Technická univerzita v Liberci

Hospodářská fakulta

Studijní program: 6209 Systémové inženýrství a informatika
Studijní obor: Podnikatelská informatika

Bezpečnost dat v informačním systému firmy Grupo Antolin Bohemia a.s.

Data security in Information System
of Grupo Antolin Bohemia a.s.

BP – PI – KIN – 102

Pavel Hroza

Vedoucí práce: Dr. Ing. Jan Skrbek, Katedra informatiky

Odborný konzultant: Jan Grim, Grupo Antolin Bohemia a.s.

Počet stran 41, počet příloh 4

25.5.2001

Katedra informatiky **Školní rok 2000/2001**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro:

PAVLA HROZU

studijní program:
Systémové inženýrství a informatika (6209R)

studijní obor č. 62 - 53 - 705
Podnikatelská informatika

Vedoucí katedry Vám ve smyslu zákona č. 111/1998 Sb. o vysokých školách a navazujících předpisů určuje tuto bakalářskou práci :

Název tématu:

Bezpečnost dat v informačním systému firmy Grupo Antolin Bohemia a.s.

Data Security in Information System of Grupo Antolin Bohemia a.s.

Zásady pro vypracování :

1. Problematika bezpečnosti dat v informačním systému
2. Popis a analýza stavu ve firmě Grupo Antolin Bohemia a.s.
3. Návrh na zvýšení úrovně bezpečnosti dat ve firmě

Rozsah bakalářské práce: 25-30
(do rozsahu nejsou započítány úvodní listy,
přehled literatury a přílohy)

Doporučená literatura:
Dobda, L. : Ochrana dat v informačních systémech, Grada, Praha 1998
Date, C., J. : An introduction to Database Systems, Addison-Wesley, 1990

Vedoucí bakalářské práce: Dr. Ing. Jan Skrbek

Odborný konzultant: Jan Grim (Grupo Antolin Bohemia a.s.)

Termín odevzdání bakalářské práce: 25.5. 2001

v.r. Jan Skrbek
Prof. Ing. Jan Ehleman, CSc.
vedoucí katedry

Technická univerzita v Liberci
Hospodářská fakulta

Prof. Ing. Jan Ehleman, CSc.
děkan Hospodářské fakulty

V Liberci dne 27.10.2000

Prohlášení

Prohlašuji, že jsem bakalářskou práci vypracoval samostatně s použitím uvedené literatur pod vedením vedoucího a konzultanta. Byl jsem seznámen s tím, že na mou bakalářskou prác se plně vztahuje zákon č. 121/2000 o právu autorském, zejména §60 (školní dílo) a § 35 (o ne výdělečném použití díla k vnitřní potřebě školy).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé práce a prohlašuji, že souhlasím s případným užitím mé práce (prodej, zapůjčení apod.).

Jsem si vědom toho, že užít své bakalářské práce či poskytnout licenci k jejímu užití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do jejich skutečné výše).

Po pěti letech si mohu tuto práci vyžádat v Univerzitní knihovně TU v Liberci, kde je uložena, a tím výše uvedená omezení vůči mé osobě končí.

V Liberci dne 25.5.2001

Pavel Hroza

Poděkování

Rád bych touto cestou poděkoval vedoucímu své bakalářské práce Dr. Ing. Janu Skrbkov
za jeho ochotu a rady při konzultacích a pracovníkům oddělení informatiky firmy Grup
Antolin Bohemia a.s. Ing. Jiřímu Rydvalovi a Janu Grimovi za jejich vstřícný přístup a pomoc
Také děkuji svým rodičům a Ivaně Škodové za jejich podněty při zpracování bakalářské práce

Resumé

Bakalářská práce se věnuje bezpečnosti informačních systémů. V teoretické části je nastíněn problematika bezpečnosti dat, jsou vysvětleny základní pojmy zabezpečení informací, postu při řešení bezpečnosti informací s důrazem na analýzu rizik a druhy bezpečnostních opatřen

Ve druhé části je provedena na příkladu informačního systému firmy Grupo Antolin Bo hemia a.s. analýza rizik a to z hlediska bezpečnosti dat i z hlediska technické základny info mačního systému. Je proveden výpočet nákladů v případě vzniku bezpečnostního incident na kritickém prvku informačního systému. V závěru práce jsou naznačeny některé postup které by vedly ke zvýšení bezpečnosti dat v informačním systému firmy Grupo Antolin Bo hemia a.s.

Bachelor thesis deals with the security of information systems. In the first part is describe the problem of data security, basic terms of data security, ways of providing data securit emphasazing the risk analysis as important part of the process and finally are describe security arrangements.

In the second part the risk analysis of information system of Grupo Antolin Bohemia a.s is performed in view of data security and security of technical facilities of information systen Part of the analysis is estimation of costs in case of security incident in critical componer of information system. In conclusion of the work some procedures leading to improvement o data security in information system of Grupo Antolin Bohemia a.s. are stated.

Obsah

Seznam obrázků

Seznam tabulek

Seznam zkratek a symbolů

a.s.	akciová společnost
BDC	Backup Domain Controller, záložní řadič domény
CAD	Computer Aided Design
CD–RW	Compact Disk – Rewriteable, zapisovatelný kompaktní disk
DAT	Digital Archive Tape
DDS	Digital Data Storage
DHCP	Dynamic host configuration protocol
EDI	Electronic data interchange, standard elektronického přenosu dat
IS	Informační systém
ISDN	Integrated Services Digital Network, digitální síť
JIT	Just in time, logistický systém
LAN	Local Area Network, lokální síť
MS	Microsoft, firma vyrábějící software
PDC	Primary Domain Controller, primární řadič domény
RAID	Redundant Array of Inexpensive Disks, redundantní pole levných disků
RAM	Random Access Memory, operační paměť
RAS	Remote Access Service, služba vzdáleného přístupu
RSA	šifrovací algoritmus
SAP R/3	informační systém pro řízení podniku
SQL	Structured Query Language, dotazovací jazyk
TCP/IP	Transmission Control Protocol/Internet Protocol, síťový protokol
TP	Twisted Pair, kroucená dvoulinka
UPS	Uniterruptable Power Supply, nepřerušitelný zdroj napájení
VW AG	Volkswagen Aktiengesellschaft, Volkswagen, akciová společnost
WWW	World Wide Web

1 Úvod

V poslední dekádě došlo k prudkému rozvoji informačních technologií. Nasazení informačníc systémů a technologií se stalo podmínkou úspěšnosti a konkurenceschopnosti firem ve všec oblastech hospodářské činnosti. Tento prudký rozvoj se nevyhnul ani České republice, pı kterou však – vzhledem k její „zaostalosti" po politické změně v roce 1989 – byly informačı technologie něčím naprosto novým a neznámým. Proto jejich zavádění do praxe probíhalo (často ještě probíhá) poměrně chaotickým způsobem bez potřebné komplexní analýzy. Mnohd dochází k tomu, že původní systém (zpočátku velmi jednoduchý, jak odpovídalo požadavkůı a prostředkům firmy na počátku její činnosti) je „za pochodu" vylepšován nebo nahrazová novým.

Problém, který je často opomíjen, se nazývá bezpečnost informačního systému. S růstei významu informačních systémů vzrůstá i hodnota dat v těchto systémech uložených, tíı ovšem také narůstají škody v případě poškození nebo vyzrazení těchto dat. Avšak tento pohle je pro mnoho řídících pracovníků zcela nový, neuvědomují si, že mnoho firem je na funkčnos svého informačního systému přímo existenčně závislých. Proto je zabezpečení informací informačním systému a zabezpečení informačního systému samotného zanedbáváno. Svo roli v tom jistě hraje i to, že zabezpečení není triviální záležitostí, implementovatelnou z krátký časový úsek bez důkladné analýzy, a že investice do řešení zabezpečení se zdají bý nevratné (není možné vyčíslit finanční přínos zabezpečení, pouze náklady na zabezpečení navíc efektivita nákladů na zabezpečení se projeví až v případě mimořádné události. Proto j účelem této bakalářské práce ukázat, co je třeba vzít v potaz při zabezpečování informačníh systému firmy.

2 Problematika bezpečnosti dat v informačním systému

2.1 Základní pojmy zabezpečení informací

V zásadě můžeme chápání zabezpečení informačního systému rozdělit do čtyř stupňů:

Paranoidní – absolutní zabezpečení, vše, co je potenciálně nebezpečné, je uživatelům zaka
záno, z důvodů bezpečnosti neexistuje žádné spojení lokálního informačního systému
vnějším světem, což vede k maximální izolaci systému.

Přísná – všechno, co není výslovně povoleno provádět, je zakázáno.

Liberální – logický opak přísné bezpečnosti, co není zakázáno, je povoleno. Liberální be
pečnostní politika je často uplatňována v prostředích, ve kterých se hrozby považují z
málo až průměrně závažné a nepominutelným požadavkem je nízká ekonomická náro
nost řešení bezpečnosti.

Promiskuitní – vše je dovoleno, i to, co by mělo být z důvodu alespoň základní ochran
zakázáno. Informační systémy s promiskuitní bezpečnostní politikou jsou obvykle pr
vozně nenákladné a zaručují pouze minimální nebo žádnou bezpečnost. Důvodem po
žívání informačních systémů tohoto typu může být ekonomičnost řešení.

Na obrázku 1 na straně 14 vidíme základní úkol zabezpečení systému. Úkolem je přesunou
incidenty A, B, C s různými následky a pravděpodobnostmi vzniku do oblasti D, ve které j
minimální riziko incidentu a jeho následky jsou minimální.

2.2 Požadavky na důvěryhodné informační systémy

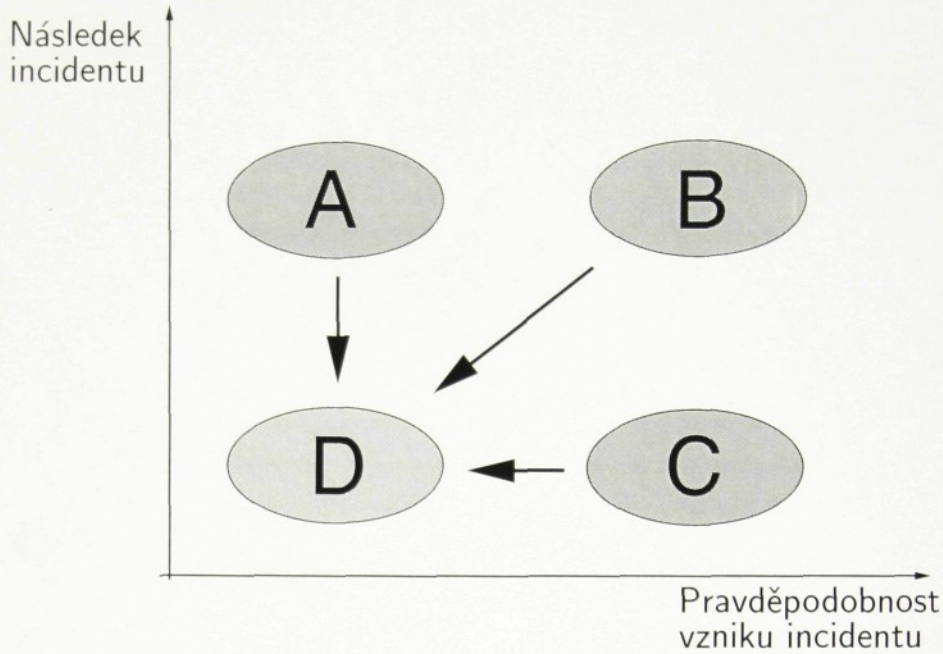
Bezpečnost informačních technologií můžeme vymezit třemi základními pojmy. Jsou to:

Důvěrnost – ochrana před prozrazením informace

Integrita – ochrana před neoprávněnou modifikací

Dostupnost – ochrana před neoprávněným odmítnutím služby nebo nemožnosti poskytnou
informaci.

Tyto základní požadavky na bezpečnost jsou společné pro všechny informační systémy a tech
nologie. Jejich vzájemná vyváženost je však závislá na definovaných požadavcích, kladených
na konkrétní systém. Důvěrnost bude určitě převažovat nad integritou a dostupností u vojen
ských a agenturních systémů a integrita dat bude určitě základním požadavkem u rozsáhlých
informačních knihoven.



Obrázek 1: Základní úloha zabezpečení

2.3 Postup řešení bezpečnosti

Proces řešení bezpečnosti představuje splnění tří základních kroků: zpracování studie bez pečnosti, bezpečnostní politiky a bezpečnostního projektu. Studie bezpečnosti je zpráva dosaženém stupni bezpečnosti. Ve studii se určí postup řešení, vycházející z potřeb a součas ného stavu.

Bezpečnostní politika je dokument, který se dělí na část:

- celkovou (globální) bezpečnostní politiku a
- systémovou bezpečnostní politiku (někdy též bezpečnostní politiku informačního sys tému)

Stejně tak i bezpečnostní projekt se může rozpadnout na několik relativně oddělených části z nichž každá má na starosti realizaci poměrně samostatné oblasti bezpečnosti.

Nosným pilířem, na němž je řešení bezpečnosti od studie až po projekt postaveno, j analýza rizik. V každém ze tří uvedených stupňů řešení se analýza rizik vyskytuje, ale pokaždé má jiné zaměření a jinou hloubku.

Studie informační bezpečnosti je obvykle východiskový dokument. Poskytuje stručný pře hled dosaženého stavu informační bezpečnosti a vytyčuje hlavní směry dalšího postupu. Sou částí studie obvykle nebývá hloubková riziková analýza, konstatování stavu se prohlásí n základě požadavků na bezpečnost, které jsou v zadání jen intuitivně definovány. Z toho plyne že studie nemůže nahradit některou bezpečnostní politiku.

Analytické práce při provádění analýzy rizik zahrnují analýzu východisek, zdrojů a pro středí (aktiv), ohrožení (koho má systém odstrašit, zdržet, identifikovat, jak útočník oblas napadne) a bezpečnostních cílů. Je třeba vyhodnotit, které hrozby, s jakou pravděpodob ností a jakým dopadem (co a jak je třeba chránit a před čím) mohou vyvolat bezpečnostn incident. Tato část je jednou z nejsložitějších analytických činností. V této fázi se analyti dostává mimo jiné i do těchto oblastí:

- zálohování výpočetního systému,
- fyzické zajištění přístupu k němu,
- požární zajištění,
- otázky úklidu a zabezpečení odpadových surovin,
- likvidace médií po uplynutí doby jejich životnosti.

Riziková analýza musí zjistit, jakými riziky jsou informační aktiva ohrožena. Riziko má vzta k pravděpodobnosti jeho uplatnění a k míře následků vzniklého bezpečnostního incidentu Výsledky rizikové analýzy jsou jedním z nejutajovanějších dokumentů, které v procesu řešen bezpečnosti vznikají. Je to pochopitelné, neboť jsou vlastně návodem, jak s jakými náklad a jakou úspěšností lze organizaci zlikvidovat nebo poškodit. Proto jsou klasifikovány v rámc organizace jako dokumenty nejvyššího stupně utajení.

Náplň analýzy rizik lze definovat jako proces porovnávání odhalovaných rizik proti přínos a ceně možných bezpečnostních opatření, stanovení implementační strategie v rámci vypra covávání systémové bezpečnostní politiky tak, aby byla v souladu s celkovou bezpečnostn politikou a posláním organizace. Model postupu při analýze rizik lze vyjádřit následujícín výčtem:

- identifikace a ocenění aktiv,
- nalezení zranitelných míst,
- odhad pravděpodobnosti využití zranitelných míst,
- výpočet očekávaných (ročních) ztrát,
- přehled použitelných opatření a jejich cen,
- odhad ročních úspor aplikací zvolených opatření.

Význam důkladného provedení analýzy rizik je zásadní. Provedením inventury a stano vením reálné hodnoty aktiv z hlediska možných škod porušením důvěrnosti, integrity, poho tovosti a nepopiratelnosti se upřesní požadavky na nutná bezpečnostní opatření. Ověří se

zda výše nákladů na zabezpečení je úměrná. Výsledkem analýzy rizik je tedy stanovení, kte rým hrozbám je informační systém vystaven, jaká jsou rizika jednotlivých hrozeb, jaké škod mohou vzniknout a které opatření hrozby odstraní. Obecný postup při analýze rizik začín evidencí aktiv a požadavků na bezpečnost, pokračuje hledáním zranitelných míst, určení hrozeb a odhadnutím rizik a výše potenciálně způsobených škod, zjištěním cen vhodnýc bezpečnostních opatření a jejich volbou.

Odhad rizik obvykle vychází ze statistik konkrétních systémů, zjišťují se počty poruch neoprávněných přístupů, velikosti souborů. Odhadují se četnosti za daný interval nebo prav děpodobnosti jednotlivých událostí. Při výpočtu očekávaných ročních ztrát obvykle nebýv problematické ocenění hardware a software, problematické bývá určení ceny dat. Při identi fikaci možných cen aktiv je třeba si klást otázky typu:

- Které právní závazky nutí organizaci zajišťovat důvěrnost a integritu dat?
- Způsobí zpřístupnění těchto dat škodu osobě či organizaci?
- Může být organizace za to stíhána?
- Dojde ke ztrátě pozice organizace na trhu?
- Může konkurence získat výhody nepoctivým způsobem?
- Dojde k obchodním ztrátám?
- Jaký je psychologický dopad nedostupnosti služby?
- Hrozí ztráta pověsti?
- Hrozí ztráta obchodních šancí a pokud ano, tak u kolika a jakých zákazníků?
- Lze zpracování dat opozdit?
- Pokud ano, kolik za to zaplatíme?
- Jaká je cena dat pro jiné osoby nebo organizace?
- Co vznikne za problémy, dojde-li ke ztrátě dat?
- Jsou data nahraditelná?
- Lze data rekonstruovat?
- Kolik práce dá rekonstrukce nebo opětovné pořízení dat?

Na závěr analýzy rizik se vypracuje přehled použitých opatření a jejich cen a provede se odhad ročních úspor získaných aplikací určených bezpečnostních opatření. V současné době

jsou již k dispozici pro automatizaci detailní analýzy rizik standardizované nástroje, různé výčtové seznamy, speciální programové systémy.

Bezpečnostní politika musí být chápána jako souhrn principů a východisek pro strategická řešení. Představuje základ pro zajištění informační bezpečnosti. Politika představuje výchozí body pro návrh a realizaci všech úspěšných standardů, směrnic, procedur a opatření. Dokument politiky je všeobecným plánem, na jehož základě se informace získávají a využívají. Určuje oblasti, ve kterých je potřeba tento proces řídit a kontrolovat. Aby byla politika efektivní, musí být definovány informace jako aktiva a současně má být určena zodpovědnost za jejich ohodnocení. K tomu je nutné definovat a přijmout jisté role uživatelů, správců a podobně.

Politika musí odpovědět nejméně na následující otázky:

- Co musí být chráněno?
- Kdo nese zodpovědnost?
- Kdy to bude efektivní?
- Jak to bude vynuceno?
- Kdy a jak to bude uvedeno do praxe?

Je třeba si uvědomit, že tu bude docházet ke střetu dvou aktivit: bezpečnostní cíle nejsou shodné s cíli obchodními a obecně se vzájemně ani nepodporují.

Bezpečnostní projekty (na rozdíl od bezpečnostních politik) představují konkrétní požadavky na provedení konkrétních činností. Bezpečnostní projekt je možné definovat pomocí jeho vstupů a výstupů. Vstupy dodává:

bezpečnostní politika – definice dotyčného objektu, požadovaná úroveň bezpečnosti, druh protiopatření, způsob hodnocení;

bezpečnostní management uplatňuje své požadavky na bezpečnost;

konzultanti bezpečnosti přicházejí s návrhem na řešení – a konečně

všichni vedoucí pracovníci mohou uplatnit požadavky na řešení bezpečnosti.

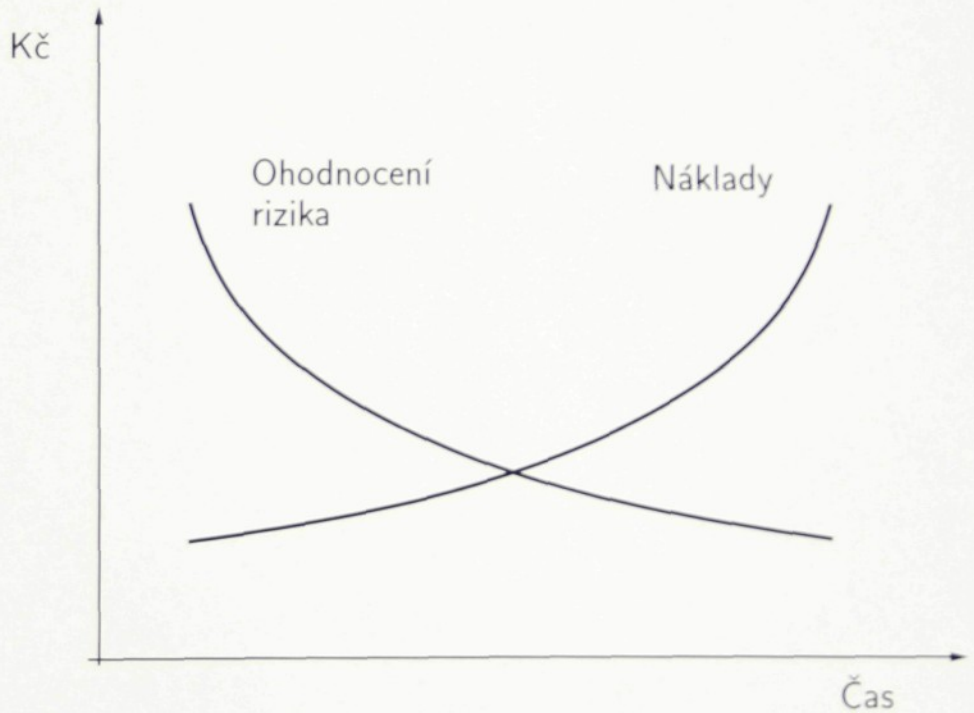
Výstupem bezpečnostního projektu je konkrétní opatření, které spadá do jedné ze dvou hlavních kategorií:

- organizační a administrativní,
- technické a technologické.

Součástí bezpečnostní analýzy je i tvorba havarijního plánu. Havarijní plán určuje, co dělat po odhalení bezpečnostního incidentu a jak postupovat, aby se udržela kontinuita činnosti organizace. Součástí havarijního plánu jsou návody jak postupovat v poskytování služeb po zjištění bezpečnostního incidentu, dohody o poskytování náhradních řešení a návod, jak postupovat při obnově činnosti informačního systému po havárii.

2.4 Náklady na řešení bezpečnosti

Náklady na řešení bezpečnosti jsou vlastně náklady na odstínění hrozeb a zranitelností, které byly zjištěny rizikovou analýzou. Všechna rizika nelze beze zbytku odstínit. Zbytkové riziko (to, jež může ohrozit naše informace) je tím větší, čím méně spolehlivě byly vykonány kroky komplexního řešení bezpečnosti a čím méně zdrojů bylo na odstínění rizik vynaloženo. Je třeba uvažovat účelnost vynaložených nákladů, investovat jen tolik, kolik odpovídá tzv. rozumné míře bezpečnosti. Jak vidíme z obrázku 2, při růstu nákladů na zabezpečení klesá riziko a od určitého bodu jsou náklady vyšší než zbytkové riziko.



Obrázek 2: Náklady na zabezpečení ve vztahu k ohodnocení rizika

2.5 Základní chráněné objekty

Plánujeme-li zavedení určitého způsobu ochrany, musíme si nejprve ujasnit, co chráníme Základní hodnoty každého informačního systému představují především:

Technická zařízení. Informační technika je zranitelná mnoha způsoby. Může být ukradena nebo buď záměrně nebo neodborným zásahem poškozena. I běžné závady některé část systému mohou způsobit nedostupnost důležitých funkcí, které informační systém zajišťuje. Rozsáhlá poškození způsobují i přírodní katastrofy.

Programové vybavení. Je možné definovat tři základní hrozby:

Ztráta dostupnosti - úmyslné, nebo i náhodné vymazání programů. Tuto ztrátu navíc zjistíme zpravidla až při pokusu o spuštění konkrétní aplikace.

Modifikace kódu programu není zpravidla rychle rozpoznatelná, určení rozsahu a následků poškození je velmi obtížné. Nejlepším řešením je nová instalace.

Softwarové pirátství - každý program je dílo, které podléhá autorskému zákonu. Každý, kdo si neoprávněně okopíruje programové vybavení, dopouští se trestného činu. Tyto krádeže jsou ale těžko zjistitelné, protože oprávněnému majiteli programu vlastně nic „neubude".

Datové struktury. Data představují největší hodnotu informačního systému. Ztráta dat je těžko finančně vyčíslitelná, jejich hodnota se může v závislosti na čase značně měnit.

2.6 Projevy vzniku škody

Škody vzniklé na informačních systémech mohou mít následující podobu:

Ztráta integrity – celistvosti, informace může být zničena nebo změněna, úmyslně nebo neúmyslně.

Ztráta dostupnosti – informace může být v určitém okamžiku nedostupná všem, nebo někomu, kteří jsou oprávněni mít k ní přístup.

Ztráta důvěrnosti – informace může být dostupná i těm, kteří nejsou oprávněni mít k ní přístup.

Přímá finanční ztráta nebo fyzické poškození

Ztráta autentičnosti informace – nelze jednoznačně určit zdroj (původce) informace.

2.7 Druhy bezpečnostních opatření

2.7.1 Organizační opatření

Obvykle nejsou příliš nákladná, avšak při jejich dodržování lze dosáhnout podstatného zvýšení úrovně bezpečnosti. Jsou realizována formou vnitropodnikových nařízení a směrnic, které musejí zahrnovat celou činnost informačního systému, řešení krizových stavů, zásady personální bezpečnosti. Těmito směrnicemi musí být jasně vymezena a delegována zodpovědnost každého pracovníka za konkrétní věc. Musí být písemná a každý pracovník se s nimi musí seznámit a toto stvrdit svým podpisem.

Organizační opatření především zahrnují tyto oblasti:

- Zásady a pravidla pro práci s výpočetní technikou v rámci organizace (například zákaz používání vlastních disket, zamykání klávesnic při odchodu z pracoviště).
- Určení stupně důvěrnosti a ochrany jednotlivých informací.
- Personální práci – výběr, školení a prověřování pracovníků.
- Stanovení stupně oprávnění pracovníků k přístupu k jednotlivým typům informací.
- Postup identifikace pracovníka, potřebné pro vstup do informačního systému.
- Pravidla pro práci s hesly a šifrovými klíči.
- Definice bezpečnostních zón a pravidla řízení vstupu do nich.
- Postup při hlášení podezřelých událostí, které mohou narušit bezpečnost IS.
- Postup při ničení nepotřebných nosičů informací.

2.7.2 Fyzická opatření

Jsou to všechna opatření, použitá k zajištění fyzické ochrany informačního systému proti náhodným a úmyslným hrozbám. Zajišťují ochranu IS pomocí technických prostředků ochrany. Informační systém je vždy umístěn v určitém fyzickém prostředí, které tvoří budovy a místnosti v nich. Úkolem fyzických opatření je zabezpečení budov, ve kterých je IS umístěn, jeho ochrana před přírodními vlivy a opatření proti vniknutí neoprávněných osob do těchto objektů. Dále fyzická opatření řeší bezpečné uložení datových nosičů s informacemi (diskety, výměnné disky, magnetické pásky) a tiskových výstupů, způsoby ničení již nepotřebných informací a médií, ochranu proti přírodním živlům a požáru. Její součástí je také zajištění nepřetržité dodávky stabilizované elektrické energie.

2.7.3 Technická opatření

Technická opatření se zabývají kvalitním výběrem a nasazením technických prostředků (hard ware) do informačního systému, zajištění jeho včasného servisu kvalitního tak, aby nenaruš požadovanou dostupnost zdrojů informace v rámci IS. K dalším okruhům řešení technických opatření patří ochrana technických prostředků před elektromagnetickým vyzařováním.

2.7.4 Programová opatření

Programová opatření umožňují chránit informace přímo v počítači pomocí programových bezpečnostních prostředků. Dělí se do tří základních skupin:

Kontrola přístupu – zabraňuje neoprávněným uživatelům v práci s informacemi, k nim nemají povolen přístup. Základním způsobem realizace je přístupové heslo.

Monitorování činnosti – složí ke sledování a zaznamenávání podezřelých aktivit uživatelů (například uživatel se hlásí z několika terminálů najednou, v nezvyklou denní dobu nebo den).

Hlášení o narušení – popřípadě pokusu o narušení do administrátorského centra

2.7.5 Šifrování

Kryptografie poskytuje řadu šifrovacích technik k utajení obsahu dat a zpráv, aby byly zabezpečeny při ukládání a přenosu. Šifrování transformuje data takovým způsobem, aby nebyla běžnými prostředky čitelná. V případě odcizení šifrovaných dat nedojde k úniku informac (pokud zloděj nezná šifrovací klíč). Šifrování je považováno za nejdokonalejší způsob zabezpečení informací zejména při přenosech pomocí veřejných komunikačních sítí.

Možnosti využití kryptografie v informačních systémech:

Šifrování komunikací – slouží k zajištění bezpečné komunikace i v případě, kdy přenosová média (například Internet) nejsou důvěryhodná.

Šifrování souborů nebo disků – používá se především pro ochranu citlivých souborů na lokálních discích nebo souborových serverech. Další možnost je šifrování informací na záložních médiích a disketách.

Zajištění integrity při přenosu – K zajištění integrity obsahu přenášené informace se používají takzvané „hashovací" funkce.

Digitální podpis – Slouží k ověření původu dat a zpráv pomocí elektronického podpisu. Jeho použití je vhodné především v informačních systémech, u nichž komunikující strany požadují průkazné ověření identity druhé strany (například bankovní operace).

2.7.6 Zálohování

Zálohování je proces, při kterém se v daném čase vytvoří jedna nebo více kopií požadovaných informací na záložních datových nosičích. Zálohování patří k jednomu z nejvýznamnějších nástrojů ochrany dat. Je to prevence, pojistka pro případ výpadku systému, selhání nebo katastrofy, která umožňuje uvést informační systém do původního nepoškozeného stavu. Vytváření záloh můžeme detailněji rozdělit na provozní zálohování a archivaci.

Provozní zálohování je vytváření pracovních kopií ve stanovených časových periodách nebo po určitých změnách hodnot. Tyto kopie se vytvářejí zejména pro obnovu informačního systému po jeho výpadku. Záložní kopie zpravidla obsahují nejen datové hodnoty, ale i parametry nastavení operačního systému a programů, uživatelských účtů a jiných důležitých položek, bez nichž by nebylo možné po totálním zhroucení informačního systému (je nutno počítat vždy s nejhorší variantou) obnovit celé informační prostředí. Kopie se zpravidla po určité době přemazávají, neukládají se dlouhodobě.

Archivace představuje pouze kopii dat, vytvořenou kvůli dlouhodobému archivování hodnot. Kopie se pořizují pouze pro dlouhodobé uložení do archivu. Zpravidla se vytváří jedna kopie.

2.7.7 Antivirová ochrana

Jako hrozbu pro informační systém je nutné chápat i viry a trojské koně. Těchto virů existuje několik desítek tisíc (unikátních virů i jejich mutací) a jejich účinky jsou různorodé. Některé jen vypíšou v určitou hodinu žertovnou zprávu, jiné zahltí počítačovou síť nebo poštovní server a některé přepíšou náhodnými daty veškeré soubory, ke kterým se dostanou. Jsou i viry, jejichž přítomnosti si nevšimnete, potichu infikují počítač a pak odesílají autorovi viru informace, které najdou, například zadávaná hesla. Infikace virem je velmi jednoduchá. Stačí spustit nakažený program, přečíst si poštovní zprávu s přílohou a podobně. Odhalit chování virů nebývá jednoduché. Může se stát, že virus bude potichu několik týdnů modifikovat soubory, uživatel bude s modifikovanými soubory pracovat a ničeho si nevšimne.

Proto je nutné se před viry chránit. Nejjednodušší ochranou jsou antivirové programy. Těchto programů existuje několik desítek od renomovaných firem. Jedná se většinou o komerční produkty, ale existují i volně šiřitelné varianty.

Antivirový program může v zásadě pracovat dvěma způsoby:

- porovnáváním souborů s databází vzorků virů, která je součástí antivirového programu
- heuristickou analýzou, která analyzuje kód viru a hlásí všechny podezřelé akce (otevřen systémového souboru, zápis do souboru a podobně).

I způsoby práce antivirového programu se mohou lišit. Program můžeme spouštět ručně, aby prověřil pevný disk nebo disketu na přítomnost virů, nebo může pracovat na pozadí práce uživatele a prověřovat všechna data, která počítačem projdou nebo se nacházejí v paměti.

3 Informační systém firmy Grupo Antolin Bohemia a.s.

Firma Grupo Antolin Bohemia a.s. se sídlem v Chrastavě je českou pobočkou španělského koncernu Grupo Antolin. Celý koncern se zabývá výrobou komponent pro automobilový průmysl (dveře, mechanismy dveří, přístrojové panely, sedačky, stropní panely a podobně), česká pobočka vyrábí dveřní panely, stropní panely, odkládací plata a protihlukové vložky pro automobilky koncernu Volkswagen, konkrétně pro vozy Škoda, Volkswagen a v menší míře i pro Audi. Vzhledem k tomu, že firma podniká v automobilovém průmyslu, což je velmi dynamický obor s velkou konkurencí, je kladen velký důraz na kvalitu dodávek, rychlost dodávek a flexibilitu.

Firma Grupo Antolin Bohemia a.s. byla založena roku 1994 a v roce 1995 zahájila výrobu. Od počátku byl ve firmě implementován komerční informační systém, postupně do dnešní doby došlo k několika změnám a v dnešní době firma využívá systém SAP R/3 německé firmy SAP AG. Se svým mateřským koncernem je firma Grupo Antolin Bohemia a.s. úzce propojena, systém SAP je provozován na serverech ve španělské centrále v Burgosu a Grupo Antolin Bohemia a.s. je do Španělska připojena pomocí připojení Frame Relay, které je kromě SAPu využíváno i pro připojení k Internetu – přes španělskou centrálu.

Firma Grupo Antolin Bohemia a.s. má v současné době 490 zaměstnanců a v roce 2000 dosáhla ročního obratu ve výši 1,6 miliardy Kč. Oddělení informatiky má čtyři zaměstnance (do března 2001 mělo pouze tři), z čehož je jeden student Technické univerzity v Liberci vykonávající svou roční praxi. Tito čtyři zaměstnanci mají na starosti celý informační systém firmy včetně hardwarové základny a nových projektů, jako je systém čárových kódů ve výrobě.

Jako operační systém serverů i stanic je využíván systém Windows NT 4.0 firmy Microsoft. Od firmy Microsoft pochází i databázový systém Microsoft SQL Server 7.0 a poštovní a groupware systém Exchange. Lokální síť firmy Grupo Antolin Bohemia a.s. je tvořena cca 80 pracovními stanicemi, 4 servery (databázový, poštovní, souborový, zálohovací) a 4 počítači pro příjem EDI dat od odběratelů (Škoda, VW, Audi).

Téměř každý pracovník administrativy má svou vlastní pracovní stanici (cca 60 stanic) a na všech provozech (sklad, výroba, údržba, expedice) se nacházejí další pracovní stanice (cca 20 stanic) pro potřeby některých pracovních míst nebo jako terminály pro přístup do systému SAP (pro výrobu). Svá data si mohou pracovníci ukládat na svůj pevný disk, nebo k tomuto účelu využít sdílený prostor na souborovém serveru o kapacitě 30 GB, který je pravidelně zálohován. Pro udržení určitého pořádku na sdíleném disku jsou vytvořeny kořenové adresáře pro jednotlivé útvary, další členění závisí již na jednotlivých uživatelích. Každý uživatel má také k dispozici svůj domácí adresář na sdíleném disku. Do tohoto adresáře má přístupová práva jen příslušný uživatel. Také tento adresář je pravidelně zálohován, ale uživateli není příliš využíván. Ohledně využívání diskového prostoru nebo ukládání dat jednotlivými uživateli není ve firmě vypracována žádná směrnice nebo doporučení.

Na každé pracovní stanici je spuštěn rezidentní modul antivirové ochrany VirusScan od firmy Network Associates a je nastavena automatická aktualizace virové báze z centrálního souboru na souborovém serveru při každém spuštění pracovní stanice. Aktualizaci souboru na souborovém serveru zajišťuje pracovník oddělení informatiky z webových stránek výrobce programu zhruba jednou týdně.

Každý uživatel má přiděleno své jednoznačné přístupové jméno, které jej identifikuje pro přístup k prostředkům lokální sítě (souborový server, tiskárny, faxový server) a k systému SAP. Na základě přístupových jmen jsou definována oprávnění přístupu k jednotlivým prostředkům sítě. Ke každému přístupovému jménu je přiděleno heslo, které má uživatel možnost měnit. Oprávnění je využíváno při přístupu k informačnímu systému SAP (každý uživatel smí vykonávat jen úlohy, povolené správcem systému), při přístupu k elektronické poště (každý uživatel má přístup jen ke své poště, pouze některé osoby, například asistentky manažerů, mohou mít povolen přístup k cizí poště) a v minimální míře na sdíleném disku (některé adresáře jsou povoleny jen některým osobám – například účtárna, personální).

Ve firmě je provozován databázový server (Microsoft SQL Server 7.0), na kterém jsou uložena došlá EDI data od odběratelů, na jejichž základě je plánována výroba. Firma je pomocí linky X.25 připojena k odběratelům a přijímá od nich systémem EDI strukturovaná data – objednávky a potvrzení dodávek. Tato data jsou zpracována, zapsána do databáze a v některých případech zapsána i do databáze systému SAP a na jejich základě probíhá plánování výroby a fakturace. Firma používá několik programů (frontendů), které zprostředkovávají pohled na doručená EDI data a pomocí nichž pracovníci plánování plánují výrobu na nejbližší období. Tyto programy jsou vytvořeny v prostředí Microsoft Access, které využívají ke svému běhu (odlehčenou verzi Runtime). Fakticky má k datům na databázovém serveru přístup každý pracovník, který má nainstalován program Microsoft Access (plnou nebo Runtime verzi).

Na obrázku 3 je nastíněna základní struktura páteřní sítě firmy Grupo Antolin Bohemia a.s. Jednotlivé počítače poskytují následující služby:

SPD01 – hlavní server firmy

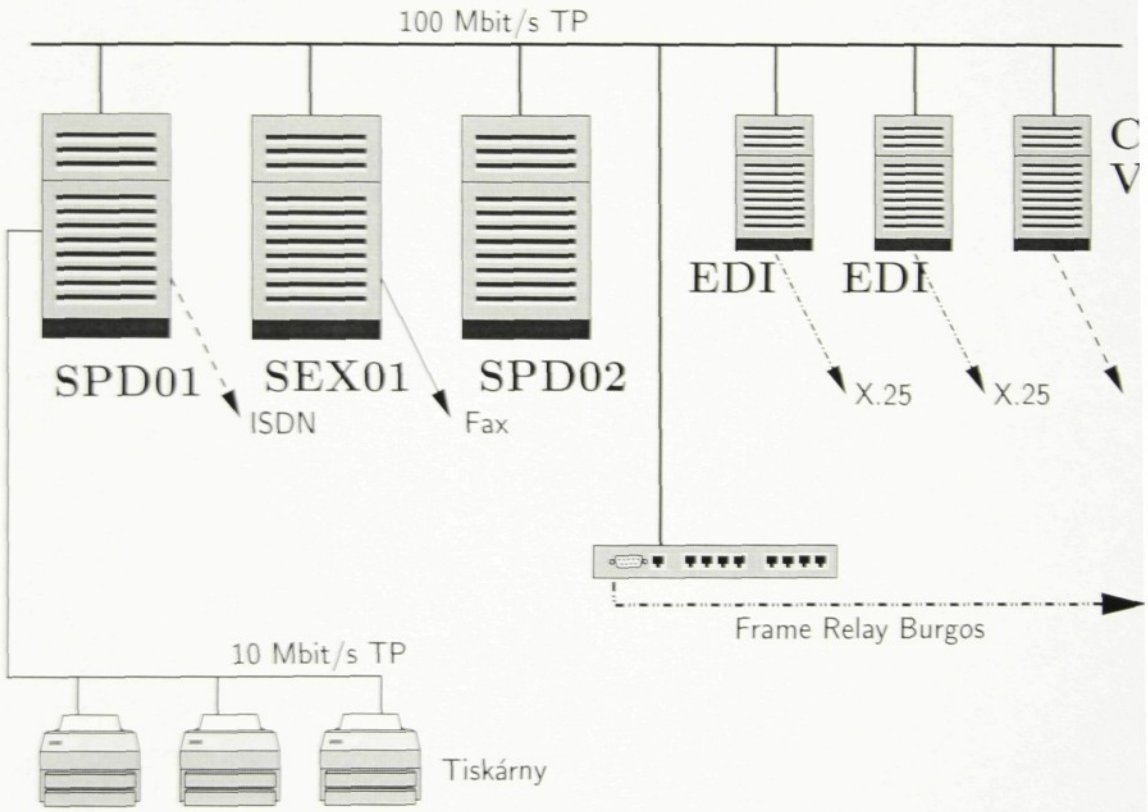
- souborový server
- tiskový server
- server vzdáleného přístupu
- DHCP server
- primární řadič domény

SPD02 – databázový server

- databázový server
- záložní řadič domény

SEX01 – poštovní server

- poštovní server
- faxový server
- záložní řadič domény



Obrázek 3: Struktura páteřní sítě

Podrobnější struktura sítě se nachází v příloze.

3.1 Hardware

Do této sekce zahrnujeme zpravidla i fyzický přístup k hardware a komunikačním prostředkům. Základním požadavkem bezpečnosti je nepřipustit přístup nepovolaných osob ke kritickým prvkům sítě nebo k místům, kde by mohla být komunikační infrastruktura firmy narušena. Součástí těchto opatření jsou i opatření o pohybu nežádoucích osob v objektu firmy. Tato opatření jsou plně v kompetenci personálního oddělení, avšak to na jejich realizaci spolupracuje s oddělením informatiky. K zamezení pohybu nežádoucích osob ve firmě slouží pracovník recepce. Tuto službu vykonává v pracovní době recepční, mimo pracovní dobu zaměstnanec bezpečnostní agentury, která provádí ostrahu objektu. Na pracovišti recepce je umístěn terminál kamerového dohledového systému s pomaloběžným nahrávacím zařízením, pomocí kterého jsou sledovány kritické prostory firmy. Jedná se zejména o prostor u serverů sítě, vchody do budovy, parkoviště, vjezdy do skladů a expedice. Záznamy nahrávacího zařízení jsou ukládány po dobu jednoho týdne a poté přepsány novými.

Dalším opatřením je dveřní systém, který funguje ve spolupráci se systémem docházky. Oba systémy využívají pro evidenci pohybu pracovníků „píchačky" ve formě čipového přívěsku, kterým zaměstnanci označují svůj příchod a odchod. Na všech dveřích jsou nainstalovány snímače a dveře jsou otevřeny až po přiložení snímače a ověření, že pracovník má právo otevírat tyto dveře. Zároveň dochází k evidenci a proto je zjistitelné, kdo a kdy dveřmi prošel.

Pro ochranu klíčových prvků sítě (servery, směrovače, ústředna, modemy) byla v únoru 2001 vybudována v prostoru přízemí administrativní budovy serverová místnost. Vznikla obestavěním stávajícího prostoru serverů. Serverová místnost je uzamykatelná. Toto opatření významně zvýšilo ochranu hardwarových prvků informačního systému před poškozením nebo odcizením.

3.1.1 Kabeláž

Jak již bylo řečeno, ve firmě Grupo Antolin Bohemia a.s. se nachází cca 80 pracovních stanic. Jedná se o výrobky firem Compaq, Hewlett-Packard a lokálních značek. Lokální síť je realizována strukturovanou kabeláží 10Mbit/s, v důležitých místech, jako jsou stanice oddělení vývoje a páteřní síť mezi jednotlivými servery stejnou technologií s rychlostí 100Mbit/s. Pracoviště skladů jsou připojena k centrálnímu rozvodu optickým kabelem. Strukturovaný rozvod byl zpočátku zaveden v základní podobě v celé firmě, jeho další rozšiřování probíhalo pak postupně, jak vyžadovaly potřeby firmy. V centrálním prostoru serverů (serverové místnosti) je umístěna skříň (rack) s patch-panely a přepínač (switch) rychlosti 100Mbit/s představující páteřní síť firmy. Jsou na něj připojeny servery a jednotlivé větve firemní sítě a v jeho prostoru se též nachází rozbočovací panel interní telefonní sítě firmy. Druhý rack se nachází v prostorách oddělení laboratoře a byl zde umístěn při rozšiřování sítě a připojování vyšších pater a hal výroby. V tomto racku se nachází směrovač 10Mbit/s. Tento rack a

kabeláž, z něj vycházející, byly zapojeny na počátku roku 1999, jak si vyžadovaly stavební úpravy administrativní budovy (rozšíření stavby a zvýšení o jedno patro). Kabeláž, vycházející z tohoto racku je nechráněná na úseku asi 1 m před vstupem do instalačních žlabů. Z obou racků vycházející kabeláž je zavedena do zásuvek typu RJ-45 na zdi. Těchto zásuvek je pouze omezené množství, zejména v administrativní budově a možnost instalace nových zásuvek je poměrně omezená, také kapacita obou racků je již téměř vyčerpána. Proto v případě modifikace struktury sítě (přidání nového síťového prvku, jako pracovní stanice nebo síťové tiskárny) je prováděno větvení v nižších úrovních – zakoupí se rozbočovač – hub a nový prvek je připojen k němu. To přispívá k zneprůhlednění struktury sítě a zhoršuje dohledávání chyb v případě poruchy sítě.

Kabeláž je v prostorách administrativní budovy vedena ve žlabech – instalačních lištách, případně ve žlabech v podlaze. Kabeláž vedoucí do skladů je v případě kabeláže zapojované v počátcích firmy vedena ve žlabech nebo optickým kabelem, v případě později realizovaných rozvodů někdy i volně podél stěn ve výšce, kde za normálních okolností nemůže dojít k poškození kabelu. Ovšem toto řešení není ideální, neboť v případě montážních prací nebo stavebních úprav na budově může být kabel lehce poškozen nebo přerušen. Zároveň tyto prostory nejsou dobře kontrolovatelné, proto zde může dojít k narušení (záměrnému) kabelu a k připojení neautorizovaného hardware (odposlech).

Dalšími dvěma využívanými typy síťového propojení je spojení skladů s administrativní budovou, které je realizováno optickým kabelem a bezdrátová síť využívaná zařízeními čárového kódu. Bezpečnost optické sítě se v podstatě zužuje na ochranu proti poškození vedení, neboť narušení vedené a instalace odposlechového zařízení nebo nového prvku sítě je časově i technicky náročná. Z hlediska ochrany proti poškození je optický kabel chráněn dobře, ochraňuje jej nejen vnější izolační a ochranná vrstva, ale i instalace do žlabů.

Bezdrátová síť je využívána zařízeními sloužícími ke značení čárových kódů ve výrobě. Tato část výroby je vyžadována dodavateli a proto je pro chod firmy naprosto nezbytná. Síť založená na bezdrátovém přenosu je sice bez kabeláže, ale riziko poškození se nám zde mění na riziko rušení případně přímého odposlechu. V případě rušení, které na rozdíl od odposlechu nemusí být příliš nákladné (stačí vysílat šum o potřebné frekvenci dostatečným výkonem) a není třeba, aby se rušící vysílač nacházel v areálu firmy, dochází k ochromení komunikace mezi mobilními zařízeními a serverem, což má za následek přechod odbavování výroby do nouzového režimu. O tom bude pojednáno později, včetně případných dopadů na plynulost výroby.

3.1.2 Hardware stanic

Vzhledem k tomu, že každý pracovník má k dispozici svou pracovní stanici, má také fyzický přístup k jejímu hardware. Stanice jsou vybírány podle požadavků pracovního místa (zejména požadavky na výkon procesoru, velikost operační paměti, velikost úložného prostoru a rychlost

grafické karty), jinak se jedná o běžné stanice z nabídky firem Compaq, Hewlett-Packard nebo místních značek. Standardní vybavení komponenty odpovídá dnešní době, proto je každá stanice vybavena disketovou jednotkou a většina nových stanic (začátek roku 2000 a později) i mechanikou CD-ROM. Proto každý pracovník může těchto jednotek použít k infikování stanice virem (o antivirovém programu bude zmíněno později) nebo (v případě disketové jednotky) k úniku firemních dat.

Stanice nejsou nijak pečetěny pro zjištění neoprávněného fyzického přístupu do vnitřku stanice. Toto opatření by ztěžovalo práci pracovníkům oddělení informatiky, kteří provádějí profylaxi a odstraňování běžných závad hardware nebo výměny komponent. Jako součást zpracování bakalářské práce byla v oddělení informatiky zavedena evidence pracovních stanic s jejich síťovými názvy, uživatelem, kterému jsou přiděleny a nadstandardními komponentami, kterými je stanice vybavena. Nově nakupované stanice a stanice, které prošly reinstalací[1], mají vytvořen evidenční list, na kterém jsou následující údaje:

- síťové jméno stanice
- osoba, jíž je stanice přidělena
- hardwarová konfigurace stanice
- typ stanice (výrobce, označení)
- programové vybavení nainstalované na stanici
- ovladače tiskáren nainstalované na stanici

Tento evidenční list zároveň slouží jako pomůcka pro instalujícího pracovníka, aby byly nainstalovány všechny požadované produkty a ve správném pořadí. Tento evidenční list je zakládán a je používán v případě problémů s pracovní stanicí. Formulář evidenčního listu se nachází v příloze.

3.1.3 Tiskárny

Ve firmě je používáno cca 20 tiskáren, jehličkových, inkoustových i výkonných laserových pro pracovní skupiny. Sedm tiskáren je umístěno v administrativní budově, ostatní se nacházejí na pracovištích výroby, údržby, expedice a podobně v jednotlivých halách. Tiskárny jsou připojeny buď k lokální stanici – to je případ tiskáren na halách, nebo jsou pomocí speciálního síťového zařízení (JetDirect) připojeny k tiskovému serveru a fyzicky jsou umístěny v jednotlivých odděleních.

Přístup pracovníků k většině tiskáren není nijak omezen (přístupovými právy). Výjimkou jsou některé tiskárny, jejichž použití by mohlo být pro zaměstnance zajímavé, ale vzhledem

[1] Operační systém stanic Microsoft Windows NT je třeba čas od času, cca jednou za půl roku, reinstalovat, neboť dochází ke zvyšování velikosti registrů, zpomalování počítače a množí se chyby operačního systému

k určení tiskárny si to oddělení informatiky nepřeje. Příkladem je barevná laserová tiskárna v oddělení laboratoře, která slouží k tisku protokolů o měření. Operační systém Microsoft Windows NT umožňuje zavést evidenci tiskových úloh s uvedením pracovníka, který tisknul, čase, kdy tisknul a délce tiskové úlohy, ale tato evidence byla po krátkém zkoušení vyřazena z provozu. Důvodem je vysoký objem tisku a s tím související rychlé zaplnění evidenčního protokolu.

V současné době není tedy možné dlouhodobě kontrolovat objemy tisků jednotlivých pracovníků.

3.2 Programová opatření

3.2.1 Zálohování

K ochraně dat před poškozením v případě výpadku hardware, útoku viru nebo živelné pohromě slouží zálohování. Toto ve firmě Grupo Antolin Bohemia a.s. chápou a proto jsou zde důležitá data zálohována. K zálohování jsou využívány digitální pásky DAT[2]. Ve firmě se nacházejí dvě mechaniky DAT, jedna s kapacitou DDS-2 (4 GB bez komprese, 8 GB s kompresí, v praxi se dosahuje kapacity cca 6 GB, vzhledem k různé efektivnosti komprese pro různé typy dat) a jedna s kapacitou DDS-3 (12 GB bez komprese, 24 GB s kompresí, v praxi cca 16 GB). Součástí spolupráce s oddělením informatiky bylo vypracování plánu zálohování, který přesně určuje, jaká data (který svazek) jsou kdy zálohována. Aktualizovaný plán zálohování se nachází v příloze.

Zálohování je rozloženo na celý týden, probíhá automaticky v noci a jediná interakce pracovníka obsluhujícího zálohování je výměna pásek a kontrola chybového souboru. Pro zálohování jsou využívány obě mechaniky a zálohování je navrženo tak, aby případná ztráta dat byla co nejmenší. Zálohování probíhá dvěma odlišnými způsoby. V týdenních intervalech probíhá absolutní zálohování na pásce s vyšší kapacitou a v denních intervalech přírůstkové zálohování souborů, které se od posledního zálohování změnily. Zálohuje se na sady o čtyřech páskách (na čtyři týdny), což umožňuje obnovit data až do doby před čtyřmi týdny, a umožňuje úspěšnou obnovu dat i v případě poškození jedné pásky.

V současné době je zálohováno týdně asi 26 GB dat a při zachování stávající technologie (pásky DAT) je možný růst až na přibližně 40 GB týdně. Po zapojení robota AIT, který umožňuje zálohování až na 20 kazet bez zásahu operátora, se ovšem toto číslo zvýší úměrně s kapacitou technologie AIT a tento zálohovací plán bude určitě změněn.

Se zálohováním úzce souvisí i archivování. Na rozdíl od zálohování, archivování slouží k vytváření stálých archivů, které již nebudou přemazávány. K archivování jsou magnetická média nevhodná vzhledem ke nestálosti magnetické vrstvy, která za několik let může ztratit uloženou informaci. Proto se k archivaci často používají zapisovatelná CD, jejichž životnost v případě kvalitního značkového média a správného uložení (sucho, chladno, správná poloha) je odhadována na desítky až stovky let. Pro účely archivace vlastní firma Grupo Antolin Bohemia a.s. zapisovací mechaniku CD-RW. Tato mechanika kromě účelu archivování slouží i k účely výměny dat útvarů vývoje jednotlivých subdodavatelů Škody Auto. Mechanika je umístěna v pracovní stanici pracovníka oddělení informatiky a její obsluhou je pověřen uživatel této pracovní stanice. Oddělení vývoje sice požadovalo zakoupení vlastní mechaniky pro zápis CD z důvodu snadnější výměny dat, avšak tento požadavek byl kvůli snížení bez-

[2] v blízké době dojde k doplnění zálohovacím robotem s technologií AIT, která má řádově vyšší kapacitu – až 50 GB na jednu pásku

pečnosti dat a nemožnosti kontroly zapisovaných dat striktně odmítnut vedoucím oddělení informatiky.

Přístup k jednotce CD-RW je omezen oprávněními na pracovní stanici, což zajišťuje, že se k pracovní stanici nemůže přihlásit jiný, než pověřený uživatel, proto není možné, aby například po pracovní době použil jednotku pro soukromé účely jiný pracovník.

3.2.2 Uložení médií

Média použitá pro zálohování a CD-ROM, na nichž jsou uloženy archivy, obsahují citlivá firemní data, která by měla být důvěrná a chráněná před vyzrazením. Také by měla být chráněna před zničením (příliš nepomůže, když záloha dat shoří spolu s originálem). Zároveň je důležité uložení médií z hlediska vlivu okolního prostředí na životnost médií a dat na nich uložených. Proto by měla být věnována pozornost i uložení médií. Měla by být uložena dostatečně daleko od originálu dat, aby se minimalizovalo riziko současného poškození originálu i kopie, měla by být uložena tak, aby přístup k nim měl pouze pověřený pracovník provádějící zálohování a případné obnovy dat a měla by být uložena souladu s pokyny výrobce o skladování.

Z hlediska bezpečnosti je tato stránka věci ve firmě Grupo Antolin Bohemia a.s. hrubě podceněna. Média jsou uložena v dřevěné skříni v uzamčené serverové místnosti. Tato místnost je sice fyzicky oddělena, ale není žádné speciální konstrukce z hlediska nedobytnosti nebo požární ochrany. V případě odcizení nejsou uložená data chráněna žádnou formou šifrování (které by při ukládání výrazně prodlužovalo dobu zálohování) a proto je může přečíst každý s odpovídajícím vybavením (což je zvláště nebezpečné u archivů, neboť jednotka CD-ROM je již standardní součástí naprosté většiny počítačů). V případě požáru dojde ke zničení serverů, originálů dat a archivních kopií. Ovšem riziko požáru snižuje po celé firmě nainstalovaný požární hlásící systém.

3.2.3 Antivirový program

Na každé pracovní stanici je nainstalován antivirový program Network Associates VirusScan. Tento program je rezidentně spuštěn a kontroluje soubory na přítomnost virů při otvírání souborů a ukládání na disk. Program funguje na bázi porovnávání obsahu souboru se svou virovou bází, která obsahuje reprezentativní vzorky kódu každého viru, který je program schopen naleznout. Tato virová báze samozřejmě postupem času zastarává a stává se neaktuální, proto je nutné ji po určité době obnovovat. To zajišťuje pracovník oddělení informatiky, který zpravidla v týdenních intervalech získává z webových stránek firmy Network Associates aktualizovaný soubor se vzorky známých virů. Program VirusScan je schopný odhalit i některé makroviry (firma využívá programy z balíku Microsoft Office, proto je zde nebezpečí makrovirů vysoké).

Součástí programu VirusScan je i plánovač, který umožňuje nastavit na určitý čas (nebo určitou událost, jako je spuštění počítače nebo aktivace šetřiče obrazovky) nastavenou akci, například prohledání pevného disku na přítomnost virů nebo aktualizaci virové báze z předem určeného místa. Právě této vlastnosti se využívá pro každodenní aktualizaci virové báze jednotlivých stanic z centrálního adresáře na serveru, kam soubor umístí po získání pracovník oddělení informatiky.

Od firmy Network Associates existuje i modul pro prohledávání elektronické pošty na přítomnost virů. Tento modul se instaluje na server elektronické pošty (Microsoft Exchange) a každou procházející zprávu prověří stejným způsobem – porovnáním s virovou bází – na přítomnost viru. Pokud je virus nalezen, je zpráva místo doručení uložena do speciálního adresáře a o situaci je zpraven správce serveru. I tento program umí vyhledávat makroviry a viry ve Visual Basicu. Příkladem viru, který je stále ještě velmi často zachycován, je virus ILoveYou a jeho mutace.

Program VirusScan je poměrně účinný, ale jeho nevýhodou je, že pro vyhledávání virů používá virovou databázi. Což na jednu stranu snižuje nebezpečí planých poplachů, ovšem na druhou stranu program nezachytí nové viry, které ještě nebyly popsány ve virové databázi (což byl například 27.4.2000 případ viru ILoveYou, který pronikl přes antivirové programy na pracovních stanicích, a tam se aktivoval – v případě, že by program VirusScan obsahoval i heuristickou analýzu kódu, je pravděpodobné, že by byl virus zachycen a zneškodněn).

3.2.4 Elektronické bankovnictví

Pro spojení s bankou, u které má Grupo Antolin Bohemia a.s. zřízeny účty, je využíváno elektronické bankovnictví. Pro tyto účely je vyhrazen samostatný počítač v úseku účtárny, který je vybaven modemem a programovým vybavením pro realizaci elektronického bankovnictví. Programové vybavení umožňuje odesílání příkazů k platbě, zjišťování zůstatků na účtech a historie pohybů na bankovních účtech.

Celá transakce pro zadání příkazů k platbě vypadá následovně (viz obrázek 4):

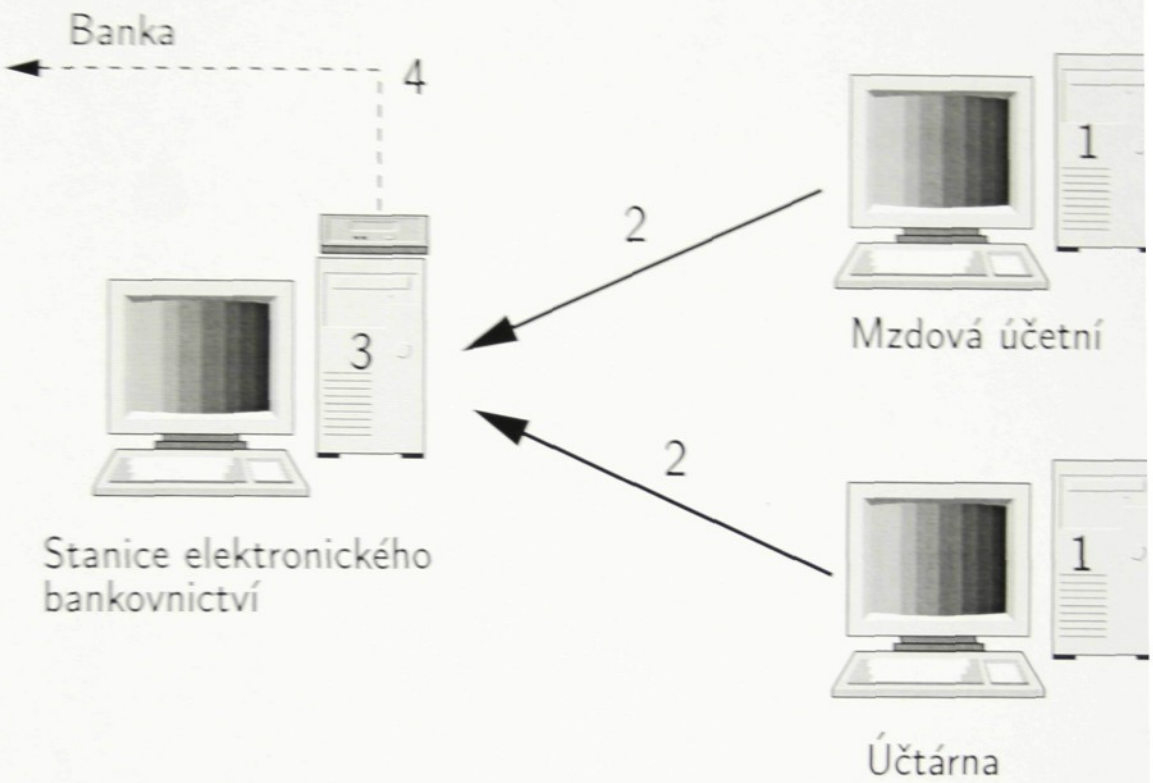
1. Z informačního systému (buď ze systému SAP nebo ze systému Helios, který se používá pro zpracování mezd[3]) je vygenerován soubor s příkazy k platbě. Soubor je v textovém tvaru a obsahuje informace o jednotlivých platebních příkazech: číslo účtu, částku, specifický a konstantní symbol, měnu a podobně. Soubor je běžně čitelný a údaje interpretovatelné.

2. Vygenerované příkazy k platbě ve formě souboru jsou převedeny na počítač s nainstalovanými aplikacemi pro elektronické bankovnictví.

3. Na tomto počítači jsou zkonvertovány z obecného formátu do specifického formátu bankovní aplikace (jedná se také o textový soubor podobného stylu).

[3] připravuje se přechod na jiný systém

4. Pomocí bankovní aplikace jsou příkazy odeslány šifrovaným spojením ke zpracování bance. Jako šifrovací metoda je použit systém RSA, který zajišťuje přenos informace přes nedůvěryhodný kanál (v tomto případě telefonní linku) bez možnosti zjištění jejího obsahu. Použití aplikace elektronického bankovnictví je vázáno na autorizaci uživatele. Proto každý uživatel aplikace musí mít vygenerován svůj profil, přidělené heslo a svůj šifrovací klíč, který jej identifikuje na straně banky. Proto je možné zpětně zjistit, který uživatel provedl odeslání příslušných příkazů do banky.



Obrázek 4: Elektronické bankovnictví

Slabým místem elektronického bankovnictví jsou body 2 a 3. Počítač s nainstalovanou aplikací pro elektronické bankovnictví je připojen v lokální síti a je v této síti běžně přístupný. Částečnou ochranou je, že k tomuto počítači, stejně jako k počítači mzdové účetní se může přihlásit pouze pověřená osoba, vše tedy závisí na bezpečném chování pověřených uživatelů. Textové soubory (před konverzí i po konverzi) jsou umístěny na pevném disku počítače v otevřené formě. Proto je zde nebezpečí úniku informací. Kdokoli může zjistit, jaké proběhly transakce, stačí mu získat tyto soubory. Diskutovatelnou otázkou je i možnost modifikace příkazů k platbě mezi body 2 a 3, případně 3 a 4.

3.2.5 Oprávnění

V podnikové síti Grupo Antolin Bohemia a.s. je něco okolo 120 uživatelů. Všichni mají svou vlastní unikátní identifikaci (přidělené uživatelské jméno, schránku elektronické pošty, profil, heslo). Spolu s identifikací uživatelů existuje možnost omezit přístup uživatelů k vybraným datům pomocí oprávnění přístupu. Každý uživatel může mít přiděleno právo číst, modifikovat či mazat, až na úroveň jednotlivých souborů. To zajišťuje, že se citlivé informace nedostanou do ruky nesprávnému uživateli. Ovšem vyžaduje to poměrně pracnou analýzu, kdo může přistupovat k jakým datům, a je nutné pro každý soubor stanovit jeho oprávnění a tato oprávnění nastavit. Použití oprávnění je důležité zejména na sdíleném disku na souborovém serveru, neboť zde si ukládají svá data všichni uživatelé sítě. Mají samozřejmě možnost ukládat si svá data na lokální disky svých pracovních stanic, a někteří to zejména s důvěrnými daty dělají, ale nevýhoda tohoto postupu je v tom, že disky lokálních stanic nejsou zálohovány. Navíc data na lokálních discích bez nastavení odpovídajících oprávnění jsou stejně zranitelná jako na sdíleném disku, částečným zlepšením bezpečnosti je, že na pracovních stanicích uživatelů, kteří pracují s důvěrnými informacemi (účtárna, elektronické bankovnictví, mzdová účetní, vedoucí personálního oddělení) je přihlášení omezeno softwarově pouze na tyto uživatele.

Na sdíleném disku jsou vytvořeny adresáře pro jednotlivé útvary firmy a útvary mají dále možnost rozšiřovat si jejich strukturu. Každý útvar si ukládá data do svého adresáře. Další struktura adresáře je plně v kompetenci každého útvaru. Neexistuje jednotná směrnice nebo předpis, který by říkal, jak mají být data v podadresářích uspořádána, proto na sdíleném disku vládne nepořádek. Většina dat je volně přístupných pro každého uživatele. Naprostá většina souborů nevyužívá pro svou ochranu oprávnění přístupu. Oprávnění jsou důsledně dodržována pouze u reportingových tabulek, požadovaných španělskou centrálou, které jsou uloženy ve zvláštním adresáři a jejichž ochrana je striktně vyžadována španělskou stranou a u důvěrných souborů, u nichž vedoucí oddělení toto vyžádali.

Pokusy zavést kontrolu přístupu na úrovni jednotlivých souborů několikrát zmařili vedoucí ostatních úseků s poukazem na to, že není možné určit osoby, které mají mít přístup k jednotlivým souborům, neboť soubory je nutné mít veřejně přístupné. Odmítli proto poskytnout údaje o zabezpečení jednotlivých souborů. Dalším pokusem zlepšit bezpečnostní situaci souborů na sdíleném disku byla snaha o přesun osobních dat nebo dat, která nemusejí být sdílena, do soukromého adresáře, který je též zálohován. Ale vzhledem ke konzervatismu uživatelů a nechuti ke změnám je v současné době kapacita disku s domácími adresáři využívána minimálně.

Současným stavem je tedy minimální zabezpečení většiny souborů, které jsou veřejně přístupné každému, kdo má právo přihlásit se k počítačové síti a bezpečnostní pravidla jsou aplikována pouze u některých souborů.

3.2.6 Přenosy dat

K propojení vnitřní sítě Grupo Antolin Bohemia a.s. s ostatními sítěmi je používáno několik spojení(viz též obrázek 3 na stránce 26). Základním je linka Frame Relay o rychlosti 128 Kbit/s pronajatá od poskytovatele telekomunikačních služeb[4]. Tato linka spojuje lokální síť Grupo Antolin Bohemia a.s. s centrální sítí společnosti Grupo Antolin, přes tuto síť je připojena k Internetu (přes firewall ve španělském Burgosu) a k sítím ostatních zahraničních poboček firmy Grupo Antolin. Provoz této linky je plně v kompetenci útvaru informatiky v Burgosu a v případě výpadku řeší nastalou situaci tento útvar. Proto se touto linkou a její bezpečností nezabývám. V případě výpadku je tato linka jištěna ISDN spojením přes pobočkovou ústřednu do centrály firmy (mezinárodní datový digitální přenos po telefonní lince) rychlostí 64 Kbit/s. Přes tuto linku probíhá veškerá komunikace firmy s centrálou, komunikace se servery systému SAP a internetový provoz, včetně služeb WWW a elektronická pošta.

Další možností externí konektivity firmy jsou dva modemy v prvním patře administrativní budovy. Jeden modem slouží pro elektronické bankovnictví a druhý pro potřeby oddělení informatiky. Oba modemy jsou proti zneužití chráněny nastavením přístupových práv – jsou povoleny jen v určitých uživatelských profilech a oba jsou nastaveny tak, že pomocí nich není možné proniknout k firemním datům – oba neodpovídají na příchozí volání a nejsou nastaveny pro přístup do lokální sítě.

Jeden ze serverů v serverové místnosti slouží i jako server dálkového přístupu. Je využíván zejména vedoucím skladu JIT v Mladé Boleslavi, který si pomocí dálkového přístupu vyzvedává svou elektronickou poštu a předává údaje útvaru expedice. Tento modem je nastaven pro příchozí volání a pro spojení vyžaduje autentizaci uživatele. Bylo by možné využívat modem i pro spojení manažerů na služebních cestách, aby si mohli i například v zahraničí vyzvedávat svou poštu, případně měli přístup k souborům v počítačové síti, ale oddělení informatiky přiděluje oprávnění jen ve velmi nutných případech na omezenou dobu. Součástí je i prohlášení o seznámení se s předpisy o používání tohoto přístupu k lokální síti (nachází se v příloze). Toto připojení probíhá po běžné telefonní lince a je proto zcela mimo kontrolu firmy.

Poslední možností přístupu k lokální síti je ISDN modem v oddělení vývoje. Tento modem je využíván pro výměnu CAD dat (výkresů) mezi odděleními vývoje jednotlivých subdodavatelů firem Škoda Auto a VW AG. Obsluha připojení probíhá přes specializovaný software pro výměnu souborů, který umožňuje pouze výměnu souborů mezi dvěma autorizovanými zdroji. Neautorizované příchozí volání je odmítnuto, při autorizovaném spojení lze soubory pouze přijmout, není možné si vyžádat soubor, který nebyl zařazen k odeslání.

[4]plánován přechod na 2Mbit/s v průběhu roku 2001

3.2.7 Organizační opatření a osvěta uživatelů

Největším problémem pro bezpečnost každého systému jsou lidé. Bezpečnostní opatření technického rázu je možné implementovat relativně bez problémů, ale organizační opatření nejsou jednoduchá. Je nutné zaměstnance donutit, aby se těmito opatřeními řídili a to není jednoduché. Sebelepší ochrana souborů pomocí přístupových práv selhává, pokud oprávněný uživatel odejde od počítače a nechá svou stanici zapnutou a sebe přihlášeného. V tomto okamžiku může kdokoliv přijít a pracovat na účtu tohoto pracovníka. Není výjimkou, že pracovník nechá svou stanici takto otevřenou i přes noc do druhého dne.

Dalším problémem, který může vést až k nepřístupnosti služby, je zneužívání prostředků firmy k soukromým účelům. Přístup k počítačové síti Internet, jehož servis je v pravomoci pracovníků centra v Burgosu, není nijak restriktován pouze pro pověřené uživatele (důvodem je nepružnost produktu MS Proxy, který neumožňuje nastavit omezení tak, aby bylo účinné), ale přístup k síti má jakýkoliv uživatel. Proto je zde nebezpečí, že uživatelé nahrají ze sítě například virus, který bude natolik nový, že jej antivirový program nezachytí. Nemusí se jednat o virus, je možné, že uživatelé svou aktivitou zaplní soukromý nebo sdílený disk, což ve svém důsledku vede k narušení služby souborového serveru.

Neopominutelnou součástí je například i zahlcování schránek elektronické pošty (a tím i místa na poštovním serveru, který tyto schránky udržuje) soukromými dopisy, obsahujícími několika-megabitové přílohy ve formě spustitelných programů. Pokud uživatel rozešle 30 svým kolegům soubor o velikosti 2 MB, na poštovním serveru zabere jen tato zpráva 60 MB.

Problémem je i možnost instalovat si na svou pracovní stanici vlastní programové vybavení. Operační systém Microsoft Windows NT sice umožňuje zablokovat zápis na disk pouze pro určité uživatele, ale ve standardní instalaci zůstávají zapisovatelné například systémové adresáře a restriktivní opatření mohou vést až k ochromení chodu operačního systému. Efektivně zabránit samostatným instalacím vlastního programového vybavení v systému Windows NT nelze (pouze částečně).

Tyto všechny problémy by bylo možno vyřešit stanovením organizačních opatření a důsledným dohledem nad jejich dodržováním. Tato organizační opatření musejí přesně definovat, co je zakázáno a jak se má pracovník ve vztahu s informačním systémem firmy chovat, ale i sankce, které následují v případě porušení nařízení. Každý pracovník se musí s organizačními opatřeními prokazatelně seznámit. Vhodným místem na uvedení těchto pravidel je například kolektivní smlouva.

3.2.8 Dostupnost služeb

V době, kdy stále více úloh zpracování dat je centralizováno a přesouváno na pověřené servery, je otázka dostupnosti služeb velmi důležitá. Čím více je úloha centralizována, tím více uživatelů je závislých na provozu centrálního uzlu sítě a tím nepříjemnější a škodlivější je

výpadek tohoto uzlu. Proto bezproblémový chod sítě závisí na několika málo centrálních počítačích a při výpadku některého z nich je ochromena práce všech uživatelů, kteří závisí na službách poskytovaných tímto počítačem. To je zvláště důležité v případě výpadku počítače, na jehož službách závisí vlastní chod celé počítačové sítě, jako je například DHCP server. Při jeho výpadku dochází během několika hodin k totálnímu rozpadu celé sítě, která poté bez jeho spolupráce prakticky zaniká. Ovšem službami podobné důležitosti jsou i tiskový server, souborový server, databázový server a podobně. V následujícím seznamu je vidět, jak jsou jednotlivé služby zálohovány a jaké nebezpečí hrozí v případě jejich výpadku. Hodnocení je použito podobné jako ve škole: 1... nejlepší, 5... nejhorší zálohování služby.

- DHCP server
  - maximální doba výpadku 1 hodina
  - důsledky výpadku: rozpad sítě, nemožnost komunikace
  - zálohování služby: není
  - zálohování dat souvisejících se službou: výpis nastavení
  - postižené útvary: všechny
  - hodnocení 5
- EDI server
  - maximální doba výpadku 2-4 hodiny
  - důsledky výpadku: nemožnost plánování, fakturace, při delším výpadku zastavení výroby
  - zálohování služby: 2 identické servery, 2 linky X.25
  - zálohování dat produkovaných službou: zálohování
  - postižené útvary: plánování, účtárna, expedice, výroba
  - hodnocení 3
- databázový server
  - maximální doba výpadku 1 hodina
  - důsledky výpadku: nemožnost plánování, fakturace, zpomalení výroby – havarijní plán
  - zálohování služby: redundantní komponenty - RAID diskové pole, zdvojené napájení, 2x UPS
  - zálohování dat produkovaných službou: týdenní zálohování, zálohování EDI dat před příchodem na SQL – dvojí záloha

- postižené útvary: výroba, plánování, účtárna, expedice
- hodnocení 4

- Poštovní server
  - maximální doba výpadku 24 hodin
  - důsledky výpadku: Ukončení příjmu a posílání elektronické pošty
  - zálohování služby: UPS
  - zálohování dat produkovaných službou: týdenní zálohování
  - postižené útvary: všechny kromě výroby
  - hodnocení 3

- Souborový server
  - maximální doba výpadku 12 hodin
  - důsledky výpadku: Ukončení zpracování dat
  - zálohování služby: diskové pole RAID, zrcadlení startovacího disku, UPS
  - zálohování dat produkovaných službou: denní zálohování
  - postižené útvary: všechny kromě výroby
  - hodnocení 4

- Tiskový server
  - maximální doba výpadku 12 hodin
  - důsledky výpadku: nefunkčnost tiskáren
  - zálohování služby: UPS, tiskárny u pracovních stanic
  - postižené útvary: administrativa, účtárna, prodej, technologie, kvalita,
  - hodnocení 5

- Server vzdáleného přístupu
  - maximální doba výpadku 48 hodin
  - důsledky výpadku: Ztráta spojení s JIT skladem Mladá Boleslav
  - zálohování služby: UPS
  - postižené útvary: JIT sklad
  - hodnocení 5

- Faxový server
  - maximální doba výpadku 24 hodin
  - důsledky výpadku: není příjem objednávek pro expedici a plánování
  - zálohování služby: manuální faxy
  - zálohování dat produkovaných službou: centrálně se nezálohuje
  - postižené útvary: expedice, plánování, údržba
  - hodnocení 3
- Doménový server
  - maximální doba výpadku 1 hodina
  - důsledky výpadku: Rozpad sítě, nemožnost komunikace
  - zálohování služby: Záložní doménové řadiče
  - postižené útvary: všechny
  - hodnocení 2
- Přenosy dat vývoj
  - maximální doba výpadku 24 hodin
  - důsledky výpadku: Narušení výměny dat oddělení vývoje
  - zálohování služby: není
  - zálohování dat produkovaných službou: denní zálohování, export databáze komunikačního programu (ostatní účastníci, nastavení programu) po každé změně
  - postižené útvary: vývoj
  - hodnocení 5

V tabulce 1 jsou znovu shrnuty nejdůležitější údaje o službách. Je vidět, že pro chod sítě jsou některé funkce zcela nezbytné a jejich výpadek je velkým nebezpečím pro celou firmu. Seznam vypadá velice hrozivě, je nutné si ale uvědomit, že ideálního stavu není možné v praxi dosáhnout. Například záloha databázového serveru pomocí zrcadlení serverů je sice teoreticky možná a pro případ výpadku služby téměř neprůstřelná, ale v praxi ji není možné dosáhnout bez vysokých finančních nákladů. Druhý databázový server znamená zakoupení další licence pro provoz serveru a dalších několik licencí pro klienty, což znamená finanční náklady řádově ve výši desítek až stovky tisíc korun.

Součástí zajištění dostupnosti služeb je i dostatečné zajištění dodávky elektrické energie. To je velmi důležité, také proto, že ve větvi elektrické sítě, ke které je připojen objekt firmy Grupo Antolin Bohemia a.s. dochází někdy ke kolísání napětí a někdy je dodávané napětí

Služba	Maximální doba výpadku	Postižené útvary	Hodnocení
DHCP server	1 hodina	všechny	5
EDI server	2 – 4 hodiny	plánování, účtárna, expedice, výroba	3
databázový server	1 hodina	výroba, plánování, expedice, účtárna	4
poštovní server	24 hodin	všechny kromě výroby	3
souborový server	12 hodin	všechny kromě výroby	4
tiskový server	12 hodin	administrativní budova	5
server vzdáleného přístupu	48 hodin	JIT sklad	5
faxový server	24 hodin	expedice, plánování, údržba	3
doménový server	1 hodina	všechny	2
přenosy dat – vývoj	24 hodin	vývoj	5

Tabulka 1: Kritické služby

nižší než nominální (podpětí). V tomto případě však již zatížené servery mohou vykazovat nestabilitu. Proto je každý důležitý prvek sítě (servery, směrovače, modemy, páskové mechaniky) připojen na zařízení UPS typu On-Line UPS, které zajišťuje nepřerušovaný přívod elektrické energie po dobu výpadku (maximálně však cca 1 hodinu) a částečnou ochranu před rázy v elektrické síti.

3.2.9 Databázový server

Jak je vidět, naprosto nezbytným pro chod celého podniku (jeho nosné části – výroby) je fungující databázový server. Na tomto serveru jsou zapisovány do databáze došlá EDI data, podle kterých probíhá plánování, fakturace a expedice, ale zejména data přímo řídící systém čárových kódů výroby. Na tomto systému (systém byl zaveden v květnu 2001) je závislá výroba, která při jeho nefunkčnosti nemůže efektivně fungovat. V případě výpadku služby (zdárný chod systému čárových kódů závisí na databázovém serveru, řídícím počítači bezdrátové komunikace a komunikačním kanálu – bezdrátové síti) je nutno použít náhradní havarijní plán, který kromě jiného způsobí ztrátu plynulosti výroby a zpomalí výrobu.

Pro zpracování odvolávek se využívá několik samostatných databází, jejichž struktura závisí na typu přijímané odvolávky. Struktura EDI dat je pevně dána a normována, k implementaci zpracování existují implementační příručky, které vytvářejí odběratelé. Tyto databáze jsou umístěny na databázovém serveru a pracovníci oddělení plánování a expedice k nim přistupují prostřednictvím aplikací vytvořených pro tento účel buď dodavatelskou firmou

nebo pracovníky oddělení informatiky. K přístupu k databázím je používán hromadný účet na databázovém serveru, tento účet má omezená privilegia pouze na zpracování uvedených databází.

3.2.10 Odhad nákladů při havárii databázového serveru

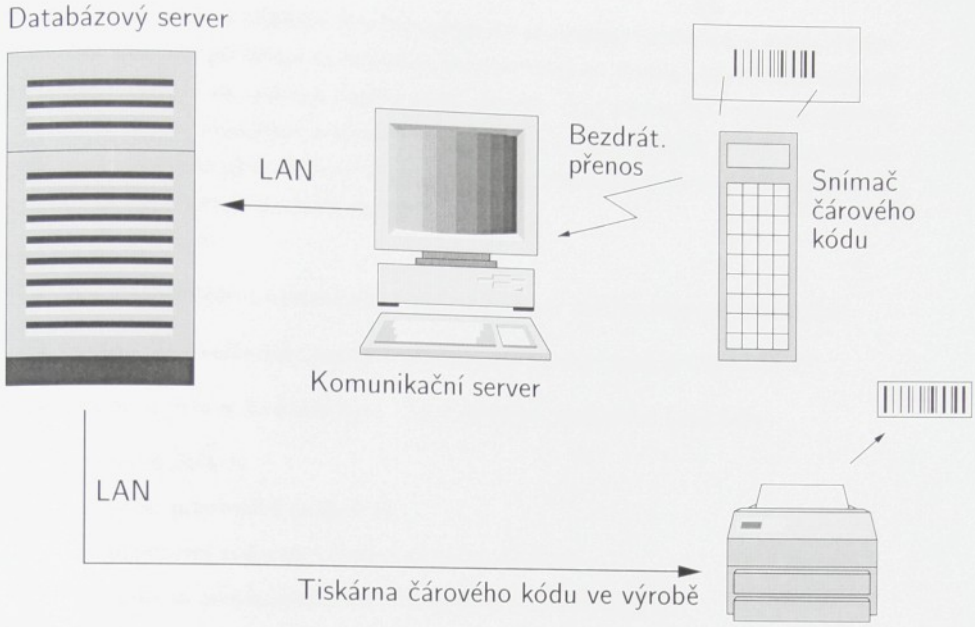
Databázový server je proti výpadku částečně chráněn. Počítač, na kterém je server provozován, je značkový a je určen pro nasazení v kritických aplikacích. Proto je vybaven zdvojeným procesorem (jedná se o dvouprocesorový stroj, který je schopen v případě poruchy jednoho procesoru pokračovat pouze s jedním), problémem může být chyba paměti RAM, která je sdílena oběma procesory. Jako úložný prostor se využívá čtveřice disků SCSI, které jsou spojeny do diskového pole typu RAID 5, kritické oddíly, zejména startovací oddíl, který je pro chod operačního systému Windows NT nezbytný, jsou zrcadleny. Počítač by proto měl být schopen pokračovat v práci i při poruše jednoho pevného disku. V případě výpadku elektrické energie je počítač vybaven dvěma nezávislými zdroji, zálohovanými samostatnými UPS a připojenými na různé fáze. V případě výpadku jednoho zdroje je druhý zdroj schopen napájet celý počítač sám. V případě totální havárie serveru je připraven plán postupu, pomocí něhož je možné provést kompletní reinstalaci serveru a zprovoznění služby do čtyř hodin od výpadku. Tento plán ovšem předpokládá, že nebude nutná výměna některé části hardware nebo že tato součást bude ve firmě okamžitě připravena k výměně. V případě havárie například základní desky se doba výpadku prodlužuje o dobu dodání nové součásti dodavatelem, což může být i několik dní.

V případě havárie databázového serveru přestanou být na server zapisována data EDI od odběratelů, což jsou podklady pro plánování a fakturaci. Tato data jsou však stále přijímána EDI servery a zálohována na nich, proto výpadek až do doby 24 hodin není pro chod firmy z hlediska EDI kritický.

Jakýkoliv výpadek je ovšem kritický pro systém čárových kódů. Tento systém sestává ze čtyř komponent(viz obrázek 5):

- přenosných snímačů čárových kódů,
- komunikačního serveru bezdrátové sítě,
- databázového serveru,
- tiskáren čárového kódu ve výrobě.

Podle kódu sejmutého ze vzorového sešitu dojde k zápisu do databáze, zaregistrování dokončení výroby dílu na databázovém serveru, zapsání náležitostí dílu (čas výroby, pracovník, který vyrobil, linka, stav kontejneru) a tisku etikety na polepení dílu a kontejneru. Tento systém funguje na 11 linkách zcela a na dalších linkách pouze k tisku a registraci kontejnerových etiket. Na každé z jedenácti linek dojde denně k tisku a použití 300 až 500 etiket, přičemž tisk jedné etikety trvá od 1 do 2 vteřin.



Obrázek 5: Zpracování čárového kódu

V případě havárie systému dojde k přechodu na havarijní plán, který funguje takto:

1. Pověřený pracovník linky (obsluha snímače) jde za pracovníkem informatiky, kde mu budou na základě poskytnutých údajů vytištěny etikety.

2. Pracovník informatiky požadavek zanese do off-line databáze, kterou udržuje na svém počítači a jejíž obsah po zprovoznění služby synchronizuje s hlavní databází na databázovém serveru.

3. Provoz na lince pokračuje do té doby, než na lince dojdou etikety, pak se vše opakuje od začátku.

4. V případě změny výroby na lince je nutné etikety stornovat a vytisknout nové s aktualizovanými údaji.

Hlavní problém je v tom, že při havarijním plánu jsou etikety tištěny dávkově a systém není tak pružný jako při tisku jednotlivých etiket přímo na lince. Pracovník informatiky se také musí plně věnovat tisku etiket a nemůže vykonávat svou práci a v neposlední řadě dojde ke koncentraci požadavků všech linek (kdy každá má v normálním případě k dispozici

2 tiskárny) na jedinou tiskárnu. Dochází proto ke zpomalení výroby asi o jednu třetinu, zpomalení nastávají při čekání na tisk etiket na jedné tiskárně. Z těchto údajů budu vycházet při odhadu nákladů na výpadek databázového serveru. Jako náklady zde chápeme náklady mzdové, které jsou nejnižšími prokazatelnými náklady. Celkové náklady budou samozřejmě vyšší, ale jejich částka již není přesně vyčíslitelná. Proto jako náklady uvažuji náklady mzdové, a nikoliv pracovníkem přidanou hodnotu.

Náklady zahrnují:

- plné vytížení jednoho pracovníka informatiky – pro obsluhu tiskárny 100 Kč/hod
- vytížení pracovníka informatiky – práce na odstranění výpadku 100 Kč/hod
- zpomalení výroby na každé lince – to je řešitelné přesčasovou prací linky.
  - počet linek 11
  - počet pracovníků na lince 15
  - přesčasová práce na 1 hodinu výpadku 20 minut
  - sazba za přesčasovou práci 50% (přesčasy na noční směně)
  - hodinová mzda dělníka 60 Kč
  - odvody placené zaměstnavatelem 35% (26% zdravotní a 9% sociální pojištění)

  Pro zjednodušení jsou započteny pouze linky, které tisknou výrobkové etikety.

$$N = 11 * 15 * 0.33 * 60 * 1.5 * 1.35 = 6620$$

  mzdové náklady na přímé pracovníky jsou tedy 6620 Kč za hodinu výpadku.

- Náklady na elektřinu, osvětlení a podobně. Tyto náklady pro zjednodušení zahrneme mezi fixní náklady a do výpočtu neuvažujeme.

Nyní uvažujme tři scénáře. Každý scénář představuje různě závažnou poruchu s různě dlouhou dobou odstávky:

1. Porucha síťové karty, tím pádem ztráta komunikace. Řešením je výměna za náhradní obyčejnou (pomalejší) síťovou kartu a přepojení na segment sítě s rychlostí 10Mbit/s. Doba odstávky 2 hodiny, náklady odstávky (reprezentované mzdovými náklady) ve výši 13 640 Kč.

2. Porušení registru operačního systému Windows NT, zhroucení systému. Řešením je reinstalace systému, reinstalace databázového serveru, obnovení dat ze zálohy. Doba odstávky 5 hodin, nedošlo k narušení plynulosti expedice odběratelům. Náklady odstávky 34 100 Kč.

3. Porucha základní desky, zastavení systému. Řešením je výměna základní desky, kterou je ovšem nutno objednat u dodavatele. Doba odstávky 24 hodin, 2 osmihodinové směny, došlo k narušení expedice výrobků k odběrateli, nesplnění dodávky z důvodu zdržení. V tomto případě je nutno k mzdovým nákladům, které činí 109 120 Kč, připočíst náklady další. Vzhledem k tomu, že nebyla dodržena doba dodávky k zákazníkovi, došlo ke zdržení dodávky, vstupují do kalkulace i smluvní pokuty za nedodržení termínu dodání. Mohlo se stát, že odběratel byl nucen vzhledem k nedoručení zásilky zastavit linku a náklady na zastavení linky a zdržení výroby přefakturuje dodavateli, který situaci způsobil. Dalším důsledkem, jehož vliv může být dlouhodobý, je možnost snížení ratingu (hodnocení) dodavatele a z toho plynoucí ztráta části zakázek nebo zákazníka. A tyto škody se již mohou pohybovat v úrovni ročních tržeb, čili v řádu desítek či stovek milionů a mohou být pro firmu a její přežití kritické.

3.2.11 Informační systém SAP

Servery informačního systému SAP se nacházejí v centrále firmy ve španělském Burgosu a jsou společné pro celou firmu. Struktura informačního systému SAP je trojvrstevná: klient, aplikační server, databázový server. Klient systému SAP se spojí s aplikačním serverem, se kterým komunikuje prostřednictvím vyhrazené aplikace SAPclient. Aplikační server transformuje požadavky klienta na dotazy jazyka SQL, které odesílá na databázový server (také Microsoft SQL Server 7.0 na platformě Intel a operačním systému Windows NT). Ten je zpracuje a aplikačnímu serveru zašle zpět výsledky. Aplikační server je přetvoří na data zobrazitelná klientem a předá klientovi. Ten je pak zobrazí uživateli. Aplikační server také na základě požadavků uživatele (předanými klientem) odesílá tiskové úlohy na lokální tiskárny, nebo například odesílá elektronickou poštu (interně v systému SAP).

Aplikační i databázový server se nacházejí v Burgosu. Klient a aplikační server spolu komunikují proprietárním aplikačním protokolem (síťovým protokolem je TCP/IP) a aplikační a databázový server komunikují aplikačním protokolem databázového serveru. Na databázovém serveru jsou všechna data informačního systému reprezentována jako velké množství tabulek, relací, pohledů, procedur a dotazů. Jako položky v tabulkách jsou uloženy i údaje o oprávnění jednotlivých uživatelů na provádění jednotlivých transakcí (takzvané profily). To znamená, že pokud je databázový server dostupný přímo pomocí databázového klienta, nikoliv jen přes aplikační server, že uživatel s právem přístupu k databázovému serveru může modifikovat údaje „za zády“ aplikačního serveru a tak si například jednoduchou modifikací položky v tabulce přidělit nejvyšší oprávnění přístupu. Dalším nebezpečím je možnost ztráty integrity dat plynoucí z „ruční“ modifikace dat.

Tato situace byla možná až do poloviny minulého roku, kdy byly databázové servery ve španělské centrále přesunuty za firewall a přístup byl umožněn pouze aplikačním serverům. V současné době je tedy přístup možný pouze pomocí programu SAPclient v souladu s oprávněními systému SAP.

4 Návrh na zvýšení bezpečnosti dat

V této části bych rád nastínil řešení některých problémů, které se vyskytují v bezpečnosti dat firmy Grupo Antolin Bohemia a.s. Tento návrh samozřejmě není vyčerpávající, celá riziková analýza, bezpečnostní politika a bezpečnostní projekty by dohromady daly dokument mnohem obsáhlejší a mnohem podrobnější. Takovýto dokument by ovšem vzhledem ke své konkrétnosti měl statut důvěrné zprávy a firma Grupo Antolin Bohemia a.s. by jistě nesvolila k jeho publikaci. Proto nastíním řešení pouze některých problémů, které se v informačním systému Grupo Antolin Bohemia a.s. vyskytují.

4.1 Kabeláž

Neočekávaně prudký růst lokální sítě způsobil, že kabeláž, nainstalovaná při adaptaci budovy, již nestačí potřebám firmy. Při jejím rozšiřování se postupovalo nejjednodušším a nejrychlejším způsobem. Ale toto připojování způsobilo neprůhlednost a složitost síťové struktury. Proto by bylo vhodné celou strukturu zjednodušit, vyvarovat se kaskádového řazení rozbočovačů a tím ulehčit některým segmentům sítě převedením zátěže na jiné, méně vytížené segmenty. Toto opatření ovšem znamená podrobně prověřit celou síťovou strukturu a změny dělat v době, kdy síť není používána (o víkendu). Celý postup se zdá být jednoduchý, ale znamená to, že každý kabel musí být popsán (je uděláno), musí být vytvořena kaskádní mapa celé sítě, včetně všech síťových prvků (rozbočovače, stanice, síťové tiskárny) a musí být připraven plán, nové, zjednodušené struktury.

Výhodou tohoto projektu je zjednodušení a zprůhlednění síťové struktury, odlehčení zatížených segmentů a omezení vlivu chyb kabeláže, neboť segmenty budou zatíženy rovnoměrně.

4.2 Tiskárny

Není nutné, aby u každé tiskárny byli definováni uživatelé, kteří tiskárnu mohou používat. U specializovaných tiskáren, sloužících pouze pro potřeby jednoho oddělení (zmíněná barevná laserová tiskárna) je to možné a žádoucí, avšak u tiskáren sloužících pro celé patro nebo budovu je to nemožné. Uživatelé si totiž mohou volit na jakou tiskárnu svou úlohu odešlou. V závislosti na požadavcích na kvalitu mohou tisknout na barevné inkoustové tiskárně v přízemí nebo na inkoustovém víceúčelovém zařízení v prvním patře, v případě větších objemů tisku mohou použít laserové tiskárny pro pracovní skupiny v každém patře. Není nutné, aby uživatelé měli pevně určeno, kterou tiskárnu mohou a kterou nemohou použít. Důležité ale je, aby oddělení informatiky mělo přehled, kdo kdy a jak velkou úlohu vytisknul. Této evidence je možné využít pro kontrolu, zda některý zaměstnanec nepoužívá tiskárny pro soukromé účely nebo zda netiskne nepřiměřeně velké objemy. Tato alespoň základní evidence by byla potřebná, zejména u rychlých laserových tiskáren LaserJet 5000, které jsou určeny pro pracovní skupiny a proto mají vysokou rychlost tisku. Jak již bylo řečeno, evidence byla

krátkou dobu v provozu, ale vzhledem k rychlému růstu souboru protokolu byla opět vyřazena z činnosti.

Jako alespoň částečné, kompromisní řešení by bylo zapínat evidenci pouze na víkendy. V mimopracovní dny neprobíhá tolik tiskových úloh, proto by velikost protokolu nenarůstala tak rychle. Zároveň každý větší objem tisku (který by se tím pádem v evidenci neztrácel ve velkém množství malých tiskových úloh) by bylo možné lehce odhalit a požadovat na zaměstnanci vysvětlení (už samotný fakt, že zaměstnanec o víkendu tisknul, je podezřelý).

4.3 Elektronické bankovnictví

Data uložená na počítači používaném pro elektronické bankovnictví jsou ohrožena. Je ohrožena jejich důvěrnost, neboť při nepozornosti nebo nedbalosti obsluhy počítače je možno získat seznam transakcí na bankovních účtech za poměrně dlouhou dobu do minulosti. Tato data by pak mohla být zneužita nebo by se mohla dostat do nepovolaných rukou (například seznam výplat). V součinnosti se seznamem bankovních účtů, na které jsou jednotlivým zaměstnancům zasílány výplaty, je velmi jednoduché odvodit výši mzdy každého zaměstnance.

Proto je nutné, aby po každé transakci byly datové soubory buď zničeny (smazány) nebo zašifrovány tak, aby je nemohl získat nikdo, kdo k těmto souborům nemá mít přístup. Zároveň je nutné, aby pracovník na této stanici dodržoval základní úkony bezpečnosti, například při opuštění stanice zamknul klávesnici a monitor, při odchodu se odhlásil a podobně.

4.4 Databázový server

Uživatelé databázového serveru, pracující s databázemi EDI dat, používají jednotný účet. Tento účet má kromě oprávnění číst a provádět selektivní dotazy i oprávnění zápisu do databáze. To je nutné pro chod programů pracujících s EDI daty, neboť programy při své práci modifikují obsahy některých tabulek. Programy neumožňují modifikovat jiná pole a jiné tabulky, než pevně dané, ovšem toto omezení je dáno pouze v programech, nikoli na databázovém serveru. Proto je možné pomocí nástrojů pro správce, případně programátorských nástrojů, modifikovat jiné položky. Tyto nástroje ovšem nemají běžní uživatelé nainstalovány.

Instalaci administrátorského nástroje zvládne i běžný uživatel a v tom případě má možnost upravovat i jiná pole. Řešením je definice sady oprávnění na databázovém serveru tak, aby nebyla narušena funkce programů, ale byla znemožněna neoprávněná manipulace s ostatními daty, současně s přechodem od hromadného účtu k účtům jednotlivých uživatelů, kteří se budou na databázovém serveru autorizovat pomocí svého přihlašovacího jména a hesla. Zároveň bude každému uživateli nastaveno oprávnění pouze pro příslušnou databázi a úroveň přístupu. Pomocí transakčního protokolu je pak možné sledovat práci jednotlivých uživatelů.

Nová bezpečnostní politika by poté vypadala následovně:

- Právo k zápisu do databáze má pouze zvláštní uživatel. Pod autorizací tohoto uživatele zapisují obslužné programy na EDI serverech došlá EDI data.
- Ostatní uživatelé se hlásí k databázovému serveru pomocí svého uživatelského jména a hesla. Mají oprávnění číst příslušné databáze a modifikovat pouze pole, jejichž modifikace je vyžadována programy (frontendy) uživatele.

Aplikace této politiky vyžaduje

1. Určit, kteří uživatelé mají na databázovém serveru pracovat
2. Určit, jaká oprávnění k jakým databázím má mít každý tento uživatel
3. Založit uživatele a nastavit jejich oprávnění
4. Prověřit správnou funkci programů

V tomto případě nemůže uživatel způsobit při použití administračního programu žádné škody – může modifikovat pouze některé položky, které mají pro obslužné programy informační význam.

Vzhledem k absolutně nezbytné funkci databázového serveru a nákladům při jeho výpadku by bylo vhodné nainstalovat na jiný server sítě (pravděpodobně poštovní server, který je nejméně zatížen) záložní databázový server, který by byl spouštěn pouze v případě výpadku hlavního databázového serveru a okamžitě by převzal jeho funkci. Náklady na další licenci jsou srovnatelné s náklady způsobenými výpadkem databázového serveru a dlouhodobě je toto řešení ekonomicky opodstatněné.

Dalším nutným opatřením je zajištění služeb souvisejících s chodem sítě, na nichž je databázový server přímo závislý. Jedná se o službu doménového serveru a serveru DHCP. Služba doménového serveru je zajištěna dostatečně, při výpadku primárního řadiče domény přechází řízení automaticky (funkce operačního systému Windows NT) na záložní řadič domény (tyto řadiče jsou ve firmě Grupo Antolin Bohemia a.s. dva), ale služba DHCP, která řídí přidělování IP adres, zálohována není. Je proto bezpodmínečně nutné na jiném serveru sítě spustit záložní server DHCP a zajistit sdílení databáze služby DHCP.

4.5 Oprávnění na sdíleném disku

Podobná situace je i na sdíleném disku s kapacitou 30 GB. Na tomto disku je ukládána většina pracovních dokumentů, jako jsou zprávy, analýzy, objednávky, pracovní dopisy a pouze malá část z nich je chráněna pomocí oprávnění. Ideálním stavem je, když jsou chráněny všechny soubory, ale to je zřejmě stav nedosažitelný. Bylo by nutno projít všechny soubory a v závislosti na tom, kdo může tento soubor vidět, nastavit jeho oprávnění. To však vyžaduje spolupráci všech vlastníků souborů a ze zkušeností se ukazuje, že to je téměř nemožné.

4.6 Školení uživatelů

Důležitou součástí bezpečnosti sítě (nejdůležitější součástí) je i zvyšování odborné úrovně uživatelů. Uživatelé musejí být seznámeni s důsledky svého chování a musejí se aktivně podílet na ochraně dat. Proto je nutné pořádat pravidelná školení o bezpečném chování v rámci informačního systému. Je nutno si uvědomit, že lidé pracující s informačním systémem představují největší hrozbu. Proto je nutné školením uživatelů tuto hrozbu minimalizovat. Uživatelé by měli být školeni zejména

- virové problematice a způsobech, jak zabránit infekci
  - elektronickou poštou
  - programem nahraným z Internetu
  - přineseným programem
- problematice bezpečného chování v síti
  - opouštění stanice
  - zatěžování síťových prostředků
  - zneužívání síťových prostředků
- efektivním využívání prostředků informačního systému
  - možnostmi zabezpečení poskytovanými operačním systémem

4.7 Organizační opatření

Jednou z nejdůležitějších součástí ochrany dat jsou organizační opatření. Tato opatření existují, firma je držitelem certifikátu jakosti a jednou z podmínek pro udělení certifikátu jakosti je i vytvoření směrnic a postupů pro všechny činnosti vykonávané ve firmě. Proto existují směrnice z oblasti personální, z oblasti informatiky, přístupu k informačnímu systému, práci v informačním systému, archivační a skartační řád, ve kterých jsou všechny činnosti definovány.

Součástí opatření by měly být i definice činností, zakázaných z hlediska bezpečnosti informačního systému. Měly by být definovány právně závazným způsobem (kolektivní smlouva, vyhláška ředitele) a pracovníci by s nimi měli být prokazatelně seznámeni. Je možné definovat zakázané činnosti velmi obecně. Tento přístup je jednodušší (nevyžaduje dlouhé přípravy) a je flexibilní, neboť je možná aplikace na širokou škálu prohřešků. Je také možné definovat činnosti velmi konkrétně, ale zde existuje nebezpečí, že některé zakázané činnosti zůstanou nepokryty.

Je vhodné zakázat:

- používání výpočetní, telekomunikační a kancelářské techniky za jiným než pracovním účelem,
- omezování ostatních uživatelů vnitropodnikové sítě nadměrným využívání přenosové a úložné kapacity,
- ohrožování bezpečnosti informačního systému a dat, chování směřující k takovému ohrožování,
- obtěžování ostatních uživatelů vnitropodnikové sítě nebo celosvětové sítě Internet nežádoucími aktivitami,
- kopírování firemních dat a jejich vynášení mimo prostory firmy.

Takto formulovaná nařízení pokrývají většinu aktivit uživatelů informačního systému, které by mohly vést k poškození nebo úniku dat nebo narušení chodu sítě.

Součástí organizačních opatření by měly být definované postihy za porušení těchto opatření, uživatelé musí vědět, že za rizikové chování může následovat postih. Při stanovení postihů je ovšem nutné vycházet z příslušných ustanovení Zákoníku práce.

5 Závěr

Vidíme, že zabezpečení firemního informačního systému je komplexní úkol, nejedná se pouze o souhrn nahodilých samostatných činností. Před vlastní implementací bezpečnostního projektu je nutná podrobná analýza rizik, která nám ukáže na slabá místa v systému a pomůže při plánování bezpečnostní politiky. Je nutno přiměřeně zabezpečit všechny části informačního systému, neboť bezpečnostní politika musí být vyvážená. V opačném případě nemají silná bezpečnostní opatření žádný smysl, pokud je lze obejít díky slabé ochraně jiné části systému. Je nutno mít na paměti, že systém je tak bezpečný, jak bezpečný je jeho nejslabší prvek.

Je však nutné také pečlivě zvažovat ekonomické stránky celého procesu zabezpečení. Investice do zabezpečení dat mají smysl pouze do chvíle, kdy nepřevyšují hodnotu zbytkového rizika, které v uvažovaném systému existuje.

V poslední době se začíná ukazovat, že vzhledem k rostoucímu významu informačních technologií pro chod firmy a stálému připojování firem na celosvětovou komunikační infrastrukturu získává zabezpečení informací ve firmě obrovskou důležitost. Firmy, které ještě dnes nevěnují bezpečnosti svých dat dostatečnou pozornost, poznají, že bez adekvátní ochrany svých investic nejsou schopné dlouhodobě působit na trhu, aniž by byla ohrožena jejich existence. Čím později začne firma aplikovat bezpečnostní projekty, tím nákladnější a náročnější bude upravit zaběhnutý systém tak, aby splňoval náročná kritéria na bezpečnost informací.

Z praxe je zřejmé, že největší problémy nepůsobí opatření technická, která jsou relativně jednoduše analyzovatelná, aplikovatelná a jejich funkčnost kontrolovatelná, ale opatření organizační, která závisí na chování uživatelů. Prosadit dodržování těchto opatření do praxe, navíc ve firmě, která upravuje svůj fungující informační systém k větší bezpečnosti, je bez silného dohledu a uplatňování represivní politiky téměř nerealizovatelné. Uživatelé si neuvědomují dopad svého chování a celé následky vidí až ve chvíli, kdy už je pozdě. Z tohoto důvodu bych kladl největší důraz při zavádění bezpečnostní politiky na organizační opatření, jejich dodržování a na stálou osvětu a vzdělávání uživatelů.

Seznam literatury

1. Curtis: *Business Information System*, 3.ed, Addison Wesley, Reading MA 1999
2. Date, C.J.: *An introduction to Database System*, 5.ed, Addison Wesley, Reading MA 1990
3. Dobda, Luboš: *Ochrana dat v informačních systémech*, 1.vyd, Grada, Praha 1998
4. Kovacich, Gerald L.: *Průvodce bezpečnostního pracovníka informačních systémů*, 1.vyd, UNIS Publishing, Brno 2000
5. Rodryčová, Staša: *Bezpečnost informací jako podmínka prosperity firmy*, 1.vyd, Grada, Praha 2000
6. Voříšek: *Strategické řízení informačních systémů a systémová integrace*, Management Press, Praha 1997
7. Žid, Benáčková, Kunstová, Svoboda: *Orientace ve světě informatiky*, Management Press, Praha 1998

Přílohy

1. Harmonogram zálohování
2. Evidenční list stanice
3. Struktura sítě firmy Grupo Antolin Bohemia a.s.
4. Prohlášení o seznámení s ustanoveními

Server	Pondělí	Úterý	Středa	Čtvrtek	Pátek	Sobota	Neděle	Popis	Absolutní	Rychlost
CZIBHSPD01			G1		G1		G4	Hlavní doménový server	20 GB	
CZIBHSEX01						G3	G4	Exchange server	10 GB	
CZIBHSPD		G2		G2			G5	Unix	50 GB	240 MB/s
CZIBHSPD02			G1		G1	G3		SQL server	2 GB	
CZIBHW0155	G1		G1			G3		RVS Cad	6 GB	
CZIBHW0155						G3		RVS Cad, databáze, nastavení		
CZIBHW50						G3		EDI, databáze, nastavení		
CZIBHW80						G3		EDI, databáze, nastavení		

Přírustkové
Absolutní, lichý
Absolutní, sudý

G - jednotlivé skupiny pásek

Skupina	Kolik
G1	1
G2	1
G3	1
G4	3
G5	4
Celkem	10

Absolutní zálohy se budou uchovávat 4, potom se začne přepisovat od nejstarších.
Přírustkových záloh se bude uchovávat 5 v případě provedení zálohy 1 x týdně, 10 v případě provedení zálohy 2 x týdně.

Instalace nového počítače

Datum _____

Umístění _____ *Typ počítače* _____

Jméno počítače _____ _____

Síťová karta _____ *Sériové číslo* _____

Grafická karta _____ *Dodavatel* _____

Zvuková karta _____ *Číslo faktury* _____

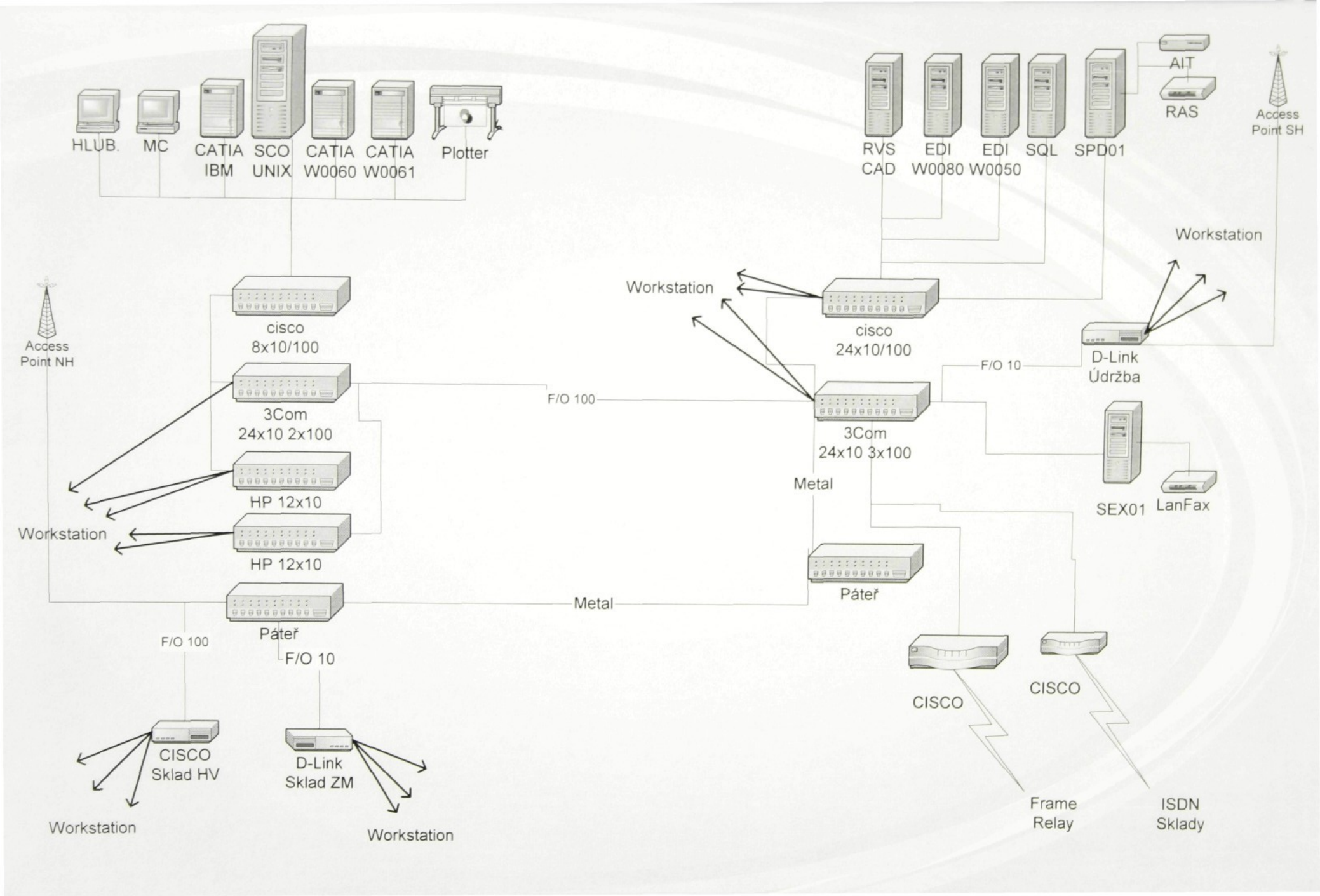
Standard

- Windows .....
- Síť
- Klávesnice
- Service pack
- Grafika
- Audio
- Zvětšit registr
- Povolit změnu času
- MS Office standard
- Service Packy
- Rozchodit Excel
- Outlook .....
- Internet Explorer 5.x
- Zkrátit pauzu při startu
- Acrobat Reader 4.0
- SAP
  - SAPclient
  - SAPlgpad
  - Zástupce na plochu
  - RFC
  - Proměnná
  - SAPlogon menu
- Ikony jakost
- Antivir
- AutoUpdate+Schedule
- Access Runtime
- MDAC
- WinZip
- Tiskárny
  - 850c
  - 1150c
  - Plotter
- NumLock
- Natáhnout disk
- Myšoidní ovladače

Rozšíření

- GED Slovníky
- LanFax
- Sony Route Planner
- Hotel Guide
- AutoCAD
- Publisher
- Docházka
- MS Project

Poznámka:


HLUB.
MC
CATIA IBM
SCO UNIX
CATIA W0060
CATIA W0061
Plotter
RVS CAD
EDI W0080
EDI W0050
SQL
SPD01
AIT
RAS
Access Point SH
Workstation
Workstation
cisco 24x10/100
D-Link Údržba
F/O 10
Access Point NH
cisco 8x10/100
3Com 24x10 2x100
F/O 100
3Com 24x10 3x100
HP 12x10
Metal
SEX01
LanFax
Workstation
HP 12x10
Páteř
Metal
Páteř
F/O 100
F/O 10
CISCO
CISCO
CISCO Sklad HV
D-Link Sklad ZM
Workstation
Workstation
Frame Relay
ISDN Sklady

Prohlášení

Byl jsem seznámen s ustanoveními Pracovního řádu vztahujícími se k bezpečnosti sítě. Podpisem se zavazuji k jejich dodržování, k nezneužívání svěřených prostředků k mimopracovním účelům a k zajištění, že těchto prostředků nezneužije jiná osoba.

V Chrastavě 2.6.2000

.....

Schválil Ing. Jiří Rydval