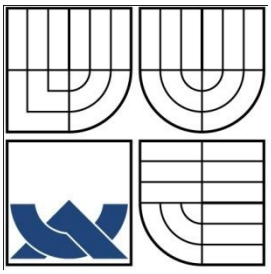
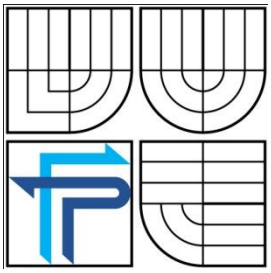


VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY



FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUT OF INFORMATICS

BEZPEČNOSTNÍ POLITIKA SPOLEČNOSTI
COMPANY´S SECURITY POLICY

BAKALÁŘSKÁ PRÁCE
BACHELOR´S THESIS

AUTOR PRÁCE
AUTHOR
DAGMAR SVOBODOVÁ

VEDOUCÍ PRÁCE
SUPERVISOR
ING. VIKTOR ONDRÁK, PH.D.

Brno 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/10
Ústav informatiky

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Dagmar Svobodová

Manažerská informatika (6209R021)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává bakalářskou práci s názvem:

Bezpečnostní politika společnosti

v anglickém jazyce:

Company´s Security Policy

Pokyny pro vypracování:

Úvod
Vymezení problému a cíle práce
Analýza současného stavu
Teoretická východiska řešení
Návrh řešení
Zhodnocení a závěr
Seznam použité literatury
Přílohy

Podle § 60 zákona č. 121/2000 Sb. (autorský zákon) v platném znění, je tato práce "Školním dílem". Využití této práce se řídí právním režimem autorského zákona. Citace povoluje Fakulta podnikatelská Vysokého učení technického v Brně. Podmínkou externího využití této práce je uzavření "Licenční smlouvy" dle autorského zákona.

Seznam odborné literatury:

CRAIGH HUNT. Konfigurace a správa sítí TCP/IP. 1.vydání. Computer press, 1997. ISBN: 80-7226-024-3.
DAVID W. CHAPMAN. Zapezpečení sítí CISCO PIX Firewall. 1.vydání. Brno, 2004.ISNB: 80-7226-963-1.
CRAIGH HUNT. Help for UNIX Systém Administrators, 2. vyd., Copyrigt, 1998. ISNB: 1-56592-322-7.
WENDELL O. CCIE Routing and Switching. 3.vydání. Cisco Press,2008. ISBN-10: 1-58720-196-8.

Vedoucí bakalářské práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/10.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ Fakulta podnikatelská

L.S.

Ing. Jiří Kříž, Ph.D.
Ředitel ústavu

doc. RNDr. Anna Putnová, Ph.D., MBA
Děkanka

V Brně, dne 7. 2. 2010

Abstrakt

Tato práce se zabývá zhodnocením stávajícího stavu zabezpečení informačních systémů a technologií v konkrétní firmě, stanovením optimálního řešení analyzovaných bezpečnostních rizik a sestavením návrhu na zlepšení.

Abstract

This thesis deals with an evaluation of the current security status of informatic systems and technologies in a specific company. It determines the optimal solution of analyzed security risks. The thesis also gives the proposals for improvements.

Klíčová slova

zranitelnost, hrozba, riziko, aktivum, bezpečnost, bezpečnostní politika, analýza rizik, řízení bezpečnosti, krizové plány, zálohování dat

Keywords

vulnerability, commination, gamble, asset, security, security policy, risk analysis, safety control, crysis plans, data backup

Bibliografická citace

SVOBODOVÁ, D. *Bezpečnostní politika společnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 79 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení:

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 15. května 2010 ……

Dagmar Svobodová

Poděkování

Děkuji vedoucímu mé bakalářské práce panu Ing. Viktoru Ondrákovi, Ph.D., za cenné rady, konzultace a připomínky, které mi poskytoval při zpracování mé bakalářské práce.

OBSAH

Úvod

Bezpečnost informací je v dnešní době stále více diskutované téma. Lidé čím dál tím více využívají informační technologie ve všech oblastech života a tím pádem roste i nebezpečí spojené se zneužitím těchto technologií. Zabránit těmto hrozbám lze soustavnou prevencí, která je však dnes velmi často podceňována.

Hlavním motivem této práce je upozornit na existující nedostatky v konfiguraci bezpečnosti a vytvořit koncept, který by měl pomáhat účinně minimalizovat rizika. Jako model pro moji práci posloužila firma E.ON Česká republika, s. r. o., která působí v oblasti energetiky. Vzhledem k stupni závislosti společnosti na IT technologiích jsem předpokládala dostatečnou informovanost o již existujících bezpečnostních opatřeních a jejich adekvátní implementaci.

Hlavní snahou mé práce je nalézt případné slabiny v zabezpečení, pro nalezené nedostatky navrhnout protiopatření a celkově zhodnotit úroveň zabezpečení, na jehož základě bych mohla navrhnout dodatečné ochranné prostředky.

Vycházím-li ze rčení, že bezpečnost není produkt, ale proces, musí být stanovena pravidla, která udrží úroveň bezpečnosti na požadované úrovni.

Vymezení problému a cíle práce

Cílem mé práce je na základě dostupných informací udělat analýzu současného provozního stavu v dodržování informačních bezpečnostních předpisů, a porovnáním s teoretickými předpoklady v řízení bezpečnosti a vnitropodnikovými bezpečnostními standardy, nelézt případné slabiny a na nalezené nedostatky navrhnout protiopatření, ať ve formě nápravy praktického dodržování bezpečnostních standardů nebo i případné doplnění bezpečnostních směrnic společnosti.

1. Analýza současného stavu

V této kapitole se zaměřím na analýzu části firmy, kde popíši strukturu společnosti, její vybavenost, závislost na hardwarovém a softwarovém vybavení, archivaci a zálohování dat a na základní prvky bezpečnostní politiky firmy. Z důvodu velikosti společnosti a rozsahu bakalářské práce se zaměřím na část realizovanou v oblasti Jižní Moravy.

1.1. Charakteristika firmy

Energetické společnosti působící ve světě pod značkou E.ON dodávají elektřinu, zemní plyn a související služby více než 25 milionům zákazníků v Evropě a USA. Společnosti skupiny E.ON v České republice dodávají elektřinu a plyn více jak 1,5mil zákazníků. Tuto skupinu tvoří následující společnosti:

- E.ON Česká republika, s.r.o. jako servisní společnost pro další společnosti,
- E.ON Energie, a.s., zajišťuje prodej elektřiny a plynu,
- E.ON Distribuce, a.s., zajišťuje správu distribuční techniky pro elektřinu a plyn,
- E.ON Trend s.r.o. , orientace na ekologickou výrobu el. energie,
- E.ON IT Česká republika, s.r.o., poskytovatel IT služeb pro skupinu v ČR,
- E.ON Servisní, s.r.o. vyčleněná provozní část E.ON ČR.

1.1.1 E.ON ČESKÁ REPUBLIKA, s.r.o.

Jedná se o společnost zaměřující se na servisní služby pro E.ON Distribuci, E.ON Trend, E.ON Energie a E.ON Servisní. Poskytuje služby technického charakteru, jako dispečerská služba, údržba technického zařízení atd., a služby netechnického zařízení, jako společné účetnictví, controlling, personalistika a péči o zákazníky, zahrnující marketing, call centrum a práci s veřejností.

Společnost E.ON ČR byla zapsána do obchodního rejstříku 2.února 1999 se sídlem České Budějovice, F.A. Gerstnera 2151/6, 370 00 s právní formou společnost s ručením omezeným.

Výpis z OR je uveden v příloze 1.

V souladu s koncepcí mateřské firmy E.ON Energie AG Germany, však nemá vlastní IT oddělení a IT služby nakupuje formou outsourcingu od společnosti E.ON IT. Nákup služeb je prováděn formou souborů SLA (Service Level Agreement) pro každou službu a takto nakoupené služby, jsou pak formou produktů distribuovány jednak do E.ON ČR a dále jsou přeprodávány do ostatních společností skupiny. Nejedná se však o úplně ryzí formu outsourcingu, neboť nezanedbatelná část služeb je poskytována na zařízení, které je v majetku E.ON ČR a E.ON Distribuce (jedná se zejména o síťovou a telekomunikační infrastrukturu). Tato koncepce je přizpůsobena legislativním požadavkům, kde dohled nad jejich dodržováním je v kompetenci ERÚ (Energetický regulační úřad).

1.1.2 Zákazníci

Společnost E.ON se zaměřuje na širokou řadu zákazníků v oblasti elektřiny a plynu (služby dodávky plynu jsou však omezeny jen na oblast Jižních Čech):

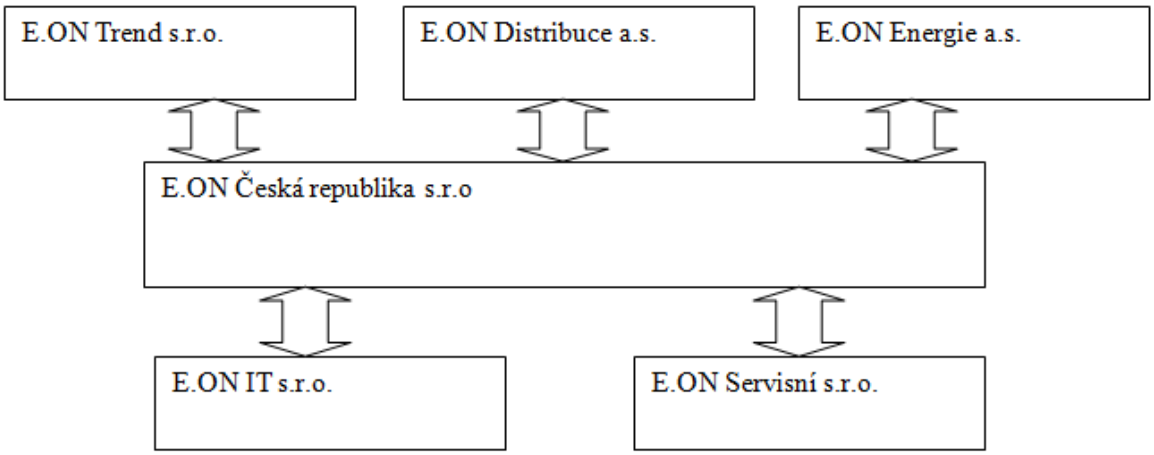
-Občané a domácnosti, cca 1,5 mil. odběrných míst pro dodávku elektřiny a cca 150 tis. odběrných míst pro dodávku plynu,

- podnikatelské subjekty, firmy a organizace,

-velkoodběratelé.

Lze konstatovat, že pro oblast maloodběru v oblasti jižních Čech a jižní Moravy jsou všichni lidé zákazníky společnosti E.ON. V oblasti distribuce nemá společnost konkurenci, tudíž každý subjekt, který odebírá elektřinu/plyn i od jiného jakéhokoliv dodavatele musí využívat „dráty“ a „trubky“ společnosti E.ON a tedy hradit poplatky spojené s distribucí médií.

1.1.3 Organizační struktura



Obrázek 1: Organizační struktura společnosti

Zdroj: vlastní.

1.2. Informační technologie používané ve firmě

V tomto bodě je nutné zmínit i historii společnosti a její předchůdce, neboť současný stav je do jisté míry ovlivněn IT strategiemi předchozích společností JME a JČE do konce r. 2004.

Společnost JME měla IT organicky začleněno jako „interní outsourcing“, kde Sekce IT vlastnila všechna ICT aktiva a náklady na provoz rozúčtovávala na jednotlivá NS[1] podle množství odebíraných služeb.

Společnost JČE vlastnila všechna ICT aktiva, ale správu těchto aktiv si nakupovala od externí společnosti IS Energy.

Vznikem společností E.ON v r. 2005 byly IT služby outsourcovány společností IS Energy s tím, že část aktiv (HW, PC, NB, periferie, servery a systémový SW) bylo převedeno do společnosti IS Energy, část aktiv (síťové a telekomunikační technologie

[1] Nákladové středisko

a aplikační SW jako ERP, SAP, GIS a speciální SW) zůstalo v majetku E.ON ČR a E.ON Distribuce. Správou všech těchto aktiv však byla pověřena společnost IS Energy. Obecné ICT standardy a strategie byla pak stanovována společnostmi E.ON ČR a IS Energy společně.

Přeměnou IS Energy na E.ON IS a nyní na E.ON IT s dominantním podílem společnosti E.ON IT Germany, přešla odpovědnost za tvorbu standardů a strategie na německou centrálu.

Je nutné poznamenat, že v návaznosti na postupné přemisťování rozhodovacích pravomocí na německou centrálu dochází k návratnému procesu, kdy část ICT aktiv, zejména dispečerská a řídící technika se vrací zpět jak správou, tak majetkově do útvarů E.ON ČR.

Nyní společnost E.ON IT hraje roli jediného dodavatele IT služeb a současně i roli systémového integrátora a správce HW i SW standardů. Záležitosti komunikačních technologií a vazba na komunikační operátory zůstávají však na E.ON ČR.

1.2.1 Poskytované služby – katalog

Tabulka 1: Katalog poskytovaných služeb

Zdroj: materiály poskytnuté firmou E.ON.

	Název IT produktu	Podrobnější definice
C401	Poskytování HW PC	PC dle aktuálního platného standardu vč. myši, klávesnice a monitoru. Na klientské stanici je nainstalován základní SW vybavení. Stanice je vybavena síťovou kartou pro připojení do LAN.
C402	Poskytování HW WS	PC ve výkonnější variantě dle platného standardu, dva monitory, duální grafická karta. Základní SW vybavení jako HW PC, určeno zejména pro pracoviště GIS.
C403	Poskytování HW NB	Notebook dle platného standardu, včetně 1ks myši, 1ks externí klávesnice a 1ks docking station. Základní SW vybavení. Stanice je vybavena sítovou kartou pro připojení do LAN. Součástí není externí monitor.
C404	Poskytování HW NB MANAGER	Služba je určena pro vyjmenované uživatele. Notebook - manager je ve stejné konfiguraci jako NB v rozšířené konfiguraci a vyšší úrovně podpory. Součástí není externí monitor.
C405	Poskytování HW typu Tiskárna1 (stolní A4/A3)	Tiskárny - lokální, dle schváleného standardu, A4/A3, čb/color, laser/inkoust.

C406	Poskytování HW typu Tiskárna2 (síť.tiskárna A4/A3)	Tiskárny - síťové, dle schváleného standardu, A4/A3, čb/color,
C407	Poskytování HW typu Plotr	Plotr - dle schváleného standardu, včetně síťové konektivity.
C408	Poskytování HW typu Periferie (scanner, tablet, docking st.)	Lokálně připojované periferie jako např. scaner, tablet, docking station, vypalovačky, čtečky čárkových kódů, přídavné monitory k NB a PC, lokální UPS, GPS apod., které nejsou součástí dodávky PC/NB/PDA.
C409	Poskytování HW typu PDA	PDA - Personal Digital Assistant, kapesní počítač, nebo smartphone podle platných standardů. Pokut obsahuje SIM kartu, je nutná provázanost na produkt 429. Umožňuje synchronizaci a přístup na Exchange (email, Kalendář, Poznámky, Úkoly), Word, Excel.
C410	Služba VIS - (e-mail,MS Office, Intranet)	Vnitropodnikový informační systém, přístup k elektronické poště, intranetu, na sdílené disky a sadu SW aplikací MS Office.
C411	Služba INTERNET	Povolení přístupu na Internet včetně bezpečnostních opatření.
C412	SAP R/3	Přidělení přístupů na základní sadu modulů SAP R/3, počítá se jeden ks produktu nezávisle na počtu používaných modulů.
C413	SAP IS-U	Zákaznický informační systém SAP IS-U podporující procesy evidence smluv, správy přístrojů, správy odečtů, fakturace, správy pohledávek, komunikace s OTE a další související aktivity.
C414	SAP BW	Přidělení přístupu do SAP BW - centrální datový sklad.
C415	SAP CRM	Zákaznický informační systém SAP CRM podporující procesy komunikace se zákazníky, včetně správy smluv a vazeb na systém SAP IS-U.
C416	TIS technický informační systém	Instalace a údržba software TOMS, vč. serverové části aplikací a databázového klienta. Seznam modulů TOMS: FM – technická evidence, MNT – údržba, PLN – Rozvoj a žádosti, OPR – Provoz, CNS – Výstavba, DES - Projekty. Počítá se jeden ks produktu nezávisle na počtu používaných modulů.
C417	GIS grafický informační systém	Instalace a údržba SW pro grafickou a geografickou dokumentaci prvků el. a plyn. distribuční soustavy, vč. údržby serverové části aplikací a databázového klienta.(LIDS V6 EDIT , LIDS V6 REVIEW, LIDS V6 iView, G/GAS, Geomedia)
C418	SW pro nákup	Služba zahrnuje komplexní SW řešení podporující proces nákupu elektřiny. Zahrnuje v sobě aplikace Xenon, Xenergie, Digrast, Tek2000, Retos, Aladin-nákup a Energes.
C419	Služba správy hist. systémů	Přístup do aplikace Enerfis (účetnictví a fakturace). Malé SŘO, SAP pro zbytkové podniky PR2 a PR3, SAP instance PR4 pro podnik E.ON ČR a.s.,SAP pro původní R/3 JCSAP4., SAP R/3 a SAP IS/U na systémech JM3, JČP a JEP, SAP CRM na systémech CR3 a CR2.
C420	Služba správa systému odečtů	Systém pro zajištění odečtů el. energie pro fakturaci a OTE, podpora systému pro dálkové odečty el. energie (Converge), Meter Reading System (MRS) pro ruční odečty MOO a SDE serveru s aplikací TOMCAT pro odesílání elektronických zpráv na OTE. Logický součet.
C421	Služba správa speciálního SW pro Services	Jedná se o aplikace typu Klient-Server, které jsou dominantně využívány a spravovány (datově) pracovníky ECR (např. ARIS, ČSNI, Normy, Námrazy, Spisová služba, Konkurzy). Logický součet - tj. počítá se jeden ks produktu nezávisle na počtu používaných modulů.
C422	Služba správa speciálního SW pro Distribution	Podpora speciálních aplikací pro oblast distribuce. PAS DAISY Off line, PAS DAISY ON line, ABI, RUPLAN, PQM,SIMONE, Reliance.
C423	Služba správa speciálního SW pro Sales	Služba zahrnuje doplňkové nonSAP aplikace pro potřeby procesů prodeje a marketingu. Součástí jsou aplikace Leonardo, SMB, MOO, zákaznický portál Synergie, Aladin, Kurýr.

C424	Služba správa IXOS	Přidělení přístupu do aplikací IXOS: oběh dokladů NOD, archivace nezákaznických smluv AgNES, archivace hromadných tisků AHT. Platba za přístup do IXOS bez ohledu na počet přístupů do aplikací.
C425	SW pro koncová zařízení	Podpora pro instalaci lokálního SW na koncových stanicích PC/NB,služba zajišťuje instalaci SW, který je v majetku jednotlivých NS a jeho provozování je v souladu s bezpečnostním konceptem. Logický součet - tj. počítá se jeden ks produktu nezávisle na počtu modulů.
C426	Služba Letter Shop	Služba hromadných tisků faktur a jiných dokumentů prostřednictvím pracoviště Letter Shop.
C427	Služba Datový přenos	Služby pro zajištění datových přenosů pro dispečinky, HDO, PQM, ochrany, atd. s rozlišením na požadovanou šířku pásma: - do 64 kbps, -do 2 Mbps, -do 10 Mbps, -do 100Mbps, -do 1 Gbps.
C428	Mobilní kancelář	Služba Mobilní kancelář umožňuje vzdálené připojení na informační zdroje společnosti, na SW aplikace společnosti při zajištění požadované bezpečnosti. Jedná se o připojení přes pevnou linku,modem, mobilní operátory. Služba neobsahuje dodání technických prostředků (telefon, MT atd.)
C429	Mobilní komunikace	Služba zajišťující dodávku a správu SIM karet pro mobilní hlasovou a datovou komunikaci včetně technických prostředků (mobilní telefon, modem).
C430	Telefonní síť	Služba zajišťující dodávku a správu pevné tel.linky včetně koncového zařízení - telefon, fax, modem.
C431	Archivace smluv	Archivace smluv.
C432	SAP EBP	Přidělení přístupu do SAP EBP (Enterprise Buyer Professional) – Nákupní košík materiálu.
C433	NonSAP Portál	Produkt zahrnuje podporu SW a HW pro aplikaci odečty plynu. Instalaci a provoz klientského systému, podporu serverové, databázové a komunikační infrastruktury včetně údržby a zálohování.
C434	SAP Call Centrum	Tato služba zahrnuje veškeré aplikace potřebné k provozu Call Centra a rozhraní na zákaznické informační systémy.
C435	HW typu multifunkční zařízení	Multifunkční zařízení scanner, fax, kopírka - dle schváleného standardu, včetně síťové konektivity.
C436	SAP HR	Přidělení přístupu do SAP HR - modul pro zpracování mezd a personální data pracovníků.
C437	Služba správa speciálního SW pro Heating plant	Služba zahrnuje doplňkové nonSAP aplikace pro potřeby procesů výroby a distribuce tepla.
C438	Hromadné tisky černobílé	Služba sdílených tisků uživatelů - platba za vytištěnou stranu A4/A3.
C439	Hromadné tisky barevné	Služba sdílených tisků uživatelů - platba za vytištěnou stranu A4/A3.
C440	SCADA	Údržba systému SCADA pro AS.
C450	Videokonference	Služba Videokonference.

1.2.1.1 HW pro poskytované služby

Tabulka 2: HW pro poskytované služby

Zdroj: materiály poskytnuté firmou E.ON.

Druh HW	počet	výrobce	počet
PC	1080	HP	950
		Dell	110
		ostatní	20
NB	1390	Fujitsu Siemens	310
		HP Compaq	30
		IBM/Lenovo	1050
tiskárny	1450	Brother	50
		HP	1300
		OKI	50
		ostatní	50
servery	130	HP/Compaq	54
		IBM	46
		Dell	8
		ostatní	22

1.2.1.2 Systémový SW

Tabulka 3: Systémový SW

Zdroj: materiály poskytnuté firmou E.ON

Typ	Produkt	verze
OS	MS Windows XP Professional	SP3
	MS Windows 2000	
	MS Windows 2000 server	
	SUN- Solaris	
	HP -UNIX	
AV	Trend Micro OfficeScan	
šifrovaní HD	SafeGuard Easy	
zabezpečení komunikace	Check Point IPSEC VPN	

1.2.1.3 Zařízení pro vzdálený přístup

Tabulka 4: Zařízení pro vzdálený přístup

Zdroj: Materiály poskytnuté firmou E.ON

Typ modemu	Operátor	počet
4G Combi card	T-Mobile	341
EDGE	T-Mobile	105
CDMA Any Data	Telefonica O2	124

1.2.2 Software

Používaný aplikační SW lze rozdělit do několika kategorií, v závislosti na účelu a oblasti použití.

Tabulka 5: Software

Zdroj: materiály poskytnuté firmou E.ON

charakter	typ	oblast použití
ERP	SAP R/3	finance
		účetnictví
		majetek
		personalistika
		controlling
	IXOS	oběh dokumentů
Obsluha zákazníků	SAP I-SU	databáze a historie zákazníků
	SAP CRM	řízení vztahu se zákazníky
	Solidus e-Care	obsluha CC
sp. SW klient - server	Converge	vzdálené odečty elektroměrů
	TIS	systém správy distribučního majetku (údržba, revize, opravy, obnova)
	GIS	dokumentační systém pro elektrické a plynové rozvody nad topologickou mapou
sp. SW lokální	cca 70 schválených položek	podpůrný SW pro technologie, jednoúčelové aplikace, apod.

1.3. Archivace a zálohování dat

Archivace a zálohování dat jsou neoddělitelně integrovány do příslušných SLA.

a) Zálohování síťových Home a Group adresářů.

   V rámci SLA HW_PC (pro uživatele produkt Poskytování HW_PC/NB/WS) je pro každý uživatelský login zajištěn tzv. Home adresář, umístěný na síťovém diskovém poli, který je plně zálohován, jeho aktuální povolená velikost je 500MB. Zde uložená data nejsou (až na omezení celkové velikosti) nijak kontrolována, je na uživateli jaká data považuje za důležitá.

   Dále jsou ještě k dispozici síťové adresáře pro skupinovou práci v rámci lokalit, nebo týmu/skupiny nebo v rámci celé skupiny E.ON ČR. Velikosti těchto adresářů jsou limitovány na základě přeložených a schválených požadavků. V tomto případě existuje možnost supervize ze strany správy diskových polí, kde je možno kontrolovat zda typy ukládaných souborů odpovídají schváleným v požadavku a kde je možno sledovat termíny posledního otevření souboru. Pro každý skupinový adresář je určen Vlastník adresáře, který schvaluje přidělování a odebírání přístupů dalším uživatelům a je odpovědný za kontrolu obsahu daného adresáře.

b) Zálohování a archivace dat sdílených aplikací.

   V tomto případě nemá uživatel možnost ovlivňovat jaká data a kde budou ukládána, ukládání dat jednotlivých uživatelů systému i databází je zabudováno do příslušné aplikace a zálohování dat je jeho součástí. Jedná se zejména o ERP systémy SAP (R/3, I-SU, CRM), technické aplikace TIS, GIS a i systém el. pošty–Exchange server.

c) Zálohování a archivace dat na koncových stanicích.

   Data na lokálních discích nejsou zálohována, je na uživateli, zda využije svůj Home adresář, nebo, vzhledem k objemu dat, použije pro archivaci CD nebo DVD disky.

Pro uvedené ukládání dat se používají RAID systémy v několika provedeních, které fungují v clustrech na oddělených lokalitách. Například pro zálohování dat dle odstavce a), dat Exchange serveru, se používá RAID v clustru, kde jednotky v rámci clusteru jsou umístěny v prostorách Servrovny Plynárenská 5 a technické místnosti v budově skladu Slatina v Brně.

Na síťových discích probíhá zálohování ve dvou cyklech:

Týdenním: V týdenním cyklu běží každý den od pondělí do soboty přírůstkové zálohy a v neděli plná záloha kromě prvního dne v měsíci.

Měsíčním: Měsíční cyklus běží tak, že každý první den v měsíci se provede plná záloha na oddělenou sadu pásek.

Po technické stránce je zálohování a archivace dat na odpovídající úrovni v poměru k důležitosti dat. Nicméně plány obnovy a kontinuity nejsou vypracovávány průběžně s technickým řešením, nejsou pravidelně udržovány a testovány.

1.4. Vzdálený přístup

Jedná se o skupinu aplikací, které umožňují vzdálené připojení na vnitřní aplikační a datové zdroje společnosti. Vzdálený přístup lze rozdělit do tří kategorií, kde všechny kategorie mají možnost využívat stejné technické prostředky pro vzdálený přístup, převažuje mobilní připojení GPRS, EDGE, CDMA, UMTS, WiFi, doplněné aplikací CheckPoint, která zajišťuje autentizaci a šifrování datového přenosu:

a) Mobilní kancelář. Tento typ přístupu zahrnuje elektronickou poštu, Intranet, Internet a uživatelské adresáře. Podle nastavených politik umožňuje přístup na vybrané aplikace.

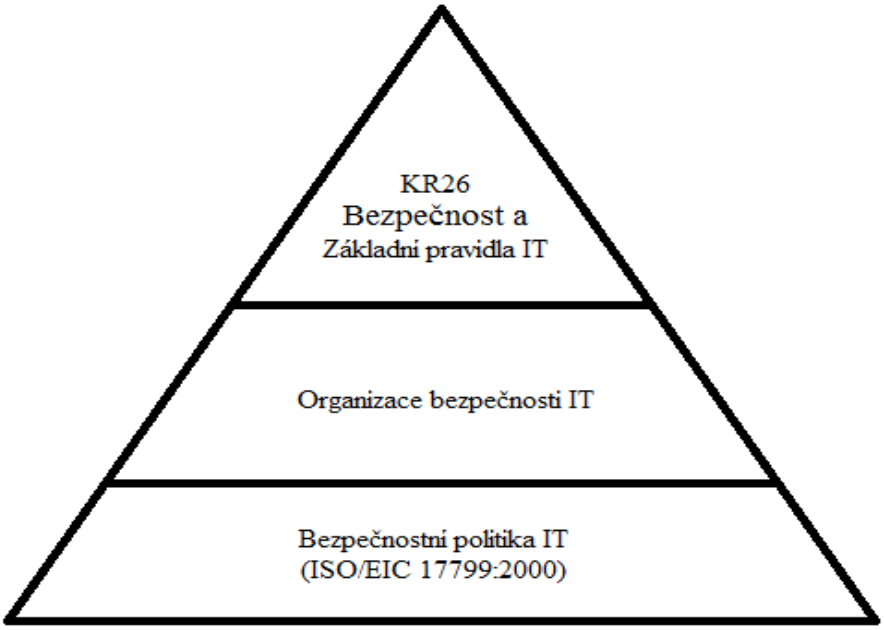
b) Vzdálený přístup na technologické zařízení. Tento typ přístupu je striktně omezen na úrovni IP adresy a portu, tam kde to charakter zařízení/aplikace umožňuje, je implementována autentizace a šifrování.

c) Vzdálený přístup pro externí společnosti. Na základě servisních smluv je vytvořen kanál pro vzdálený přístup, opět je přístup omezen IP adresou a portem, případně protokolem. Heslo pro autentizaci je vydáváno s ohledem na charakter spravované aplikace nebo zařízení, pokud nehrozí nebezpečí z prodlení, jsou hesla vydávána na základě požadavku externí společnosti jako jednorázová.

1.5. Infrastruktura a řízení procesů ICT

Jak již bylo zmíněno, ICT[2] služby jsou nakupovány formou dodávky služeb stanovené v SLA[3], za stanovení objemu a požadované úrovně je odpovědný CIO team v E.ON ČR, který podle terminologie ITIL[4] jedná jako zákazník vůči dodavateli, a současně zastupuje koncové uživatele, tj. překládá jejich požadavky na ICT služby do podoby SLA, kde následně kontroluje a vyhodnocuje způsob a míru plnění závazků. Seznam služeb s krátkým popisem je uveden v příloze x1, příklad SLA je uveden v příloze x2. Poskytovatel ICT služeb–E.ON IT je povinen zajistit požadované množství i úroveň služby, s tím, že je však vázán technologickými a bezpečnostní standardy stanovenými centrálou. V následujících částech práce budou bezpečnostní standardy podrobněji rozvedeny. Základ bezpečnostní politiky vychází z britských standardů pro bezpečnost, původní BS 7799, nyní ve verzi ISO/EIC 17799:2005, na kterou navazuje bezpečnostní směrnice společnosti E.ON - KR 26-EEA.

[2] Informační a komunikační technologie
[3] Smlouva o úrovni/kvalitě poskytovaných služeb
[4] Knihovna infrastruktury informačních technologií. Sada knižních publikací popisujících způsob řízení IT služeb a ICT infrastruktury



Obrázek 2: Grafické zobrazení struktury dokumentů jako hierarchie pravidel

Bezpečnostní infrastruktura pomáhá zajistit požadovanou úroveň ochrany informací tak, jak je definovaná bezpečnostní politikou, tj. „zajištění dostupnosti, důvěrnosti a integrity svých vlastních informací a zdrojů a také těch, které jim byly svěřeny zákazníky a obchodními partnery“.

Složení a vzájemné vazby prvků v rámci této infrastruktury vycházejí z bezpečnostních požadavků na ochranu informací.

Do seznamu Základních prvků bezpečnostní politiky patří:

- Řízení a koordinace bezpečnosti IT.
- Přidělování odpovědnosti v oblasti bezpečnosti informací.
- Klasifikace informací.
- Schvalování nasazení prostředků IT.
- Řízení vztahů s externími subjekty v oblasti IT.
- Informovanost zaměstnanců v oblasti bezpečnosti IT.
- Monitorování a řešení bezpečnostních incidentů v oblasti IT.
- Řízení kontinuity podnikatelských činností.

1.5.1 Řízení a koordinace bezpečnosti IT

Řízení a koordinace bezpečnosti IT zahrnuje:

- Koordinace bezpečnostních opatření v oblasti IT v celé firmě.
- Vyhodnocování bezpečnostní situace a bezpečnostních rizik a požadavků v oblasti IT na úrovni celé firmy.
- Schvalování bezpečnostní politiky v oblasti IT.
- Stanovení důsledků porušení bezpečnostních pravidel zaměstnanci.
- Vazbu bezpečnosti IT na vrcholový management.

Vyhodnocování bezpečnostní situace a bezpečnostních rizik a požadavků v oblasti IT na úrovni celé organizace je primárně povinností Security managera a dále pak povinností všech vedoucích na všech úrovních.

Stanovování důsledků porušení bezpečnostních pravidel se zaměřením za zaměstnance je řešeno nesystematicky. Někteří zaměstnanci podepsali přílohu směrnice o ochraně obchodního tajemství a autorských právech, a že byli s jejím obsahem seznámeni při zahájení pracovního poměru.

1.5.2 Přidělování odpovědnosti v oblasti bezpečnosti informací

Firma E.ON dodržuje v praxi koncepci jednoho vlastníka prostředků IT. Tzn., že každému prostředku IT je přidělen vlastník (ve smyslu „zodpovědné osoby“, ne právního vlastníka), který je zodpovědný za jeho používání i bezpečnost. Přidělování vlastníků probíhá různým způsobem v závislosti na tom, o jaký prostředek se jedná.

Pokud nebude výslovně uveden vlastník majetku, jedná se o majetek společnosti E.ON IT, v jiném případě bude vlastník výslovně uveden.

Nejvýznamnější infrastrukturní prostředky jako servery a koncová zařízení, jsou ve vlastnictví E.ON IT a každý kus má stanoveného správce, jedná se o roli vycházející z pracovního zařazení příslušné osoby:

- Servery podnikových aplikací a aplikací VIS (Vnitřní informační systém) jsou ve vlastnictví Správy infrastruktury.
- Serverové aplikace, vč. VIS, jsou ve vlastnictví Správy aplikací.
- Data podnikových aplikací jsou ve vlastnictví tzv. klíčových uživatelů jednotlivých aplikací/modulů: tito uživatelé určují typ přístupu k datům jimi vlastněného modulů/aplikací. Pro jednotlivé uživatele, technicky jim tato práva přidělí Administrátor na základě specifikace schválené klíčovým uživatelem.
- Data aplikací VIS jsou ve vlastnictví Správy aplikací.
- Koncové stanice (NB, PC, WS) včetně systémového SW (OS, AV) - správa je na útvaru Customer services.
- Síťová infrastruktura je v majetku E.ON Distribuce a E.ON ČR, administrace je prováděna Správou Infrastruktury.
- Telekomunikační zařízení jsou ve vlastnictví E.ON Distribuce a E.ON ČR administrace je prováděna Správou Infrastruktury a Customer services.

Oprávnění a pravomoci zaměstnanců jsou definovány jejich zařazením na určitou pozici a přidělení aktiv, za které budou zodpovědní. Delegace pravomocí přichází v úvahu v případě nepřítomnosti vlastníka. Takový případ je řešen tak, že v době nepřítomnosti vlastníka se řeší, pokud to situace dovolí, jenom operativní záležitosti a vlastníkem je buď vedoucí příslušného oddělení, nebo osoba, které je řešení problému nejbližší. Tento model se firmě dlouhodobě osvědčuje.

Ostatní zaměstnanci společnosti E.ON jsou zodpovědní za přidělované prostředky IT a nemají právo tuto zodpovědnost dále delegovat. Systémová opatření, oprávnění ke spouštění úloh a oprávnění přístupu k datům jsou přidělovány vlastníky aktiv a uživatelé nemají právo ji dále delegovat.

1.5.3 Klasifikace informací

Pracovníci jsou si vědomi toho, že v IS jsou uložena data, která jsou citlivá ve smyslu zákonů o ochraně osobních údajů a obchodního zákoníku, ale neexistuje přehled o tom, o která data přesně jde, kde jsou uložena a jakým způsobem k nim lze přistupovat. Za ochranu citlivých údajů jsou obecně zodpovědní vlastníci dat aplikací.

1.5.4 Schvalování nasazení prostředků IT

Společnost E.ON rozeznává dva typy projektů:

- Strategické: v oblasti IT jde o zavádění nových systémů, aplikací nebo postupů.
- Provozní: v oblasti IT jde o přechody na nové verze software, nahrazení starého hardware, obecně se jedná o průběžnou obnovu HW/SW.

Provozní projekty jsou řízeny CIO[5] teamem tak, aby byla dodržena úroveň bezpečnosti platná před zahájením provozního projektu.

Nasazení nových prostředků IT je možné v rámci nových projektů, nebo podléhá operativnímu řízení. Jak sem již uvedla, ve firmě existují dva typy projektů (strategické a provozní). Strategické jsou schvalovány na úrovni vedení, provozní podle rozsahu, a to v rámci plánu schváleného vedením nebo CIO managerem.

Operativnímu řízení podléhá využití nových prostředků IT malého rozsahu, což představují například nové pracovní stanice, zakoupení speciálního softwaru pro malou skupinu uživatelů a podobně. V těchto případech žádají o prostředky IT uživatelé prostřednictvím svých nadřízených. Nákup musí schválit útvar CIO.

Nákup obecně provádí útvar Logistiky. Prostředky se po nákupu stávají majetkem E.ON Distribuce nebo E.ON ČR zastoupené útvarem CIO.

[5] Jeho hlavním úkolem je přesvědčit výkonné vedení společnosti o významu IT, o nákladech spojených s poskytováním jednotlivých služeb, seznamuje vedení společnosti s možnostmi a omezeními IT, zajišťuje, aby byly určeny a obsazeny všechny role kritické pro maximalizaci přidané hodnoty ze strany IT. Určuje a ohodnocuje jednotlivá rizika, předává vedení srozumitelné informace o jednotlivých rizicích.

1.5.5 Řízení vztahů s externími subjekty v oblasti IT

Systémovým integrátorem pro oblast IT je společnost E.ON IT. Rámcová smlouva mezi společností E.ON ČR a E.ON IT je uzavřena na dobu neurčitou s výpovědní lhůtou 4 roky. Smlouva pokrývá celou oblast ICT. Pro oblast řízení vztahů s externími dodavateli neexistují psaná pravidla. Je dodržována zásada, že za práci s prostředky ve vlastnictví skupiny E.ON cizími pracovníky zodpovídá vlastník prostředků IT z řad zaměstnanců. Někteří externí pracovníci, i v rámci outsourcingu mají přidělená vysoká oprávnění. Tato oprávnění jsou částečně zdokumentována, ale není k dispozici přehled o přidělených právech.

1.5.6 Informovanost zaměstnanců v oblasti bezpečnosti IT

Zaměstnanci jsou ohledně bezpečnosti informováni několika způsoby:

- Školením.
- Elektronickou vývěskou-Intranet.
- Osobním kontaktem.

Bezpečnost je součástí školení, které je pořádáno pro zaměstnance v implementační fázi každého projektu, kde je zapotřebí zaměřit se na nové postupy. Dodatečná školení se provádí podle potřeby a na základě schválení nadřízeným.

Na internetu jsou zveřejňovány různé informace ohledně bezpečnosti, takže pracovníci je mají stále k dispozici. Podle závažnosti jsou informace barevně rozlišeny.

1.5.7 Monitorování bezpečnostních incidentů

Detekce bezpečnostních incidentů je s výjimkou firewall a antivirové ochrany pasivní. Pracuje se v režimu „až se něco stane, někdo to nahlásí“. Na důležitých místech počítačové sítě a na důležitých počítačích by měla být realizovaná aktivní detekce incidentů. Incidenty jsou řešeny dvěma způsoby:

- Kontaktováním vlastníka prostředku, kterého se incident týká.
- Nahlášením incidentu na HelpDesk[6].

V prvním případě (kontaktování osoby zodpovědné za prostředek IT) je neformálně kontaktován zodpovědný pracovník a na základě jeho doporučení jsou prováděny další kroky, které vedou k řešení vzniklého problému. Tyto incidenty se nijak neevidují. Podle vyjádření pracovníků IT vzrůstá tlak na evidenci incidentů prostřednictvím HelpDesk. Jedním z hlavních kritérií hodnocení pracovníků IT je přehled vyřešených problémů. HelpDesk je zaměstnancům přístupný jednak přes internet a jednak přes telefon. Není zajištěno zobecňování zkušeností z řešení problémů ani není možné využít stejný postup v případě stejného nebo podobného problému.

1.5.8 Řízení kontinuity podnikatelských činností

Podnikatelské aktivity společností E.ON jsou velmi silně závislé na prostředcích ICT. Nedostupnost má za důsledek okamžité (v případě řídících systémů) nebo rychlé (horizont dvou dnů v případě podnikových činností) negativní důsledky na podnikové procesy. Nedostupnost prostředků IT by značně narušila podnikatelskou činnost. Jsou sice formálně vypracovány postupy pro zajištění náhradních řešení, ale prakticky nejsou testovány a ověřeny.[7]

V případě nedostupnosti prostředků IT pracovníci spoléhají na vlastní znalosti a zkušenosti a na spolupráci externích firem na základě uzavřených servisních smluv.

1.6. Fyzické zabezpečení

Zde je nutné opět zmínit historický vývoj v budování zabezpečených oblastí pro umístění serverových farem pro aplikace typu Klient-server, pro umístění diskových polí, poštovních serverů, FW, DMZ.

[6] kontaktní místo E.ON IS
[7] Materiály poskytnuté firmou E.ON

První zabezpečený prostor vznikl na objektu Lidická, postupně se rozšiřoval, následovalo vybudování servrovny pro CallCentrum v objektu na ulici Cejl. V době přípravy sloučení JME a JČE byla vybudována servrovna, jako Datové centrum, na Plynárenské ulici. V současné době již jsou klíčové aplikace jako ERP, e-mail, FW, připojení do Internetu, přemístěny do datových center v SRN. Dále zmíněné servrovny jsou provozovány v režimu tzv. Technických místností, zajišťující datové propojení do DC SRN a provoz serverů pro některé nepřevedené aplikace.

Ve společnosti existují dvě bezpečné oblasti, ve kterých jsou umístěny prostředky ICT:

- Servrovna Lidická.
- Servrovna Plynárenská.

Tyto prostory mají kromě standardního zabezpečení (klimatizace, protipožární hlásiče, detekce pohybu) i vybavení kamerami a přístupovými terminály.

Některé IT prostředky se ale stále nacházejí mimo bezpečné zóny. Jedná se především o tzv. technické místnosti, kde jsou umístěny aktivní síťové prvky, moduly telefonních ústředen, případně dohledové servery, kanceláře s PC s daty pro banky a pro tisk faktur, kovové skříně se síťovými prvky na chodbách a podobně.

1.6.1 Ochrana proti násilnému vniknutí

Ochrana proti násilnému vniknutí obsahuje opatření proti:

- Krádeži.
- Sabotáži, vandalismu.
- Teroristickému útoku.

Servrovna Lidická:

Místnosti mají souvislé zdi probíhající souvisle od stropu až k podlaze. Okna jsou chráněna mřížemi a bezpečnostní fólií. Dveře jsou bezpečnostní. Na dveřích a oknech

jsou magnetické kontakty pro detekci otevření. V místnostech jsou detektory tříštění skla, detektory pohybu a kamery. Obraz z kamer a kontrolní signalizace čidel jsou vyvedeny na pult ostrahy budovy.

Přístup do místností je kontrolován elektronickým zámkem. Jsou definována pravidla pro přístup oprávněných osob a návštěv. Pro návštěvy platí, že musí být doprovázeny pracovníkem společnosti E.ON.

Servrovna Plynárenská:

Jedná se o prostory bývalého Datového centra, kde byly umístěny servery pro ERP systémy. Prostory byly upraveny zcela ve shodě s bezpečnostními požadavky. Místnosti bez oken, protipožární obložení, automatický hasící systém, kontrola přístupu až na úrovni otisku prstu, kamery, detektory pohybu. Prostory datového centra jdou napájeny zdvojeným systémem záložního napájení (dva nezávislé přívody NN, redundantní systém UPS a diesel agregát), dále jsou prostory vybaveny redundantním klimatizačním zařízením.

Ostatní prostory – technické místnosti: Okna jsou chráněna mřížemi a bezpečnostní fólií. Dveře nejsou bezpečnostní. Na dveřích a oknech jsou magnetické kontakty pro detekci otevření. V místnostech jsou detektory tříštění skla, detektory pohybu.

Přístup do místností je kontrolován elektronickým zámkem. Jsou definována pravidla pro přístup oprávněných osob a návštěv. Pro návštěvy platí, že musí být doprovázeny pracovníkem společnosti E.ON.

1.6.2 Ochrana proti kouři, ohni, vodě, vibracím a elektromagnetismu

Servrovna Lidická:

Je nainstalována elektrická požární signalizace (EPS). Požární a kouřová čidla jsou na stropě a v podlaze. Hlásiče jsou umístěny na stěně servrovny, na chodbě před ní a na pultě ochrany budovy. Dveře jsou protipožární s odolností 30 minut. Při instalaci kabeláže nebyly použity speciální nehořlavé kabely. V místnosti je ruční hasící přístroj.

Ve dvojité podlaze jsou umístěna čidla zaplavení. Vyvedení hlásičů je stejné jako u EPS.

Dvojitá podlaha a umístění zařízení v kovových skříních slouží jako ochrana proti mírným vibracím.

Podlaha je antistatická a kabely SK a elektrické kabely jsou uloženy podle doporučení výrobců. Jiná opatření proti statické elektřině nejsou realizovány.

Servrovna Plynárenská 5:

Je nainstalována elektrická požární signalizace (EPS). Požární a kouřová čidla jsou na stropě a v podlaze. Hlásiče jsou umístěny na stěně servrovny, na chodbě před ní a na pultu ochrany budovy. Jedná se o místnost s protipožárním obložením a automatickým hasícím systém na bázi plynu. Dveře jsou protipožární s odolností 90 min. Při instalaci kabeláže, byly použity speciální nehořlavé kabely.

V místnosti jsou i ruční hasící přístroje.

Je instalována detekce zaplavení, vzhledem k umístění, je pod místností umístěn suchý rezervoár.

Dvojitá podlaha a umístění zařízení v kovových skříních slouží jako ochrana proti mírným vibracím.

Podlaha je antistatická a kabely SK a elektrické kabely jsou uloženy podle doporučení výrobců. Jiná opatření proti statické elektřině a elektromagnetismu nejsou realizovány.

1.6.3 Ochrana proti vysoké teplotě, vlhkosti a prachu

Servrovna Lidická:

Jsou nainstalovány 3 klimatizace o výkonech 12kW, 12,5kW a 13kW.

Servrovna Plynárenská:

Je nainstalován redundantní klimatizační systém o celkovém výkonu cca 75kW, doplněn o dva zvlhčovače vzduchu.

1.7. Závěr analýzy společnosti

Celkový obraz vyvolává poněkud rozpolcený dojem – na jedné straně jsou k dispozici prakticky veškeré zdroje jak HW, tak SW charakteru, které koordinovaně mohou zajistit žádanou úroveň zabezpečení, na druhé straně tento potenciál není dostatečně využíván (syndrom Maginotovy linie). Pro definování bezpečnosti IT se na nejvyšší úroveň umísťuje směrnice KR26 (viz příloha č.3). Tato směrnice se v článcích odvolává na další navazující směrnice a postupy, tyto však nejsou výslovně uvedeny, tedy nejsou zřetelně k dispozici. Teoreticky by měly být požadavky na bezpečnost zakomponovány do definic jednotlivých procesních rolí. Procesy jsou definovány, nicméně rozpad na úroveň definice rolí není proveden, což vede k tomu, že pracovníci jsou upozorňováni na nutnost dodržování bezpečnostních standardů, ale není jasné jak, a jaké se jich konkrétně týkají. Je obecně známá statistika, že bezpečnostní incidenty jsou z cca 70% způsobeny interními uživateli a většina takových incidentů jde na konto uživatelských chyb, nehod a ignorace. Zde se potvrzuje ta skutečnost, že není naplněna myšlenka integrace bezpečnostních zásad do běžných provozních praktik formou srozumitelných bezpečnostních politik a adresným školením pracovníků.

2. Teoretická východiska řešení

V této kapitole budu vycházet zejména z bezpečnostního standardu BS 7799. Není možné v rozsahu této práce popsat všechny kapitoly, které s danou problematikou souvisí. Zaměřím se zejména na části této práce, kde jsem shledala největší nedostatky v zabezpečení společnosti.

„Zásady zabezpečení neboli bezpečnostní politika stanovuje, co se musí provést s ohledem na ochranu informací uložených v počítačích. Dobře napsané zásady musí obsahovat dostatečně jasný popis toho, „co“ udělat a „jak“ jejich vykonávání rozpoznat a změřit nebo posoudit.“[8]

Informace jsou aktiva, která mají pro organizaci hodnotu, a potřebují tedy být vhodným způsobem chráněny. Bezpečnost informací je zaměřena na širokou škálu hrozeb a zajišťuje tak kontinuitu podnikatelských činností, minimalizuje obchodní ztráty a maximalizuje návratnost investic a podnikatelských příležitostí.

„Informace mohou existovat v různých podobách. Mohou být vytištěny nebo napsány na papíře, ukládány v elektronické podobě, posílány poštou nebo elektronickou cestou, zachyceny na film nebo vyřčeny při konverzaci. Ať už se bavíme o jakékoliv formě informací nebo způsobu uložení, je nutné, aby byly informace vhodným způsobem chráněny.“[9]

„Bezpečnost informací je charakterizována jako zachování:

a) důvěrnosti- zajištění toho, aby informace byla dostupná pouze osobám oprávněným pro přístup,
b) integrity- zabezpečení správnosti a kompletnosti informací a metod zpracování,

[8] BRAGG R., RHODES-OUSLEY M., STRASSBERG K. *Network Security The Complete Reference*, 2003. Str. 95.
[9] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str.11.

c) dostupnosti- zajištění toho, aby informace a s nimi spjatá aktiva byly přístupné autorizovaným uživatelům podle jejich potřeby.“[10]

2.1. Bezpečnost informací[11]

Informace a podpůrné procesy, systémy a sítě jsou důležitými aktivy organizace. Zajištění jejich dostupnosti, integrity a důvěrnosti může být zásadní pro udržení konkurenceschopnosti, toku hotovosti, ziskovosti, právní shody a dobrého jména organizace.

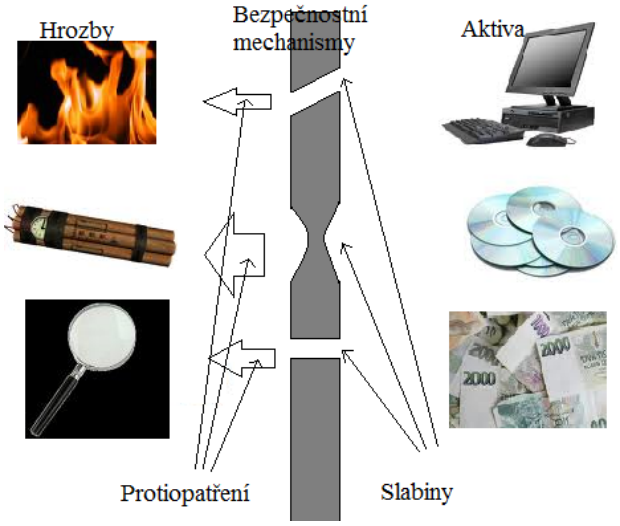
Stále rostoucí měrou jsou organizace a jejich informační systémy vystavovány bezpečnostním hrozbám z různých zdrojů, včetně počítačových podvodů, špionáží, sabotáže, vandalizmu, požáru a povodní. Zdroje škod, jako jsou počítačové viry, útoky hackerů a útoky typu odepření služby, jsou stále častější, roste jejich nebezpečnost a sofistikovanost.

Řízení bezpečnosti informací vyžaduje minimálně spoluúčast všech zaměstnanců organizace. Může rovněž zahrnovat spolupráci dodavatelů, zákazníků a majitelů organizace. V neposlední řadě může být potřebná i rada od specialistů z jiných organizací.

2.2. Bezpečnostní požadavky

Samotná aktiva v jejich vlastním okolí mají určitou hodnotu, ať už se jedná o diskety, kartotéky zaměstnanců, peníze nebo data o prodeji. Tyto aktiva v jejich vlastním okolí mají svou zranitelnost. Proto jsou instalovány bezpečnostní opatření (mechanismy), které mají za úkol informace chránit. V případě, že má bezpečnostní systém své trhliny, může poměrně snadno dojít k bezpečnostnímu incidentu, na který je potřeba reagovat protiopatřením.

[10] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 11.
[11] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 11.



Obrázek 3: Aktiva a jejich okolí.

Zdroj: vlastní.

„Je nezbytné, aby organizace určila své bezpečností požadavky. K tomu existují tři hlavní zdroje.

Prvním je odhad rizik, která organizaci hrozí. Za pomoci odhadu bezpečnostních rizik se určují hrozby působící vůči aktivům, zranitelnost ze strany hrozeb i pravděpodobnost výskytu a provádí se odhad jejich potenciálního dopadu.

Druhým zdrojem jsou požadavky zákonů, zákonných norem a smluvní požadavky, které organizace, její obchodní, smluvní partneři a poskytovatelé služeb musí splňovat.

Třetím zdrojem jsou konkrétní principy, cíle a požadavky na zpracování informací, které si organizace vytvořila pro podporu své činnosti.“[12]

2.3. Archivace a zálohování dat

„Archivace spočívá především ve shromažďování informací pro případné pozdější použití. Jedná se o uschování originálních dat mimo hlavní informační systém, aby

[12] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 11.

nezabírala jeho prostředky. Archivace dat je určena k trvalému uložení, bez možnosti dalších změn.“

„Zálohování představuje vytváření bezpečnostní kopie celého operačního systému či konkrétních dat na takové místo, kde budou v případě havárie počítače beze ztráty zachována.“ [13]

Ke ztrátě dat může dojít prakticky kdykoliv a velmi jednoduše. Faktorů, které mohou způsobit ztrátu dat je hned celá řada a i malý incident může mít pro společnost katastrofické následky. Proto by si měla každá společnost uvědomit, jakou cenu mají její data a jakou hodnotu má délka prostoje výpočetního systému v případě ztráty dat. Obecně se udává, že 94% firem, které postihne velká ztráta dat, ukončí svoji činnost do 3 měsíců, neboť nejsou schopny na trhu přežít.

Důvody, proč dochází ke ztrátě dat[14]:

a) Lidská chyba: neúmyslné smazání dat, nedbalost, chyba obsluhy, nesprávné zacházení…
b) Úmyslné zničení: virus, sabotáž, krádež, vandalismus…
c) Selhání systému: výpadek napájení, programová chyba, selhání pevného disku…
d) Přírodní živly: požár, kouř, zásah blesku, voda a podobně.

Typy záloh[15]:

a) Úplná (normální)- záloha, která zkopíruje všechny vybrané soubory na záložní médium a označí je jako zálohované. Tento druh zálohy je nejjednodušší

[13]Pavelková, L. *Zálohování a archivace* [online]. 2003-3-24 [cit. 2010-5-4]. Dostupný z www: https://akela.mendelu.cz/~lidak/bif/pavelkova.rtf
[14]*Záloha dat je důležitá a proč*. [online]. 2010 [cit. 2010-5-4]. Dostupný z www: http://www.servispc.biz/zaloha_dat.htm
[15]KANTOR, R. *Zálohování dat* [online]. 2009 [cit. 2010-5-4]. Dostupný z www: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xkantor1.htm

variantou a rovněž obnova dat je velmi snadná. Záporem je dlouhá doba potřebná pro zálohu a také zabírá nejvíce místa na zálohovacím médiu.

b) Rozdílová- zálohují se pouze data, která se změnila od minulé zálohy (ať už to byla záloha úplná, rozdílová nebo přípustková).

c) Přípustková- metoda, která dovoluje zálohovat pouze soubory změněné od poslední normální či přírůstkové zálohy. Rovněž ona označuje soubory jako zálohované. Protože se pracuje s menším objemem dat, je tato metoda mnohem rychlejší. Výhoda zkrácené doby zálohování je kompenzována poněkud obtížnější obnovou dat, protože musí mít neustále k dispozici normální zálohu a všechny navazující přírůstkové.

2.4. Bezpečností politika informací

„Cílem je definovat směr a vyjádřit podporu bezpečnosti informací ze strany vedení. Vedení organizace by mělo stanovit jasný směr postupu v oblasti bezpečnosti informací, ukázat její podporu vydáním a aktualizací bezpečnostní politiky informací platné v celé organizaci.“[16]

2.4.1 Dokument bezpečností politiky informací[17]

Dokument bezpečnostní politiky informací by měl být schválen vedením organizace, vydán a sdělen všem zaměstnancům. Měl by obsahovat vyjádření podpory vedení organizace a měl by definovat zamýšlený přístup k budování bezpečnosti informací.

Dokument by měl obsahovat následující body:

a) definice bezpečnosti informací, její cíle, rozsah a její důležitost-mechanizmus umožňující sdílení informací,

[16] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 14.
[17] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 14.

b) prohlášení vedení organizace o záměru podporovat cíle a principy bezpečnosti informací,

c) stručný výklad bezpečnostních zásad, principů a norem a požadavky zvláštní důležitosti pro organizaci, jako jsou například dodržování legislativních a smluvních požadavků, požadavky na vzdělání v oblasti bezpečnosti, zásady prevence a detekce virů, důsledky porušení bezpečnostních zásad a podobně,

d) stanovení obecných a specifických odpovědností pro oblast řízení bezpečnosti informací včetně hlášení bezpečnostních incidentů,

e) odkazy na dokumentaci, která může bezpečnostní politiku podporovat, například na detailnější bezpečnostní politiky a postupy zaměřené na specifické informační systémy nebo bezpečnostní pravidla, která by měli uživatelé dodržovat.

Dokument by měl být sdělen všem zaměstnancům organizace, včetně uživatelů, a to ve formě, která je přístupná a pochopitelná všem potenciálním příjemcům.

2.4.2 Revize a hodnocení

„Bezpečnostní politika by měla mít garanta zodpovědného za její údržbu a aktualizaci v souladu s definovaným revizním procesem. Tento proces by měl zajistit, že revize proběhne jako reakce na jakékoliv změny ovlivňující východiska původního hodnocení rizik, například: významné bezpečnostní incidenty, nové zranitelnosti nebo změny v organizační či technické infrastruktuře.

Měl by být vytvořen plán pravidelné revize:

a) efektivity politiky, prokázané příčinami, počtem a dopadem zaznamenaných bezpečnostních incidentů,

b) ceny a dopadu opatření na efektivnost provozu organizace,

c) dopadu změn na technologii.“[18]

2.5. Infrastruktura bezpečnosti informací

„Cílem je bezpečnost informací v organizaci. Měl by být vytvořen řídící rámec pro zahájení a kontrolu implementace bezpečnosti informací v organizaci.

Měla by být ustanovena adekvátní řídící fóra vedená managementem organizace, která by schvalovala politiku bezpečnosti informací, přiřazovala role v oblasti bezpečnosti informací a koordinovala implementaci bezpečnosti v organizaci. Jestliže je to nutné, pak by měl být v organizaci vytvořen specializovaný zdroj pro oblast bezpečnosti informací a měl by být dostupný pro celou organizaci. Aby bylo možné dodržovat krok s posledními trendy v odvětví bezpečnosti informací, sledovat standardy, vybírat nejvhodnější metody a zajistit vhodné styčné body v případech bezpečnostních incidentů, měly by být uzavřeny smlouvy s externími odborníky v oboru bezpečnosti informací., např. koordinace a spolupráce manažerů, uživatelů, administrátorů, aplikačních návrhářů, auditorů, bezpečnostních pracovníků a také specialistů v takových oblastech, jako je pojištění a řízení rizik.“[19]

2.5.1 Přidělování odpovědnosti v oblasti bezpečnosti informací[20]

Informace v různé podobě se mohou vyskytovat na různých místech firmy. Je důležité, aby si všichni, kdo s touto informací přicházejí do styku, uvědomili, že manipulují s něčím, co má nemalou hodnotu. Osoba, která má největší představu o tom, co by se stalo v případě zničení, ztráty či nedostupnosti zařízení, se označuje jako vlastník. Ostatní zúčastnění procesu se nazývají uživatelé.[21]

---

[18] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 14.
[19] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 15.
[20] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 15.
[21] RODRYČOVÁ, D. *Bezpečnost informací*, 2000. Str. 21.

Měla by být jednoznačně definována odpovědnost za ochranu jednotlivých aktiv a za provádění určitých bezpečnostních postupů.

Bezpečnostní politika by měla poskytovat obecné vodítko pro vymezení bezpečnostních rolí a odpovědnosti jednotlivých subjektů v organizaci. Tam, kde je to potřebné, by tato politika měla být doplněna o podrobnější interpretaci vztahující se ke specifickým místům, systémům nebo službám. Měla by být jasně definována místní odpovědnost subjektů za jednotlivá aktiva a bezpečnostní postupy, např. plánování kontinuity podnikatelských činností.

V mnoha organizacích bude jmenován vedoucí pracovník zodpovědný za bezpečnost informací, který nese veškerou odpovědnost za vývoj a implementaci bezpečnosti a který zajišťuje identifikaci opatření. Avšak odpovědnost za financování a implementaci těchto opatření bude často zůstávat na vedoucích jednotlivých útvarů organizace. Jedním obecně používaným postupem je jmenovat vlastníka pro každé informační aktivum, který se pak stane zodpovědným za každodenní bezpečnost svěřeného aktiva.

Vlastníci informačních aktiv mohou předat svou bezpečnostní odpovědnost za tato aktiva vedoucím jednotlivých útvarů organizace nebo poskytovatelům služeb. Nicméně vlastník vždy v konečném důsledku zůstává zodpovědný za bezpečnost aktiva a měl by být schopen zaručit, že jakákoliv takto delegovaná odpovědnost byla předána správně.

Je nezbytné jasně vymezit oblasti odpovědnosti jednotlivých vedoucích. Zvlášť by mělo být provedeno následující:

a) identifikování a jasné definování různých aktiv a bezpečnostních postupů spojených s každým jednotlivým systémem;
b) určení odpovědnosti relevantního vedoucího pracovníka za každé aktivum nebo bezpečnostní postup a detaily této odpovědnosti by měly být zdokumentovány;
c) jednoznačné určení a zdokumentování úrovně oprávnění jednotlivých subjektů.

Do podnikové infrastruktury spadá i Schvalovací proces pro zařízení zpracovávající informace, v kapitole Analýza současného stavu je pojmenován jako „Schvalování nasazení prostředků IT.“

2.5.2 Schvalovací proces pro zařízení zpracovávající informace[22]

Měl by být zaveden proces schvalování nových zařízení zpracovávající informace managementem. V úvahu by mělo přijít odsouhlasení nového zařízení jednotlivými vedoucími útvaru organizace, kteří schválí jejich účel a použití, v nutných případech by mělo být zkontrolováno technické a programové vybavení, aby bylo zajištěno, že je kompatibilní s ostatními systémovými prvky. Dále je potřeba zaměřit se na použití soukromých prostředků zpracovávajících pracovní informace, a protože použití osobních prostředků může znamenat vznik nových zranitelností v zabezpečení, mělo by být toto používání posouzeno a schváleno.

2.6. Klasifikace informací

„Cílem je zajistit přiměřenost ochrany informačních aktiv. Informace by měli být klasifikovány tak, aby byla naznačena jejich potřebnost, důležitost a stupeň ochrany.

Informace mohou mít různý stupeň citlivosti nebo být různě kritické. Některé prvky mohou vyžadovat vyšší úroveň bezpečnosti nebo zvláštní způsob zacházení. Měl by existovat systém bezpečnostní klasifikace, který by určoval adekvátní stupeň ochrany a který by dával uživatelům informace o nutnosti zvláštního zacházení.“[23]

[22] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 16.
[23] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 19.

2.6.1 Evidence aktiv

Organizace musí být schopna identifikovat svá aktiva v závislosti na důležitosti a hodnotě. Na základě zjištění hodnoty aktiv je organizace schopná zajišťovat úroveň ochrany odpovídající jejich hodnotě a důležitosti.

2.6.2 Směrnice pro klasifikaci

Z důvodu často se měnící citlivosti informací, je nutné počítat s jejich rekvalifikací. Informace po uplynutí určité doby přestávají být citlivé nebo kritické, například při jejich zveřejnění a podobně. Je ovšem potřeba počítat s administrativními náklady, které jsou spojeny právě s rekvalifikací. Klasifikace není neměnný proces a je potřeba si uvědomit, že informace a jejich hodnotu nelze měnit podle předem určených pravidel.

2.6.3 Značení informací a manipulace s nimi

„Pro značení informací a zacházení s nimi je důležité, aby byla definována soustava postupů. Tyto postupy musí pokrývat informační aktiva ve fyzické i elektronické podobě. Manipulační postupy by měly být definovány pro každou úroveň klasifikace tak, aby pokrývaly následující typy zpracování informací:

a) kopírování
b) uchovávání
c) přenos poštou, faxem, elektronickou poštou
d) přenos mluveným slovem, včetně mobilních telefonů, telefonních záznamníků a hlasových schránek
e) likvidace

Výstup ze systému, obsahující citlivé informace, by měl být označen odpovídajícím klasifikačním návěstím.“[24]

2.7. Bezpečnost přístupu třetích stran

Třetím stranám může být přístup povolen z mnoha různých důvodů. Mohu zde zmínit například osoby, které zajišťují služby pro organizaci, tzn. přístup pracovníků údržby pečující o technické a programové vybavení, přístup obchodních partnerů nebo partnerů ve společném podnikání, s nimiž může organizace sdílet databáze a podobně. Nesmím také opomenout smluvní strany v prostorách organizace jako je například úklid, zásobování, bezpečnostní ostraha a další externě zajišťované služby. Poměrně časté jsou i studentské praxe, konzultační činnosti nebo podobné krátkodobé akce.

„Tam, kde z činnosti organizace vyplývá potřeba přístupu třetí strany, by mělo být provedeno zhodnocení rizik plynoucích z tohoto přístupu tak, aby se zjistily důsledky z hlediska bezpečnosti a aby se definovaly požadavky na opatření. Opatření by měla být schválena a definována ve smlouvě s třetí stranou.“ [25]

2.8. Outsourcing

„Cílem je zachovat bezpečnost informací v případech, kdy zodpovědnost za zpracování informací byla přenesena na jinou organizaci.

Při zajištění činností jinou organizací by měla smlouva mezi stranami pokrývat rizika, bezpečnostní opatření a postupy pro informační systémy, sítě nebo samostatné počítače.“[26]

[24] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 20.
[25] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 17.
[26] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 18.

Bezpečnostní požadavky ve smlouvách o zabezpečení zdrojů mimo organizaci by měli být definovány a schváleny již ve smlouvě mezi organizací a stranami, na které se provoz převádí.

Smlouva by měla obsahovat[27]:

a) jak budou splněny právní požadavky na provoz těchto systémů;

b) jak se zajistí, aby si všechny smluvní strany včetně subdodavatelů byly vědomi své odpovědnosti za bezpečnost;

c) jak bude udržována a testována integrita a důvěrnost aktiv organizace;

d) jaká logická a fyzická opatření budou použita pro omezení přístupu oprávněných uživatelů k citlivým informacím organizace;

e) jak bude v případě havárie zajištěna dostupnost služeb;

f) jaká úroveň bezpečnosti bude zajištěna u zařízení patřících třetí straně;

g) právo auditu.

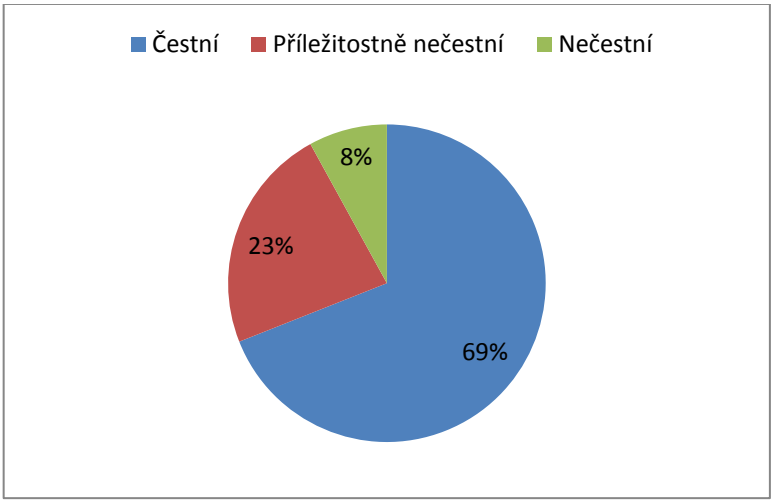
2.9. Personální bezpečnost[28]

Obecně se dá říci, že personální bezpečnost je základním druhem zajištění ochrany utajovaných informací. Do personální bezpečnosti spadá i povinnost pravidelného proškolování zaměstnanců a tím i spojené snížení rizika lidské chyby, krádeže, podvodu či zneužití prostředků organizace. Zaměstnanci by měli podepsat smlouvu o zachování důvěrnosti jako součást pracovních podmínek. U osob jako jsou příležitostní pracovníci nebo uživatelé třetí strany, se kterými nebyla podepsána pracovní smlouva, musí být podepsána smlouva o zachování důvěrnosti ještě před tím, než jim bude umožněn přístup k prostředkům organizace.

[27] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 19.

[28] *Personální bezpečnost* [online]. 1998-8-1 [cit. 2010-3-11]. Dostupný z www: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/

„Lidé představují hazardní zdroje, s nimiž se musí pracovat. Tedy je na místě povšimnout si některých statistik (např. Ministerstvo spravedlnosti ČR, 1997). Ty ukazují, že asi 8 procent lidí je nečestných-jsou schopni bez skrupulí páchat běžné kriminální činy. Pokud se týká trestných činů s vysokým stupněm nebezpečnosti, je toto procento jen nepatrně nižší. Asi 23 procent je sice navenek zcela loajálních a jeví se jako čestní, ale pod tlakem okolností mohou sáhnout k nečestným praktikám. Okolnosti, které je k tomu mohou donutit, jsou různé, od lásky k nenávisti, od nedostatků peněz k jejich nadbytku a z toho plynoucí morální degradaci. A konečně třetí skupina lidí, přibližně tedy více než tři čtvrtiny, jsou lidé čestní. Je důležité zabývat se bezpečnosti informací nejen s přihlédnutím k první (osmiprocentní) skupině obyvatel, ale je třeba brát v úvahu i druhou (dvacetiprocentní) skupinu potencionálně nečestných“[29]



Graf 1: Lidské hrozby

Zdroj: RODRYČOVÁ, D. *Bezpečnost informací*

2.10. Monitorování a řešení bezpečnostních incidentů

Incidenty, které mohou ohrozit bezpečnost, by měli být co nejdříve hlášeny se stanovenými řídícími cestami. Cílem je minimalizovat škody způsobené bezpečnostními incidenty a chybami, sledovat je a ponaučit se z nich.

[29] RODRYČOVÁ, D. *Bezpečnost informací*, 2000. Str. 15.

„Všichni zaměstnanci a smluvní strany by měli znát postupy hlášení různých typů incidentů (narušení bezpečnosti, možné hrozby, slabiny nebo chybné fungování), které mohou mít dopad na bezpečnost aktiv organizace. Zjištěné bezpečnostní incidenty nebo podezření by měli ihned hlásit na určené místo.“[30]

2.11. Řízení kontinuity[31]

Obecně se plánování kontinuity definuje jako komplexní proces na sebe navazujících činností, které nereagují až na vzniklý problém, ale snaží se haváriím předcházet. Za riziko (havárii) lze považovat přírodní katastrofu, cílený útok na organizaci, selhání služeb dodavatelů nebo virový útok, chyba administrátora či chyba technologií poskytující služby.

Prakticky každý výpadek má za následek ztrátu zisku, produktivity popřípadě i úbytek zákazníků.

Zjednodušeně řečeno, správně zvládnuté řízení kontinuity má za cíl, že v okamžiku havárie, budou všichni zaměstnanci vědět co dělat. Jedním z hlavních výstupů tohoto procesu je tzv. Business Continuity Plan, který slouží jako scénář, jak co nejefektivněji obnovit normální chod společnosti.

2.12. Postup při řízení změn

Úvodem bych ráda upozornila na fakt, že bezpečnost informačních systémů není jen síťové propojení, servery a software, ale že zahrnuje i budovy, dokumenty a to nejpodstatnější – lidi. V další části práce se zaměřím na zjištěné nedostatky a jak je lze

[30] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 22.
[31] *Řízení kontinuity činností* [online]. 2009 [cit.2009-3-11]. Dostupný z www: http://www.aec.cz/cz/sluzby/rizeni-kontinuity-cinnosti

efektivně eliminovat, či úplně odstranit. V této části práce budu vycházet především z použitého zdroje *Information Security and Employee Behaviour*, od autora *Agnuse McIlwraitha*.

Hlavní myšlenkou je víceliniová obrana, kterou má společnost nastavenou. Jedná se o menší pravděpodobnost penetrace (průniku) a širší možnosti pro detekci útoku. Mnoho lidí si může myslet, že několik vrstev technologií jako FW, IDS, DMZ zahrnuje hlubokou ochranu, avšak na základě publikovaných průzkumů a analýz vyplynulo, že největší ohrožení pro naše technologické prostředí jsou lidé/zaměstnanci sami. Nejde jen o jednorázové odstranění zjištěných nedostatků, ale o způsob, jak nastavit celý proces průběžného zlepšování uvědomění všech pracovníků a jejich další postupné změny chování v oblasti vnímání informační bezpečnosti.

Praktická strategie a techniky:

Nejedná se o metodu, ale se o sadu doporučení a konstrukcí, které mohou být lehce adoptovány pro reálné použití v organizaci. Níže uvedený systém je orientován na jednotlivé kroky, které zahrnují řadu akcí.

a) řízení podle skutečnosti
b) cíle a úkoly
c) plánování
d) implementace opatření
e) zpětná vazba

ad a) iniciativa v uvědomění informační bezpečnost začíná sérií otázek:

- Je nutné uskutečnit takovou iniciativu?
- Co je nutné pro to udělat?
- Jaké je povědomí o bezpečnosti u zaměstnanců a na jaké úrovni?
- Co uživatelé znají (prokazatelné vědomosti a znalosti)?
- Jak vnímají aktuální situaci/stanoviska?

- Jaké je jejich chování?

Zjišťování úrovně znalostí, stanovisek a chování je technika dobře známá např. v marketingu. Hlavní záměr uvědomovacích iniciativ je snaha změnit chování, avšak za předpokladu, že pracovníci budou rozumět důvodům, proč má ke změně dojít. Prvním krokem je získání základní informace o stavu bezpečnostního povědomí. Jednou z pomůcek pro stanovení „kde a kdy“ investovat do bezpečnosti je Riziková analýza (RA). Jsou používány různé metody, např. Cobra – Security risk analysis. Dalším základním aspektem řízení podle skutečnosti je identifikace a klasifikace potencionálně dotčených pracovníků. Obvykle se užívá dělení podle pracovního zařazení, typu práce nebo umístění. Z tohoto členění obvykle vyplývá i návaznost na rozdílné způsoby komunikace, které lze pro daný účel použít (např. intranet, školení, zprávy apod.).

Ad b) tento krok zahrnuje takové kroky jako:

- Informace pro zaměstnance o rozsahu iniciativy.
- Provedení základních školení pro relevantní skupiny v rozsahu schválených standardů.
- Identifikace a stanovení jednotlivých úkolů (na základě analýz a expertních posudků).
- Cíle mají vyšší úroveň než úkoly.

Např. cíl je:

zajistit, aby všichni zaměstnanci znali jejich osobní roli a s tím spojenou odpovědnost v rámci bezpečnostní politiky.

Ad c) Plánováním ve smyslu tohoto bodu se myslí stanovení rozumných časových horizontů s ohledem na předpokládaný rozsah a jeho splnění. V konkrétním zaměření na dané cíle se jedná o plánování na několik let se standardním cyklem „Plan-> Do-> Check-> Act“. Několikaleté plánování vychází na základě zkušeností a prostého faktu, že změna „firemní kultury“ spotřebuje nejvíce času a přináší výsledky se značným časovým odstupem. Existuje řada způsobů, jak pobídnout zaměstnance ke změně jejich

chování – od systémů tvrdých nařízení až po systém motivačních pobídek. Při tomto porovnání je možné rozeznat jak „zdravá“ je společnost. Některé taktiky zdůrazňují, že nejlepší výsledky jsou při inkrementálních (postupných) změnách než systém „velkého třesku“. Dalším motivačním krokem může být princip reciprocity – „něco za něco“ a nemalý význam má i budování týmového podvědomí.

Ad d) Implementace – v tomto kroku je již realizován plán jednotlivých připravených změnových kroků. Obvykle až při realizaci změn se ukáže, jak kvalitní byla příprava v předchozích krocích a zda časování akcí bylo správné.

Ad f) Zpětná vazba – za předpokladu, že metriky byly stanoveny s odpovídající citlivostí, bychom měly průběžně dostávat informace, jak jsou úkoly plněny, jakým způsobem se mění chování a přístup zaměstnanců a tedy, jak je naplňován stanovený cíl.

2.13. Fyzické zabezpečení[32]

Cílem fyzického zabezpečení je předcházet neautorizovanému přístupu, poškození a zásahům do prostor a informací organizace.

Prostředky IT, které zpracovávají kritické nebo citlivé informace organizace, by měli být umístěny v bezpečných zónách s odpovídajícími bezpečnostními bariérami a vstupními kontrolami. Jejich ochrana by měla odpovídat zjištěným rizikům. Organizace by měly využívat bezpečností perimetr k ochraně oblastí, ochraňujících prostředky pro zpracování informací. Bezpečnostní perimetr je cokoliv, co vytváří bariéru, např. zdi, vstupní turniket na karty nebo recepce. Jeho umístění a úroveň by měla vycházet z kapitoly Hodnocení rizik.

Podle vhodnosti by měla být implementována následující doporučení:

[32] BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. 2001. Str. 23.

a) Bezpečnostní perimetr by měl být jasně definován.

b) Perimetr budovy nebo oblasti obsahující prostředky pro zpracování informací by měl být v řádném stavu (tj. neměl by obsahovat slabá, lehce proniknutelná místa).

c) Pro kontrolu fyzického přístupu do objektu nebo budovy by mělo být využíváno recepce nebo jiných prostředků. Vstup by měl být umožněn pouze oprávněným osobám.

d) Fyzické bariéry by měly sahat od podlahy až po strop, aby chránily v případě potřeby před neoprávněným vstupem, požárem či povodní.

e) Požární dveře by měli obsahovat alarm a měli by být stále zavřené.

2.13.1 Kontroly vstupu osob

Mělo by být zaručeno, že do bezpečných oblastí mají přístup oprávněné osoby.

Měla by být zvážena následující opatření:

a) Návštěvníci vstupující do bezpečných zón, kteří nejsou prověřeni, by měli být pod dohledem (datum a čas příchodu a odchodu by měl být zaznamenán). Návštěvníci by měli získávat oprávnění přístupu jen ze specifického důvodu a měli by být seznámeni s předpisy o bezpečnostních požadavcích.

b) Přístup k citlivým informacím a prostředkům zpracovávající informace by měl být kontrolován a umožněn pouze oprávněným osobám. Auditní záznam by měl být bezpečně uchováván.

c) Od všeho personálu by měla být požadována nějaká forma viditelné identifikace a personál by měl vyzvat každého cizince bez doprovodu a bez viditelného označení k prokázání oprávnění.

d) Přístupová práva do zabezpečených oblastí by měla být pravidelně kontrolována a aktualizována.

2.13.2 Zabezpečení kanceláří, místností a zařízení

Výběr a návrh bezpečné oblasti by měl brát v úvahu možnosti poškození požárem, zatopením, výbuchem, občanskými nepokoji a jinými druhy přírodních nebo lidských hrozeb. Počítat by se mělo i s odpovídajícími úpravami a normami pro bezpečnost a ochranu zdraví při práci.

Měla by být zvážena následující opatření:

a) Důležitá zařízení by měla být situována tak, aby nebyla veřejně přístupná.

b) Budovy by měly být nenápadné, aby co nejméně naznačovaly jejich účel.

c) Dveře a okna by měly být uzamčeny, pokud jsou bez dohledu. U oken, zejména pokud se jedná o přízemí, by mělo být zváženo využití externích ochranných prvků.

d) Vnější dveře a dosažitelná okna by měla být chráněna vhodným detekčním systémem pravidelně testovaným a odpovídajícím průmyslovým normám.

e) Prostředky pro zpracování informací spravované organizací by měly být fyzicky odděleny od prostředků třetích stran.

f) Adresáře a interní telefonní seznamy, na jejichž základě by mohlo být zjištěno umístění prostředků pro zpracování citlivých informací, by neměly být přímo přístupné veřejnosti.

3. Návrh řešení

Tato část práce vycházela porovnáním analýzy současného stavu s teoretickými předpoklady a obsahem bezpečnostních směrnic společnosti. Porovnáním těchto informací vyplynuly rozdíly, které lze považovat za nedostatky v BP, na které je potřeba se zaměřit a jejich případné následky eliminovat či odstranit. Návrh bezpečností politiky není jednorázová akce, jedná se o velmi zdlouhavý, prakticky nikdy nekončící proces, kde dominantní úlohu představují lidé – zaměstnanci, v rolích uživatelů i správců. Sestavení bezpečností politiky je jedna věc, ovšem pravidla a způsob jejich dodržování je důležitý proces, který nesmí být podceněn.

Je obecně známá statistika, že bezpečnostní incidenty jsou z cca 70% způsobeny interními uživateli a většina takových incidentů jde na konto uživatelských chyb, nehod a ignorace. Zde se potvrzuje ta skutečnost, že není naplněna myšlenka integrace bezpečnostních zásad do běžných provozních praktik formou srozumitelných bezpečnostních politik a adresným školením pracovníků.

Zhodnocení:

Plnění požadavků bezpečnosti ve vztahu analýza-teorie-ustanovení vnitřních směrnic:

- Inventura a klasifikace.
- Bezpečnost komunikací.
- Auditování.
- Fyzická bezpečnost a bezpečnost prostředí.
- Řízení přístupu.
- Interní a legislativní pravidla.
- Secure network a Operative Management.
- Bezpečnost v Managementu HR.
- Havarijní plánování.
- Vývoj a údržba systémů.
- Odhad a akceptace rizik.
- Externí partneři.

3.1. Inventura a klasifikace (Směrnice BP-IT-1)

IT cíle spojené s procesy hlavní činnosti v rámci E.ON Energy Group jsou identifikovány a klasifikovány podle stupně ochrany, které jsou požadovány. To zahrnuje informace, které musí být obecně chráněny, jako jsou hardware a software.

Pracovníci jsou si vědomi toho, že v IS jsou uložena data, která jsou citlivá ve smyslu důvěrnosti firemních dat, zákonů o ochraně osobních údajů a obchodního zákoníku, ale neexistuje přehled o tom, o která data přesně jde, kde jsou uložena a jakým způsobem k nim lze přistupovat. Inventární seznamy, jak je požadováno ve směrnici, jsou jen částečně k dispozici.

Neexistují psaná pravidla, podle kterých by zaměstnanci byli schopni sami rozhodnout/rozeznat, jak a která konkrétní data jsou citlivá na zajištění potřebné míry zabezpečení. Oprávnění a pravomoci jsou zaměstnancům přidělovány podle jejich zařazení na určitou pozici. Delegace pravomocí přichází v úvahu v případě nepřítomnosti vlastníka. Takový případ je řešen tak, že v době nepřítomnosti vlastníka se řeší pouze operativní záležitosti a vlastníkem je vedoucí příslušného oddělení, nebo osoba, které je řešení problému nejbližší.

Nedostatek jsem však nalezla ve slabé definici zařazení, tzn., že není jasně definován rozsah oprávnění a tomu odpovídajících povinností.

Navrhuji:

Splnit požadavky na klasifikaci dat formou inventárních seznamů a určit konkrétní stupeň zabezpečení pro konkrétní cíle.

Určit období pro reklasifikaci, neboť citlivost se časem mění. Cílem je zajistit, aby se zbytečně nechránily údaje, u kterých to není nutné.

Stanovit postupy pro ustanovení vlastníka důležitého aktiva IT v inventárních seznamech a pro případ jeho dlouhodobé nepřítomnosti. Cílem je zajištění kontinuity bezpečnosti všech prostředků IT.

Oddělení Řízení rizika vypracují dokument, který bude obsahovat:

- Pravidla pro sestavení inventárních seznamů, které budou obsahovat všechny potřebné informace-tzn., identifikaci vlastníka, charakter dat a požadavek na zabezpečení pro každý IT cíl i pro každou skupinu.
- Popis důvěrných informací, takovým způsobem, aby uživatelé byli schopni rozpoznat citlivost informací.
- Označení důvěrných informací bude snadno pochopitelné a umístěné na jasně definovaném místě.
- Pro reklasifikaci dokumentů navrhuji roční periodu.

Oddělení interního auditu bude odpovědné za:

- Kontrolu a zajištění toho, aby byl inventární seznam správný a kompletní.

3.2. Bezpečnost komunikací (Směrnice BP-IT-2)

V praktickém procesu, dodržování ustanovení této směrnice není v rozporu se skutečným stavem, případný nesoulad je ve věci jasné klasifikace přenášených informací, kterou řeší jiná směrnice. V povolení přístupu na Internet nejsou žádné varianty, přístup je buď povolen, nebo ne, případné znepřístupnění jistých webových stránek je zabezpečováno mimo uživatele a správu v rámci skupiny E.ON ČR.

Při používání bezdrátových technologií pro síťové připojení však nejsou ošetřena všechna rizika. Použití WLAN technologií na přenosných zařízeních je podmíněno zajištěním šifrování datového toku.

Navrhuji:

Důslednější provádění informačních kampaní k lepšímu povědomí o zařazování dat z pohledu citlivosti na bezpečnost a manipulací s nimi, zejména při použití přenosných zařízení.

Za přípravu a obsah kampaní je odpovědný CIO team, průběžná kontrola je v kompetenci vedoucích jednotlivých útvarů. Pravidelným proškolováním zaměstnanců by se měla prohloubit jejich orientace ve věci manipulace s citlivými daty.

3.3. Auditování (Směrnice BP-IT-3)

Audit je cílená zkouška situace ve srovnání se stanoveným standardem. Pro informační bezpečnost může být tento standard dán vnitřními směrnicemi nebo obecně akceptovanými národními a mezinárodními standardy.

Koncepty pro audit v rámci E.ON ČR sice existují, ale jsou jen velmi rámcové a z pohledu nejvyšší úrovně, tedy neřeší detaily. Monitorovací systém pro audit není automatizovaný, aktivuje se jen na základě již vzniklého incidentu nebo požadavku.

Náprava v tomto případě není možná, ve směrnici uvedený rozsah monitoringu není uvažován pro úroveň tzv. Business Unit tvořené skupinou E.ON v ČR, ale až pro několik BU a je prováděn v Německu. Je nutné zdůraznit, že správa ICT systémů v rámci všech skupin E.ON v současnosti prochází obrovskou restrukturalizací a již není možné zjistit „jak to bylo“ a ještě horší je zjistit „jak to bude“.

Navrhuji:

CIO team každý měsíc vyhodnotí provozní reporty generované poskytovatelem služeb a tyto dokumenty předá oddělení interního auditu pro případ provedení vlastního auditu. I přes zmíněnou restrukturalizaci, není možné tyto kontroly nevykonávat, tzn., že oddělení interního auditu bude zabezpečovat vyhodnocování reportů až do doby, kdy bude monitorování systémů automatizováno.

Oddělení interního auditu vypracuje zadávací dokument pro monitorování systému, který bude splňovat:

1. Budou určeny cíle a specifikace monitorování systému.
2. Zařízení pro monitoring a reportování dat musí být chráněno proti neautorizovanému přístupu a neautorizovaným změnám v report souborech.
3. Stanoví, za jakých podmínek budou reporty přezkoumávány.
4. Soubory reportů budou pravidelně zálohovány k možnosti pozdějšího přezkoumání.
5. Monitorování systémových událostí a síťového provozu může být prováděno jen autorizovanou a kvalifikovanou osobou.
6. Každý zaměstnanec si musí být vědom toho, že všechny události ve vztahu k zabezpečení jsou monitorovány a zaznamenávány.

3.4. Fyzická bezpečnost a bezpečnost prostředí (Směrnice BP-IT-4)

Některé IT prostředky se stále nacházejí mimo bezpečné zóny. Jedná se především o tzv. technické místnosti, kde jsou umístěny aktivní síťové prvky, moduly telefonních ústředen, případně dohledové servery. Na jedné straně jsou tyto místa převážně v prostorách běžným návštěvníkům nepřístupná, ovšem v případě cíleného útoku, nejsou nijak mimořádně zabezpečena. Obsahují pouze obyčejný zámek a bezpečnostní systém. Není vypracovaný jmenný seznam s rozsahem oprávnění pro jednotlivé sledované prostory, dokumentace o záznamech přístupů není vedena s požadovanou důsledností, nejsou vypracována jednotná pravidla pro energetické a neenergetické prostory, není důsledně dodržen princip oddělení technologií. Jinou nesledovanou kategorií, z pohledu směrnice, jsou paměťová média – domnívám se, že z důvodu absence inventury (viz bod 3.1) není v dostatečné míře uvědomění o závažnosti případného konfliktu při manipulaci s FD, CD, DVD a externími paměťovými médii.

Navrhuji:
Provést důslednou inventuru zařízení v technických místnostech, doplnit jejich klasifikaci z pohledu bezpečnosti a nastavit odpovídající opatření dle nejvyššího

požadavku pro daný objekt, dále sjednotit a zveřejnit pravidla pro přístup do těchto prostor, včetně monitorování a záznamů o návštěvách, vytváření reportů a jejich auditování.

Náprava ve věci manipulací s paměťovými médii musí opět začít u inventury a klasifikace ve věci přístupu k informacím a důsledného pravidelného proškolování a prověřování, zda jsou manipulace s médii prováděny korektně ve shodě se zněním směrnice.

Přípravu osnovy pro školení zajistí CIO team.

Dále, CIO team zajistí detailní audit veškerého IT vybavení a následně pomocí směrnice BT-IT-4 navrhne realizaci opatření, aby byla aktiva chráněna podle jejich citlivosti.

Navrhuji, aby bylo využito auditu IT, který vyplyne z kapitoly 3.1. a následně oddělení Řízení rizik za pomocí směrnice o Fyzické bezpečnosti a bezpečnosti prostředí, zařadí aktiva do příslušných kategorií.

3.5. Řízení přístupů (Směrnice BP-IT-5)

Přidělování přístupových práv a oprávnění je v podstatě prováděno systémem „dědictví“, kdy je rozsah oprávnění posuzován podle toho, co měl předchozí pracovník eventuelně pracovník se stejnou rolí, s tím, že v podvědomí jednotlivých vedoucích útvarů, kteří schvalují požadavky, je zakořeněno, že poskytovatel služby je ten subjekt odpovědný za přidělená oprávnění. Z valné většiny si neuvědomují, že tato odpovědnost je na nich. Pro dokumentaci a sledování použití ID se zvláštními oprávněními nejsou formálně vypracována pravidla a celkový přehled/report těchto ID není veden.

Navrhuji:

Znovu se zde potvrzuje absence podrobné inventury IT aktiv s přidělením odpovědností a znalostí o účelu a použití příslušného aktiva, na které by navazoval systém povolených přístupů.

Tento bod zajistí CIO team, tzn., že:

- Vypracuje dokument o přidělování přístupových práv a jejich rozsahu.
- Vypracuje dokument o zvláštních oprávněních.
- Vypracuje pravidla o celkovém přehledu používání ID.

3.6. Interní a legislativní pravidla (Směrnice BP-IT-6)

Společnost E.ON Energie Group má odpovídající mechanismy pro zajištění souladu s předpisy a zákony autorských práv, patentových zákonů a licenčních smluv.

Ustanovení směrnice je dodržováno jen neúplně, doklady o nákupech licencí na SW jsou ukládány na straně logistiky – nákupu, kde jsou archivovány smlouvy a objednávky ale jen z pohledu účetnictví, provozní dokumentace ve smyslu směrnice je udržována jen částečně a dohledání např. platnosti licencí či placené údržby (SW maintenance) je velmi obtížné. Opět je nutné zdůraznit, že absencí inventury IT aktiv není pro běžného uživatele dohledatelné, zda který konkrétní SW je ve společnosti povolen a za jakých podmínek. Monitoring používání IT prostředků je prováděn až na vyžádání, nepravidelně je provedena inventura instalovaného SW. Problém s instalací nepovoleného SW by měla řešit implementace tzv. EDTS (E.ON Desktop Standard) kdy při každém zapnutí uživatelského počítače bude prováděna kontrola na instalovaný SW a případné nesrovnalosti proti standardu dané kategorie budou eliminovány

Navrhuji:

Použít doporučení vyplývající z ITIL Service Support, instalovat a provozovat CMDB (Configuration Management Database). Tento krok by byl téměř ideální řešení pro odstranění slabých míst nejen z pohledu sledování licencí, ale i z pohledu již několikrát zmiňované potřeby pro inventuru IT aktiv.

Zajistí oddělení CIO teamu ve spolupráci s poskytovatelem služeb.

3.7. Síťová a provozní bezpečnost (Směrnice BP-IT-7)

V rámci E.ON Energie Group a jejich zákazníků je mnoho systémů IT propojeno. Ochrana infrastruktury sítě je proto základem pro bezpečnost IT, která je celopodniková. Musí být zřízena infrastruktura sítě, která plní definované požadavky týkající se důvěrnosti, integrity, dostupnosti a odpovědnosti. Jednotlivé body, které jsou uvedeny v následujících kapitolách, se týkají všech vlastníků IT systému v rámci IT infrastruktury.

Oproti ostatním směrnicím je tato nejobsáhlejší. Tato směrnice je zaměřena na poskytovatele služeb a správu aktiv, které jsou pro uživatele skryté. Lze konstatovat, že provozní postupy jsou zdokumentovány jen částečně, taktéž záznamy prováděných činností jsou spíše zaměřeny na vykazování odpracovaných hodin, méně na popis co bylo vykonáno. Je dost zřejmé, že prováděné činnosti, pokud jsou dokumentovány, tak jsou dokumentovány jen jednotlivými pracovníky, neexistuje něco jako společná databáze, s takovou informační hodnotou, aby např. zastupující pracovník pročtením záznamu u konkrétního zařízení mohl snadněji zjistit problém nebo naopak jakou předchozí činností byly či nebyly změněny parametry, konfigurace apod. Vzhledem k neustálým změnám je velký problém dokončování projektů. Nedostatkem zdrojů, ať lidských či finančních, jsou provedeny jen nejnutnější klíčové akce a na dokončení už nezbývají kapacity.

Tento proces je nejmarkantnější při předávání výstupu projektu do provozu, kdy přebírá správu provozní útvar, ale přebírá de facto „polotovar“ se kterým je následně nucen dělat opatření se kterými nepočítal.

Navrhuji:

V tomto případě se jedná ne o jednorázovou akci, ale o soubor akcí, které budou směrovat k naplnění požadavků směrnice. Jak jsem mohla zjistit, v rámci posledního

restrukturalizačního projektu jsou plánovány kroky v souladu s ITIL, které by měly vést k nastavení procesů, které budou plně vyhovovat požadavkům směrnice.

CIO team vypracuje zadání pro vytvoření databáze, která bude obsahovat a zdokumentovávat provozní postupy a záznamy prováděných činností. Musí to být zajištěno takovým způsobem, aby provozní zaměstnanci tyto záznamy prováděli, a budou stanoveny postihy za neplnění těchto povinností. Za kontrolu bude odpovědný útvar CIO.

Zálohování dat - po technické stránce je zálohování a archivace dat na odpovídající úrovni v poměru k důležitosti dat. Nicméně plány obnovy a kontinuity nejsou vypracovávány průběžně s technickým řešením, nejsou pravidelně udržovány a testovány.

Proto navrhuji, aby byl vypracován plán obnovy dat, kde budou použity vhodné metody k určení zda:

- Zda mohou být všechna data obnovena.
- Postup zálohování je reálný.
- Je k dispozici dostatečná dokumentace pro vytváření zálohování, které povolí náhradní pověřený zaměstnanec pro obnovení dat.
- Doba, která je požadována na obnovu dat splňuje požadavky týkající se dostupnosti.

3.8. Bezpečnost v řízení HR (Směrnice BP-IT-8)

Lze konstatovat, že formální stránka uvedené směrnice, ve věci zmíněných dokumentů, se naplňuje, co však doposud není splněno, je vlastní rozsah a konkrétní náplň pro praktické školení.

Navrhuji:

Sestavit srozumitelnou bezpečnostní příručku, jak v elektronické tak i v tištěné formě, a současně pořádat průběžná školení se závěrečným otestováním na porozumění problematiky.

Průběžně vyhodnocovat zmíněné testy a věnovat i pozornost tomu, co školené zaměstnance zajímá, kde vidí problémy a nedostatky.

Příručku vypracuje CIO team ve spolupráci s personálním útvarem a postará se i o pravidelné vyhodnocování. Navrhuji, aby školení probíhaly dvěma způsoby:

a) školení přímým nadřízeným – minimálně dvakrát ročně. Při tomto školení bude kladena zodpovědnost na jednotlivé vedoucí, aby školení nebylo pouze formální, ale aby školená témata pro podřízené byla srozumitelná a konkrétní. Podklady pro tato školení budou připravována Security managerem CIO teamu a vyvěšována na intranetu.

b) školení externí firmou – jednou ročně pro všechny zaměstnance. Pracovník externí firmy bude provádět nejprve školení a poté se více zaměří na aktuální, nová témata. Součástí tohoto typu školení bude závěrečný anonymní test znalostí posluchačů. Tento test poslouží k průzkumu znalostí mezi zaměstnanci a ukazuje, na co se další školení musí více zaměřit.

Kromě toho budou školeni všichni zaměstnanci, kteří vstupují do zaměstnaneckého poměru a dostanou k používání PC, NB či jiná zařízení pro přístup k informacím.

Obsahem školení budou zejména oblasti:

1) Cíle a principy bezpečného používání výpočetní a komunikační techniky.
2) Vysvětlení základních pojmů bezpečnosti IT.
3) Ochrana proti škodlivému SW -viry a antivirová ochrana, spam, spyware, hoax, phishing, pharming atd.
4) Elektronická pošta – správné chování při odesílání a příjmu.
5) Elektronický podpis – význam, použití a ochrana.

6) Hesla – volba správného hesla, uchování hesla, ochrana hesla.
7) Internet – bezpečné chování na internetu.
8) Ochrana dat -zákonné normy, klasifikace dat, uchovávání, přenos, likvidace, zálohování, archivace dat, kdo je vlastník dat.
9) Sociální inženýrství – co to je, jak se proti němu bránit.
10) Bezpečnostní incidenty – chování při mimořádných událostech.
11) Ochrana přenosných počítačů.

3.9. Havarijní plánování (Směrnice BP-IT-9)

Krizový stav je událost, která může způsobit značně velkou škodu a nemůže být řešena prostřednictvím běžných provozních procesů z důvodu narušení po čas nápravy.

Pokud by byl dotázán pracovník útvaru poskytující IT služby, zřejmě by na otázku existence havarijních plánů odpověděl kladně, na otázku jak by tyto plány byly naplňovány už je odpověď nejasná. Opět musím poukázat na momentální situaci, kdy se mění organizační struktura poskytovatele a provádí se přesuny zařízení, v minulém období byly havarijní plány připravovány, ale nebyly odzkoušeny, resp. byly otestovány simulací. Předpokládám, že po „usazení“ nové organizační struktury budou stávající havarijní plány aktualizovány a měl by být i dostatečný kapacitní potenciál na reálné otestování.

Navrhuji:

Oddělení CIO společně s koordinátory procesů definují krizové plány a určí strategii postupů, která bude následně platná pro celou skupinu, a jenž zaručí provozuschopnost kritických obchodních procesů.

Bude vypracován dokument, který bude obsahovat:

1) Návod jak postupovat bezprostředně po mimořádné události,
2) kontakty na členy Krizového štábu,

3) seznam kritických funkcí vzhledem k IT a v jakém pořadí je třeba je obnovovat,
4) náhradní pracoviště pro obnovu provozu,
5) způsob spolupráce s Krizovým štábem,
6) seznam a umístění materiálů umístěných mimo sídlo atd.

Dále by mělo docházet k testování havarijního plánu, tzn., jak budou plány fungovat v reálném životě. Testování by mělo probíhat v několika vrstvách, od technických testů přes simulaci pro zaměstnance v řídících pozicích v krizových týmech po simulaci havárie, které se zúčastní všichni zaměstnanci.

Následně bych doporučovala zrealizovat zpětnou vazbu se zaměřením:

a) na povědomí zaměstnanců o havarijních plánech
b) zjištění slabých míst v havarijních scénářích
c) směr dalšího školení a případně jeho zlepšení
d) kde by bylo potřeba současný stav změnit

Co se týče zpětné vazby o povědomí zaměstnanců v oblasti IT bezpečnosti, navrhuji systém sociálního inženýrství, o kterém by s předstihem věděli jen osoby vrcholového managementu a na základě výsledků testu se poměrně snadno vyhodnotí, jak si zaměstnanci vedou v krizové situaci. Podobné testy by se provozovaly pravidelně.

3.10. Vývoj a údržba systémů (Směrnice BP-IT-10)

Uvedená směrnice je směrována na útvary, které provádí vývoj SW, pro posuzovaný rozsah posouzení bezpečnosti je zde uváděn pro úplnost, v posuzované společnosti nedochází k vývoji SW, vývoj je zajišťován outsourcingem a v tomto případě je ustanovení směrnice dodrženo. Není však vedena jednotná dokumentace pro údržbové činnosti, resp. není naplněno znění směrnice v požadavku na vypracování sady pravidel pro vykonávání údržbových prací.

Navrhuji:

CIO team vypracuje zadání pro prováděcí předpis pro údržby se zahrnutím interních i externích zdrojů.

3.11. Odhad a akceptace rizik (Směrnice BP-IT-11)

V této podnikové směrnici jsem neobjevila žádný rozpor mezi dokumentem a tím, jakým způsobem je realizováno havarijní plánování.

3.12. Externí partneři (Směrnice BP-IT-12)

Kontakt s externími partnery je specifikován ve dvou oblastech. První oblast se týká outsourcingu, přičemž zpracovávané informace jsou poskytovány jiné společnosti, která není součástí skupiny E.ON nebo jejích Business Units. Druhá oblast zahrnuje fyzický a logický přístup ze strany externích partnerů - technici nebo konzultanti. Smlouvy s externími partnery musí být formulovány takovým způsobem, aby byly chráněny důvěrné prostředky IT.

Vazby s externími partnery jsou řešeny formou SLA (Service Level Agreement) v oblasti outsourcingu ICT služeb (E.ON IT) a minoritně smlouvami s jinými subjekty.

Dominantně se smluvní vazby s dalšími externími partnery nechávají na outsourcingovém partnerovi a pokud dojde ke změnám, jsou z pohledu E.ON ČR řešeny změnovým řízením v SLA. V této oblasti není zjevný rozpor s ustanovením směrnice.

4. Zhodnocení a závěr

V této bakalářské práci jsem se zaměřila na společnost E.ON Česká republika, s. r. o. a pokusila se analyzovat její zabezpečení v oblasti IT. Tato společnost je na technických prostředcích závislá a výpadek či ztráta dat by pro firmu mohly představovat fatální následky.

Prvním krokem při zpracování této práce bylo analyzovat současný stav bezpečnostních politik, kde jsem se zaměřila na analýzu využívaného hardwaru a softwaru, archivaci a zálohování dat a na infrastrukturu a řízení procesů ICT. V této analýze jsem zjistila řadu nedostatků různé úrovně závažnosti, a je tedy zapotřebí, aplikovat prostředky, které by případná rizika či hrozby eliminovaly.

Skupina E.ON má vytvořených mnoho směrnic, které z velké míry vycházejí z bezpečnostního standardu 7799 a které jsou tvořeny v Německu. Tyto směrnice obsahují veškeré teoretické předpoklady ohledně bezpečnosti IT a definují oprávnění uživatelů či postup při řízení rizik. Slabé místo jsou však lidé-zaměstnanci, kteří těmto směrnicím zcela nerozumí a tím pádem dané postupy odmítají.

V části vlastního návrhu řešení jsem se tedy pokusila upozornit na části, které jsou po teoretické stránce v pořádku, ale praktické využití zaostává. Navrhla jsem řešení, jak by se mohlo postupovat k dosažení toho, aby směrnice měly význam, tzn., aby jim lidé lépe porozuměli. Společnost vložila do vytvoření směrnic a postupů řadu finančních či jiných prostředků a je tedy škoda, aby předem stanovených cílů nebylo dosaženo z důvodu špatné implementace.

Seznam použité literatury

Knižní publikace

1) BRAGG R., RHODES-OUSLEY M., STRASSBERG K. *Network Security The Complete Reference*. 1. vydání. United States: McGraw-Hill Professional, 2003.896s. ISNB: 0072226978.

2) ENDORF C., SCHULTZ E., MELLANDER J. D*etekce a prevence počítačového útoku*. Praha: Grada, 2005. 356s. ISNB: 8024710358.

3) MAIWALD, E. *Network Security A Beginner's Guide*. United States: McGraw-Hill Companies, 2001. 400s. ISNB: 072133244.

4) MCILWRAITH, A. *Information Security and Employee Behaviour*. England: Grower Publishing Company, 2005. 165s. ISNB: 566086476.

5) MLÝNEK, J. *Zabezpečení obchodních informací*. Brno: Computer press, 2007. 154s. ISNB: 8025115114.

6) RODRYČOVÁ, D. *Bezpečnost informací jako podmínka prosperity firmy*. Praha: Grada, 2000. 144s. ISNB: 8071691445.

7) THO, I. *Managing the Risk sof IT Outsourcing*. United Kingdom: Copyright, 2005. 206s. ISNB: 750665742.

8) TOWNSEND, JAMES J., RIZ, D., SCHAFFER, D. *Bulding Portals, Internets, and Corporate Web Sites Using Microsoft Servers.* 1.vydání. United States: Copyright, 2004. 517s. ISNB: 321159632.

Internetové zdroje

9) *Řízení kontinuity činností* [online]. 2009 [cit.2009-3-11]. Dostupný z www: http://www.aec.cz/cz/sluzby/rizeni-kontinuity-cinnosti

10) *Personální bezpečnost* [online]. 1998-8-1 [cit. 2010-3-11]. Dostupný z www: http://www.nbu.cz/cs/ochrana-utajovanych-informaci/personalni-bezpecnost/obecne-k-personalni-bezpecnosti/

11) KANTOR, R. *Zálohování dat* [online]. 2009 [cit. 2010-5-4]. Dostupný z www: http://www.fi.muni.cz/usr/jkucera/pv109/2003/xkantor1.htm

12) PAVELKOVÁ, L. Zálohování a archivace [online]. 2003-3-24 [cit. 2010-5-4]. *Dostupný z www: https://akela.mendelu.cz/~lidak/bif/pavelkova.rtf*

Normy

BS 7799-1:1999 *Information Security Management : Part1: Code of practice for information security management*. Praha : Risk Analysis Consultants, 2001. 69 s.

Seznam obrázků

Seznam tabulek

Seznam grafů

Seznam příloh

Přílohy

Příloha 1: Výpis z OR

Předmět podnikání:

a) Výroba měřicích, zkušebních, navigačních, optických a fotografických přístrojů a zařízení.

b) Provozování vodovodů a kanalizací a úprava a rozvod vody.

c) Ubytovací služby.

d) Opravy a údržba potřeb pro domácnost, předmětů kulturní povahy, výrobků jemné mechaniky, optických přístrojů a měřidel.

e) Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály.

f) Poradenská a konzultační činnost, zpracování odborných studií a posudků.

g) Reklamní činnost, marketing, mediální zastoupení.

h) Služby v oblasti administrativní správy a služby organizačně hospodářské povahy.

i) Mimoškolní výchova a vzdělávání, pořádání kurzů, školení, včetně lektorské činnosti.

j) Výroba elektronických součástek, elektrických zařízení a výroba a opravy elektrických strojů, přístrojů a elektronických zařízení pracujících na malém napětí.

k) Nakládání s odpady (vyjma nebezpečných).

l) Zprostředkování obchodu a služeb.

m) Velkoobchod a maloobchod.

n) Zastavárenská činnost a maloobchod s použitým zbožím.

o) Údržba motorových vozidel a jejich příslušenství.

p) Skladování, balení zboží, manipulace s nákladem a technické činnosti v dopravě.

q) Pronájem a půjčování věcí movitých.

r) Projektování elektrických zařízení.

s) Testování, měření, analýzy a kontroly.

t) Poskytování technických služeb.

Příloha 2: Poskytování HW typu PC

Krátký popis služby, systému:

Služba obsahuje poskytování HW klientské stanice dle níže uvedeného provedení, operačního systému, základního SW, síťové konektivity a datový prostor na serveru. Služba zahrnuje i zvláštní specifikaci NB M – notebook pro managery s příslušenstvím.

Podmíněnost služby

Poskytování této služby je podmíněno následujícími službami:

Název SLA	**Číslo SLA**
DMK = Mobilní kancelář (pro specifikaci NB M)	CZ_300_2_017_10_00_DMK
TMO = Správa mobilních telefonů (pro specifikaci NB M)	CZ_300_9_003_10_00_TMO

Rámcové podmínky:

Toto SLA se řídí podmínkami uvedenými ve „Smlouvě o poskytování ICT služeb“ a je její přílohou.

Pro realizaci správy předpokládáme od objednatele zajištění následujících bodů:

- V případě, že SW licence zůstávají ve vlastnictví Objednatele je nutné, aby instalované aplikace byly Objednatelem prokazatelně vlastněny.
- Instalaci (existenci) potřebné kabeláže v objektech Objednatele ukončené v datových rozvaděčích;
- Zajištění napájení v objektech Objednatele, do míst kde jsou umístěna dodaná zařízení (PC, aktivní prvky sítě, servery).
- Zajištění místa pro umístění dodaného zařízení (aktivní prvky sítě).

Všeobecný popis, popis systému, poznámky:

PC (klientská stanice) je základním vybavením uživatele informačních technologií. Toto pracoviště je tvořeno osobním počítačem v rámci těchto specifikací:

- (PC) včetně myši, klávesnice a monitoru;
- (WS) specifikace (PC), další monitor, duální grafická karta;
- (NB) notebook;
- (NB M) specifikace (NB), vyšší úroveň personifikovaných služeb.

Na klientské stanici je nainstalován základní SW obsahující antivirovou ochranu stanice, komprimační SW, jazykový slovník, prohlížeč PDF souborů a internetový prohlížeč. Klientská stanice je vybavena síťovou kartou pro připojení do LAN Objednatele. Technologický standard pro SLA je dohodnut pro dané vyjednávací období a jeho parametry jsou popsány v příloze č.5.

Dále jsou součástí služby:

- Souborové servery
  - Přístup k uživatelským „home“ adresářům pro ukládání dat;
  - Přístup ke sdíleným adresářům pro skupinovou práci:
    - Skupinový přístup v rámci lokalit,
    - Skupinový přístup v rámci celé ECH.
- Servisní servery:
  - pro automatizovaný update AV a operačních systémů MS Windows na klientských stanicích a serverech;
  - pro centrální zálohování;
  - pro management klientských stanic a serverů;
    Servery jsou vybaveny síťovou kartou pro připojení do LAN. Servery jsou pravidelně zálohovány. Standard pro zálohování je uveden v kap.12.
- Zajištění záložního napájení serverů a aktivních prvků sítě;
- Zálohovací zařízení pro stanovené lokality;
- Racky pro uložení serverů.

Dále služba zajišťuje síťovou konektivitu umožňující spojení mezi klientskou stanicí a dalšími zařízeními jako jsou servery, tiskárny a podobně, i mezi těmito zařízeními vzájemně. Standardním rozhraním pro spojení mezi těmito zařízeními je síť Ethernet.

Všechny postupy a činnosti, které nejsou vyjmenovány v odstavci „Rozsah služby“ popř. jsou vyjmenovány v odstavci „Omezení rozsahu služby“ a Objednatel je vyžaduje, jsou předmětem dalšího jednání.

Rozsah služby:

Služba zahrnuje tyto hlavní činnosti:

Klientské služby

Dodání

- Dodání a instalace klientské stanice;
- Dodání, instalace a konfigurace operačního systému klientské stanice;
- Dodání, instalace AV software na klientu včetně nastavení rezidentní ochrany;
- Dodání, instalace a konfigurace základního software;
- Zavedení klientské stanice do technické evidence.

Provoz

- Správa klientské stanice
- Správa a pravidelná údržba hardware klientské stanice - kontrola správné činnosti systémových komponent (diagnostika HW klientské stanice);
- Správa a pravidelná údržba operačního systému včetně instalace service pack, nových verzí ovladačů a kontrola funkčnosti systému komponent (diagnostika OS klientské stanice);
- Správa a pravidelná údržba AV SW na klientu a kontrola funkčnosti rezidentní ochrany a

dezinfekce klientských stanic;
- Správa základního SW;
- Vedení technické evidence včetně aktuálního umístění zařízení;
- Řešení provozních problémů zahrnující výjezdy k odstranění závad klientské stanice v místě Objednatele;
- Záruční a pozáruční opravy - zajišťování oprav pro hardware, který je předmětem dodávky;
- Konzultace k provozu klientských stanic.

Změny

- Výměna klientské stanice ve stanovených intervalech obměn nebo v souladu se standardem platným na dané vyjednávací období;
- Rekonfigurace a reinstalace klientské stanice, ověření funkčnosti klientské stanice po provedení změny;
- Přestěhování klientské stanice;
- Vyřazení zařízení z technické evidence.

Serverové služby

Dodání

- Dodání a instalace serveru;
- Dodání a instalace HW;
- Dodání, instalace a konfigurace operačního systému;
- Dodání, instalace AV software na serveru včetně nastavení rezidentní ochrany;
- Dodání, instalace a konfigurace UPS;
- Dodání, instalace a konfigurace zálohovacího hardware a software;
- Zavedení serveru do technické evidence.

Provoz

- Řízení provozu serverů;
- Správa a údržba hardware serveru - kontrola správné činnosti systémových komponent (diagnostika hardware serveru);
- Správa a pravidelná údržba operačního systému včetně instalace service pack, nových verzí ovladačů a kontrola funkčnosti systému komponent (diagnostika OS serveru);
- Správa a pravidelná údržba AV software na serveru, kontrola funkčnosti rezidentní ochrany a dezinfekce serverů;
- Správa uživatelů v systému Active Direktory;
- Vedení technické evidence včetně aktuálního umístění zařízení;
- Zálohování dat;
- Řešení provozních problémů zahrnující výjezdy k odstranění závad serveru v místě Objednatele;
- Záruční a pozáruční opravy - zajišťování oprav pro hardware, který je předmětem dodávky;
- Konzultace k provozu serverů.

Změny

- Výměny serverů ve stanovených intervalech obměn nebo souladu se standardem platným na dané vyjednávací období;
- Rekonfigurace a reinstalace serveru, ověření funkčnosti serveru po provedení změny;
- Přestěhování serveru;
- Vyřazení zařízení z technické evidence.

Síťové služby

Dodání

- Zřízení služby v rámci sjednaného rozsahu dodávky v dané lokalitě.

Provoz

- Řízení provozu datových sítí včetně dohledových prostředků sítě zahrnujícího potřebný HW a SW;
- Správa a provoz aktivních prvků datové sítě (hardware, software);
- Správa a pronájem datových okruhů;
- Správa strukturované kabeláže v objektech Objednatele;
- Řešení provozních problémů, opravy poruch aktivních prvků datové sítě, výjezdy k odstranění závad v místě Objednatele;
- Zajištění náhradních dílů a záložních zařízení;
- Servisní podpora výrobce zařízení.

Změny

- Obnova provozovaných prvků datové sítě v souladu se standardem platným na dané vyjednávací období uvedeným v příloze č.5.

Povinnosti a součinnosti Objednatele

Objednatel umožní oprávněným pracovníkům Poskytovatele přístup na svá pracoviště a do míst umístění technologií z důvodu:

- poskytnutí uživatelské podpory;
- instalace a správa hardware a software.

Dále

- uživatel nesmí měnit konfiguraci hardware / software;
- na návrh Poskytovatele schvaluje Objednatel standardy a obměny serverů, síťových technologi a klientských stanic pro vyjednávací období;
- Objednavatel zajistí předání dokumentace Strukturované Kabeláže v objektech.

Omezení rozsahu služby

Součástí dodávky služby není:

- Dodávka spotřebního materiálu (např. disket, CD nosičů);
- Dodání, instalace a konfigurace doplňkových hardwarových komponent (viz služba Periferie)
  např. externí HDD a CD mechaniky, filtry na monitory, bezdrátové periferie k VT;
- Realizace případných nových funkčností a rozšíření „datové sítě“ v dané lokalitě nebo do dalších lokalit a objektů;
- Případné rozšíření funkčnosti nebo rozsahu služby je nutno řešit samostatně mimo tuto službu a po dokončení projektu je možno navýšit rozsah služby. Náklady na tuto práci nejsou zahrnuty do nákladů služby a budou účtovány Objednateli zvlášť.

Charakteristiky služby

Charakteristika	**Popis**	**Sjednaná úroveň dodávky služby**	**Měrná jednotka**
Dodací lhůta	Dodací lhůta je období od podání požadavku na zřízení nebo změnu služby po podepsání předávacího protokolu nebo jiného dohodnutého způsobu převzetí uživatelem.	20	Pd *
Reakční doba	Je doba mezi zaregistrováním požadavku Objednatele a zahájením jeho řešení, případně předání na příslušného řešitele či řešitelskou skupinu.	viz kapitola 9	min.
Počet stanic (min/max)	Poskytovatel eviduje dodanou klientskou stanici a její konfiguraci včetně aktuálního umístění zařízení.	PC+WS 1050/1250 NB+NBM 650/850	ks.

(*) Pracovní dny

Reakční doba na problém a čas řešení problému

Typ problému/ incidentu	**1. úroveň podpory**		**2. úroveň podpory**		**3. úroveň podpory**	
	Potvrzení přijetí	Vyřešení nebo předání na vyšší úroveň podpory	Zahájení reakce	Vyřešení nebo předání na vyšší úroveň podpory	Zahájení reakce	Návrh způsobu řešení
incident	okamžitě (*)	<= 30 min.	<= 4 hod	<= 1 den	<= 2 dny	<= 6 dní

(*) Bez zbytečného prodlení

Předávací místo služby a místa plnění

Předávací místo služby: sídla Objednatele

Místa plnění: Místa plnění služby jsou objekty a pracoviště Objednatele v lokalitách uvedených v příloze č.6.

Provozní doba služby/Doba poskytování podpory

Provozní doba služby	**Po**	**Út-Čt**	**Pá**	**So**	**Ne**	**Svátek**	**Poznámka**
Provozní doba služby	00-24h	00-24h	00-24h	00-24h	00-24h	00-24h	Provozní doba nezahrnuje dobu plánované údržby.

Doba poskytování podpory	**Po**	**Út-Čt**	**Pá**	**So**	**Ne**	**Svátek**	**Poznámka**
Bronze	7-17h	7-17h	7-17h				
Silver	7-20h	7-20h	7-20h				Podpora od 17:00 do 20:00 je formou pohotovosti.

Způsob reakce v pracovní době s podporou:

Od konce pracovní doby je třeba odečíst stanovenou dobu reakce podle úrovně podpory. Incidenty přijaté po této době jsou vyřešeny nebo předány na vyšší úroveň až následující den.

Způsob reakce poskytování podpory ve specifikaci NB M

Pro poskytování podpory uživatelům NB M je ustanovena personalizovaná podpora. Priority při řešení incidentů jsou dány rolí uživatele a v případě rovnosti rolí pořadím nahlášení incidentu uživatelem. Uživatelské role a z nich vyplývající priority jednotlivých uživatelů stanoví za Objednatele CIO.

Pokud je potřeba zásahu podpory v jiné lokalitě, než ve které je podpora umístěna, je nutné k reakční době připočíst čas potřebný na přemístění podpory.

Při aktivaci pohotovosti bude podpora na místě do doby odpovídající dojezdu (průměrná rychlost 50 km/h) plus dvě hodiny (pořadí zpracování je dáno prioritou uživatele).

Časy pro ukládání dat a doba obnovy systému

Data na klientských stanicích nejsou zálohována.

Na síťových discích probíhá zálohování ve dvou cyklech:

- týdenním: V týdenním cyklu běží každý den od pondělí do soboty přírůstkové zálohy a v neděli plná záloha kromě prvního dne v měsíci.

- měsíčním: Měsíční cyklus běží tak že každý první den v měsíci se provede plná záloha na oddělenou sadu pásek.

Příloha 3: směrnice KR 26

1 Cíle

Prvořadým úkolem IT bezpečnosti ve skupině E.ON Energie je zajištění dostupnosti, důvěrnosti a integrity svých vlastních informací a zdrojů, a také těch, které jim byly svěřeny zákazníky a obchodními partnery.
IT bezpečnost by měla zajistit srozumitelnost, spolehlivost a správnost procesů tak, že cíle společnosti budou dosaženy, a poškození vyvolaná výskytem neočekávaných událostí jsou předvídána nebo omezována. Procesy podporované IT jsou vždy vystavovány do oblasti konfliktů, které nastanou mezi zabezpečením, funkcionalitou a náklady na realizaci a provoz.

2 Rozsah platnosti

Koncernová směrnice platí pro E.ON Energie AG a domácích a zahraničních společnosti, které patří do základu konsolidace E.ON Energie AG. Zásady bezpečnosti IT a z nich odvozené směrnice a pokyny k realizaci[3] se týkají společné infrastruktury IT, kterou tyto společnosti využívají (např. corporate network), popř. společných uživatelských systémů (např. SAP R/3); jinak se musí prosadit další opatření, aby se zaručila bezpečnost společně používané infrastruktury IT a aplikací.
Zde formulovaná pravidla (podle znázornění v příloze 2) jsou v souladu s informační bezpečnostní politikou společnosti E.ON AG.
E.ON Energie AG očekává, že se i ostatní společnosti holdingu v tuzemsku a zahraničí, které v současné době nevyužívají společnou infrastrukturu, budou podílet na organizaci bezpečnosti IT a mají, vyhlašují a dodržují shodné zásady.
Úkoly, práva a povinnosti, které zajišťuje osoba pověřená ve společnosti ochranou dat (Data Protection Officer) dle německého spolkového zákona na ochranu dat (Bundesdatenschutzgesetz), zůstávají nedotčené a dále se nebudou uvádět.
E.ON Audit Service a zvláště auditor jsou zodpovědní za činnosti týkající se IT bezpečnosti v oddělení auditu a kontroly.
V případě externích smluvních partnerů musí být zajištěny regulační a dodatkové smlouvy, které odrážejí záměr těchto směrnic. Pokud není externí partner schopen nebo je schopen jen částečně implementovat tyto směrnice, potom musí být určeno samostatné rozhraní pro externího partnera, které musí být monitorováno ve shodě s principy IT zabezpečení.

3 Bezpečnost se týká všech!

Každý zaměstnanec skupiny E.ON Energie je zodpovědný, v rozsahu svých povinností, za vykonávání uvědomělého bezpečnostního chování. Všichni zaměstnanci jsou povzbuzováni k identifikaci sebe sama s předmětem IT zabezpečení a trvalému zajišťování provozní bezpečnosti.
Úspěšná implementace IT bezpečnostní politiky závisí významně na podpoře všech zaměstnanců a dostatečném pocitu zodpovědnosti. Bez plné akceptace tohoto principu a aktivní spolupráce mezi všemi zúčastněnými ve společnosti nemůže být IT bezpečnostní politika úspěšně implementována.

4 Zodpovědnosti / pravomoci

4.1 Bezpečnost je úkol celého managementu

Sledování a aktualizace bezpečnostní strategie IT včetně odvozené politiky a opatření je úkolem celého managementu. Potřebné informace pro tento účel poskytuje reportování IT zabezpečení ve společnosti.
V rámci svých manažerských úkolů jsou všichni vedoucí pracovníci skupiny E.ON Energie zodpovědní za podporu postoje všech zaměstnanců k bezpečnosti IT s cílem soustavného a trvalého zlepšování IT bezpečnostního povědomí pro oblast jejich zodpovědnosti. Za tímto účelem podporují všechny úrovně vedení pokročilá a doplňková školení zaměstnanců stejně tak, jako uvolnění nezbytného vybavení.
Vedoucí pracovníci skupiny E.ON jsou ve své organizační jednotce odpovědni za úplné uplatnění zásad bezpečnosti IT a za splnění úkolů bezpečnosti IT, které jim byly uloženy.
Blíže toto upravuje dokument o organizaci bezpečnosti IT, který je všem zaměstnancům E.ON Energie AG k dispozici na intranetu.

4.2 Information Security Officer

Information Security Officer E.ON Energie AG je zodpovědný za koordinaci a řízení témat IT zabezpečení ve společnosti. Je kontaktní osobou pro všechny zaměstnance z otázkách zabezpečení IT. Reportuje „Board of Management“ po dohodě s IT CIO.
IT Security Forum poskytuje Information Security Officer odborná doporučení a podporu.
Další detaily této funkce a analogických funkcí v obchodních společnostech je možné nalézt v dokumentaci popisující organizaci bezpečnosti IT.

5 Vlastnictví

Za účelem zajištění přiměřené a vyrovnané výměny informací v procesech, a pro vytvoření jasné zodpovědnosti jsou určeni vlastníci všech informací a procesů, které předávají tyto informace ve skupině E.ON Energie.
Tito vlastníci jsou zodpovědní za určení úrovně IT zabezpečení nezbytné pro informace.
Za účelem určení příslušné úrovně IT zabezpečení je využito standardizovaného skupinového předpisu pro klasifikaci informací.

6 Školení a tvorba povědomí

Zaměstnanci skupiny E.ON Energie jsou oprávněni a kvalifikováni k plnění svých povinností. K podpoře jejich vysoké úrovně se zdokonalují jejich vědomosti a schopnosti v pravidelných školících kurzech, které obsahují nezbytné informace o IT zabezpečení.
Zaměstnanci externích společností budou důvěrně seznámeni s příslušnými směrnicemi IT bezpečnosti vhodným způsobem.

7 Směrnice

Principy IT zabezpečení ve skupině E.ON Energie jsou detailizovány a zdůvodněny v IT bezpečnostních směrnicích a souvisejících postupech, které jsou přizpůsobeny na míru procesům, informacím, systémům a organizačním jednotkám společnosti.

Bezpečnost IT Všechny směrnice a postupy odvozené z principů IT zabezpečení jsou pravidelně revidovány na časovou platnost, obsahovou správnost, vhodnost a proveditelnost. Podle potřeby jsou zkontrolovány nebo nahrazeny aktualizovanými dokumenty.
Information Security Officer E.ON Energie AG (nebo IT Security Manager/IT Security Officer provozní společnosti) je zodpovědný za koordinaci těchto revizí.

8 Práce s incidenty

IT bezpečnostní incidenty jsou vyšetřovány bez výjimky a bez prodlení. Poučení z incidentů na základě výsledků vyšetřování jsou implementována a zaměstnanci jsou informováni o výsledcích vyšetřování incidentů vhodným způsobem.
Vyšetřování významných IT bezpečnostních incidentů by mělo být koordinováno skrze IT Security Managera po dohodě s Information Security Officerem a IT Security Auditorem. IT Security Manager je centrální bod pro komunikaci a návrhy pro oblast IT Security.

9 Prověřování a kontrola

Úroveň zabezpečení IT dosažena v E.ON Energie Group v rámci organizačních jednotek, procesů a systémů bude monitorována s využitím kombinace periodicky se opakujících kontrol a zkoušek.
IT auditor bezpečnosti bude také vykonávat zkoušky v rámci kontrol IT zabezpečení. Bude neprodleně komunikovat jakékoliv požadavky na rozhodnutí realizace potřebných činností vyplývajících z provedených kontrol ve shodě s doporučeními auditu a skupinových směrnic.
Monitorování na každodenní bázi je realizováno příslušným poskytovatelem služby po dohodě s Information Security Officerem.

10 Přestupky IT bezpečnosti

Úmyslné jednání zaměstnanců nebo jednání z hrubé nedbalosti, které poškozuje pověst skupiny E.ON Energie nebo ohrožuje zájmy společnosti, jeho zaměstnanců, zákazníků anebo obchodních partnerů, bude posuzováno jako porušení zásad bezpečnosti IT. Kromě toho mohou být dotčeny i další právní předpisy.

11 Zákony a předpisy

Zaměstnanci skupiny E.ON Energie jsou povinni plnit celostátní, národní a mezinárodní legislativu a dodatečná opatření pro IT zabezpečení. K plnění budou zaměstnanci podporování organizací IT zabezpečení, která transformuje právo a předpisy do podoby směrnic, a vhodným způsobem o tom zaměstnance informuje.
Základem pro koncepce a směrnice pro bezpečnost IT jsou, mimo jiné:

- Obchodní zákoník HGB,
- Spolkový zákon o ochraně dat BDSG,
- Zásady řádného zpracování dat (GODV),
- Zásady řádných účetních systémů podporovaných zpracováním dat (pracovní společenství pro hospodářskou správu AWV),

- Zásady řádného archivování účetnictví, stanoviska a oznámení odborného výboru pro moderní účtovací systémy institutu pro auditory registr. spol. (IDW) FAMA,
- Stanoviska „Odborného výboru Řádnost a kontrola zpracování dat OPDV.

Mezinárodní právo bude respektováno na základě konkrétního příkladu, např. mezistátní výměna dat.