VYSOKÁ ŠKOLA BÁŇSKÁ -

TECHNICKÁ UNIVERZITA OSTRAVA

Hornicko-geologická fakulta

Institut ekonomiky a systémů řízení

METODIKY PRO BEZPEČNOST IS A JEJICH IMPLEMENTACE

METHODOLOGY OF THE SECURITY OF IS AND THEIR IMPLEMENTATION

Bakalářská práce

Autor: František Král

Vedoucí bakalářské práce: Ing. Roman Danel, Ph.D.

Ostrava 2015

VŠB - Technická univerzita Ostrava
Hornicko-geologická fakulta
Institut ekonomiky a systémů řízení

Zadání bakalářské práce

Student: **František Král**

Studijní program: B2102 Nerostné suroviny

Studijní obor: 6209R013 Informační a systémový management

Téma: Metodiky pro bezpečnost IS a jejich implementace
Methodology of the Security of IS and Their Implementation

Zásady pro vypracování:

Analyzujte dostupné metodiky pro bezpečnost informačních systémů a na základě provedené analýzy formulujte doporučení pro aplikaci těchto metodik s cílem nastavení vnitropodnikové bezpečnostní politiky a dodržování pravidel uživatelů využívajících IT/ICT.

Práci zpracujte podle následující osnovy:
1. Úvod
2. Přehled metodik pro bezpečnost IS
3. Realizace opatření, audit a protokolování
4. Autentizace a řízené přístupy
5. Datová, personální, komunikační a síťová bezpečnost
6. Právní a etické aspekty bezpečnosti IS
7. Doporučení pro tvorbu IT směrnic, havarijního plánu a bezpečnostní politiky
8. Závěr

Doporučený roszah práce: 35 stran

Seznam doporučené odborné literatury:

[1] HUBNER, M. *Pohled nejen CIO na informační bezpečnost : příručka manažera.* Praha: TATE International, 2012. ISBN: 978-80-86813-25-7
[2] DOUCEK, P. *Řízení bezpečnosti informací.* Praha: ProfessionalPublishing, 2011, 240 stran. ISBN: 978-80-7431-050-8
[3] DOBDA, L. *Ochrana dat v informačních systémech.* Praha: Grada, 2001, 286 stran. ISBN: 80-7169-479-7
[4] DOSEDĚL, T. *Počítačová bezpečnost a ochrana dat.* ComputerPress 2004. 200 stran. ISBN: 80-251-0106-1
[5] POŽÁR, J. *Informační bezpečnost.* Plzeň: 2005, 311 stran. ISBN: 80-86898-38-5

Formální náležitosti a rozsah bakalářské práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí bakalářské práce: **Ing. Roman Danel, Ph.D.**

Datum zadání: 31.10.2014

Datum odevzdání: 30.04.2015

doc. Ing. Šárka Vilamová, Ph.D.
vedoucí institutu

prof. Ing. Vojtech Dirner, CSc.
děkan fakulty

Prohlašuji, že:

- Celou bakalářskou práci včetně příloh, jsem vypracoval samostatně a uvedl jsem všechny použité podklady a literaturu.

- Byl jsem seznámen s tím, že na moji bakalářskou práci se plně vztahuje zákon č.121/2000 Sb. - autorský zákon, zejména § 35 – využití díla v rámci občanských a náboženských obřadů, v rámci školních představení a využití díla školního a § 60 – školní dílo.

- Beru na vědomí, že Vysoká škola báňská – Technická univerzita Ostrava (dále jen VŠB - TUO) má právo nevýdělečně, ke své vnitřní potřebě, bakalářskou práci užít (§ 35 odst. 3).

- Souhlasím s tím, že jeden výtisk bakalářské práce bude uložen v Ústřední knihovně VŠB - TUO k prezenčnímu nahlédnutí a jeden výtisk bude uložen u vedoucího bakalářské práce. Souhlasím s tím, že údaje o bakalářské práci, obsažené v Záznamu o závěrečné práci, umístěném v příloze mé bakalářské práce, budou zveřejněny v informačním systému VŠB-TUO.

- Bylo sjednáno, že s VŠB - TUO, v případě zájmu z její strany, uzavřu licenční smlouvu s oprávněním užít dílo v rozsahu § 12 odst. 4 autorského zákona.

- Bylo sjednáno, že užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití mohu jen se souhlasem VŠB - TUO, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly VŠB - TUO na vytvoření díla vynaloženy (až do jejich skutečné výše).

V Ostravě dne 27. 4. 2015 …..……

František Král

Poděkování

Prostřednictvím této bakalářské práce bych chtěl poděkovat především své rodině, která mne po celou dobu studia podporovala. Dále bych chtěl poděkovat panu Ing. Petru Mendlovi za poskytnuté konzultace a zodpovězené dotazy. V neposlední řadě chci poděkovat také svému vedoucímu bakalářské práce panu Ing. Romanu Danelovi, Ph.D. za věcné připomínky k mé práci.

Anotace

Práce seznamuje s metodikami COBIT a ITIL. Praktická část obsahuje realizaci a opatření v nejmenované společnosti. V této části je popsaná analýza stávajícího stavu IS a plně zabezpečené řešení. V dalších kapitolách se autor zabývá autentizací a řízením přístupů, personální bezpečností, právními a etickými aspekty. Závěrem je doporučení pro tvorbu IT směrnic, havarijního plánu a bezpečnostní politiky.

Klíčová slova

BEZPEČNOST, COBIT, ITIL, ICT, IT, HAVARIJNÍ PLÁN, NAS.

Summary

This paper introduces the methodologies COBIT and ITIL. The practical part includes the implementation and procuration of an unnamed company. This part describes the analysis of the current state of IS and fully secure solution. In subsequent chapters I deal with authentication and access controls, personnel security, legal and ethical aspects. Finally, I give the recommendation for the creation of IT directives, emergency plan and security policy.

Keywords:

SAFETY, COBIT, ITIL, ICT, IT, EMERGENCY PLAN, NAS.

OBSAH

Seznam zkratek

České zkratky

IS	informační systém
IT	informační technologie
NAS	datové úložiště na síti

Cizojazyčné zkratky

CCTA	Central Computer and Telecomunications Agency
COBIT	Control Objectives for Information and Related Technology
DRP	Disaster recovery plans
ICT	Information and Communication Technology
ISACA	Information Systems Audit and Control Foundation
ITIL	Information Technology Infrastructure Library
NAS	Network Attached Storage
RAID	Redundant Array of Inexpensive/Independent Disks
SIEM	Security Information and Event Management

1 Úvod

Pro svou bakalářskou práci jsem si vybral téma metodiky pro bezpečnost IS a jejich implementace. S rostoucí potřebou informačních technologií a jejich využívání ve všech oblastech života se dostáváme do nutnosti ochrany dat a informací před ztrátou, zneužitím, kriminalitou, neoprávněným přístupem a celkovým zneužitím potřebných informací.

Při přenosu a zpracování velkého objemu dat je nezbytné zabezpečit, aby nedocházelo ke ztrátě a k neoprávněné modifikaci dat a informací. Je důležité předcházet neúmyslnému poškození dat, jako např. při přenosu dat, vadám hardwaru, živelným pohromám a úmyslné modifikaci. Problematikou bezpečnosti je nutné se zabývat i z důvodu možného kybernetického útoku na bezpečnostní, vojenské, finanční a energetické složky. Metodiky pro informační bezpečnost vyžadují ucelené opatření, různé techniky a nové metody.

Cílem mé práce je analýza dostupné metodiky pro bezpečnost informačních systémů, nastavení vnitropodnikové bezpečnostní politiky a vytvoření zásad bezpečnostních pravidel uživatelů využívajících IT/ICT.

Práce je strukturovaná do těchto kapitol:

Přehled metodik pro bezpečnost IS - v této části jsou popsané metodiky pro bezpečnost IS a porovnání metodik COBIT A ITIL.

Realizace opatření, audit a protokolování - na základě provedené analýzy byla navrhnuta doporučení s cílem efektivního využití bezpečnosti informačního systému.

Autentizace a řízené přístupy – v této kapitole jsou popsány principy řízených přístupů a jejich procesy.

Datová, personální, komunikační a síťová bezpečnost – tato část se zabývá bezpečností osobních údajů, popisem personální bezpečnosti a etap životního cyklu personálu.

Právní a etické aspekty bezpečnosti – zde je zohledněna právní ochranná informace dle autorského práva a informační etika.

Doporučení pro tvorbu IT směrnic, havarijního plánu a bezpečnostní politiky – v předposlední kapitole jsou uvedena doporučení tvorby IT směrnic, havarijního plánu a formulace zásady bezpečnosti IT pro uživatele.

Závěr – závěrečná kapitola je souhrnem výsledků a cílů bakalářské práce.

2 Přehled metodik pro bezpečnost IS

Pro zabezpečení informačních systémů existuje mnoho metodik. V této části práce zde bude popsána metodika COBIT a ITIL. Využití metodik COBIT a ITIL je významným krokem optimalizací a řízení informačních technologií. Podmínkou úspěchu zavedení těchto metodik je jejich správné nastavení pro konkrétní prostředí organizace a posléze následné dodržování a kontrola. Pokud se dosáhne úspěšné aplikace, ještě více zefektivníme využívání stávajících technologií, dosáhneme významných úspor a spolehlivosti. V tabulce č. 1 je popsáno srovnání třech metodik.

Tabulka 1 Srovnání metodik [vlastní zdroj]

KRITÉRIA	COBIT 5	ITIL V3	ISO 27000
Vydáno	2012	2007	2005
Sektor určení	ITSM	IT řízení	ISM
Forma	Standarty/Praktiky	Standarty/Praktiky	NORMY
Dle velikosti	Střední, velká	Střední, velká	Velká
Bezplatná dokumentace	Ano	Ne	Ne
Certifikace	Ano	Ne	Ano

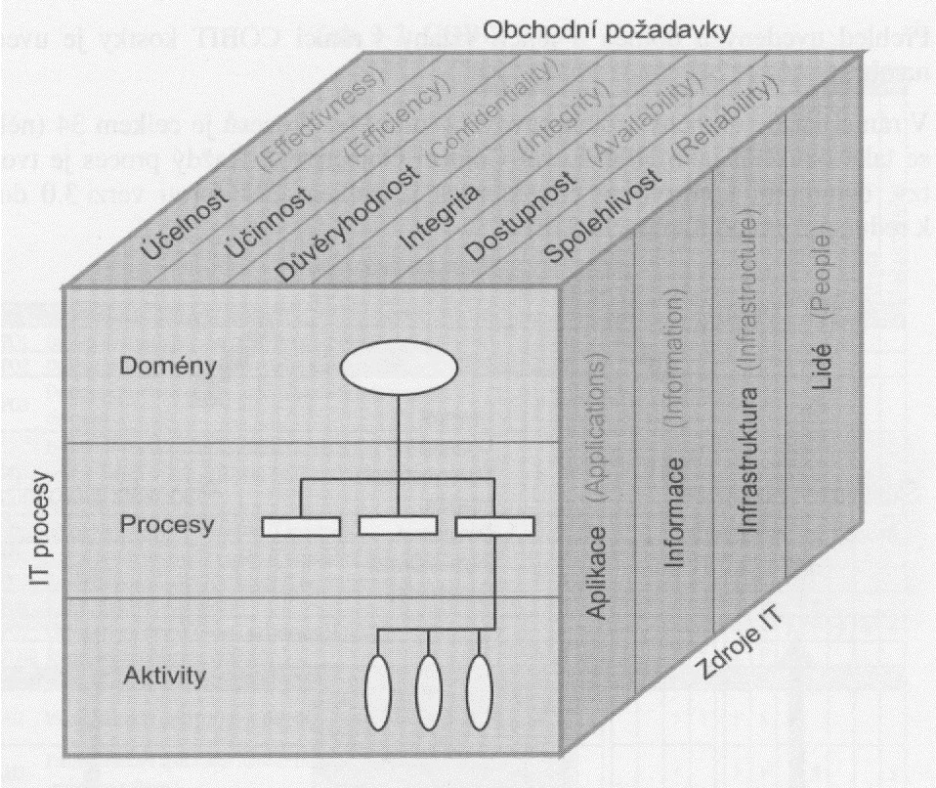
2.1 COBIT

Metodika COBIT (Control Objectives for Information and Related Technology) byla vytvořena asociací ISACA (Information Systems Audit and Control Foundation). Tato metodika je jedním ze základních nástrojů řízení informatiky (ITGovernance). Jedná se o souhrn praktik, které by měly minimalizovat IT rizika a z využití dostupných zdrojů umožnit dosažení strategických cílů. Metodika je převážně určena manažerům k posuzování funkčnosti ICT a auditorům pro systém řízení ICT. Jeho výhodou je velmi jednoduchá, rychle pochopitelná schematičnost. Na rozdíl od ITIL, která bude popsána níže, se nezabývá každodenními činnostmi a operativou. COBIT se postupně stává standardem pro hodnocení úrovně provádění procesu IT.[1]

První verze byla vydaná v roce 1996. Postupně došlo k rozšíření o implementační, auditní nebo manažerské postupy. V roce 2007 byla uvedená čtvrtá verze, kde došlo zprůhlednění jednotlivých vazeb řízení a přibyly nové části (např. Cobit Secutity Basaline, IT Assurance Guide). Aktuální verze COBIT 5 se objevila v 1. čtvrtletí roku 2012.

Metodika COBIT byla vytvořena na strategických cílech organizací, IT procesech a IT zdrojích. Všechny tři uvedené složky vystihuje tzv. COBIT kostka uvedena na obr. 1.

[1] DOUCEK, P. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011, 240 stran. ISBN: 978-80-7431-050-8



Obrázek 1 Kostka COBIT [DOUCEK, P. Řízení bezpečnosti informací]

Na tomto modelu je velice dobře znázorněná základní koncepce. Z COBIT kostky jsou zřetelné jednotlivé úrovně. Mezi základní definice domén patří čtyři:

- Plánování organizace
- Pořízení a implementace
- Provoz
- Monitorování a hodnocení

Zdroje informatiky:

- Aplikace (Applications)
- Informace (Information)
- Infrastruktura (Infrastrukture)
- Lidé (People)

Informační kritéria:

- Efektivnost (požadavek na včasné doručení korektní informace)
- Účinnost (požadavky na zpracování informací nejproduktivnějším způsobem)
- Důvěryhodnost (oblast ochrany důležitých informací proti prozrazení)
- Integrita
- Dostupnost (požadavky na dostupné informace)

- Soulad (soulad se zákony, směrnicemi)
- Spolehlivost (požadavek vhodných informaci pro rozhodování manažerů)

2.2 ITIL

ITIL (Information Technology Infrastructure Library) je mezinárodně uznávaným standardem v oblasti řízení IT. Jedná se o soubor knih, který popisuje procesní způsob řízení služeb IT. Koncepce ITIL vznikla počátkem 80 let v Anglii. Britská vláda měla potřebu najít způsob, kterým by řešila znepokojený stav v řízení IT ve státních organizacích. Tímto úkolem pověřila státní agenturu CCTA (Central Computer and Telecomunications Agency) vypracováním uceleného souboru nejlepších zkušeností v oblasti řízení služeb a procesů IT. Tento koncept byl vytvořen zkušenými bezpečnostními experty, kteří využili své zkušenosti z praxe. Jedním z požadavku byla možnost využití této metodiky nejen pro vládní, ale i pro soukromé organizace. CCTA provedla hloubkovou analýzu ve většině společností, které se podílely na službách pro britskou vládu. Na základě provedené analýzy byly vybrány nejlepší zkušenosti řízení informatických služeb organizací. První verze metodiky byla rozdělena do 46 svazků dle potřeb britských úřadů. Publikace se vydávaly postupně s ohledem na soukromé organizace dodávající informační technologie britské vládě, což vedlo k postupnému uplatnění této metodiky i v soukromých organizacích.

K prvnímu znatelnému přepracování došlo na přelomu roku 2001. V původní verzi se objevovaly duplicity. Metodika byla značně nepřehledná. Následně došlo k přepracování a snížení počtu svazků na 11 knih:[2]

- Service Support
- Service Delivery
- The Business Perspective Volume1
- The Business Perspective Volume2
- Application Management
- ICT Infrastructure Management
- Security Management
- Software Asset Management
- Planning to Implement Service Management
- Small-Scale Implementation
- Introduction to ITIL

Zásadní knihy jsou Service Support (podpora služeb) a Service Delivery (dodávka služeb).

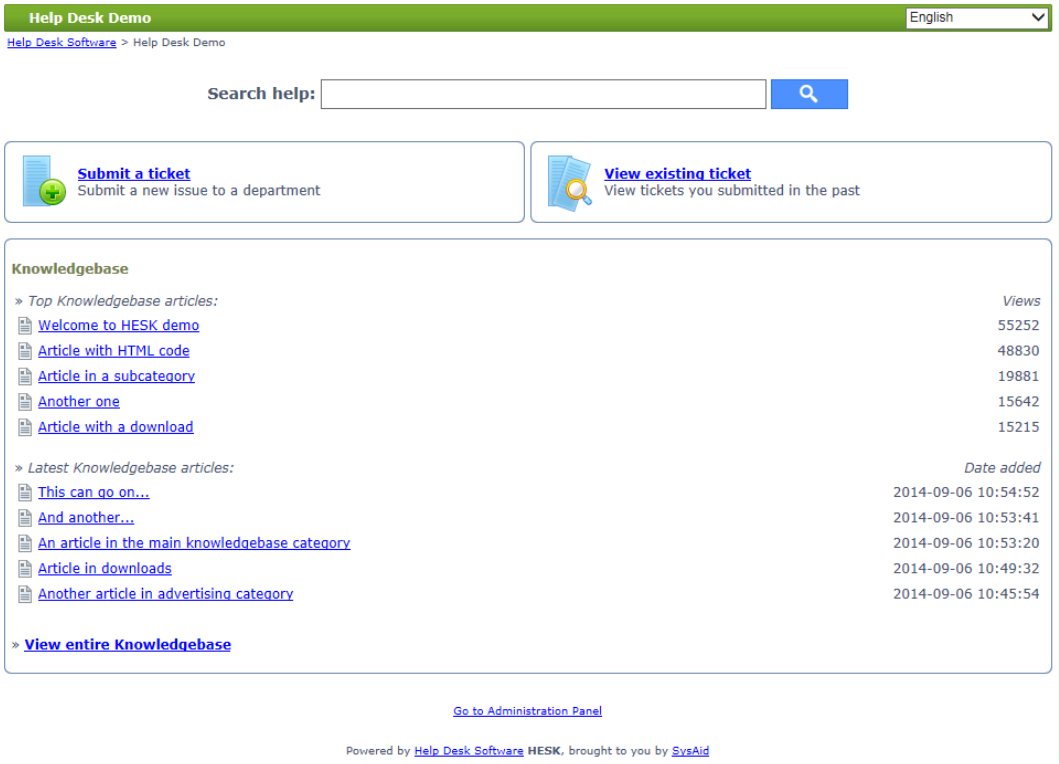
[2] DOUCEK, P. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011, 240 stran. ISBN: 978-80-7431-050-8

Service Support popisuje:

Incident Management – proces je odpovědný za včasnou detekci incidentů. Hledá způsob omezení výpadku služby. Služba nemůže ovlivnit počet incidentů, ale pouze jejich dobu trvání. Vhodné je vytvoření znalostní databáze, která umožní rychlé vyhledání předchozích incidentů. V případě chybějícího procesu se značně prodlužuje doba reakce efektivního zásahu, což má za následek ovlivnění kvality služeb.

Problem Management – proces efektivně a účinně analyzuje základní příčiny incidentů. Výsledkem je odhalení chyb a poskytnutí trvalého řešení.

Service desk – jedná se o kontaktní místo správy incidentů. Při nahlášení je potřeba rozdělení důležitosti a přiřazení konkrétnímu řešiteli. Po odstranění incidentů nesmí být opomenuto kontaktování uživatele o vyřešení. Dovoluji si zmínit volně stažitelnou webovou aplikaci Hesk, která svou bohatou sadou funkcí patří k oblíbeným nástrojům service desku. Jedná se o samoobslužní portál.



Obrázek 2 Prostředí webového portálu HESK [http://www.hesk.com/demo/]

Configuration Management – proces správy konfigurací. Při správném používání a aktualizování konfigurační databáze získáme ucelený přehled nad službou.

Change Management – proces správy změn. Tento proces řídí celý životní cyklus změn od návrhu až po ostré nasazení. Zabývá se všemi změnami služeb všech úrovní správy.

Release Management – proces zajišťující distribuci a nasazení změny do IT infrastruktury. Zajišťuje soulad technického i organizačního aspektu nasazení. [6]

Service Support popisuje:

Service Level Management – správa úrovně služeb (řízení kvality služeb SLA). Jedná se o zdroj informací všech poskytovaných služeb povolaným osobám.

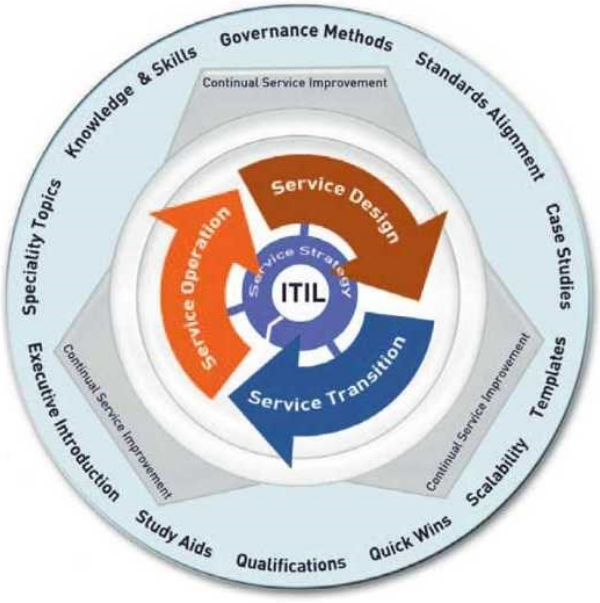
Availability Management – proces zajištění schopnosti požadavků a dostupnosti za přiměřených nákladů. Jedná se o protiopatření proti rizikům ohrožující dostupnost. Snahou je nákladová optimalizace úrovně dostupnosti.

Capacity Management – zajišťuje současné a budoucí požadavky na kapacitu a výkon. Cílem je dosažení efektivního investičního plánování. Investice do rozvoje infrastruktury jsou koordinovány a tvorba IT rozpočtu je transparentní. Účelem je poskytnout pracoviště se správou všech záležitostí, které souvisí s kapacitou informačních technologií a zdrojů schválených požadavků.

Financial Managament – proces nám poskytuje přehled evidence nákladů na poskytování IT služeb. Efektivním způsobem realizuje návrh financování dodávky služeb. Poskytuje nám zdroje na sestavení rozpočtů podnikové IT infrastruktury, které podléhají schvalování.

IT Service Continuity Management – proces vytváří plány obnovy hrozícího rizika výpadku. Služby jsou poskytnuté na základě dohodnutého časového plánu. Tohoto procesu dosahujeme pravidelnou analýzou na zmírnění výskytu rizika.

V květnu roku 2007 byla vydaná verze ITIL V3, která opět redukuje počet knih. Tehdy došlo k celkové změně koncepce podřízené životnímu cyklu IT služeb.



Obrázek 3 Základní model ITIL V3 [http://www.systemonline.cz/sprava-it/mate-duvod-prejit-na-itil-v3.htm]

ITIL V3 rozdělíme do pěti fází:

- Service Strategy
- Service Desing
- Service Transition
- Service Operation
- Continual Service Improvment

Service Strategy – popisuje shodu propojení organizace se strategií okruhu informatiky. Obsahem je formulace služeb, strategie ITSM a vymezení poskytovatelů služeb.

Service Desing – jejím obsahem je návrh IT služeb a architektury informačního systému v organizaci, včetně různých forem sourcingu.

Service Transition – obsahuje návrhy na implementaci služeb do ostrého nasazení. Zahrnuje procesy změnového řízení, správu verzí, doporučené kontroly služeb realizované do ostrého provozu apod.

Service Operation – zahrnuje zprávu služeb v produkčním prostředí. Popisuje služby a monitoruje problémy, stabilitu mezi službou a její cenou.

Continual Service Improvment – pomáhá optimalizovat a vylepšovat poskytované informační služby. Definuje postup, jak řídit zlepšování procesů a jejich porovnání s dlouhodobými cíli při zachování vysoké kvality.

Hlavní body pro úspěšnou implementaci ITIL:

- Schválení implementace Top Managementem organizace
- Zmonitorování stávajícího prostředí
- Naplánování dílčích činností
- Definování cíle projektu

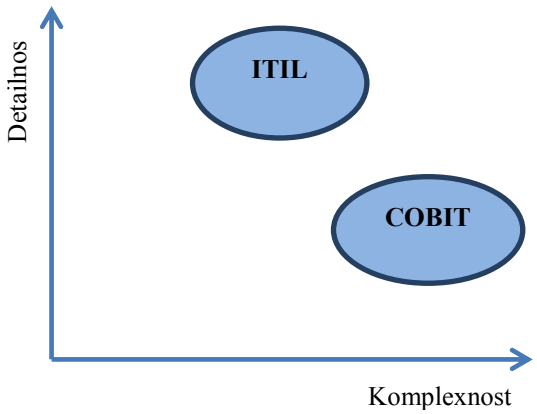
2.3 IT GOVERANCE

Používá se zkratka ITG a jedná se o řízení informačních technologií. Její hlavním cílem je návratnost investice. Pečlivě posuzuje jednotlivé rozhodnutí a cíleně směřuje investice proudící do IT. ITG by nám mělo v případě správného uchopení poskytnout efektivní rozhodování na základě pravdivých informací s pohledem na unikátnost podniku. IT je element, který umožňuje růst a vývoj podniku.

2.4 Porovnání metodik COBIT a ITIL

Metodika COBIT je komplexnější a oproti ní metodika ITIL řeší některé oblasti detailněji. Implementace a dodávky jsou v metodice ITIL propracovanější než u metodiky

COBIT. Ale můžeme konstatovat, že každou novou verzí dochází ke sbližování metodik s tím, že si každá metodika ponechává svojí jedinečnosti, pro kterou byla vytvořena. Odborníci doporučují obě metodiky kombinovat, aby se dosáhlo maximálního splnění požadavků na konkrétní prostředí. Proto vznikají různé nástroje mapování procesů obou metodik. Obrázek č. 4 ukazuje graf, ze kterého plyne komplexnost metodiky COBIT a detailnost metodiky ITIL.[3]



Obrázek 4 Porovnání metodik COBIT a ITIL [DOUCEK, P. Řízení bezpečnosti informací]

[3] DOUCEK, P. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011, 240 stran. ISBN: 978-80-7431-050-8

3 Realizace opatření, audit a protokolování

3.1 Realizace opatření

V nejmenované společnosti pohybující se v oblasti energetiky jsem byl zaměstnán na pozici IT specialista. Společnost v době mého nástupu zaměstnávala kolem 400 zaměstnanců. Stávající IT oddělení bylo složeno z třech zaměstnanců. Hlavním záměrem společnosti bylo sestavit nový tým IT oddělení, zprůhlednit veškeré finanční toky, snížit výdaje na výpočetní techniku, zlepšit podporu k uživatelům a celkově zefektivnit IT oddělení.

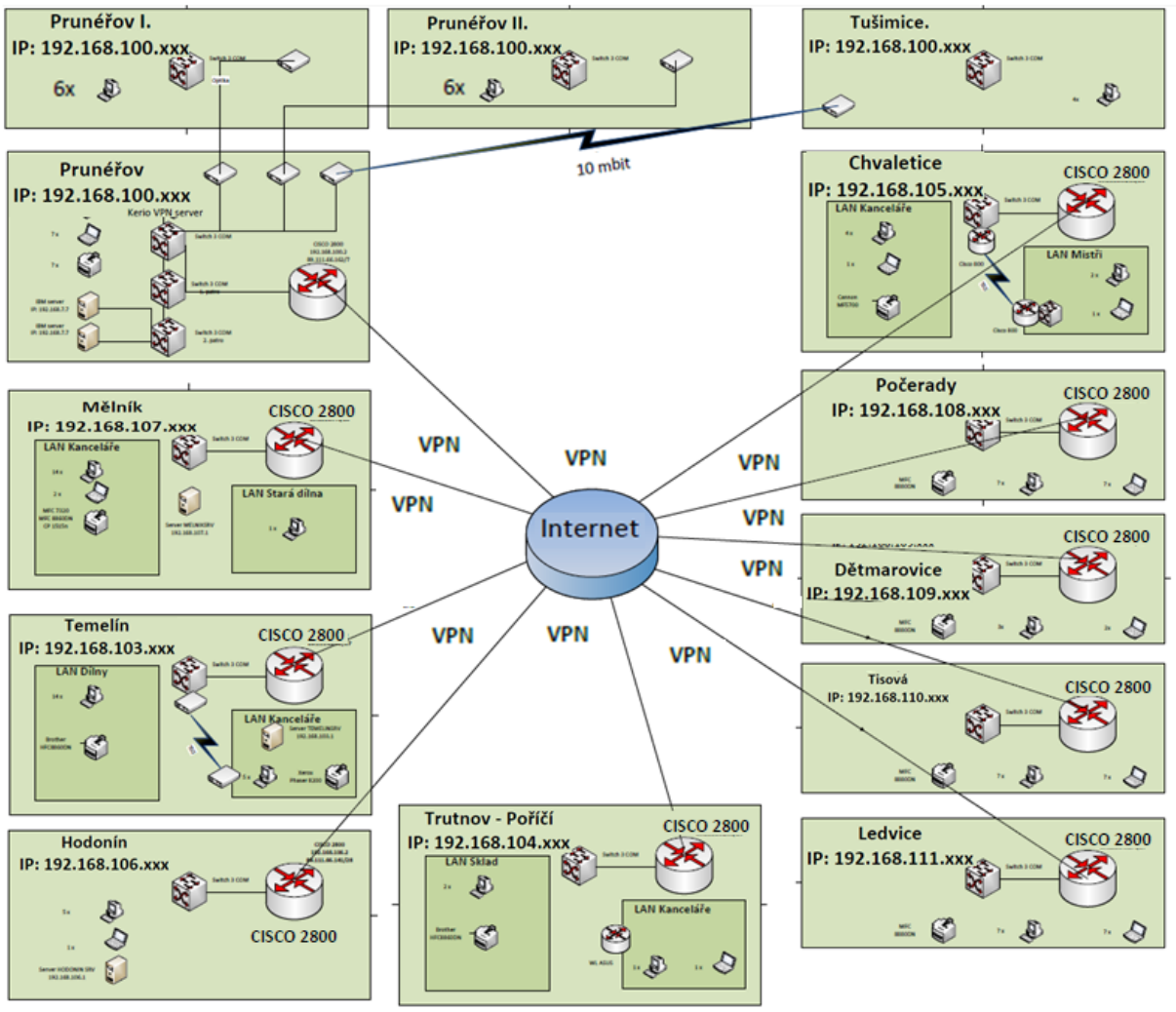
Předem bylo upozorněno na arogantnost a nespolupráci stávajících zaměstnanců IT oddělení. S vedením firmy byly domluveny hlavní body činnosti:

- provést analýzu stávajícího stavu infrastruktury
- prověřit stávající zastaralé servery a realizace nového řešení
- provést audit HW a softwaru (doporučit řešení průběžného monitorování)
- zefektivnit využití tisku a snížit náklady na tisk

Podpora nejvyššího managementu byla jedním z hlavních bodů úspěšného dotažení zadaných cílů a také velkým předpokladem úspěšného nastavení nových pravidel.

3.1.1 Analýza stávajícího stavu IS

Centrála společnosti je propojena s jednotlivými středisky přes aktivní prvky CISCO. Aktivní prvky jsou spravovány externí organizací včetně zajištěni konektivity. Bohužel neexistovala žádná mapa celé infrastruktury a ani seznam jednotlivých aktivních prvků včetně seznamu vybavení, což mělo za důsledek nepřehlednost vnitropodnikové struktury. Ve spolupráci s externím dodavatelem služeb zajišťující support na CISCO, byla vytvořena mapa jednotlivých lokalit, kde se vyznačily vnitřní ip adresy. Všechny lokality byly propojeny síťovými prvky CISCO, což zajišťovalo dostatečnou stabilitu a bezpečnost. Slabším místem byla nízká konektivita - převážně 2 - 5 Mbit/s, a to mělo za následek pomalé zpracování dat mezi centrálou. Při jednání s poskytovatelem internetu se podařilo vyjednat při zachování stávajících poplatků navýšení dostatečné konektivity na 20 Mbit/s.



Obrázek 5 Mapa středisek [vlastní zdroj]

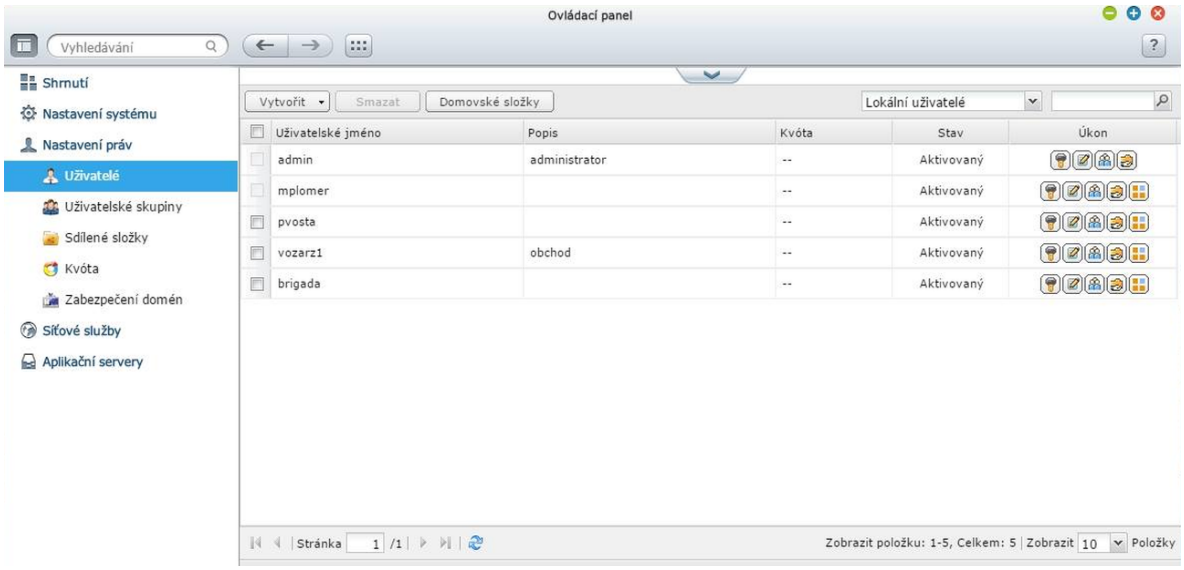
Ve třech střediscích se nacházely souborové servery, které sloužily jako datová úložiště. Bohužel se jednalo o zastaralý neznačkový hardware, který byl nestabilní, a tím hrozila ztráta cenných dat. Dalším nedostatkem byla nezálohovaná data a absence zajištění před náhlým výpadkem elektrické energie. Jednotlivé komponenty již nebylo možné zakoupit.

V případě náhlé neočekávané kolize, byl nutný výjezd IT technika. Jelikož vzdálenost střediska byla ve stovkách kilometrů, tak doba reakce byla několik hodin. Průměrná reakce zásahu od nahlášení incidentu se pohybovala kolem třech hodin. V případě ztráty dat byl časový nárůst neakceptovatelný. Zvažovalo se najít adekvátní řešení, které nahradí zastaralé zařízení. Hlavní body opatření byly bezpečnost, přehlednost, rychlost a stabilita zařízení. Po důkladné analýze stávajícího stavu došlo k realizaci a nahrazení zastaralých souborových serverů za datové uložiště (NAS). Byla vybraná značka SYNALOGYC a model DS214. V tabulce č. 2 jsou uvedené technické parametry datového úložiště.

Tabulka 2 Technické parametry Synology DiskStation DS214+ [vlastní zdroj]

Synology DiskStation DS214+	
Počet pozic pro disk	2x SATA
Podpora RAID	RAID0, RAID1
Rychlost čtení	202 MB/s
Rychlost zápisu	140 MB/s
Spotřeba ve Stan-by	9,26W
Provozní spotřeba	27,62W
Rozhraní	USB2,USB3,eSata
Ethernet	2 x LAN 1GB/s
HDD	2 ks WD Red 1000GB
Rozměr h, s, v	232x103,5x157 mm

Před přesunem dat proběhla důkladná analýza stávajícího stavu aktuálních dat včetně duplicity. Byl sestaven seznam uživatelů přistupujících k jednotlivým složkám a datům. NAS úložiště, bylo nakonfigurováno na poměrně jednoduchou a efektivní ochranu zrcadlení (mirroring), též značeno RAID1. Jedná se o současný zápis na dva disky. V případě výpadku jednoho z disku je ihned k dispozici pracovní kopie. Jediná nevýhoda je dvojnásobná kapacitní spotřeba diskové kapacity, pomalejší zápis a v případě smazání dat hrozí ztráta dat. V uživatelském rozhraní NAS byly vytvořeny uživatelské skupiny dle pracovních pozic. Uživatelské rozhraní Synology obrázek č. 6.



Obrázek 6 Nastavení práv Synology DiskStation DS214 [vlastní zdroj]

K jednotlivým skupinám se přiřadily uživatelské účty, což vedlo velké časové úspoře a přehlednosti při založení nebo rušení účtu do budoucna. Struktura stávajících složek zůstala zachovaná pro lepší adaptaci uživatelů. Přesun dat proběhl mimo pracovní dobu, aby nedošlo k modifikaci dat v průběhu přenosu na nové zařízení. Po kompletním

přenosu proběhly náhodné testy zabezpečení a kontrola přístupu k datům. Zálohování dat se nakonfigurovalo dle zálohovacího plánu, který probíhal centrálně každý večer dle zálohovacího plánu.

Hlavní přínosem tohoto řešení bylo protokolování přístupu k datům. Docházelo k dohadům mezi uživateli, že si smazali a přesunuli soubory, aniž by si to sami uvědomili. Datové uložiště mělo jednu z funkcí - obnovu smazaných dat. V případě, že došlo k neopatrnosti uživatele, bylo možné vzdáleně obnovit během krátké doby smazaná data. Mezi hlavními bezpečnostními prvky proběhla opatření omezení k vybraným aplikacím, uživatelský přístup (pravidla pro sílu hesla), HW šifrování dat, integrovaný firewall. Nové zařízení vykazuje několikanásobnou úsporu energie, takže pro případ náhlého výpadku elektrické energie byl dostačující záložní zdroj nižší cenové kategorie. V tabulce č. 2 uvádím hlavní klady nasazení NAS.

Tabulka 3 Přínosy NAS [vlastní zdroj]

KLADY [+]	ZÁPORY [-]
Velice nízká spotřeba energie oproti serveru	Externí napájecí adapter
Dostupná cena	Pomalé náhledy u Photo Station
Rychlost přenosu dat a zpracování	
Dostačující bezpečnost	
Protokolování	
Atraktivní poměr cena/možnosti/výkon	
Kompaktní, tichý, bezúdržbový systém	
Jednodušší správa oproti starším serverům	
Velice nízká spotřeba energie oproti serveru	
Dvě síťová rozhraní LAN	

3.1.2 Prověření serverů a realizace nového řešení

Ve společnosti byly instalovány dva centrální servery IBM X3500 v podobných (nikoliv shodných) konfiguracích. Na každém z nich byly instalovány jiné aplikace (vše v prostředí Windows Server 2008), což znamená, že výpadek každého z těchto serverů měl omezit nebo dokonce zcela znemožnit práci uživatelů v síti.

Shledané nedostatky serverů a serverovny:

- nedostačující kapacita operační paměti
- malá kapacita diskového pole
- rok po záruce bez zajištění supportu
- nefunkční záložní UPC s nízkou kapacitou
- žádné zálohování serveru
- nepořádek v serverovně

- přístup nekompetentních osob do serverovny

Data nebyla pravidelně zálohovaná. Nebyl však žádný zálohovací systém, který by dovolil úplnou obnovu serveru (tzv. “bare metal recovery”).

Výpadek každého ze serverů znamenal v konečném důsledku představu nutnosti reinstalace všech aplikací na novém (opraveném nebo vyměněném) serveru a obnovu dat z pořizované zálohy s tím, že následně bude nutno manuálně doplnit data z období mezi poslední zálohou a výpadkem. Všechny tyto činnosti byly kromě časové náročnosti náročné i na kvalifikaci systémových pracovníků, přičemž k řadě činností lze využít externí firmu jen obtížně. Nutným předpokladem je totiž poměrně dobrá znalost celého prostředí.

Kromě těchto dvou serverů byl používán ještě třetí, který slouží jako firewall se softwarem Kerio. To je však ve skutečnosti běžná pracovní stanice s velmi stabilní konfigurací, není tedy problém mít v záloze připravený systémový disk nebo celý počítač s další instalací a ten v případě potřeby téměř ihned zprovoznit. Firewall měl zrcadlený disk, což zajišťovalo ochranu v případě poškození jednoho z lokálních disků. Image disk byl zálohován na DVD médiu.

Zcela bezpečné výpočetní prostředí prakticky neexistovalo a nebylo ho možné vytvořit. Zamýšlenému cíli je možné se přiblížit jedině zdvojováním (obecně spíše násobením) všech kritických zařízení a systémů. V takovém hardwarově zabezpečeném systému pak je možno použitím vhodných systémů docílit i automatického přechodu mezi hlavním a záložním systémem nejlépe bez zásahu obsluhy, případně s pouze minimálními zásahy ze strany obsluhy. V ideálním stavu dojde k přepnutí systémů zcela automaticky bez toho, že by tuto skutečnost uživatelé vůbec zaregistrovali. Ale i stav, který si vyžádá např. restart počítačů, případně krátkou odstávku je většinou výrazně přijatelnější, než jedno či vícedenní přerušení provozu v případě jednoduché nezabezpečené infrastruktury.

Základem pro řešení problematiky zabezpečení je samozřejmě vhodný hardware. Všechny prvky v systému musí být nějakým způsobem zdvojeny (nebo znásobeny, ale pro jednoduchost dále mluvíme jen o zdvojování), především se jedná o síťovou infrastrukturu, servery a jejich datová úložiště. To je však jen první, i když nezbytný krok.

Bezpečnost z vnějšího pohledu je dána především spolehlivostí celého systému, tj. toho, jak se chová vůči uživateli. Běžným způsobem, kterým se na úrovni systému tato problematika dříve přednostně řešila, je spojování výpočetních systémů do clusterů. Jako cluster se označuje skupina dvou či více počítačů, které sdílejí stejné aplikace, jsou schopny pracovat nad shodnými daty. Vhodnými HW i SW prostředky je zajištěno to, že při výpadku jedné části dojde k převzetí její funkce další částí systému, tak, aby nedošlo ke ztrátě kontinuity dat a funkce celého systému. Servery v clusteru spolu komunikují zvláštním odděleným spojem a stále jsou tedy navzájem informovány o stavu clusteru jako celku.

3.1.3 Virtualizace

Výrazné zjednodušení situace přineslo přemístění aplikačních serverů do virtuálního prostředí. Operační systémy pro virtualizace jsou již postaveny na technologii clusterů a virtuální servery, které na nich běží, již tedy nemusí další funkce podporovat.

Běžně používané virtualizační SW platformy jsou dnes celkem tři. Základní prostředky virtualizace jsou k dispozici v některých edicích Microsoft serveru, tedy v principu zdarma, trpí však mnoha neduhy a nedostatky.

Firmou, která je leaderem v procesu virtualizace je VMware. Dá se dnes říci, že VMware v podstatě určuje směr vývoje této oblasti a nabízí nejširší portfolio funkcí.

Posledním významným hráčem je firma Citrix, která se primárně zabývá terminálovými řešeními, ale v poslední době vstupuje i do oblasti serverové virtualizace.

Vzhledem k dominantnímu postavení VMware, je uveden v dalším textu často odkaz na tento systém.

Při použití této osvědčené virtualizační platformy VMware je tedy možno postavit cluster s tímto softwarem a využívat veškeré prostředky, které tento software poskytuje. Jednotlivé servery pak běží v tomto prostředí zcela nezávisle na hardware, což kromě možnosti přenosu aplikace z jednoho fyzického serveru na druhý (dokonce i za běhu systému) přináší další významné zjednodušení případné obnovy. Celý server je vlastně jediným souborem na disku (tzv. image) a lze ho nejen transportovat, ale i spouštět na jiném hardware, pokud na něm bude opět instalován základní virtualizační systém.

Samozřejmě, že ne všechny aplikace fungují na virtuální platformě, ale takových je jen mizivé množství (převážně se jedná o případy využívající speciální HW prostředky v serveru) a především jsou již dnes při vývoji nové verze pro virtuální prostředí testovány a certifikovány.

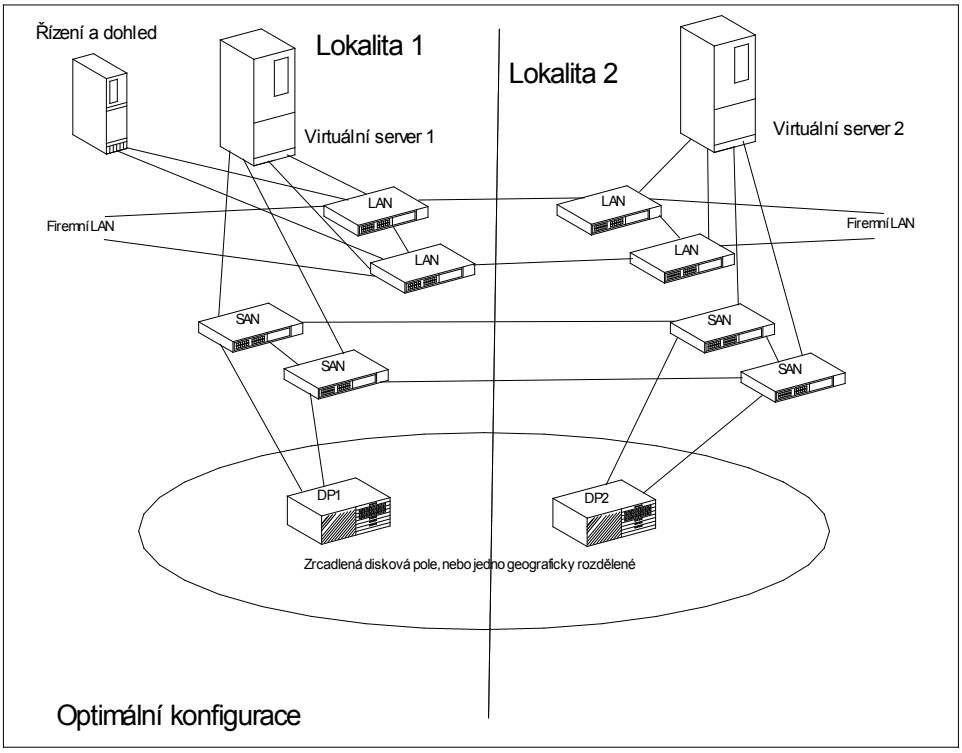
Z těchto důvodů se doporučil přechod k virtualizaci a tím výrazně zjednodušit správu spolehlivosti centra.

3.1.4 Plně zabezpečené řešení

Pokud máme postihnout všechny aspekty, které mohou způsobit poruchu systému, musíme vzít v úvahu i živelné události, tj. požár, resp. zatopení (když ne povodeň, tak postačí i prasklé vodovodní potrubí).

Ideální stav je tedy takový, kdy je systém rozdělen na nejméně dvě částí, které jsou umístěny v oddělených prostorech, nejlépe dvou budovách a jsou propojeny dvěma fyzicky oddělenými spoji. Pokud říkáme systém, tak tím jsou myšleny jak servery, tak i disková úložiště.

Blokové schéma takového ideálního řešení složeného ze dvou částí je uvedeno na následujícím obrázku.



Obrázek 7 Blokové schéma optimálního řešení [Vlastní zdroj]

Především disková úložiště musí být volena tak, aby zajistila shodná data v obou polovinách (zrcadlení dat nebo distribuovaný diskový systém, jakým je např. HP Lefthand) a možnost přístupů pro oba servery do každé části úložiště (dva servery jsou jenom abstrakcí, fyzicky jich může být samozřejmě na „každé straně“ více).

Připojení diskových úložišť musí být tedy také takové, aby umožnilo síťový přístup více serverům, tedy FC nebo iSCSI.

Naopak lokální disky serverů nyní mohou být použity pouze pro zavádění systému a stačí jejich minimální velikost.

Z hlediska síťové komunikace musí být systém také zdvojený. Podle náročnosti aplikací pak může být požadováno i více připojení pro každý server.

Vzhledem k tomu, že na virtuálním prostředí běží více aplikací (tedy serverů) najednou, bývá obvykle zapotřebí i více operační paměti než u běžného serveru.

Pokud jsou jednotlivé fyzické servery zcela HW totožné, je možno provozovat systém se všemi jeho výhodami. V extrémním případě, dokonce v takovém režimu, že

aplikace běží na obou polovinách systému a speciálním prostředky je její běh synchronizován. V takovém případě je přepnutí skutečně okamžité a bez výpadků.

Ale i v případě ne zcela shodného HW je běžně možno použít režim tzv. aktiv – pasiv, kdy aplikace běží na jednom serveru, a v případě jeho výpadku je okamžitě spuštěna na druhém. Dojde tím sice k přerušení provozu, případně nekonzistenci dat, ale následky - především doba do nového zprovoznění - jsou nesrovnatelně menší než při běžném řešení.

3.1.5 Navrhnuté řešení obměny serverů

Bylo vytvořeno několik variant možných řešení dané problematiky. První varianta byla s popisem té nejkomplexnější (a tím i nejdražší) varianty a postupně se navrhovaly možné ústupky s klesající finanční náročností.

První varianta HW

Předpokládaná instalace dvou serverů HP DL380pG8, každý osazen 2 procesory Intel 2 GHz, 6 jader, osazeno 64 GB RAM, redundantní zdroje napájení a ventilátory, a dále pak dva disky 146GB, 2,5“ pro operační systém. Součástí serverů tříletá záruka se zásahem druhý den na místě.

Jako předpoklad společného diskové úložiště, bylo použito diskové pole HP MSA2000 s iSCSI konektivitou. Pole je osazeno dvěma řadiči, každý s dvojitým interface 1Gbit/s, dvěma zdroji a v základní sestavě má 24 slotů na disky 2,5“ (dualportové). Jedinou neredundantní částí je tedy základní šasi, vše ostatní je zdvojeno.

V tomto odhadu se počítalo s osazením 18 ks disků s 600 GB, což podle konfigurace RAID přináší kapacitu od 5 do 10 TB, tedy více než dostatečnou v porovnání s potřebami.

Servery budou nainstalovány v rámu HP o velkosti 42 HE (cca 210 cm) a hloubce 1100 mm, v něm budou dva záložní zdroje s výkonem 2200 VA každý – dva opět kvůli redundanci.

K propojení serverů se zbytkem sítě budou sloužit dva switche HP 24port propojené 10GB spojem, tak aby opět byla dodržena redundance. Zvolená kategorie switchů nemá redundantní napájení, ale použitím dvou switchů a vhodným propojením je možno docílit funkčnosti i při výpadku zdroje u jednoho z dvojice.

Druhá totožná dvojice switchů vytvoří iSCSI síť, která má být vždy od sítě LAN oddělena.

Toto řešení by bylo možno postupně i fyzicky rozdělit na dvě oddělené části pro zvýšení fyzické bezpečnosti (diskové pole by ovšem bylo jen v jedné z nich, ve druhé by pak mohlo být zálohovací zařízení)

Cena tohoto HW řešení je přibližně 930 tis. Kč.

A) s malým omezením

Při snaze o úsporu při zachování funkčnosti je možno použít jen jeden zdroj UPS (druhý zdroj zařízení připojit k nezálohovanému zdroji napájení). Také by bylo možno použít jednu dvojici switchů s oddělením sítí technologií VLAN a dále pak použít menší diskovou kapacitu (3 TB místo 5 TB).

Takto koncipovaný hardware poskytne plnou funkčnost s následnou možností rozšíření na plné řešení.

Cena po této úpravě poklesne na 760 tis. Kč.

Varianta software

A) plný software

Jako základní virtualizační software byl navržen k použití VMware, jeho použití přináší značný komfort provozu, správy a zálohování systému.

Vzhledem k tomu, že není předpokládán provoz více než 3 fyzických serverů, je možno použít výhodný startovací balíček pro 3 host servery + dohledové centrum. Povinnou položkou je nejméně jednoletý support (včetně práva použití nových verzí). V tomto okamžiku je kalkulováno s cenou tříletého supportu.

Dále pak je třeba pořídit operační systémy Microsoft. Podle počtu provozovaných virtuálních serverů je třeba příslušného počtu licencí. U MS Serveru2012 platí, že jedna licence Standard je pro max. 2 virtuální servery. Jedna licence Datacenter je pak omezena pouze na 1 fyzický server s max. 4 procesory bez omezení počtu jader a virtuálních instancí. V tomto odhadu počítám s licencí Datacenter pro každý server.

Cena OLP licence je trochu vyšší než OEM (především u verze Datacenter), ale přináší možnost instalace na nový server i v budoucnosti. Cena případné Select licence je téměř shodná s OLP.

K tomu je třeba dále pořídit příslušný počet licencí koncových stanic, v našem případě se jedná o 170 licencí. Ty mohou být opět dvou typů, a to na zařízení a na uživatele. Licence na uživatele je o poznání dražší než na zařízení, totéž platí o dalších licencích pro terminálový přístup. Zde je počítáno s 30 licencemi. Volba typu licence závisí na našem způsobu využívání počítačů.

Poslední položkou je nový SQL server, ten se kupuje podle počtu jader procesorů, na kterých je server (a to i virtuální) provozován. Jedna licence je na 2 jádra, ale minimální počet zakoupených licencí je 2, což bohatě vystačí.

Cena popsaného software vychází přibližně na 860 tis. Kč.

B) OEM Software, licence na zařízení

Prvním krokem ke snížení ceny je rozhodnutí, že použijeme OEM software, a že je pro nás výhodné použít licenci na zařízení, nikoliv na uživatele. Dále pak lze zakoupit pouze 1rok podpory VMware.

Již tímto se cena software sníží na cca 645 tis. Kč, z hlediska kvality řešení se však nejedná o téměř žádný ústupek.

C) OEM Software, licence Standard bez VMware

Další úspora v oblasti software již přináší mírné funkční omezení. VMware není nutno pořizovat, technologie HyperV je součástí licencí serverů, ovšem nemá některé výhodné funkce VMware. Pokud nám vystačí provoz max. 6 virtuálních serverů, pak je možno kumulovat licence OS Standard za nižší cenu než je Datacenter.

Těmito kroky se cena SW sníží na cca 460 tis. Kč.

Tabulka 4 Výsledné kombinace nákladů [vlastní zdroj]

			Software		
			OLP+Device	OEM+User	STD - VMware
			860	645	460
HW	Plný	930	1790	1575	1390
	Omezený	760	1620	1405	1220

Tak jak bylo popsáno v předchozím textu je tedy možné plné řešení s případnými malými kompromisy pořídit za cenu v rozmezí 1,2 - 1,8 mil. Kč.

Levnější řešení s funkčním omezením

Virtualizaci je možno zahájit v prvním kroku pořízením 1 serveru bez diskového pole s interními disky, tedy v podstatě lepší náhradou zastaralého serveru s OS W2003, ale s virtualizací.

V tomto případě bude HW stát cca 290 tis. Kč a SW bez VMware s OEM licencemi Standard pak celkem cca 410 tis. Kč, celé řešení tedy nepřekročí 700 tis. Kč. Přitom stále existuje možnost jej postupně rozšířit na některé z výše uvedených, bez ztráty investic (snad kromě nákladů na instalaci některého software).

Další úsporu cca 50 tis. Kč lze docílit downgradováním nově zakoupených licencí na verzi 2008 a tím umožnit použití dnes provozovaných 90 ks CAL.

Nouzové řešení bez Virtualizace

Posledním krokem ke snížení předpokládaných nákladů je pak úplné „obětování“ virtualizace a pouze pořízení nových licencí na server se systémem 2003 (a samozřejmě i nové SQL), licence zde samozřejmě nemohou být OEM, přesto však cena klesne na cca 350 tis Kč.

Doplňkové funkce.

Až dosud se autor nezabýval centrálním zálohováním.

Zálohování

Vhodným kompromisem mezi samostatnou mechanikou a druhou knihovnou může být v našem případě autoloader s 8 sloty, pásky lze navíc umísťovat do kazet po 4ks a tyto kazety případně ukládat na vhodném místě. Z hlediska celkového objemu dat postačí technologie LTO4, která je cenově výhodná a má kapacitu 1,6 TB dat (komprimovaných) na pásku. 4 kazety pak musí tedy plně vystačit na týdenní zálohu (základ + denní přírůstky).

Jako vhodný software byl doporučen produkt CA Arcserve, který je cenově přijatelný a přitom podporuje jak zálohu na úrovni souborového systémy, databází, ale i na úrovni diskových obrazů VMware i HyperV.

Pro instalaci byl mimořádně vhodný jeden z uvolněných serverů IBM, protože není vhodné zálohovací server provozovat ve virtuálním prostředí. Tento server by zároveň mohl sloužit pro správu virtuálních serverů (systém Vcenter), zde je řada argumentů pro i proti tomu, aby tento server byl virtualizován. Většina organizací však dává přednost fyzickému serveru v této roli.

Cena zálohovacího systému v popsané konfiguraci pak vychází na cca 240 tis. Kč. Cenu je nutno přičíst k některé z výše uvedených variant.

Tabulka 5 Náklady na zálohovací zařízení [vlastní zdroj]

Zálohování na pásky , pro plnou variantu	
Zálohovací zařízení Autoloader 8slot, LTO-4 (1,6 TBx8), SAS vč. řadiče.	
CA ARCserve Backup r16 for Windows OLP+1YVM	
CA ARCserve Backup r16 for Win VM Agent per Host License OLP+1YVM	
CA ARCserve Backup r16 Win Agent for MS SQL OLP+1YVM	
Celkem	**240 000 Kč**

Společnost se rozhodla pro nejlepší a nejdražší variantu A) plný HW + A) plný software + zálohování na pásky viz tabulka. Jedinou nevýhodou byly pořizovací náklady.

Efektivnější využití tisku

V každé kanceláři se vyskytoval nadměrný počet tiskáren připojených na LPT port, které byly sdíleny mezi jednotlivými PC stanicemi. IT oddělení bylo neustále vytěžováno nefunkčností tisků, výměnou tonerů a poruchovostí zastaralých tiskáren. Stávající řešení nebylo efektivní. Při změně HW a OS se vyskytoval problém s nekompatibilitou ovladačů.

Byla zahájena spolupráce se společností Konica Minolta, která nabídla k pronajmutí kopírovací stroje Bizhub C220. Na každé podlaží byla instalována jedna kopírka. A zastaralé kopírky byly odprodány zaměstnancům.

Tabulka 6 Centralizace tisků [vlastní zdroj]

KLADY [+]	ZÁPORY [-]
úspora nákladu na tisk	čas uživatelů
rozúčtování nákladu na uživatele	pořizovací náklady pronájem
zabezpečení tisku	
shodné nastavení pro všechny uživatele	
možnost skenování do pdf a odeslání na email	
úspora času IT oddělení	
vzdálená správa	

3.1.6 Audit a protokolování

Společnost k evidenci HW a softwaru používala softwarový produkt AuditPro. Bylo zjištěno, že aplikace je nainstalovaná jen na třetině PC a bylo nezbytné provést celoplošnou instalaci. Tento modulární systém se skládá z několika hlavních modulů: evidence majetku, modul monitoru využití počítačů, softwarů, tiskáren a internetu.

AuditPro se dělí na dvě části - aplikační a databázová. Aplikace se nainstalovala v prostředí MS Windows server 2008, a databáze na MS SQL 2010. Na všechny stanice byla potřeba nainstalovat klienta, který přenášel naskenované informace do hlavního programu umístěného na serveru. Výhoda AuditPro byla, že umožňoval automatickou údržbu historie změn. Tak pokud došlo ke změně HW, nebo softwaru, vše se zaznamenalo v protokolu.

Po celoplošné instalaci klienta, byly zjištěny nedostatky v nastavení administrátorského účtu na koncových stanicích. Tento nedostatek měl za příčinu nadměrné množství stažených dat z internetu. Jednalo se hlavně o filmy ve formátu avi a zakázaný software.

Odstranění nedostatků koncových stanic

Veškeré koncové stanice se překonfigurovaly a připojily do lokální domény centrálního serveru. U všech PC byl odebrán lokální administrátorský účet. Na základě tohoto nastavení již uživatelé nemohli provádět instalace bez vědomí IT technika. Dalším nastavení bylo vzdálené připojení plochy, což umožňovalo vzdálenou obsluhu připojení IT technika.

AuditPro nám umožňovalo na základě získaných dat okamžité zpracování reportů evidence HW, software, vytížení PC a mnoho další funkcionality. Prostřednictvím takto získaných informací došlo efektivnějšímu plánování investic. Bylo zjištěno 30 procent nevyhovujícího hardwaru, který se postupně dle plánu investic aktualizoval. Aby se postupně sjednotil HW, přešlo se na jednoho výrobce, což byl DELL. Hlavní přínosy sjednocení HW jsou popsány v tabulce číslo 7.

Tabulka 7 Obnova a sjednocení HW [vlastní zdroj]

KLADY [+]	ZÁPORY [-]
sjednocení HW - lepší přehled IT technika	vstupní náklady
sjednocený SW - kompatibilita	prvotní instalace
servisní podpora na 5 let	
stabilnější a rychlejší HW	
jeden image soubor pro všechen nový HW	
výrazná úspora času IT oddělení	
efektivnější přínos práce uživatelů	
stabilní vzdálená správa	

Hlavní přínosy nasazení Auditpro

- kompletní evidence HW a softwaru
- možnost online vysledovat nedostačující HW
- přehled využívání softwaru a HW
- protokolování volného místa na disku, který uživatel a kdy se nalogoval
- protokolování spuštěného softwaru (přehled zakázaného softwaru)
- protokolování tisků
- protokolování využívání internetu dle kategorizace

4 Autentizace a řízené přístupy

4.1 Principy řízených přístupů

Řízení přístupu rozdělujeme na tři základní prvky:

- identifikace
- autentizace
- autorizace

Identifikace

Jedná se o proces rozpoznání entity (systémem). Obvykle za pomocí prostředků IT zpracovatelných uživatelských jmen. Jména bývají unikátní v rámci skupiny dle systémové politiky.

Autentizace

Autentizace je proces ověřování identity subjektu. Jedná se o ověření pravosti, kde „autentický“ znamená původní. Pomocí autentizace zajišťujeme ochranu před neplatnou identitou. Jedná se o proces, kdy se subjekt vydává za někoho, kým není. V informatice se autentizace používá ověření identity uživatele. Nejpoužívanější základními metody jsou:

- podle toho, s čím uživatel disponuje (bezkontaktní chip, RSA SecurID token apod.)
- podle toho, co uživatel zná (kombinace jména a hesla, nebo PIN)
- podle biometrie (oční sítnice, otisk prstu)
- podle toho, co uživatel zná (správná odpověď na vygenerovanou otázku)

Obrázek 8 RSA SecurID Token [http://en.wikipedia.org/wiki/RSA_SecurID]

Autorizace

Autorizace je povolení, schválení, oprávnění k získání přístupu k informacím. Jedná se o přistoupení k určitým zdrojům (např. složkám, souborům, tiskárnám, serverům). Předpokladem autorizace uživatele je schválená autentizace.

4.2 Řízený přístup

V každé síti je důležité řídit bezpečnost. Řízený přístup využívá identifikaci a autentizaci přidělení práv. Po úspěšné autentizaci je možné uživateli přidělit přístupová práva. Ověřuje se uživatel, uživatelská skupina a počítač. Uživatelská práva mohou být přidělena skupinovým a uživatelským účtům. Tato práva umožní uživatelům řízený přístup k souborům a složkám. Změny uživatelských práv může provádět osoba s administrátorským oprávněním.

5 Datová, personální, komunikační a síťová bezpečnost

5.1 Datová bezpečnost

Jednou z hlavních povinností pracovníků IT oddělení je zajistit bezpečnost osobních údajů. Je potřeba nastavit taková pravidla a vhodná opatření na ochranu osobních údajů, aby nedošlo ke ztrátě, změnám, neoprávněnému přístupu, poškození, zneužití informací. Hlavně pokud je zpracování dat v sítí, nebo přenosných médiích.

Aplikovaná opatření by měla být v souladu s možnými riziky organizace. Jedná se o neustálý proces analýz rizik. Bezpečnost osobních údajů má zajistit každý subjekt, který zpracovává osobní údaje.

Nastavení pravidel osobních údajů obnáší zavedení odpovídajících technických opatření. Je nutné vytvořit dokumentace, která bude popisovat pravidla a postupy zpracovávání osobních údajů. Při zavádění bezpečnostních opatření je potřeba uplatňovat uznané bezpečnostní standardy a používat opatření na ochranu osobních údajů. Pochopitelné je, že opatření zpracování osobních údajů závisí na prostředí, ve kterém jsou údaje zpracovávány.

V případě využití informační technologie může být provedeno zabezpečení dat dle bezpečnostních opatření:

- Nemožnost popření – nemožnost popřít změny osobních údajů
- Spolehlivost – zamezení poskytování informací neoprávněným
- Dostupnost – obstarání, na požádání bude možné zpřístupnit informace, na určitou dobu oprávněnou osobou
- Integrita – obstarání, že likvidace osobních údajů neproběhne neoprávněným způsobem a údaje nebudou upraveny
- Odpovědnost – obstarání, že činnost může být jednoznačně udělena určenému subjektu
- Záměna – znemožnění neměnnosti postupů a výsledků

Požadavky pro automatické zpracování osobních údajů

- fyzické osoby pracující s osobními údaji mají nastavené odpovídající uživatelské oprávnění
- pro automatizované zpracování osobních údajů zajistit přístup pouze oprávněným osobám
- zamezit neoprávněnému přístupu k nosičům osobních údajů
- zamezení neoprávněnému kopírování, čtení, mazání záznamů, přenosu obsahující osobní údaje

- vést elektronickou evidenci záznamů, která nám umožní zjistit, kdo s osobními údaji pracoval

5.2 Personální bezpečnost

5.2.1 Co je to personální bezpečnost

Nedílnou součástí informačního systému jsou jeho uživatelé - zaměstnanci firmy, a to na všech úrovních firemní hierarchie. Řada majitelů IS se soustředí na zajištění technických a programových bezpečnostních opatřeních, ale velice často opomíjí vliv lidského faktoru. Lidské jednání se dá velice těžko odhadnout, a proto může představovat určitou potenciální hrozbu na činnost informačního systému. Ve více případech se jedná o selhání ze strany vlastních zaměstnanců. Selhání zaměstnanců může být jak záměrné (krádež, zlomyslnost, pomsta), tak i neúmyslné (neznalost, nezkušenost) a způsobí škodu. Na rozdíl od ostatních technických subjektů je problematické očekávané chování lidí předem změřit nebo nastavit. Většina firem považuje kvalitní personál za jeden z nejhodnotnějších „majetků“ podniku. Personální problematice je proto nutné věnovat stejně významnou pozornost, jako ostatním oblastem bezpečnosti.

Zabezpečení IS před nežádoucím negativním vlivem lidského faktoru zajišťuje personální bezpečnost. Hlavním úkolem je nastavení a zavedení směrnic a požadavků na vlastnosti zaměstnanců IS, systém jejich výběru, zaškolení a výchovy a průběžných kontrol. Nejčastěji opomíjenou částí počítačové bezpečnosti je správné chování k zaměstnancům a sledování jejich životního cyklu ve firmě.

5.2.2 Životní cyklus personálu

Životní cyklus personálu se skládá z následujících etap:

- *výběr nových zaměstnanců na základě předem definovaných požadavků*
- *základní příprava a zaškolení nových pracovníků*
- *průběžné zkvalitňování personálů*
- *ukončení pracovního poměru a odchod z pracoviště.*

Výběr nových zaměstnanců

Klíčovým cílem každé organizace je získání a následné udržení kvalitního personálů. V praxi tento úkol není tak jednoduchý. Už od přípravy popisu práce určité pozice, zaměstnavatel musí zvážit několik pohledů a kritérií. Prvním kritériem je stanovení odborných požadavků, včetně kvalifikace, jazykové znalosti, organizační a řídící schopnosti, praxe a podobně, samozřejmě, v závislosti na pracovní pozice. Druhým a neméně významným kritériem výběru musí být morální, osobní a pracovní vlastnosti kandidáta. Důležitými vlastnostmi jsou pracovní spolehlivost, poctivost, psychická odolnost a dobré rodinné zázemí. Odbornou kvalifikaci uchazeče je snadné změřit pomoci

přezkoušení znalostí ústní nebo písemnou formou. Morální hodnoty jsou těžko změřitelné. Zkušení HR manažeři ovládají různé techniky k posouzení morálních hodnot potenciálního kandidáta. Velký význam mají reference z minulých pracovišť a od předchozích nadřízených, doporučení vlastních zaměstnanců, kterým důvěřujeme, ale také i různé formy psychotestů. Od uchazečů je vhodné požadovat úřední výpis z rejstříku trestů a potvrzení od lékaře o nepoužívání drog a alkoholu.

Nejpřísnější kritéria musí splňovat uchazeči, u kterých se předpokládá přístup k citlivým informacím.

Základní příprava a zaškolení nových pracovníků

Každý nově přijatý zaměstnanec by se měl po seznámení s pracovní náplní seznámit i s bezpečnostními předpisy a směrnicemi organizace. Základními zásady jsou práce s důvěrnými informacemi, pravidelná změna hesla, odhlášení se od systému při opuštění pracoviště atd. Absolvování tohoto bezpečnostního školení je vhodné písemně potvrdit podpisem vyškoleného pracovníka. To vylučuje pozdější námitky a výmluvy pracovníků, že s těmito bezpečnostními pravidly nebyly seznámení. V případě určitých pozic je potřeba dodatečně provést odborné školení anebo online výuku.

Nově přijatý pracovník, obzvlášť v průběhu zkušebního období, by neměl mít přístup k citlivým informacím. S časem a se získáním důvěry by se jeho „bezpečnostní oprávnění“ mělo postupně zvyšovat. Je výhodné vytvořit několik typů uživatelů s přesně definovanými pravomocemi a jim příslušejícími oprávněními v IS. Příslušný pracovník IT po konzultaci s personálním oddělením by měl při přijetí zařadit zaměstnance do jedné z kategorií a podle toho postupovat při vytváření jeho uživatelského účtu. Tato standardní konfigurace může být kdykoliv modifikována dle potřeb firmy a/nebo konkrétního zaměstnance.

Průběžné zkvalitňování personálů

Kvalitní personál je největším majetkem firmy. Cílem každé firmy je udržení si kvalitního, zaškoleného a důvěryhodného personálu. Samozřejmě je to i otázka ochrany vložených investic do tohoto personálu. Dobrá firemní kultura a atmosféra, pocit sounáležitosti s organizací, pocit důležitosti a oceněni, hmotný stimul, pracovní perspektiva, sociální a rozvojové programy, jsou to jen některá z faktorů, ovlivňujících rozhodnutí zaměstnance zůstat ve firmě.

Bezpečnostní kvality se dosahuje trénováním, kontrolou dodržování bezpečnostních požadavků a směrnic a průběžnými bezpečnostními školeními. Je důležité včasné zjišťování příčin negativních jednání pracovníků, analýza příčin a následné zapracování závěrů do opatření, která takovému jednání mají v budoucnu zamezit.

Zaměstnanci by měli být seznámeni se všemi směrnicemi týkajícími se jejich odpovědnosti za bezpečné využívání IS. Nedílnou součástí školení mají být i základy

bezpečného chování – řada pracovníků například dost dobře nechápe, že heslo je tajná informace, která se nesděluje spolupracovníkům, ani nepoznamenává na kousek papíru přilepený na monitor.

Proškolit by se měli i pracovníci oddělení IT. Jejich úkolem je nejen konfigurace konkrétních bezpečnostních prostředků, ale také školení řadových uživatelů. Pracovnici IT musí být seznámeni s bezpečnostní politikou firmy i konkrétními směrnicemi, kterým by měli rozumět.

Ukončení pracovního poměru a odchod z pracoviště

Při rozvázání pracovního poměru může docházet k nepříjemným záležitostem. Odcházející zaměstnanec si s sebou odnáší také všechny vědomosti, firemní zkušenosti a informace včetně důvěrných, které během působení ve své funkci získal. Zaměstnavatel navíc ztrácí přehled o jeho další činnosti. Při rozvázání pracovního poměru musí být odcházející pracovník poučen o svých povinnostech vůči bývalému zaměstnavateli. Řada firem vyžaduje zachování mlčenlivosti po určitou dobu po jeho odchodu ze zaměstnání. Některé firmy při podpisu pracovní smlouvy zavazují své zaměstnance, že v případě odchodu, nemohou být zaměstnáni v konkurenční firmě po určitou dobu po ukončení pracovní smlouvy.

Ze strany IT, kromě fyzického odebrání počítače a jeho případné reinstalace pro nového zaměstnance, je třeba zrušit všechna oprávnění v IS (zrušit emailovou schránku, změnit případná sdílená hesla, ke kterým měl zaměstnanec přístup, vyřadit adresu jeho notebooku z firewallu a podobně), která zaměstnanec za svou kariéru ve firmě nasbíral.

Směrnice a nařízení jako opatření

Základním dokumentem firemní bezpečnosti je bezpečnostní politika firmy. Její součástí jsou informace o analýze rizik a zvolených bezpečnostních opatřeních, havarijní plány pro jednotlivé krizové situace a základní principy personální politiky z bezpečnostního hlediska.

Úkolem těchto směrnic by mělo být podávání konkrétních návodů k řešení všech situací. Tyto směrnice se vytváří ve spolupráci s vedoucími pracovníky příslušných oddělení.

Velká část nařízení se týká pracovníků oddělení IT. Nařízení musí stanovit postupy při vytváření jednotlivých uživatelských účtů, jejich modifikaci i rušení. Nařízení se má týkat i konfigurací jednotlivých konkrétních programů, zajištění fyzické bezpečnosti a podobně.

Zbývající směrnice se týká běžných uživatelů. Tato směrnice řeší pravidla používání firemní počítačové sítě, stanovuje omezení a sankce za porušení těchto pravidel.

5.3 Komunikační a síťová bezpečnost

V rozsáhlých komunikačních systémech je velmi složité sledovat datové toky, jejich ukládání na média a distribuce. Jedná se o jedno z nejvíce zranitelných míst. Data mohou být napadena za různým účelem.

Jedná se o technické prostředky propojené v síti. Pokud není síť zabezpečená, tak nám vzniká nebezpečný kanál, přes který může dojít úniku dat a informací. Mezi hrozby síťové bezpečnosti můžeme zařadit:

- **odposlech dat** - útočník má dvě možnosti: komunikaci jen pasivně odposlouchávat, nebo se stát aktivním prostředníkem, který komunikaci zprostředkovává. Proti uvedenému útoku se můžeme bránit pomocí zabezpečených komunikačních protokolů například HTTPS. Je pochopitelné, že se o této skutečnosti nemusí uživatel dozvědět.
- **sdílení dat** – různé složky, soubory, tiskárny umožňují v případě nezabezpečení jednoduchý přístup k datům a rychlému rozšíření virů včetně neoprávněné modifikace dat.
- **phishing** - jedná se o útok, během kterého přiměje útočník uživatele zadat jeho přihlašovací údaje na falešné přihlašovací stránce. Útočník vytvoří návnadu. Poté uživatelům rozešle odkaz na tuto stránku, často s textem o nutnosti přihlášení kvůli změně hesla. Pokud uživatel přistoupí na tuto hru a zadá své přihlašovací údaje, útočník je zneužije v opravdové službě, aby nevzbuzoval podezření. Moderní webové prohlížeče obsahují prvky obrany proti těmto útokům (kontrola proti známým phishingovým stránkám), mnohé napoví i nesouhlasící certifikát v případě šifrovaného spojení (HTTPS). Prioritou je ostražitost pokaždé, kdy nás libovolná služba vyzývá k přihlášení, změně hesla s odkazem na místo, kde se má zadání provést.
- **malware -** je program určený k poškození a infiltrace počítačového systému. Jedná se o různé viry, trojské koně a další. Může se jednat o destruktivní dopad, nebo se snažit získat kontrolu nad infikovaným objektem. Napadený objekt se může stát součástí tzv. botnetu, který se využije například k rozesílání spamu atd. Jedna z možností je sledování aktivity uživatele a získání citlivých dat, například přihlašovacích údajů k webovým službám a jiných přístupů. Základem ochrany proti malware je pravidelná aktualizace operačního systému, komunikačních aplikací, použití antivirového programu, sítového firewallu a jejich aktualizace. Samozřejmostí by měla být zvýšená obezřetnost při stahování softwaru a spouštění z neznámých zdrojů.

Ochrana proti těmto útokům

- ochrana integrity síťového kanálu
- šifrování přenášených dat

- autentizace spojení
- detekce integrity zpráv
- kontrola a monitorování externích zařízení (usb flash, ext. HDD atd)

SIEM (Security Information and Event Management**)**

SIEM řeší incidenty na základě předdefinovaných pravidel, což přináší včasné upozornění na kritické události a řízení bezpečnosti napříč celou společností.

Obrázek 9 Systém pro správu bezpečnostních informací – vstupy a výstupy

[http://www.systemonline.cz/it-security/it-bezpecnost-2.0-od-technologii-k-procesum.htm]

Systém nám zajišťuje:

- reálný sběr dat a logů
- reporting
- analýzu incidentů
- generování výstrah
- souvztažnost událostí

Hlavní důvod nasazení je snížení počtu bezpečnostních událostí.

6 Právní a etické aspekty bezpečnosti IS

6.1 Právní ochrana informací

Ochranu software můžeme rozdělit na více částí - právní ochrana informací dle autorského zákona, softwarové patenty, trestního zákoníku, ochrana proti nekalé soutěži jednání zaměstnanců.

6.1.1 Ochrana autorskoprávní

Za autorské dílo je považován software, jehož vlastnictví řeší Autorský zákon. Jako literární dílo musí být chráněný programy a mít shodnou úroveň ochrany, jak stanoví úmluva z pohledu počítačových programů. Autorský zákon říká, že „počítačový program, bez ohledu na formu jeho vyjádření, včetně přípravných koncepčních materiálů, je chráněn jako dílo literární“. [4]

Úprava autorských práv je dána právem státu[5], na kterém území autorské vztahy vznikly. V případě, že v České republice oprávněný vlastník nabyl licenci k počítačovému programu, bude se na něj vztahovat autorský zákon, dle právního řadu České republiky. Autorské právo v České republice upravuje zákon č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů ve znění pozdějších předpisů.

6.1.2 Ochrana právem osobností

Autorem se může stát člověk, tedy fyzická osoba, která vytvoří autorské dílo. Autorství se nemůže koupit, postoupit nebo převést. Autor se nemůže vzdát osobnostních práv. Práva jsou chráněna po smrti autora a nepřevoditelná. Stejné téma mohou stvořit dva autoři, ale každý z nich stvoří jiné autorské dílo. Autor má nárok na rozhodnutí zveřejnění svého autorského díla a nárokovat si autorství. Autor, který vytvoří autorské dílo zůstane navždy autorem.

Předmětem dědictví mohou být majetková práva autora a mohou být autorem převedena na jinou osobu. Patří sem právo rozmnožovat, pronajímat a vystavovat díla.

6.1.3 Autorskoprávní nároky

Pokud dojde k neoprávněnému zásahu do majetkových a osobnostních práv, může si poškozený nárokovat následující:

[4] Srov. § 65 odst. 1 autorského zákona.

Satisfakce – v případě finanční satisfakce je možná dohoda mezi žalobcem a žalovaným. Jedna z možností je omluva a finanční vypořádání. Dle okolností soud určí výši peněžní satisfakce a přihlédne k závažnosti.

- Určení autorství – potvrzení o svém autorství, že je nositelem autorských práv si může nárokovat poškozený.
- Zakázat neoprávněný zásah do svého práva – pokud došlo k neoprávněnému zásahu práv poškozeného, může dojít k výzvě ukončení činnosti.
- Zveřejnění rozsudku – žalobce může v případě úspěšnosti požadovat pokrytí soudních nákladů. Soud určí rozsah pokrytí.
- Odškodnění za způsobenou škodu – poškozený má nárok na náhradu ušlého zisku ceny licence software dle platného ceníku v době porušení autorských práv.
- Konsekvence následků – v případě neoprávněných napodobenin má poškozený nárok na jejich odstranění.

6.1.4 Licenční smlouva

V obchodním zákoníku a v jednotlivých právních zákonech najdeme ustanovení o licenční smlouvě. Licenční smlouva je přímo upravena autorským zákonem jako základní smluvní typ autorského práva. Jako autor a nabyvatel bývají označeny licenční smlouvy.

Nabyvatel licence je oprávněný licenční dílo užívat. Licence mohou být nevýhradní nebo výhradní (či exkluzivní). Pokud se jedná o výhradní licenci, tak autor nemá oprávnění s dílem sám dále nakládat.

Licence se uděluje za úplatu či bez nároku autora na odměnu. Rozsah omezení licence může být, a to buď:

- omezením časovým
- regionem působností
- počtem (např. umožnění instalace programu jen na jednom PC)
- kvalitou

Členění software z hlediska obsahu licence

- **Software svobodný** – může být šířen za poplatek nebo zdarma, je volně šiřitelný a povoleno jeho užívání. Jsou povolené dostatečné změny původní verze. Do svobodného software spadá Public domain, Open Source, software s GNU GPL licencí. Zdrojový kód musí být dostupný
- **Software nesvobodný** – uživatel nemá k dispozici zdrojový kód a nesmí provádět úpravy díla.

„Další typy licencí jsou OEM, copyleft, multilicence, transakční licence v cloudu atd.

Dle Autorského zákoníku lze licenční smlouvu uzavřít i specifickým způsobem:

- *Shrink wrap – otevřením krabice*
- *Click wrap – odkliknutím licenčních podmínek po instalaci SW*
- *Browse wrap – potvrzením návštěvou odkazu na Internetu*

Obsahové náležitosti licenční smlouvy

- *Specifikace SW*
- *Způsob používání SW*
- *Rozsah licence (množstevní, časové, územní…)*
- *Odměna za licenci (jednorázová nebo formou licenčních poplatků) nebo bezúplatnost*
- *Právo na přiměřenou dodatečnou odměnu (v případě, že nabyvatel vytvoří s vyžitím licencovaného sw zisk řádově neúměrný odměně za licenci*“ (Danel)

6.1.5 Ochrana patentová

Jak bylo zmíněno již výše, právní úprava ochrany software je v České republice upravena autorským zákonem. Stejně jako laterální dílo je počítačový program chráněn autorským zákonem.

„*Co se patentovatelnosti software týče, platí ze zákona, že „kdokoli smí vytvořit software shodné funkcionality, pokud to není protiprávní“. Za protiprávní se považuje např. využití zdrojového kódu získaného reverzním inženýrstvím.*

Předmětem patentu nemůže být vizuální podoba software. Výjimkou je situace, kdy dojde k porušení zákazu nekalé soutěže. Do této kategorie patří situace, kdy software napodobuje vzhled úspěšného software a parazituje na pověsti a úspěchu cizího SW.

Ochrana software patenty byla Evropským patentovým úřadem zamítnuta; počítačový program není považován za vynález. Výjimkou je stav, kdy software má prokazatelný technický efekt“ (Danel)[6]

6.1.6 Právní ochrana informací a dat

V současné době nám informační technologie umožňují zpracovat velké množství dat. Dříve lidé neměli takový velký přístup k mnoha informacím. Značně narostlo riziko průnik do soukromí člověka. Proto významnou roli zvýšení důvěry uživatelů zastává ochrana osobních údajů.

Hlavním zákonem, který upravuje ochranu osobních údajů v České republice je zákon č. 101/2000 Sb., zákon o ochraně osobních údajů a o změně některých zákonů (dále

[6] Jansa, L. - Otveřel, P.: Softwarové právo - praktický průvodce právní problematikou v IT. ComputerPress Brno, 2011. ISBN 978-80-251-3458-0

jen „zákon o ochraně osobních údajů“), který je nedílnou součástí právního řádu České republiky, a to ve dvou směrech[7]

6.2 Etické aspekty bezpečnosti IT

Bezpečnostní pracovníci IT ve většině případů mají přístup k důvěrným informacím a údajům. Ovládají sítě a systémy společnosti, a to vše jim dává velkou moc. Tato pravomoc může být zneužita, a to buď úmyslně, nebo neúmyslně. V současné době neexistují žádné standardizované požadavky pro bezpečnostní IT personál. Sdružení a organizace pro IT profesionál začínají řešit etické otázky, ale opět tam chybí požadavek pro bezpečnostní IT pracovníky, aby k těmto organizacím patřili.

Etika je filozofická disciplína. Předmětem etiky jsou hodnotící soudy, které se rozlišují pochopením dobrého a špatného. Informační etika je dílčí částí samotné etiky, která se zabývá morálními principy a pravidly souvisejícími se zpracováním důvěrných informací. Etika by se měla tedy zaměřovat na pravidla správného lidského chování a jejich uplatňování v praxi.

V současné době, kdy role internetu hraje nesmírnou úlohu, vzniká otázka, je-li informační etika určitou aplikací standardní etiky do IT, anebo jde o novou etickou teorii vyvolanou závažnými změnami, které souvisejí s rapidním rozvojem v oblasti IT.

Informační etika by měla být nástrojem, jak hodnotit, zda nakládání s informacemi je správné či nesprávné, a také k posouzení širších dopadů vybraných struktur použitých transformací informací.

Podobně jako v ekonomice, se rozděluje informační etika na mikroetiku a makroetiku. Mikroetika se zabývá mikroetickými problémy, např. ochranou duševní vlastnictví. Makroetika se věnuje makroetickým problémům, které souvisejí s dopady IT na organizaci.

Mikroetický problém

- obchod s osobními údaji
- nedodržování citačních zásad
- respektování autorských práv
- obchodní tajemství
- počítačová kriminalita
- falšování informací
- soukromí

[7] Ochrana osobních údajů. Vybrané otázky. Příručka pro podnikatele., Tisk: TRIBUN EU, s. r. o. Pro Úřad pro ochranu osobních údajů vydala Masarykova univerzita, 2011. ISBN 978-80-210-5572-8

Makroetický problém

- digitální rozdělení společnosti
- spojení IT a moci
- IT ve výuce

7 Doporučení pro tvorbu IT směrnic, havarijního plánu a bezpečnostní politiky

7.1 Havarijní plán

Havarijní plán, nebo-li DRP (disaster recovery plans), je jednou z hlavních součástí IS organizace. Jedná se o soupis bodů, jak se zachovat v případě neočekávané havárie a udržet chod informačních technologií, a pokud je to možné - eliminovat možné ztráty. Může dojít k selhání hardwaru, poškození přírodními živly, selhání lidského faktoru, nebo napadení IS. Pomocí důkladné analýzy rizik a dopadům můžeme rizikům předcházet, nebo je omezit. Pokud si určíme rizikové oblasti organizace, je možné si vypracovat seznam jednotlivých bodů opatření. Veškeré náklady na obnovu musí být v rovnováze s dopadem na organizaci.

Organizace při aplikování DRP musí provést aktualizace interních dokumentů, seznámit kompetentní osoby, a v případě dodávky služeb externí organizaci, projednat změnu smluvních vztahů. Havarijní plán musí obsahovat soupis činností, jak postupovat v případě mimořádné události. Musí se vytvořit seznam osob a kontaktů, které budou neprodleně informovány v případě havárie, kontakty na externí organizace zajišťující dodávku služeb, plán obnovy. Součásti má být plán nouzového provozu, který udrží provoz v omezené míře do doby navrácení stabilního stavu. V plánech je dobré uvést odhadnutou dobu realizace obnovy.

Příprava havarijního plánu

- analýza rizik
- zmapování procesů organizace
- implementování havarijního plánování
- testování funkčnosti

Analýza rizik

Rozdělení jednotlivých rizik dle jejich dopadů. Analýza se provádí na samém počátku každého bezpečnostního projektu.

Zmapování procesů organizace

Musí být vytipovány jednotlivé procesy organizace, které jsou závislé na běhu IS. Budou popsány zdroje, které se podílejí na chodu procesů, jejich selhání by ohrozilo plynulý chod organizace. Zpracuje se odhad skutečných finančních ztrát.

Implementování havarijního plánování

Jedná se o proces seznámení zaměstnanců s požadavky, které jsou na ně kladeny. Spuštění nácviku, při kterém se ověří účinnost DPR.

Testování funkčností

Převážně se provádí 1x za rok. Ověřuje se funkčnost a zakomponují se nové změny.

Hlavní zásady plánu obnovy

- rozdělení priority obnovy, kritické zdroje se obnovují např. do 30 minut, další do 4 hodin atd.
- provádět roční revizi používaných aplikací a roztřídit je dle priorit obnovy
- držet pohotovostní tým
- vytvořit plán na udržení kritických aplikací
- definovat uchování záznamů po havárii
- jasně definovat povinnosti zaměstnanců při procesu obnovy[8]

7.2 IT Směrnice

Bezpečnostní politika firmy je jedním ze základních dokumentů bezpečnosti firmy. Jejím obsahem je havarijní plán krizových situací, bezpečnostní opatření a personální politika. Technické pojmy bezpečnostní politiky nejsou moc srozumitelné většině uživatelů, a z tohoto důvodu se vytváří konkrétní směrnice a nařízení.

Směrnice je návodem k řešení vyskytujících se situací. Do procesu tvorby směrnice by měl vždy být zapojen člověk znalý firemních předpisů, jako je např. manažér odpovědný za politiku integrovaného systému managementu (ISM). Převážně se do připomínkování dané směrnice zapojí tým vrcholového managementu. Velká část nařízení se týká zaměstnanců IT oddělení. Řeší pravidla používání IT, stanovuje omezení i sankce. Oblast bezpečnosti by se měla promítnout do pracovního řádu příslušné společnosti.

7.3 Zásady bezpečnosti IT pro uživatele

Obecná pravidla

- Všechny pracovní stanice, servery, technické komponenty, počítačové sítě a programové vybavení IS společnosti jsou považované za výhradní vlastnictví společnosti a mohou být používané jen pro pracovní účely.
- Všechny informace a údaje (data) v IS společnosti, jsou považované za její výhradní vlastnictví a musí být zpracovávané jako důvěrné. Prozrazení nebo

[8] HALBICH Čestmír, BRECHLEROVÁ Dagmar, Bezpečnost informačních systémů vybrané kapitoly, Česká zemědělská univerzita v Praze, 2003, 96 stran. ISBN: 80-213-1090-1

zpřístupnění informací neoprávněným osobám je zakázáno a bude postihováno v souladu s personální politikou společnosti.

- Zaměstnanec zodpovídá za ochranu aktiv IS (PC, servery, technické zařízení, údaje apod.) před jejich prozrazením, zpřístupněním neoprávněným osobám, zničením nebo krádeží, dodržováním opatření stanovených ve směrnicích, předpisech a pracovních postupech společnosti.
- Zaměstnanci nesmí zneužívat výpočetní zdroje společnosti na činnosti, které nesouvisí s jejich pracovní náplní, nebo můžou vést k omezení práce ostatních uživatelů (rozesílání hromadných nebo řetězových zpráv elektronické pošty, nadměrné trávení času na internetu).

Hesla

- Zaměstnanec zodpovídá za správu svých přístupových hesel do systémů společnosti a ručí za nezneužití svých hesel a za aktivity, které byly v systému vykonané pod jeho uživatelským jménem, pokud se neprokáže opak.
- Heslo do počítačové sítě společnosti se mění každých 60 dnů, opakovaní hesel je možné nejdříve po použití 5 jiných hesel.
- Zvolené heslo je nutné udržovat v tajnosti, to především znamená:
    - Své heslo se nesmí nikomu sdělit (správci systémů mají vlastní účty se silným oprávněním, zajišťující jim dostatečné oprávnění pro podporu IT).
    - Hesla se nesmí nikam poznamenávat v textové formě (např. do souborů).
    - Přednastavená hesla (např. nově zřízený přístup do aplikace) je nutné co nejdříve nahradit vlastními hesly.
    - Nepoužívat v soukromí stejná hesla, jako na pracovišti.
    - Ztrátu, prozrazení nebo podezření na prozrazení hesla je zaměstnanec povinen ihned hlásit zodpovědnému zaměstnanci oddělení IT.
- Pro tvorbu hesla platí následující pravidla:
    - Hesla musí mít délku nejméně šesti znaků.
    - Jako heslo se nesmí zvolit pravidelné tvary na klávesnici, data, ani slova ze slovníků.
    - Musí se použít nejméně dva z následujících druhů znaků - velká písmena, malá písmena, čísla (např. Ufe59J8).

Dodatečné metody ochrany přístupu

Pokud pro přístup do některých aplikací je nutná další ochrana přístupu (např. čipová karta pro přístup k bance), je pracovník vlastnící tyto prostředky povinen:

- Zajistit bezpečnost těchto prostředků proti zneužití
- Okamžitě svému nadřízenému a vedoucímu útvaru IT hlásit ztrátu těchto prostředků

Opuštění pracoviště

Při jakémkoli, i krátkodobém opuštění pracoviště, je zaměstnanec povinen zajistit PC proti neoprávněnému užití:

- Vypnutím PC
- Uzamčením obrazovky chráněné heslem

V opačném případě odpovídá za případné škody uživatel, pod kterým byly provedeny aktivity směřující ke škodě.

Zaměstnanec musí zabezpečit, aby se před odchodem z pracoviště na jeho pracovním místě nenacházely volně dostupné důvěrné nebo jinak citlivé materiály a dokumenty.

Neoprávněný přístup

Je zakázáno jakýmkoli způsobem se pokoušet získat neoprávněný přístup nad rámec přístupů nezbytně nutných pro určené pracovní činnosti.

Bezpečnost dat

Každý zaměstnanec musí zajistit maximální možnou ochranu dat. V případě, že není určen stupeň citlivosti dat, přistupuje se k datům jako důvěrným.

Citlivosti dat

Data jsou v následujících třídách citlivosti:

- Veřejná – veřejně přístupná data
- Důvěrná – tvoří obchodní tajemství firmy
- Tajná
- Přísně tajná

Stupeň citlivosti dat určuje vedoucí oddělení, kde data vznikají, nebo jsou zpracovávány.

Zálohování osobních dat

Data je nutné ukládat na síťové disky. Tajná a přísně tajná data musí být uložena v příslušných složkách definovaných níže, viz. Pravidla pro umístění dat.

Data na lokálních discích nejsou zálohována a jejich bezpečnost je plně v odpovědnosti uživatele.

Manipulace s přenosnými datovými médii

Je zakázáno ukládat na přenosná média (CD, DVD, Flash disky) data s citlivostí důvěrná, tajná a přísně tajná.

Pravidla pro umístění dat

Zaměstnanec má k dispozici následující základní síťové disky:

- srv2\public:\ „Společná složka“. Slouží pro sdílení velkokapacitních dokumentů mezi uživateli z různých úseků.
- srv2\0000XX:\ Obsahuje síťové aplikace, složky jednotlivých skupin uživatelů. Slouží pro sdílení dokumentů mezi zaměstnanci stejného úseku.
- srv2\xyz:\Osobní složka s přístupem jen pro daného zaměstnance.

Instalace a použití hardware a software

Je zakázáno:

- Instalovat na zařízení společnosti SW bez souhlasu vedoucího oddělení IT.
- Připojovat cizí zařízení k síti společnosti.
- Měnit jakkoli HW společnosti (instalace pamětí, karet …).
- Přenášet nebo přepojovat zařízení (s výjimkou mobilních zařízení) bez souhlasu vedoucího oddělení IT.
- Měnit jakkoli nastavení počítače mající vliv na bezpečnost.
- Zaměstnanec není oprávněn modifikovat programové vybavení nebo nastavení pracovních stanic. V případě tohoto požadavku je potřebné kontaktovat autorizované zaměstnance zodpovědné za oblast informačních technologií (oddělení Informačních technologií).
- Zaměstnanci zodpovídají za dodržování autorských práv a licenčních podmínek, které se vztahují k materiálům a programům, které používají. Je zakázáno vytvářet nelegální kopie materiálů a programů, které jsou chráněny autorskými právy, nebo zpřístupnit tyto materiály jiným zaměstnancům pro potřeby kopírování.
- Je zakázáno vyslovit souhlas s licenčními podmínkami bez písemného souhlasu vedoucího oddělení IT, případně zodpovědného autorizovaného zaměstnance. Je také zakázáno stahovat materiál, za který se vybírají poplatky bez písemného souhlasu vedoucího oddělení IT.

Použití elektronické pošty

Je zakázáno:

- Přesměrovávat firemní e-mail na jakékoliv schránky mimo společnost a obráceně.
- Přistupovat z firmy k jiným, než firemním e-mailovým účtům (přidávat soukromé účty do aplikace Outlook …).

- Elektronická pošta standardně nezaručuje důvěrnost přenášených údajů, proto prostřednictvím ní nesmí být posílány důvěrné informace. V případě takového požadavku je potřeba kontaktovat zodpovědné zaměstnance IT, kteří dodatečnými prostředky zajistí bezpečnost přenášených údajů.
- Je zakázáno využívat elektronickou poštu na posílání urážlivých, výhružných, útočných, rasistických, pornografických, řetězových a jiných nevhodných zpráv. Takové zprávy poškozují dobré jméno společnosti a vůči odesilateli budou vyvozeny důsledky v souladu s personální politikou společnosti.

Ochrana před viry a spyware

- Na antivirovou ochranu pracovních stanic je primárně určen schválený systém, který je automaticky pravidelně aktualizován. Jeho odinstalování, zablokování nebo změna konfigurace je zakázána.
- Před instalací aplikací, software a utilit musí být instalační média zkontrolována na přítomnost virů. Je zakázáno instalovat programy přímo z internetu.
- Je zakázáno spouštět nevyžádané, podezřelé přílohy elektronické pošty od neznámých odesilatelů, stahovat zakázané soubory z internetu a jiných veřejných sítí, používat diskety nebo pevné disky z jiných zdrojů než ze společnosti a pod. V případě potřeby spouštění nebo uložení podezřelého souboru musí být nejdříve zaměstnancem IT vykonána kontrola na přítomnost virů.
- V případě podezření z napadení virem je potřebné tuto skutečnost okamžitě hlásit příslušnému zaměstnanci oddělení IT, který vykoná potřebná opatření. Až do jeho příchodu je zakázáno používat „nakaženou“ pracovní stanici. Zaměstnanci se nesmí pokoušet vymazat, nebo jinak odstranit podezřelý soubor.
- V případě „nakažení“ pracovní stanice nebo počítačové sítě společnosti, které je důsledkem nedodržení uvedených pravidel, budou vůči zaměstnanci vyvozeny důsledky v souladu s personální politikou společnosti.

Příznaky možné virové infekce mohou zahrnovat:

- Nevysvětlitelné chování systému (např. častý výskyt chybových hlášení, pády programů, pády celého počítače atd.).
- Neustálý pokles dostupné paměti.
- Nevysvětlitelně pomalé síťové připojení.

Mobilní zařízení

Tyto zásady se týkají mobilních zařízení, na kterých jsou data společnosti. Jedná se zejména o:

- Notebooky
- PDA
- Mobilní telefony

- Flash paměti

Přístupy a ukládání dat:

- Přístup k těmto zařízením musí být pokud možno zajištěn heslem.
- Tajná a přísně tajná data musí být pokud možno šifrována.

Ochrana proti zneužití dat a zařízení:

- Nesmí se umožnit neoprávněným osobám sledovat obrazovku počítače.
- Při cestách letadlem nesmíte odbavovat přenosná IT zařízení jako zavazadla.
- Nesmíte nechávat přenosná IT zařízení na viditelném místě ve vašem automobilu nebo v hotelovém pokoji.
- Zařízení ukládat v trezoru hotelu – nenechávat na recepci.

Internet

- Nestahovat žádná data z internetu s výjimkou dat potřebných pro práci v rámci organizace.
- Využívat přístupu k internetu pouze pro pracovní účely.
- Jakékoli podezřelé chování hlásit pracovníkům IT.
- Používání veřejných služeb (elektronická pošta, hostování webových stránek) a účast na veřejných internetových fórech s použitím firemní adresy elektronické pošty nebo uživatelského jména společnosti a odvozenin je zakázáno, pokud není specificky vyžadováno pro pracovní účely.
- Zvláště je zakázáno:
    - Přistupovat k sociálním sítím (Facebook, Twitter atd.).
    - Messenger s výjimkou služeb využívaných společností a schválených vedoucím útvaru IT.
    - Přistupovat ke schránkám zábavného charakteru.

Monitorování práce

- Veškerá komunikace prostřednictvím elektronických kanálů společnosti a všechny údaje zpracované v IS, se pokládají za pracovní. Vzhledem k tomu může společnost monitorovat všechny aktivity v IS.

8 Závěr

Spolu s vývojem nových informačních technologií dochází současně ke zvyšování rizik, která ohrožují tyto technologie. Ochrana informačních systémů proti úmyslným a neúmyslným útokům by měla být hlavní prioritou všech uživatelů systémů. K zajištění informační bezpečnosti v malých i velkých firmách je třeba nalezení efektivních metod a postupů. V současné době existuje velké množství metodik, které směřují k optimalizaci a efektivnímu řízení v oblasti informační bezpečnosti. Podmínkou úspěchu zavedení těchto metodik je výborná znalost prostředí, zajištění příčin rizik a schopnost omezit, nejlépe zcela zabránit možným útokům na systém. Důležité je správné nastavení těchto metodik pro konkrétní prostředí organizace a následné dodržování zásad bezpečnosti a pravidelná kontrola. Není výjimkou, že se metodiky kombinují, aby se dosáhlo maximálního splnění požadavků na dané prostředí. V případě úspěšné aplikace dosáhne firma významných úspor, spolehlivosti a efektivity ve využívání informačních systémů. Dosáhne minimalizace možných ztrát, které vzniknou v důsledku zneužití a poškození těchto systémů.

Obsahem teoretické části práce byla analýza dostupných metodik pro bezpečnost informačních systému. Byly popsány procesy metodik COBIT, ITIL, zhodnocení kritérií metodik a v závěru kapitoly porovnání těchto metodik. V kapitole komunikační a síťová bezpečnost byla uvedena možná rizika v nezabezpečené počítačové síti a doporučená ochrana proti těmto útokům. V další teoretické části byly zmíněny právní, personální a etické aspekty zaměřené na ochranu osobních údajů a autorského zákona. V předposlední kapitole jsou uvedena doporučení na vytvoření havarijního plánu a formulace zásad bezpečnosti IT pro uživatele.

Výsledkem této práce je zprůhlednění většiny procesů informačních technologií, nastavení bezpečnosti před ztrátou dat a efektivnější využití výpočetní techniky po zavedení pravidel bezpečnostní politiky. Na základě provedené podrobné analýzy a zavedení nových bezpečnostních standardů došlo ke snížení rizik souvisejících s nedostupností, únikem či ztrátou dat. Po aplikování metodiky řízení incidentů a instalaci samoobslužného portálu, byla zavedena evidence incidentů a vytvořena znalostní báze pro další řešení, která přinesla uživatelům mnohonásobně kratší dobu při řešení zadaných incidentů. Další úsporu přineslo zavedení zásady bezpečnosti IT pro uživatele, která byla největším přínosem pro IT oddělení, kde na základě těchto pravidel došlo ke snížení incidentů a ztrátě dat. Zásluhou obnoveného hardwaru s nižší spotřebou byla uspořena elektrická energie. Po kompletní obměně počítačových stanic a přenosných počítačů byl u těchto zařízení nastaven servis s odezvou na odstranění závady do 24 hodin a tím vznikla další časová úspora ve prospěch IT oddělení. Zavedením centrálního tisku došlo k optimalizaci nákladů na polovinu v porovnání se stávajícím stavem.

Nastavení a doporučení nových pravidel vedlo k úspoře jednoho personálního obsazení na IT oddělení z tříčlenné skupiny na dvoučlennou. Všechny tyto metodiky a pravidla přinesly zjednodušení a zrychlení práce zaměstnanců a ekonomický užitek společnosti.

SEZNAM POUŽITÉ LITERATURY

[1] DANEL, Roman. Metodiky řízení ICT: ITIL, COBIT, IT GOVERNANCE. [online]. [cit.2015-03-15].Dostupné z: <http://homel.vsb.cz/~dan11/aps/texty/Danel%20-%20APS%20-%20Metodiky%20rizeni%20ICT.pdf>.

[2] DOBDA, L. Ochrana dat v informačních systémech. Praha: Grada, 2001, 286 stran.SBN: 80-7169-479-7

[3] DOUCEK, P. Řízení bezpečnosti informací. Praha: Professional Publishing, 2011, 240 stran. ISBN: 978-80-7431-050-8

[4] DOSEDĚL, T.: Počítačová bezpečnost a ochrana dat. ComputerPress 2004. 200 stran. ISBN: 80-251-0106-1

[5] HALBICH Čestmír, BRECHLEROVÁ Dagmar, Bezpečnost informačních systémů vybrané kapitoly, Česká zemědělská univerzita v Praze, 2003, 96 stran. ISBN: 80-213-1090-1

[6] HUBNER, M. Pohled nejen CIO na informační bezpečnost: příručka manažera. Praha: TATE International, 2012. ISBN: 978-80-86813-25-7

[7] JANSA, L. - Otveřel, P.: Softwarové právo - praktický průvodce právní problematikou v IT. ComputerPress Brno, 2011, 340 stran, ISBN: 978-80-251-3458-0.

[8] MAISNER Martin a kol., Základy softwarového práva, Praha: Wolters Kluwer ČR, 2011, 356 stran ISBN: 978-80-7357-638-7

[9] Ochrana osobních údajů.: Praha: Masarykova univerzita, 2011, 53 stran, ISBN: 978-80-210-5572-8

[10] POUR Jan, GÁLA Libor, ŠEDIVÁ Zuzana. Podniková informatika: Praha: Grada, 2009, 496 stran. ISBN: 978-80-247-2615-1

[11] PROCHÁZKA Jaroslav, KLIMEŠ Cyril. Provozujte IT jinak: Praha: Grada, 2011, 288 stran. ISBN: 978-80-247-4137-6

[12] POŽÁR, J. Informační bezpečnost. Plzeň: 2005, 311 stran. ISBN: 80-86898-38-5

[13] SMEJKAL Vladimír, RAIS Karel. Řízení rizik ve firmách a jiných organizací: Praha: Grada, 2013, 488 stran. ISBN: 978-80-247-4644-9

SEZNAM OBRÁZKŮ

SEZNAM TABULEK