního systému. V prostorech firmy se nachází kancelář určená k realizaci zakázek, kancelář určená pro styk s veřejností a přijímání zakázek, místnost s výrobními technologiemi, ateliér k realizaci fotografických zakázek a sklad, ve kterém má firma zásoby k realizaci zakázek.

V pracovní kanceláři se nachází tři stolní počítače, jeden notebook a tiskový server s operačními systémy Microsoft Windows. Dále je zde datový server s OS Linux, který firma využívá k ukládání veškerých zákaznických dat, informací o dodavatelích a účetní agendy. Každý z externích pracovníků má doma k dispozici notebook s přístupem do vnitropodnikové sítě firmy. Správa IT je v kompetencích jednoho ze zaměstnanců firmy.

9.1.3 Cíle a strategie řešení bezpečnosti

V současné době je bezpečnost informací ve firmě zajištěna zabezpečovacím systémem s detektory pohybu. Vchod do firmy má bezpečnostní zámek a spolu s kanceláří pro styk s veřejností je snímán bezpečnostní kamerou. Prostory, ve kterých dochází ve firmě k nakládání s informacemi, jsou přístupné z prostor pro styk s veřejností bez jakéhokoliv zabezpečení přístupu neoprávněnými osobami. Pracovní kancelář je opatřena hlásičem požáru.

Informace, se kterými firma pracuje, lze rozdělit na:

- *citlivé informace* obchodního charakteru, která se týkají hlavní činnosti firmy, mají tržní hodnotu, a firma má zájem je chránit,
- *ostatní informace* dostupné volně veřejnosti.

Firma má vypracovaný Pracovní řád, Provozní řád konkrétních technologií a Zásady bezpečnosti práce s konkrétními technologiemi. Bezpečnost informací před neoprávněným přístupem je zajištěna nastavením přístupových práv uživatele, činnosti uživatelů informačního systému firmy jsou zaznamenávány do logů na serveru. Firemní data na serveru jsou zabezpečena proti selhání pevného disku metodou RAID 1. Zálohování dat probíhá manuálně jednou měsíčně zaměstnancem, který má na starost kompletní správu IT.

Vnitřní firemní síť je od Internetu oddělena routerem s firewallem. Na každé pracovní stanici je nainstalovaný antivir s implementovaným antispywarem. K datům na datový server se uživatelé musí autentizovat svým uživatelským jménem a heslem. Datový a tiskový server je napájen záložním zdrojem energie.

Zaměstnanci jsou poučeni správcem IT o základním chování v oblasti bezpečnosti. V případě nejasností, otázek a nestandardních událostí zpravidla správce kontaktují.

Cílem řešení bezpečnosti je za pomoci analýzy rizik identifikovat všechna aktiva firmy, která se podílejí na ochraně citlivých obchodních informací a dat. Na základě této analýzy budou majiteli firmy doporučena opatření, která zajistí ochranu klíčových rizikových oblastí.

9.1.4 Identifikace a ohodnocení aktiv

Uvažovaná aktiva, která by mohla mít za následek porušení důvěrnosti, integrity a dostupnosti dat firmy, jsou zpracována v tabulce č. 1. Při ohodnocení aktiv je použita stupnice od 1 do 5, přičemž nejdůležitější aktiva jsou označena hodnotou 5 a zanedbatelná hodnota aktiv je označena 1.

Tabulka 1 - Identifikace a ohodnocení aktiv

Skupina aktiv	Identifikovaná aktiva	Hodnota aktiva
Firma	Dobré jméno firmy	5
	Know-how	5
	Zaměstnanci	5
Objekty	Budova firmy	5
Hardware	Datový server	5
	Tiskový server	5
	Stolní počítače	2
	Výrobní technologie	4
	Notebooky	4
Software	Licence k OS	3
	Licence k aplikačnímu SW	4
Databáze	Databáze zakázek	5
	Databáze zákazníků	5
	Účetní agenda	5
	Databáze zaměstnanců	3
	Databáze dodavatelů	3
Komunikační zařízení	Telefony	2
	Routery	3
Služby	Připojení serveru	5
	Připojení počítačů	4
	Připojení k Internetu	3

9.1.5 Identifikace a ohodnocení hrozeb a zranitelností, pravděpodobnost výskytu

Pro aktiva identifikovaná v tabulce č. 1 jsou identifikovány hrozby a zranitelnosti. Pro ohodnocení rizik jsou použity následující kategorie:

- *vysoká hodnota rizika* (3) – bezpečnostní opatření na odstranění rizika není možné ani při nasazení neomezených zdrojů, nebo je možné s vynaložením významných zdrojů,
- *střední hodnota rizika* (2) – bezpečnostní opatření na odstranění rizika je přípustné z hlediska nákladů i času,
- *nízká hodnota rizika* (1) – pro odstranění rizika není potřeba žádné bezpečnostní opatření.

Akceptují se jen nízké hodnoty rizika. Ostatní se musí řešit.

Tabulka 2 - Identifikace a ohodnocení hrozeb

Identifikovaná hrozba	Hodnota hrozby
Selhání hardware	3
Selhání aplikačního software	3
Selhání operačního systému	2
Zpronevěření aktiv	3
Požár	2
Povodeň	1
Infekce škodlivým kódem	2
Neúmyslná modifikace	3
Ztráta dat	2
Selhání komunikačních služeb	3
Kompromitace účtu	2
Škodlivý software (vir, spyware)	1
Vyzrazení informací pracovníky firmy	2
Odposlech	1

Poškození majetku	3
Krádež	3
Výpadek proudu	2
Extrémní prostředí	2
Chyba personálu	2
Vniknutí do vnitřní sítě firmy	2

Určení slabých míst systému, které mohou umožnit působení hrozeb, můžeme podle citlivosti aktiva na působení dané hrozby ohodnotit následovně:

- *velmi vysoká hodnota zranitelnosti* (4)
- *vysoká hodnota zranitelnosti* (3)
- *střední hodnota zranitelnosti* (2)
- *nízká hodnota zranitelnosti* (1)

Analýza rizik bude provedena metodou vyhodnocující pravděpodobnost incidentu a jeho dopad. Nejprve se doplní identifikovaná aktiva a jejich hodnota. Poté je nutné k jednotlivým aktivům identifikovat hrozby, zranitelnosti a existující opatření. Dále se odhadne pravděpodobnost incidentu, že daná hrozba využije zranitelnosti a ohrozí tím dané aktivum. Pravděpodobnost incidentu je snižována existujícími opatřeními. Dopad, jako další parametr, je zvolen shodný s hodnotou aktiva. Míra rizika je vypočtena vynásobením pravděpodobnosti incidentu a dopadu. Třídy pravděpodobnosti jsou rozděleny následovně:

- *velmi nízká pravděpodobnost* (1) – pod 20 %, vznik rizika je téměř vyloučený,
- *nízká pravděpodobnost* (2) – 20 – 40 %, vznik rizika je málo pravděpodobný, ale možný,
- *střední pravděpodobnost* (3) – 41 – 60 %, riziko může někdy vzniknout během činnosti nebo životnosti,
- *vysoká pravděpodobnost* (4) – 61 – 80 %, riziko může vzniknout několikrát během činnosti nebo životnosti,
- *velmi vysoká pravděpodobnost* (5) – nad 80 %, riziko může vznikat velmi často.

Tabulka 3 – Identifikace a ohodnocení zranitelností, pravděpodobnost výskytu

Identifikovaná zranitelnost	Hodnota zranit.	Pravd. výskytu
Nedostatečná fyzická ochrana budovy	4	1
Umístění, kde hrozí záplava	3	2
Nestabilní dodávka energie	2	3
Nebezpečí vlhkosti, prachu	1	3
Nebezpečí výkyvu teploty	3	5
Citlivost na elektromagnetické záření	2	1
Nedostatečná údržba IT	2	3
Nedostatečná autentizace uživatele	2	4
Nedostatečné řízení hesel	3	5
Nesprávné přidělení přístupových práv	2	2
Nekontrolované používání PC	2	2
Nedostatek dokumentace	1	4
Nedostatek zálohovacích kopií	2	4
Nekontrolované tištění dokumentů	2	3
Nedostatečná bezpečnostní školení	2	2
Nedostatek povědomí o bezpečnosti	1	2
Nesprávné používání HW a SW	2	3
Nedostatek monitorování	1	3
Odcizení notebooku	3	4
Nesprávná konfigurace Wi-Fi	3	5
Přístup nepovolanými osobami	3	5

9.1.6 Míra rizika

Míru rizika lze posoudit na základě matice rizika, které je postavena následovně:

Tabulka 4 - Míra rizika

P / D	1	2	3	4
1	1	4	6	12
2	2	7	10	13
3	3	9	15	17
4	5	11	16	19
5	8	14	18	20

Výsledná hodnota míry rizika je kategorizována:

- *přijatelné riziko* (1 – 3) – systém je bezpečný, postačí běžné postupy,
- *mírné riziko* (4 – 10) – systém je bezpečný s podmínkou školení pracovníků,
- *nežádoucí riziko* (11 – 15) – systém je nebezpečný, nutné uplatnit bezpečnostní opatření,
- *nepřijatelné riziko* (16 – 20) systém je nepřijatelný, je nutné odstavení systému a okamžité uplatnění bezpečnostních opatření.

Tabulka 5 - Míra rizika identifikovaných zranitelností

Identifikovaná zranitelnost	Míra rizika
Nedostatečná fyzická ochrana budovy	12
Umístění, kde hrozí záplava	11
Nestabilní dodávka energie	10
Nebezpečí vlhkosti, prachu	3
Nebezpečí výkyvu teploty	18
Citlivost na elektromagnetické záření	4

Nedostatečná údržba IT	10
Nedostatečná autentizace uživatele	12
Nedostatečné řízení hesel	18
Nesprávné přidělení přístupových práv	7
Nekontrolované používání PC	7
Nedostatek dokumentace	5
Nedostatek zálohovacích kopií	12
Nekontrolované tištění dokumentů	10
Nedostatečná bezpečnostní školení	7
Nedostatek povědomí o bezpečnosti	2
Nesprávné používání HW a SW	10
Nedostatek monitorování	3
Odcizení notebooku	16
Nesprávná konfigurace Wi-Fi	18
Přístup nepovolanými osobami	18

9.1.7 Shrnutí

Analýza rizik ukázala, že nejvíce zranitelnými místy je nedostatečné řízení hesel (nedostatečně bezpečná hesla), možnost přístupu nepovolaných osob do jiných místností než určených pro styk s veřejností (nezabezpečené dveře do pracovní kanceláře, skladu, technologické místnosti i ateliéru), nebezpečí výkyvu teplot (vysoká teplota v místnostech s výrobními technologiemi), vniknutí do vnitřní sítě firmy (špatná konfigurace Wi-Fi sítě) a odcizení notebooků (možnost zneužití přístupu do vnitropodnikové sítě).

Možností, jak řešit tato rizika, je mnoho a závisí na konkrétních požadavcích firmy a jejích finančních možnostech.

9.1.8 Doporučení a navrhované změny

Navrhované řešení pro nedostatečné řízení hesel je provést firemní nařízení, které bude specifikovat konkrétní požadavky na bezpečné heslo. Doporučuji firmě, aby zaměstnanci pro přístup do vnitropodnikové sítě a informačního systému používali hesla s minimálně osmi znaky, které budou obsahovat velká a malá písmena, číslice, případně speciální znaky.

K zamezení přístupu nepovolaných osob do jiných místností než určených pro styk s veřejností doporučuji firmě zavést dveřní systém založený na principu identifikačních čipových karet nebo biometrický systém. Vzhledem k velikosti firmy a finančním možnostem se jeví jako přijatelnější řešení používání čipových karet.

Nebezpečí výkyvu teplot je vhodné řešit umístěním klimatizace do technologické místnosti, aby nedošlo k přehřátí strojů.

Před vniknutím do vnitřní sítě firmy by měl být překonfigurován bezdrátový přístup do sítě. Jako první změnu navrhuji použít místo stávajícího WEP klíče, novější WPA2 klíč, který provádí autentizaci přístupu do sítě pomocí novějšího a kvalitnějšího šifrování. Druhá změna je využít seznam MAC adres klientů, kterým bude povoleno připojit se do vnitřní sítě firmy. Tento přístup by měl být umožněn pouze pro zařízení, která využívají jen zaměstnanci firmy. Poslední navrhovanou změnou je zakázání konfigurace Wi-Fi routeru pomocí bezdrátového připojení.

Ochrana notebooků před odcizením a zneužitím přístupu do vnitropodnikové sítě (dále jen VPN) by měla být zajištěna především fyzickými opatřeními. Zaměstnanci by neměli nechávat notebook v osobním automobilu, nebo kdekoliv jinde bez dozoru. Navrhuji využít program pro šifrování pevného disku a velmi silné heslo pro přístup do VPN. Na každém notebooku, využívajícím přístup do VPN, musí být nainstalovaný a aktualizovaný antivirový program a musí zde také být pravidelně aktualizovaný operační systém. Zaměstnanci musí být seznámeni s pravidly užívání a přihlašování k VPN. Silně nedoporučuji přihlašovat se do VPN skrze nezabezpečené Wi-Fi sítě.

9.2 PŘÍLOHA Č. 2 - LEGISLATIVA ČESKÉ REPUBLIKY

Souhrn nejdůležitějších zákonů (ve znění pozdějších předpisů) a vyhlášek České republiky týkající se bezpečnosti organizace a projektů bezpečnostní politiky:

Ústavní zákon č. 23/1991 Sb., kterým se uvozuje Listina základních práv a svobod
Zákon č. 93/2009 Sb., o auditorech a o změně některých zákonů
Zákon č. 101/2000 Sb., o ochraně osobních údajů
Zákon č. 106/1999 Sb., o svobodném přístupu k informacím
Zákon č. 121/2000 Sb., zákon o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů
Zákon č. 127/2005 Sb., o elektronických komunikacích
Zákon č. 140/1961 Sb., trestní zákon
Zákon č. 151/2000 Sb., o telekomunikacích
Zákon č. 227/2000 Sb., o elektronickém podpisu
Zákon č. 240/2000 Sb., o krizovém řešení a o změně některých zákonů
Zákon č. 365/2000 Sb., o informačních systémech veřejné správy
Zákon č. 412/2005 Sb., o ochraně utajovaných skutečností
Zákon č. 480/2004 Sb., o některých službách informační společnosti
Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů
Zákon č. 513/1991 Sb., obchodní zákoník
Vyhláška č. 56/1999 Sb., o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu
Vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění *vyhlášky č. 19/2008 Sb.*

9.3 PŘÍLOHA Č. 3 - NORMY A BEZPEČNOSTNÍ STANDARDY

Některé další normy a bezpečnostní standardy, vydávané společně Mezinárodní organizací pro normalizaci (ISO) a Mezinárodní elektrotechnickou komisí (IEC), které se týkají problematiky informační bezpečnosti a nebyly zmíněny v práci, jsou:

ČSN ISO/IEC 13335-1 (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 1: Pojetí a modely bezpečnosti IT)

ČSN ISO/IEC 13335-2 (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 2: Řízení a plánování bezpečnosti IT)

ČSN ISO/IEC 13335-3 (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 3: Techniky pro řízení bezpečnosti IT)

ČSN ISO/IEC 13335-4 (Informační technologie – Směrnice pro řízení bezpečnosti IT – Část 4: Výběr ochranných opatření)

ČSN ISO/IEC 17799 (Informační technologie – Soubor postupů pro řízení informační bezpečnosti)

ČSN ISO/IEC 15408-1 (Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 1: Úvod a všeobecný model)

ČSN ISO/IEC 15408-2 (Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 2: Bezpečnostní funkční komponenty)

ČSN ISO/IEC 15408-3 (Informační technologie – Bezpečnostní techniky – Kritéria pro hodnocení bezpečnosti IT – Část 3: Komponenty bezpečnostních záruk)
ČSN ISO/IEC 15816 (Informační technologie – Bezpečnostní techniky – Bezpečnostní informační objekty pro řízení přístupu)

ČSN ISO/IEC 18043 (Informační technologie – Bezpečnostní techniky – Výběr, implementace a provoz systémů detekce narušení bezpečnosti)

ČSN ISO/IEC 18044 (Informační technologie – Bezpečnostní techniky – Řízení incidentů v oblasti informační bezpečnosti)

ČSN ISO/IEC 27001 (Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací – Požadavky)

ČSN ISO/IEC 27005 (Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací)

ČSN ISO/IEC 27006 (Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací)

BS ISO/IEC 27031 (Informační technologie – Bezpečnostní techniky – Pokyny pro zajištění kontinuity provozu informačních a komunikačních technologií)

ČSN ISO/IEC 9798 (Informační technologie – Bezpečnostní techniky – Mechanismy autentizace entit)

ČSN ISO/IEC 10118 (Informační technologie – Bezpečnostní techniky – Hašovací funkce)

ČSN ISO/IEC 13888 (Informační technologie – Bezpečnostní techniky – Nepopiratelnost)

ČSN ISO/IEC 14888 (Informační technologie – Bezpečnostní techniky – Digitální podpisy s dodatkem)