Univerzita Pardubice

Fakulta ekonomicko-správní

Bezpečný přenos dat ve firmě a ve státní správě

Věra Džbánková, DiS.

Bakalářská práce
2014

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Věra Džbánková, DiS.**
Osobní číslo:	**E12921**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Bezpečný přenos dat ve firmě a ve státní správě**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Z á s a d y p r o v y p r a c o v á n í :

Cílem práce je zjistit, jak lze dnes dostatečně bezpečným způsobem přenášet data v rámci firmy, mezi firmami a při komunikaci se státní správou. Zaměřit se na různé úrovně utajovaných skutečností. Možnosti napadení přenášených dat a vhodná obrana proti takovýmto útokům. Pořizovací a provozní náklady na zvolená řešení. Sestavení několika případových studií pro různé typy firem.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

1. **SOSINSKY, Barrie A. Mistrovství - počítačové sítě: [vše, co potřebujete vědět o správě sítí]. Vyd. 1. Brno: Computer Press, 2010, 840 s. ISBN 978-802-5133-637.**
2. **KÁLLAY, Fedor. Počítačové sítě LAN/MAN/WAN a jejich aplikace. 2. aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1.**
3. **LAPÁČEK, Jiří. Jak na datovou schránku a elektronickou komunikaci s úřady. 1. vyd. Brno: Computer Press, 2012, 197 s. ISBN 978-80-251-3680-5.**

Vedoucí bakalářské práce: **Ing. Martin Novák**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. října 2014**

Termín odevzdání bakalářské práce: **30. dubna 2015**

L.S.

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

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 1. října 2014

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 30. 6. 2015 Věra Džbánková, DiS.

PODĚKOVÁNÍ:

Tímto bych ráda poděkovala svému vedoucímu práce inženýru Martinu Novákovi za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

Také bych ráda poděkovala mému kamarádovi a také příteli, bez nich by tato práce nevznikla.

ANOTACE

Tato práce bude sloužit pro pochopení toho, jak mají jednotlivé firmy zabezpečit svůj informační systém. Tudíž bude sloužit studentům jako návod k tomu jak firmu správně a účelně zabezpečit. V této práci studenti zjistí, že před vlastním návrhem nějakého zabezpečení je důležité vědět, co firma dělá, jaký má informační systém, jaká ji hrozí rizika při přenosu a ukládání dat a především jaké informace jsou pro ni prioritní k utajení. Velkou roli zde také hrají pořizovací a provozní náklady na zvolená řešení zabezpečení informačního systému.

KLÍČOVÁ SLOVA

Počítačové sítě, ukládání dat, datové schránky, hackerské útoky, klasifikace informací, případové studie

TITLE

Secure data transfer in a company and in the state administration

ANNOTATION

This work will serve for understanding how individual companies have to secure their information systems. Therefore it will serve students as a guide how to ensure properly and efficiently the company. In this work the students will find that prior to any draft of security it is important to know what the company does, what the information system is, what risks threaten during transmission and storage of data, and especially what information is the priority for its classification. A major role is also played by acquisition and operating costs of the chosen security solution for information system.

KEYWORDS

Computer networks, data storage, data boxes, hacker attacks, classification of information, case studies

OBSAH

SEZNAM TABULEK

SEZNAM ILUSTRACÍ

SEZNAM ZKRATEK A ZNAČEK

LAN	Lokální datová síť (Local Area Network)
MAN	Městská datová síť (Metropolitan Area Network)
WAN	Datová síť pro největší vzdálenosti (Wide Area Network)
NOS	Síťový operační systém (Network Operating Systém)
IS	Informační systém
PC	Osobní počítač (Personal Computer)
EID	Elektronická výměna dokumentů (Elektronic Data Interchange).
ERP	Plánování podnikových zdrojů (Enterprise Resource Plannig System)
RAID	Technologie diskových polí (Redundant Array of Inexpensive Disks)
OVM	Orgán veřejné moci
PO	Právnická osoba
PFO	Podnikající fyzická osoba
FO	Fyzická osoba
EPO	Elektronické podání pro finanční správu
XML	Rozšiřitelný značkovací jazyk (Extensible Markup Language)
ICMP	Protokol ze sady protokolů internetu (Internet Control Message Protocol)
DoS	Odepření služby (Denial of Service)
DNS	Hierarchický systém doménových jmen (Domain Name System)
DDoS	Distribuované útoky DoS (Distributed Dos)
MITM	Muž uprostřed (Man-In-The-Middle)
CD	Kompaktní disk (Digital Disc)
DVD	Digitální víceúčelový disk (Digital Versatile Disc)
USB flash	Paměťové přenosové médium (Universal Serial Bus)
IDS	Systému detekce průniků (Instrusion Detection Systems)

SSL	Protokol pro šifrování komunikace (Secure Socket Layer)
ISO	Mezinárodní organizace pro normalizaci (International Organization for Standardization)
IEC	Mezinárodní elektrotechnická komise (International Electrotechnical Commission)
NDA	Dohoda o mlčenlivosti (Non Disclosure Agreement)
PHP	Skriptovací programovací jazyk (Hypertext Prerocessor)
MySQL	Databázový systém
XSS	Cross site scripting
HTML	Značkovací jazyk pro tvorbu webových stránek (Hypertext Markup Language)
API	Rozhraní pro programování aplikací (Application Programming Interface)

ÚVOD

V této bakalářské práci se zaměřím na bezpečný přenos dat ve firmě, mezi firmami a při komunikaci se státní správou. Pokusím se vysvětlit, jak lze dnes dostatečně bezpečně přenášet data a jaké jsou možnosti napadení těchto dat. V tomto směru je také důležitý způsob ukládání dat a vytváření jejich záloh, pro případ znehodnocení nebo ztráty dat. Také se zaměříme na různé druhy utajovaných skutečností ať už ve smyslu zákona o ochraně osobních údajů, ale také v tom smyslu jak si jednotlivé firmy svá data klasifikují, podle toho které jsou pro ně důležité utajit a které jsou vlastně určeny už ze své podstaty ke zveřejnění.

V závěru práce uvedu dvě případové studie, které se týkají různých druhů fiktivních firem. Fiktivní firmy budou v této práci využity proto, že reálné firmy nechtějí a vlastně ani nemohou poskytovat informace o tom, jak zabezpečují svá data. Toto opatření je nutné proto, aby firemní zabezpečení vůbec fungovalo. Na těchto firmách budu demonstrovat postup výběru zabezpečení firemních informačních systémů. Každá firma potřebuje jiné zabezpečení a jeho výběr závisí především na činnosti firmy, jaký informační systém firma používá, jaká jí hrozí rizika při přenosu a uchovávání dat, jaké informace jsou pro firmu prioritní a v neposlední řadě tento výběr závisí na pořizovacích a provozních nákladech na zvolená řešení ochrany dat.

Cílem práce tedy je poukázat na to, že každá firma je vždy jiná a potřebuje jiné řešení ochrany dat. Vždy se musí uvažovat individuálně a pro každou firmu určit to řešení, které je pro firmu adekvátní z hlediska stupně a kvality ochrany a samozřejmě tomu odpovídající ceny.

1 PŘENOS A UKLÁDÁNÍ DAT V RÁMCI FIRMY

V současnosti je charakteristické pronikání počítačové techniky do všech oblastí našeho života. Jedním z důvodů je neomezená možnost agregace, uschovávání a využívání informací. Spojování počítačů do počítačových sítí je dnes nevyhnutelným trendem a nutnou podmínkou distribuovaného přístupu k informačním zdrojům a využívání síťových aplikací. [1]

1.1 Klasifikace počítačových sítí

Počítačové sítě se třídí podle různých hledisek. Pro potřeby této bakalářské práce postačí hledisko, které třídí sítě podle rozlehlosti nebo územního dosahu.

Podle rozlehlosti nebo územního dosahu třídíme sítě na:

- **LAN** (Local Area Network) jsou lokální datové sítě pokrývající území dané lokality. Jejich dosah obvykle nepřesahuje 10 km (např. budova, závod apod.) [1]
- **MAN** (Metropolitan Area Network) jsou městské datové sítě pokrývající území města, tedy řádově desítky km, skládající se obvykle ze vzdálených sítí LAN. [1]
- **WAN** (Wide Area Network) jsou datové sítě pro největší vzdálenosti. Nejsou svým rozsahem omezené, přičemž pokrývají území států i celých kontinentů.[1]

1.2 Používané typy uzlů v počítačových sítích

Počítačová síť vytváří prostředí pro vzájemné propojování jednotlivých počítačů sítě. Uzly počítačové sítě můžeme rozlišovat podle funkce, kterou vykonávají, podle jejich využití v rámci sítě a podle vzájemné závislosti. [1]

Každý počítač zapojený do sítě může být:

Pracovní stanice (Work Station) – je to uzel využívající služby. [1]

Je to koncový uzel informačního systému využívaný uživatelem. Zde běží procesy klientů zpřístupňující služby vybraných serverů. Pracovní stanice se používá k vysílání, příjmu, prezentaci dat a lokálnímu zpracování úloh informačních systémů. [1]

Server (Server) – je to uzel poskytující služby v rámci informačního systému. [1]

Server poskytuje svoje služby pracovním stanicím sítě. Funkci serveru určuje speciální programové vybavení, označované jako síťový operační systém NOS (Network Operating System). NOS zabezpečuje vlastní implementaci služeb serverů, komunikaci pracovních stanic se servery a kontrolu a řízení přístupu klientů k příslušným službám serverů. [1]

1.3 Aplikace počítačových sítí v oblasti informačních systémů

Základní doménou počítačových sítí jsou právě informační systémy podniků, ve kterých počítače a počítačové sítě už tradičně plní funkci komunikačního a zpracovatelského subsystému. Počítačové sítě kromě zabezpečení základní komunikace mezi komponentami informačního systému nabízí i celou řadu podpůrných funkcí a služeb využívaných v rámci celého informačního systému. Uplatňují se nejen při budování místních informačních systémů (sítě LAN), ale přímo podporují tvorbu distribuovaných informačních systémů s neomezeným dosahem a globální působností (sítě WAN). [1]

1.3.1 Počítačové sítě jsou obvykle využívány jako:

Integrující prostředí pro vzájemné propojení heterogenních prvků informačního systému, kdy počítačová síť podporuje heterogenní prostředky výpočetní techniky, např. počítače různých tříd (mainframe, mini počítače, PC), terminály nebo periferní zařízení (disková pole, tiskárny). Toto prostředí umožňuje vzájemnou komunikaci a spolupráci různých počítačových systémů v rámci informačního systému.[1]

Informační systém s integrovanými službami, v němž počítačová síť poskytuje informačnímu systému svoje vnitřní aplikační služby. Počítačová síť obvykle pro informační systém zabezpečuje služby diferencovaného přístupu k datům a aplikacím informačního systému, služby zabezpečení dat a ověřování přístupu ke zdrojům sítě, podpůrné služby pro distribuované zpracování apod. [1]

1.3.2 Nejčastěji používané služby

K nejčastěji používaným službám počítačových sítí v informačních systémech patří následující elementární služby:

Souběžné sdílení technických prostředků v síti (tiskárny, disky, modemy), při němž je dané technické zařízení přístupné v rámci celé sítě více uživatelům. [1]

Souběžné sdílení společných dat v síti. Jedná se například o přístup k velkým objemům společných dat v souborech a databázích informačních systémů, kdy počítačová síť zabezpečuje souběžné zpracování dat a synchronizaci přístupu k nim ze strany uživatelů. [1]

Elektronická pošta (E-mail) je používána velmi často k off-line komunikaci uživatelů sítě prostřednictvím elektronických poštovních schránek.[1]

Elektronická výměna dokumentů EID (Elektronic Data Interchange). Vyvinuta jako náhrada klasického systému obchodování prostřednictvím výměny dokumentu v papírové

formě (objednávky, faktury, ceníky). Služba EID je definována jako elektronická výměna strukturovaných standardních zpráv mezi aplikacemi dvou nezávislých subjektů. [1]

Adresářové služby. V globálních sítích existuje mechanismus jednotného přístupu k informacím z libovolného místa sítě, který je platný pro celou síť. Proto je v síti třeba definovat centrální databázi, která by spravovala všechny potřebné informace globální sítě a byla dostupná z libovolného místa sítě. Globální databáze slouží pro uživatele, pro aplikační služby a zařízení celé sítě. Může obsahovat v jednotné formě nejrůznorodější informace: od uživatelských účtů, hesel a konfiguračních dat sítě, až po informace používané aplikačními službami, například adresáře uživatelů elektronické pošty nebo seznamy klientů EDI. [1]

Monitorování a vzdálené řízení (Remote Control) jiných stanic a prvků sítě. Často se používá při dálkovém přístupu do sítě, přímém ovládání a monitorování vzdálených prvků informačních systémů. [1]

Interaktivní video v dnešní době moderní služba zabezpečující přenos obrazu a zvuku v reálném čase (on-line) mezi uzly informačního systému. Vyznačuje se vysokými nároky na šířku přenosového pásma sítě a požadavky na konstantní zpoždění přenosu. [1]

1.4 Způsob přenosu dat

Firma si tedy vytvoří informační systém propojením pracovních stanic (PC, notebooků, tabletů,…) a serverů. Přímo v budově firmy se většinou jedná o místní síť LAN. Firma ale může mít různé pobočky ve městě, potom se jedná o síť MAN. Také se může jednat o mezinárodní firmu, potom se jedná o síť WAN. V této bakalářské práci se budu zabývat pouze zabezpečením firem sídlících v jedné budově, takže všechny firmy v případových studiích budou zapojeny do sítě LAN, která ale ovšem může být zapojena do MAN nebo WAN, ale jejich zabezpečením se již zabývat nebudu.

Firmy také samozřejmě využívají jednotlivé služby, které jsou popsány výše. Záleží, ale také na tom jakým způsobem tyto služby využívá. Může využívat propojení jednotlivých pracovních stanic a serveru s určitými možnostmi sdílení dat. Tady činí největší problém správné určení toho, kdo ke kterým datům bude mít přístup a jak s nimi může nakládat. Tohle všechno si musí firma rozmyslet a správně nakonfigurovat, jinak může nastat bezpečnostní ohrožení ze strany zaměstnanců.

1.5 ERP systém

Počítačové sítě poskytují velké množství služeb a v podnicích je nutné tyto služby nějakým způsobem koordinovat. To zajišťuje ERP systém (Enterprise Resource Plannig System) neboli plánování podnikových zdrojů.

Hlavními vlastnostmi ERP jsou schopnost automatizovat a integrovat základní podnikové procesy, sdílet společná data a zpracovávat je v rámci celého podniku, vytvářet a zpřístupňovat informace v reálném čase. ERP se snaží sloučit různé oblasti činností a funkcí napříč celým podnikem až k jednotlivým programovým úlohám sloužícím různým potřebám organizačních složek podniku. [2]

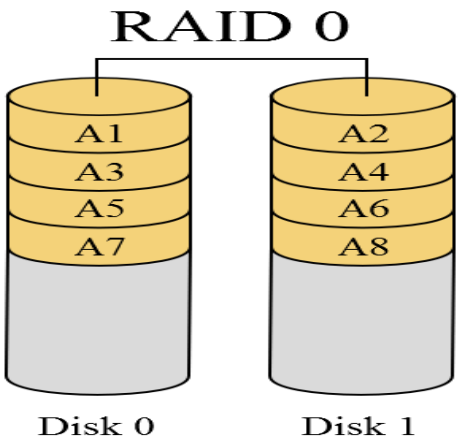
1.6 Bezpečné ukládání dat

Firma má propojené počítače např. v LAN, používá různé služby a například i ERP systém a má také server, na který ukládá data. Nestačí, však data jenom ukládat musí se nějak zabezpečit, že nedojde k jejich ztracení nebo znehodnocení. Samozřejmostí současné doby je pravidelná záloha dat, může se však také stát, že selže pevný disk v serveru a data, která se od poslední zálohy vytvořila, jsou nenávratně ztracena. K předcházení tomuto problému bylo vytvořeno RAID (Redundant Array of Inexpensive Disks).

RAID je spojení dvou a více pevných disků v jeden či více logických, a to na hardwarové úrovni. Typů RAID polí je vícero právě podle počtu pevných disků a podle toho, zda chcete mít data zálohovaná (zrcadlená – mirroring) nebo jestli chcete zvýšit výkon disku tzv. stripingem (prokládáním), anebo zkombinovat obojí. [3]

1.6.1 RAID 0

Tomuto poli se někdy říká STRIP nebo STRIPPING (strip = proužek), protože řadič zapisuje data střídavě na jednotlivé disky. RAID 0 se vytvoří spojením 2 a více disků do série. Výsledná kapacita disku je součtem velikostí jednotlivých disků. Protože řadič při čtení a zápisu přistupuje střídavě k jednotlivým diskům, je výsledná rychlost dána (téměř) násobkem rychlosti počtu disků. Daní za rychlost je nižší bezpečnost - v případě ztráty jednoho disku přicházíme o všechna data bez možnosti obnovení. Tento typ polí se používá tam, kde chceme mít maximální výkon při zpracování velkých souborů, například při zpracování videa. Nepoužívá se na ukládání důležitých dat. [4]

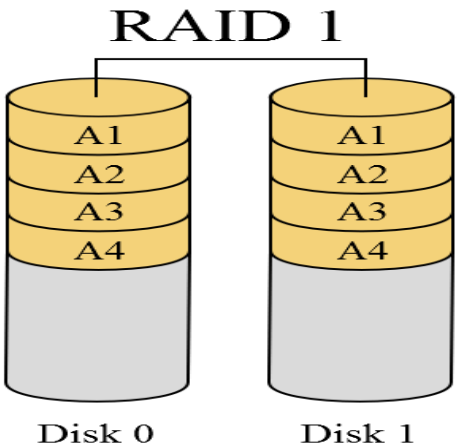


Obrázek 1: RAID 0

Zdroj:[3]

1.6.2 RAID 1

Tomuto poli se také říká MIRROR nebo MIRORRING (mirror = zrcadlo), protože dochází k zrcadlení dat. Zapojením disků do RAID 1 zvyšujeme bezpečnost, řadič data zapisuje současně na dva a více disků. Výsledná kapacita a rychlost se nezvyšuje, je dána kapacitou a rychlostí jednoho disku. Výsledná bezpečnost roste podle počtu použitých disků. Tento typ polí se používá tam, kde nám jde o bezpečnost dat - porucha disku neovlivňuje dostupnost dat, dokud nám zůstává alespoň jeden disk. Levné řešení pro zvýšení bezpečnosti dat. [4]



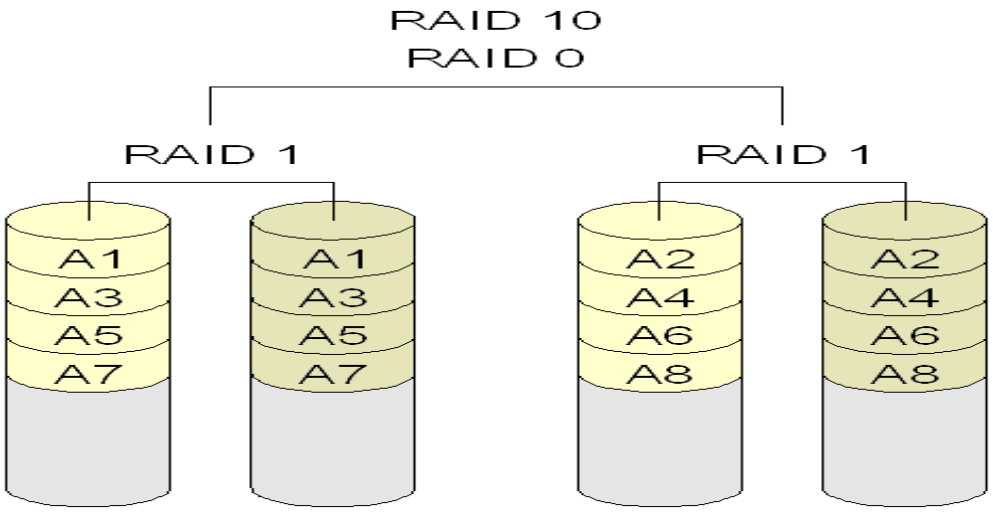
Obrázek 2: RAID 1

Zdroj:[3]

1.6.3 RAID 1+0

Tento typ zapojení disků je kombinací RAID 1 a RAID 0, někdy se mu říká RAID 10. Principem je zapojení skupin zrcadlených disků RAID 1 sériově do pole RAID 0. Získáváme vyšší kapacitu disku a vyšší rychlost (násobek počtu skupin) a současně se zvyšuje i

bezpečnost dat, protože máme disky zapojeny v jednotlivých skupinách zrcadleně. Tohle pole je sice finančně nejvíc náročné (počet disků), ale dosahujeme nejvyšší výkon (vyvážené čtení a zápis) při zachování bezpečnosti. Pole je bezpečné, pokud v každé skupině zůstane minimálně jeden disk. [4]

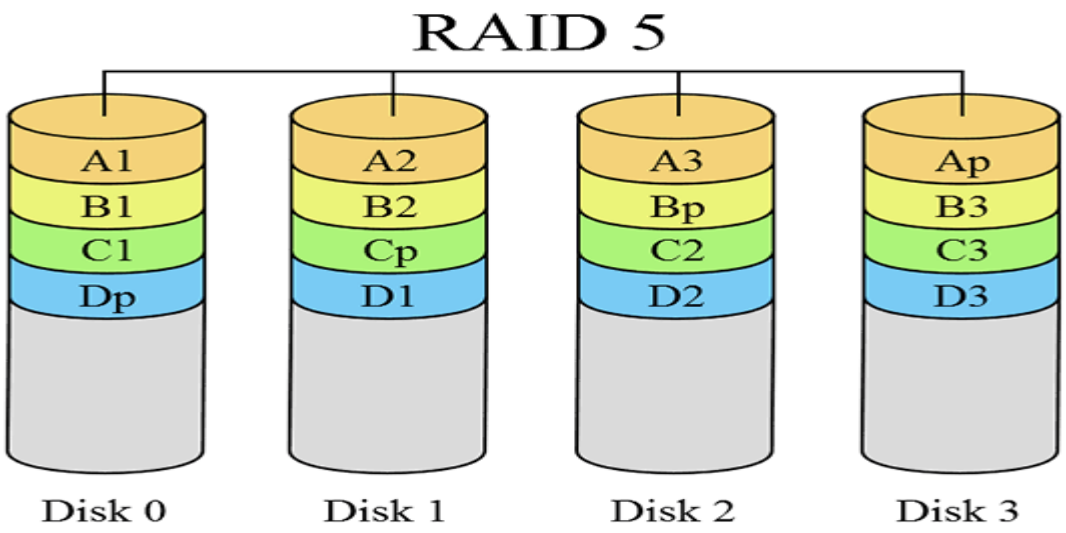


Obrázek 3: RAID 1+0

Zdroj:[3]

1.6.4 RAID 5

Tento typ diskového pole vytvoříme minimálně ze tří fyzických disků. Počet použitých disků si označíme, jako N. Řadič zapisuje střídavě na N-1 disků a na poslední disk (redundantní) zapisuje tzv. kontrolní součet (paritu). Pomocí tohoto kontrolního součtu je řadič schopný zrekonstruovat data na jakémkoliv disku, který by selhal. Použitím tohoto typu pole získáme vyšší kapacitu, která je dána součtem velikostí N-1 použitých disků. Získáme vyšší rychlost čtení, protože řadič čte z několika disků současně. Rychlost zápisu se mírně zpomalí, protože řadič musí dopočítávat a zapisovat kontrolní součet na redundantní disk. Při poruše jednoho disku (i disku s kontrolními součty) zůstává diskové pole dále funkční. Je to velmi rozšířené použití RAID u firemních serverů jako kompromis mezi cenou, bezpečností a zvýšením výkonu ve srovnání s jednotlivými disky. [4]



Obrázek 4: RAID 5

Zdroj:[3]

Právě bylo popsáno, jak se přenášejí a ukládají data ve firmě. Před tím, než vůbec začne uvažovat o zabezpečení firemního informačního systému je nutné tyto informace znát.

Dále je důležité vědět, jak komunikují firmy mezi sebou a jak komunikují se státní správou, protože to také sebou nese určitá bezpečnostní rizika. Komunikace mezi firmami a mezi firmou a státní správou budou popsány v následujících dvou kapitolách.

2 PŘENOS DAT MEZI FIRMAMI

V současné době komunikují firmy mezi sebou téměř výhradně elektronicky. Firmy mohou komunikovat pomocí EID (Elektronická výměna dokumentů), nebo pomocí e-mailů. K tomu, aby byla komunikace pomocí e-mailů důvěryhodná, se využívají elektronické podpisy.

2.1.1 Zákon o elektronickém podpisu č. 227/2000 Sb.

Pro účely tohoto zákona se rozumí elektronickým podpisem údaje v elektronické podobě, které jsou připojené k datové zprávě nebo jsou s ní logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k datové zprávě. [5]

Pro účely tohoto zákona se rozumí zaručeným elektronickým podpisem elektronický podpis, který splňuje následující požadavky:

- je jednoznačně spojen s podepisující osobou,
- umožňuje identifikaci podepisující osoby ve vztahu k datové zprávě,
- byl vytvořen a připojen k datové zprávě pomocí prostředků, které podepisující osoba může udržet pod svou výhradní kontrolou,
- je k datové zprávě, ke které se vztahuje, připojen takovým způsobem, že je možno zjistit jakoukoliv následnou změnu dat. [5]

2.1.2 Způsob komunikace mezi firmami pomocí e-mailů

Firmy, které chtějí s ostatními firmami komunikovat pomocí e-mailů, si tedy pořídí elektronický podpis od uznávané certifikační autority, jejichž seznam je pravidelně zveřejňován a aktualizován. Jsou zde například autority Verisign, Thawte, GeoTrust, GoDaddy, Comodo a také české certifikační autority PostSignum QCA České pošty a 1. CA (První certifikační autorita). [6]

Pokud při komunikaci tento elektronický podpis připojí k datové zprávě, může si druhá firma být jistá, že komunikuje s tím, s kým si myslí (že to není nějaký útočník) a že data, která firma posílá, nebyla během přenosu nějak pozměněna.

3 PŘENOS DAT PŘI KOMUNIKACI SE STÁTNÍ SPRÁVOU

Firmy komunikující se státní správou lze rozdělit do dvou skupin: ty co datové schránky mají a ty co datové schránky nemají.

3.1 Firmy, které mají datové schránky

Datové schránky slouží ke komunikaci podnikatelů, fyzických osob prostě prakticky kohokoliv, kdo si schránku zřídí s orgány veřejné moci.

Definice datové schránky ze zákona je následující:

Datová schránka je elektronické úložiště, které je určeno k doručování orgány veřejné moci a k provádění úkonů vůči orgánům veřejné moci. [7]

Datová schránka je elektronické úložiště, které slouží k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.[7]

Datové schránky zřizuje a spravuje Ministerstvo vnitra. Provozovatelem Informačního systému datových schránek je držitel poštovní licence. [7]

Typy datových schránek

Způsob, respektive proces zřízení datové schránky se liší podle typu subjektu, pro který má být datová schránka zřízena. Typ subjektu určuje, zda se jedná o datovou schránku zřizovanou ze zákona, tedy automaticky, nebo o datovou schránku zřizovanou na žádost.

Zřizují se čtyři základní druhy datových schránek:

- Datová schránka orgánů veřejné moci (OVM),
- datová schránka pro právnické osoby (PO),
- datová schránka pro fyzické osoby podnikající (PFO),
- datová schránka pro fyzické osoby (FO). [7]

Datové schránky zřizované ze zákona jsou pro tyto typy subjektů: orgán veřejné moci, notář, exekutor, právnická osoba zapsaná v obchodním rejstříku, právnická osoba zřízená zákonem, advokát, daňový poradce a insolvenční správce. [8]

Datovou schránku na žádost si může pořídit prakticky kdokoliv tedy fyzická osoba, podnikající fyzická osoba, právnická osoba nezapsaná v obchodním rejstříku i zahraniční subjekty. [8]

Integrovaný systém datových schránek doručuje informace ze schránky odesílatele do schránky příjemce ve formě datových zpráv. Odesílatelem i příjemcem může být obecně fyzická osoba, podnikající fyzická osoba, právnická osoba a orgán veřejné moci. Jestliže tedy bude chtít běžný občan podat daňové přiznání elektronickou cestou, bude se jednat o komunikaci z datové schránky fyzické osoby do datové schránky orgánu veřejné moci. [7]

Cílem zavedení systému datových schránek je tedy umožnit vést korespondenci s orgány státní moci v elektronické podobě. Tento systém plně nahrazuje klasický způsob doručování zásilek v listinné podobě. Je nutné si uvědomit, že jakmile si založíte datovou schránu, bude vám korespondence od orgánů veřejné moci doručována elektronicky. Z toho vyplývají i určité povinnosti, jako je pravidelně kontrolovat obsah datové schránky, neboť datové zprávy do ní dodané mají stejnou právní platnost jako ty, pro které si musíte dojít na poštu. Navíc zde je nutno mít stále na paměti, že zde nelze zahodit oznámení o doručení zásilky do koše a myslet si, že když úřední zprávu nepřevezmete, jako by neexistovala. Před „elektronickým úředním šimlem“ není úniku a většina datových zpráv je považována automaticky za doručené po deseti dnech od vložení do vaší schránky (takzvané doručení fikcí), ať je vaše odezva jakákoliv – tedy i když svou datovou schránku budete ignorovat.[7]

3.2 Firmy, které nemají datové schránky

Firmy, které si nemusí na základě zákona zřídit datovou schránku a neučinili tak, mají tři možnosti, jak komunikovat s úřady:

- osobně se na úřad dostavit,
- podání přes EPO (tak lze komunikovat pouze s daňovou správou),
- zaslání e-mailem.

3.2.1 Podání přes EPO

Finanční správa v souladu s platnou legislativou připravila pro veřejnost možnost podávat daňová podání, přiznání, hlášení a další písemnosti v elektronické podobě. K tomuto účelu souší aplikace „Elektronická podání pro finanční správu“ (EPO). [9]

Použití aplikace EPO nutně neznamená, že poplatník zde vyplněné daňové přiznání podá na finanční úřad elektronicky. Může, ale nemusí. Jako výstup má možnost zvolit následující varianty:

- odeslání podání elektronicky s použitím uznávaného elektronického podpisu,

- odeslání podání elektronicky bez použití uznávaného elektronického podpisu, s nutností doručení z EPO vytištěného Potvrzení z podání, tzv. E-tiskopisu, do 5 kalendářních dnů na finanční úřad,
- uložení podání k odeslání do datové schránky poplatníka a následné odeslání ve formátu XML do datové schránky správce daně,
- vytištění přiznání (případně uložení) a následné doručení na finanční úřad v písemné podobě s vlastnoručním podpisem (černobílý výstup není na závadu). [10]

3.2.2 Zaslání e-mailem

Zaslání přes e-mail může v některých podatelnách fungovat bez zaručeného elektronického podpisu, ale pouze pokud se jedná o žádosti o poskytnutí informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím (§14), ve znění pozdějších předpisů a různá oznámení a podněty občanů. [11]

Pokud se jedná o nějaké oficiální podání a ne jenom žádost o poskytnutí informace, musí firma použít zaručený elektronický podpis (zaručený elektronický podpis vysvětlen v kapitole 4.4.1 SSL protokol).

Nyní máme informace o tom, jak se přenáší data ve firmě, mezi firmami a při komunikaci se státní správou. Dále je důležité vědět o bezpečnosti dat, a jaká rizika nám při přenosu těchto dat hrozí.

4 HACKERSKÉ ÚTOKY A OBRANA PROTI NIM

Všechny sítě jsou v každém okamžiku ohroženy stále propracovanějšími a neustále se vyvíjejícími útoky. Snad každý den se dozvídáme o nejnovějších virech, trojských koních a červech. [12]

Na zabezpečení sítě neexistuje jednoduchý návod. Každý bezpečnostní systém může být prolomen, pokud ne zvenčí, tak zcela jistě zevnitř. Nejlepší metodou zabezpečení je proto zavedení několika bezpečnostních vrstev, takže pokud chce útočních získat neoprávněný přístup musí postupně prolomit dvě nebo více bariér. Další dvě nedocenitelné metody spočívají v pravidelných změnách hesel a bezpečném oddělení různých částí sítě. [12]

4.1 Bezpečnost dat

Bezpečnost dat lze definovat jako zajištěnost proti hrozbám, minimalizaci rizik a komplex administrativních, technických, logických a fyzických opatření pro prevenci a detekci neautorizovaného využití dat. I z tohoto důvodu je nutné si vymezit rámec, který má na bezpečnost dat zásadní vliv, kde bezpečnost v informačním prostředí lze zjednodušeně rozdělit na následující domény:

- **komunikační bezpečnost** - ochranu přenášených dat a zamezování nežádoucího datového provozu,
- **fyzickou bezpečnost** - ochranu před přírodními hrozbami, jako je například požár, a fyzickými útočníky, například zábranou, detektory pohybu atp.,
- **personální bezpečnost** - ochranu před vnitřními útočníky již při náboru, během jejich práce i po skončení pracovního poměru,
- **bezpečnost informačních systémů a technologií** - ochranu infrastruktury informačních systémů uchovávající data v elektronické podobě proti relevantním hrozbám typu neautorizovaný přístup, maligní software (viry, trojské koně), výpadky systému apod. [13]

Základní bezpečnostní atributy v těchto doménách jsou:

- **důvěrnost** - prevence neautorizovaného vyzrazení dat,
- **integrita** - prevence neautorizované úpravy dat,
- **dostupnost** - prevence ztráty přístupu k datům. [13]

4.2 Zranitelná místa v síti

Zranitelné místo nebo zjednodušené zranitelnost (vulnerability) je slabé místo, které může být zneužito k neoprávněnému přístupu do systému. Existuje ohromné množství způsobů, jak lze systémy kompromitovat: uhodnutím hesla, prostřednictvím viru nebo trojského koně, díky softwarové chybě, spustitelnému programu nebo skriptu běžícímu uvnitř systému nebo vložením kódu s pomocí neošetřeného vstupu. Pokud se zranitelnost stane veřejně známou a začne se používat na mnoha místech k útokům na podobné systémy, stane se z ní takzvané zneužití. [12]

Každý software má chyby, které lze využívat. Zranitelná místa odstraňují firmy pravidelnými aktualizacemi ihned, jakmile se o nich dozví. Po zveřejnění aktualizace ji obvykle ihned začnou ověřovat lidé, kteří mají zájem na útoky prostřednictvím příslušné zranitelnosti. Může se pak rychle objevit automatizovaný útok, který vadu zneužívá, a často bývá velmi účinný, protože aktualizace systémů zabere nějaký čas. Útoky tohoto typu se nazývají zneužitím prvního dne (Zero Day Exploits). [12]

Praxí ověřené doporučení říká: vyhněte se útokům prvního dne včasnou aktualizací všech systémů ihned, jakmile jsou opravy zranitelných míst k dispozici. Mnoho systémových správců se této rady obává, protože rychlá aplikace neověřených záplat s sebou může nést své vlastní problémy. [12]

Odhalení síťových zranitelností lze zajistit také pravidelnými prověrkami sítě s pomocí nástrojů pro analýzu rizik, kterým se někdy říká skenery zranitelností (vulnerability scanner). Jejich funkce spočívá ve zjištění otevřených portů v oblasti sítě dané vstupními IP adresami, sestavením seznamu operačních systémů a aplikací, které v této oblasti běží, a nalezení známých zranitelností. Tímto způsobem pracují skenery portů, síťové skenery a skenery webových serverů. Po skončení průzkumu sítě skener sestaví mapu sítě a vytvoří výstupní zprávu. Jednotlivým zranitelnostem se také dají přiřadit váhy, aby měl administrátor přehled, kterým aktivitám vedoucím k nápravě zabezpečení sítě by měl dát přednost. [12]

Zranitelná místa vedou k následujícím bezpečnostním problémům:

- Útočník může spustit příkaz tak, jako kdyby se jednalo o jiného uživatele
- Útočník získá přístup k datům, k nimž nemá příslušná oprávnění
- Útočník se může vydávat za někoho jiného
- Útočník je schopen vyvolat situace, při kterých je služba ostatním uživatelům nedostupná. [12]

4.3 Slabá místa k napadení

Bezpečnostní síť je nejčastěji prolomena z externí sítě směrem dovnitř. Útoky se typicky soustřeďují na zranitelná místa v softwaru i hardwaru. Zneužití takových zranitelností, která umožňují dostat se až do vnitřní sítě, jsou často nejefektivnější, protože se mohou odehrávat zcela nepozorovaně. [12]

Mezi nejčastější slabá místa, která útočníci napadají, patří:

- **Zvenku: dostupnost systému** – počítačové prvky v síti je možné přetížit všesměrovým vysíláním ICMP paketů, jejichž výsledkem je záplava odpovědí na systém oběti (takzvaný „smurf" útok).
- **Zvenku: odepření služby (DoS, Denial of Service)** – při tomto typu útoky je služba zahlcena požadavky útočníka. Obvyklým příkladem útoku je zahlcení názvových DNS serverů; pokud je úspěšný není možné překládat adresy některých systémů na Internetu nebo v interní síti, následkem čehož jsou pro oprávněné uživatele nedostupné.
- **Zvenku: Distribuované útoky DoS (DDoS)** – provádí je koordinovaně větší množství napadených systémů, které si útočníci ponechávají pro podobná využití ve spícím stavu. Při útoku se na povel útočníka všechny najednou probudí a vzniká z nich takzvaný botnet (ze sousloví robot network, tedy robotická síť).
- **Zvenku/zevnitř: autentizace** – při podvržení autentizacích údajů se útočník začne vydávat za jiného uživatele.
- **Data při přenosu** – datový komunikační provoz může být v průběhu přenosu zachycen a pozměněn, a pak odeslán na původní místo určení. Tento typ útoku bývá označování zkratkou MITM (Man-In-The-Middle, tedy muž uprostřed). Data lze také pouze odposlouchávat.
- **Zevnitř: červi, trojské koně a další zadní vrátka** – poskytují útočníkovi možnost ovládat systémy uvnitř sítě a získat tak spící agenty pro další útoky. Zadní vrátka mívají formu spustitelných programů nebo algoritmů, které jsou schopné obcházet autentizaci v síti, provádět škodlivé akce a přitom zůstat neodhalené.
- **Přímý přístup zevnitř** – útoky mohou být také neseny na médiích, jako jsou optické CD nebo DVD disky, USB flash disky, přenosné pevné disky a další. [12]

4.3.1 Rootkit

Jednou z forem nástrojů pro zadní vrátka jsou takzvané rootkity Je počítačový program (nebo skupina několika programů), který zásadním způsobem mění chod operačního systému a který slouží ke skrývání. Jedná se o software, který se umí šikovně schovat v systému v podobě ovladače na velmi nízké úrovni nebo modulu v jádře operačního systému. Proto velmi snadno unikají detekci, neobjevují se ve výpisech souborového systému a v seznamu běžících procesů se mohou tvářit jako zcela obyčejné programy. Může skrývat sebe sama nebo další aplikace např. viry, sledovací programy, programy pro vzdálenou správu – ty mohou nadále existovat na počítači a dále škodit aniž o tom koncový uživatel ví. [12][14]

4.3.2 Trojský kůň

Zřejmě nejjednodušším druhem škodlivého programu je trojský kůň. Takový program se snaží uživatele něčím zaujmout a vytvářet dojem užitečnosti – aby uživatel neodolal a spustil jej na svém počítači. Jeho vedlejší úlohu jsou však činnosti, o nichž uživatel netuší a mohou být velmi nepříjemné (mazání souborů, zjišťování hesel apod.). V jiných případech hackeři přidávají k běžným programům nějakou dodatečnou funkčnost (trojského koně) jako kamufláž svých aktivit. Díky tomu pak mohou zpětně vypátrat daný systém a používat jej později (tzv. zadní vrátka, která po instalaci umožní vzdálené řízení počítače). Naštěstí není schopen šířit se samovolně na další počítače. [15][16]

4.3.3 Spyware

Mnohé firmy se zajímají o to, na co se lidé na internetu dívají a co hledají. A obzvláště se zajímají o to, jaké druhy výrobků si lidé kupují. Proto také některé firmy zabývající se koncovým prodejem nabízejí k instalaci malé aplikace, které sbírají informace a zobrazují uživatelům přesně cílenou reklamu. Spyware sbírá informace o uživateli a odesílá je firmám přes internet. [15]

4.3.4 Červ (worm)

Tento termín označuje kód, který se také šíří mezi počítači, ale buď běží pouze v operační paměti, nebo se ukládá na disk do samostatných souborů, jejichž spuštění při startu počítače si zajistí vhodnou modifikací souborů řídících start počítače. Od viru jej odlišuje neschopnost vkládat se do jiných programů. [16]

4.3.5 Viry

Je to kód, který sám sebe replikuje a vkládá do jiných programů. V okamžiku, kdy je infikovaný program spuštěn, dojde také k aktivaci viru. Viry kromě svých schopností šíření také často obsahují kód na destrukci dat uživatele, případně na jejich kompromitaci (např. otevřením zadních vrátek). Tento kód nemusí být spuštěn při každé aktivaci viru, ale třeba pouze k zadanému datu, což umožňuje viru fungovat skrytě, aniž by nějak uživatele upozornil na svoji přítomnost v infikovaném systému. [16]

Druhy virů

Počítačové viry se dělí do několika skupin, podle toho, jaké objekty napadají:

Boot viry

Napadají systémové oblasti disku. Dříve se tyto viry šířily hlavně pomocí disket v počítačích, které měly povoleno zavádění systému z disketové mechaniky a v mechanice byla disketa s boot virem. V současně době jsou spíše hrozbou USB disky, které tak účinně obejdou instalovaný bezpečnostní software na koncovém PC. Viry na USB pro své šíření využívají vlastnost automatického otevření média díky úpravě souboru autorun.inf, který řídí automatické spuštění po vložení USB disku do počítače. Systém Windows ve standardním nastavení automaticky vykoná příkazy popsané v tomto souboru. Tedy ke spuštění viru může dojít už při samotném vložení USB paměti do počítače! Automatické spouštění se týká i jiných médií, jako jsou například CD a DVD disky.[17] [18]

Souborové viry

Napadají pouze soubory. Přesněji řečeno soubory, které obsahují prováděný kód – programy. V napadeném programu přepíší část kódu svým vlastním, nebo vlastní kód k programu připojí a tím změní jeho velikost a chování. [18]

Multipartitní viry

Napadají soubory i systémové oblasti disku. S výhodou kombinují možnosti boot virů i souborových virů. [18]

Makroviry

Napadají datové soubory – dokumenty vytvořené v některých kancelářských aplikacích. Využívají toho, že soubory neobsahují pouze data, ale i makra, která viry využívají ke svému šíření. Jsou napadány především dokumenty MS Office, výjimečně byly zaznamenány i případy dokumentů jiných aplikací. [18]

4.3.6 Přetečení zásobníku (buffer overflow)

Buffer je oblast paměti, která obvykle obsahuje předem definované množství dat. K přetečení bufferu dojde v případě, když se nějaký program pokusí do bufferu vložit data, která jsou větší než samotný buffer. [15]

Když data přesáhnou velikost bufferu, mohou nadbytečná data „přetéct“ do sousední paměťové lokace, čímž se poškodí platnost dat, což může vést ke změně prováděcí toku a instrukcí. Tím se umožňuje do různých spouštěcích míst vkládat různý kód. Tento kód může na systémové úrovni umožnit vzdálený přístup a poskytnout tak neautorizovaný přístup nejenom hackerům, ale i replikujícímu se škodlivému softwaru. [15]

4.3.7 Útoky přes webové stránky

V předchozích letech se tato hrozba týkala především webových serverů poskytujících nelegální software (warez) nebo pornografický obsah. Návštěvníci ostatních „normálních“ webových serverů se mohli cítit relativně v bezpečí. V současné době jsou však útoky z webových stránek (web-based attacks) nejčastějším způsobem šíření škodlivého kódu. [17]

Typický útok z webových stránek má následující průběh:

Útočník vyhledává jakékoliv (ideálně hojně navštěvované) webové servery a pokouší se do jejich obsahu implantovat škodlivý kód nebo skrytý odkaz, který na škodlivý kód hostovaný na jiném webovém serveru odkazuje. K vložení škodlivého kódu útočník zneužívá existující chyby webového serveru nebo chyby, které jsou obsaženy v kódu hostovaných webových stránek. [17]

Škodlivý kód umístěný na webový server se při přístupu uživatele na webové stránky příslušného serveru stáhne do prohlížeče počítače uživatele. [17]

Škodlivý kód se v počítači uživatele aktivuje a provede naplánované akce – sběr uživatelských hesel, šíření na další počítače v síti, instalace trojského koně a čekání na další příkazy. [17]

Další využívanou možností jak zajistit spuštění škodlivého kódu s potřebným oprávněním, je oklamání uživatele. Může se jednat např. o oznámení, že je potřeba nainstalovat novou (velmi užitečnou) softwarovou komponentu. Jedná se však pouze o další škodlivý kód. [17]

4.3.8 Injection flaw

Data jsou od uživatele odesílána do aplikace a následně zpracována pomocí interpreterů (interpreterem může být například PHP nebo MySQL) jako součást příkazu nebo dotazu. Tato data zkoušejí hackeři pozměnit tak, aby nekontrolovatelně vykonaly jejich příkazy. Tyto chyby pak umožňují útočníkům vytvářet, číst, aktualizovat a mazat jakákoli v aplikaci dostupná data. V horším případě získají takto útočníci přístup až do provozních systémů ukrytých za firewallem. [19]

4.3.9 Cross site scripting (XSS)

Jde o nejběžnější chybu zabezpečení webových aplikací. XSS vznikne v okamžiku, kdy aplikace odesílá uživatelská data webovému prohlížeči, aniž by nejprve tento obsah ověřila nebo zašifrovala. To umožní hackerům spustit škodlivé skripty v prohlížeči a číst uživatelské relace, změnit webové stránky či řídit malwarové útoky. Útoky jsou obvykle vykonávány prostřednictvím JavaScriptu, který umožňuje hackerům manipulovat s jakoukoli vlastností stránky. [19]

4.4 Principy bezpečného návrhu sítí

Bezpečnostní opatření by se měla soustřeďovat na tři základní úrovně zabezpečení:

- **Ohodnocení rizik a prevence** – nejefektivnějšími preventivními technologiemi pro ošetření rizik jsou řízení přístupu uživatelů, kryptografie a firewally.
- **Detekce hrozeb** – mezi systémy pro detekci hrozeb patří antivirové skenery a detektory pro rozpoznání dalších typů škodlivého softwaru (malware), systému detekce průniků IDS (Instrusion Detection Systems), audit událostí a heuristická analýza záznamů o událostech.
- **Reakce na incidenty** – při zjištění průniků a dalších typů útoků je třeba adekvátně reagovat, například vytvořit karantény pro systémy a podsítě, obnovit systémy do korektního stavu ze zálohy, vyléčit nákazu a upgradovat systémy kvůli lepší bezpečnosti. [12]

Z pohledu nákladů a obtížnosti jsou výše uvedené tři úrovně zabezpečení seřazeny tak, že se cena typicky zvyšuje postupně na každé další úrovni o jeden řád. To znamená, že detekce průniků stojí desetkrát více než preventivní opatření, a reakce na incidenty může být až stokrát nákladnější než prevence. [12]

Jedním z důležitých principů bezpečného návrhu sítí je minimalizace takzvaného útočného povrchu (attack surface) systému nebo sítě. Jde o to, jak moc je systém vystaven nebezpečí tím, že je přístupný uživatelům a potenciálním útočníkům. Profil útočného povrchu se skládá z následujících prvků:

- Protokoly běžící v síti nebo systému
- Síťová rozhraní, která odpovídají na dotazy nebo zprávy
- Otevřené porty
- Dostupné služby běžící na počítači
- Položky, které vkládají či vyplňují uživatelé. [12]

Čím méně existuje možných cestiček, kudy by útočník mohl vniknout do systému, tím nižší jsou bezpečnostní rizika. [12]

4.4.1 SSL protokol

Protokol SSL (Secure Socket Layer) šifruje komunikaci mezi dvěma stranami (prohlížeč uživatele a server, dvojice serverů, poštovní klient a server apod.) a brání uživatele proti odposlechu. [20]

SSL spojení funguje na principu asymetrické šifry. Každá z komunikujících stran má dvojici šifrovacích klíčů – veřejný a soukromý. Veřejný klíč je nutné zveřejnit a zajistit jeho správné předání všem, kteří jej budou chtít použít. Pokud pomocí tohoto klíče kdokoliv zašifruje zprávu, je zajištěno, že ji bude moci rozšifrovat jen majitel použitého veřejného klíče odpovídajícím soukromým klíčem – webový server, server elektronické pošty. Adresy stránek zabezpečených pomocí SSL začínají výrazem https://. Prohlížeč také zabezpečené stránky označuje ikonkou zámku ve stavové liště. Moderní prohlížeče zobrazují ikonku zámku rovněž v řádku adresy a podbarvují tuto řádku různými barvami (zelená pro plně vyhovující, žlutá nebo oranžová pro částečně vyhovující, tj. například vyhovující certifikát, ale vydaný pro jinou doménu, červená pak pro nevyhovující certifikát). [20]

Důvěryhodnost certifikátu

Výběr správné a důvěryhodné certifikační autority je důležitý. Certifikát důvěryhodné certifikační autority nezobrazuje v prohlížeči návštěvníka žádné varování o nedůvěryhodnosti. Naopak, certifikáty nedůvěryhodných autorit a vlastní (tzv. selfsigned) certifikáty nemají na webu místo. Prohlížeč zákazníka jim nedůvěřuje, protože není možné ověřit pravost podpisu

certifikační autority. Prohlížeč návštěvníka vašich stránek od návštěvy odrazuje, protože nedůvěryhodný certifikát může pocházet i od útočníka, což nelze vyloučit. [21]

Pokud firma nemá datovou schránku a přesto chce komunikovat s úřady elektronicky, měla by si pořídit certifikát od akreditovaných certifikačních autorit (možnosti komunikace firmy se státní správou uvedeny v kapitole 3.2 Firmy, které nemají datové schránky).

Ministerstvo vnitra udělilo akreditaci k působení jako akreditovaný poskytovatel certifikačních služeb těmto subjektům: První certifikační autorita, a. s., Česká pošta, s. p. a eIdentity, a. s. [22]

4.4.2 Firewall

Firewall je skupinou bezpečnostních opatření, jež izolují a chrání systémy před zlovolnými aktivitami. Základem tohoto druhu ochrany je oddělení sítí prostřednictvím hardwarového zařízení (fyzických síťových rozhraní) v jednom počítači. Firewally mohou být implementovány v softwaru nebo jako software instalovaný na vyhrazený hardware, případně jde rovnou o hardwarová zařízení. Některé firewally běží v prostředí operačního systému, například Linuxu nebo Windows, jiné mají podobu „černé skříňky“, tedy neproniknutelné krabice se svým vlastním operačním systémem. [12]

Firewally členíme do následujících skupin:

- Personální firewally
- Firewally ve směrovačích
- Hardwarové firewally
- Proxy firewally
- Serverové firewally.[12]

Běžné firewally mají často vlastnosti, které pokrývají více než jednu z těchto kategorií. Při srovnání firewallů přicházejí na řadu tři faktory: jejich vlastnosti, výkonnost (měřená propustností) a cena. [12]

4.4.3 IDS/IPS

Primární funkcí IDS je shromažďovat informace o probíhající síťové komunikaci nebo logovaných událostech a následně na základě svých schopností rozhodnout, zda se jedná o legální aktivitu, nebo probíhající útok. IDS je pasivním zařízením, které pouze monitoruje a detekuje. [23]

Tyto systémy již sledují a v případě IPS i reagují na reálný provoz na síti, tedy na otevřených portech. Pokud IPS zaznamená například útok typu port scan, nebo DoS, dokáže na základě sady definovaných pravidel na situaci pružně reagovat, a tedy nejen vyrozumět administrátory, ale i provést patřičnou akci (blokace IP, přesměrování provozu atd.). [19]

4.4.1 Patch management

Dalším velmi důležitým bodem je patch management, a to i kdyby měl znamenat jen zapnutí aktualizací aplikací Microsoft prostřednictvím služby Windows Update. Nicméně dnes je stále evidentnější, že útočníci čím dál častěji cílí na aplikace třetích stran (typicky webové prohlížeče), takže je nutné pravidelně aktualizovat veškerý software na počítači. Mimo jiné také proto, že dodavatelé počítačů dnes instalují na PC celou řadu aplikací, které běžní uživatelé nevyužijí a často ani nevědí, že je mají, ale které představují bezpečnostní riziko. Vedle pravidelného, ideálně automaticky nastaveného patch managementu se také doporučuje používat v podniku co nejméně různých typů softwarů – čím více softwarových programů, tím vyšší i riziko. [24]

4.4.1 Ochrana před Cross site scripting (XSS)

Jako ochranu lze použít seznam typu whitelist k validaci všech příchozích dat, který umožní odmítnout veškerá data nespecifikovaná v tomto seznamu jako nesprávná. Tento přístup je opakem seznamu blacklist, který odmítá veškeré jmenované nežádoucí vstupy. [19]

Další možností je při vkládání dat od uživatele do HTML stránky odfiltrovat „nebezpečné“ znaky z uživatelského vstupu (např. „<“, „>“, uvozovky a apostrofy) respektive je převést na příslušné HTML entity, na což lze použít dostupné funkce (např. v jazyce PHP je to funkce htmlspecialchars). [19]

Ve formulářích, chatech a jiných prvcích, kde může uživatel vložit svůj vstup, zakázat používání HTML značek (což ale není možné vždy). Nic nezkazíte také zavedením tzv. CAPTCHA kódu, který je uživatel nucen vyplnit před odesláním formuláře. Pravdou totiž je, že většina skutečných útoků na stránky se děje plně automatizovaně pomocí robotů. Přítomnost obrázkového kódu robotovi znemožní odeslání obsahu formuláře na váš server. [19]

4.4.2 Ochrana před Injection flaw

Jak ochránit aplikaci před touto hrozbou? Nepoužívejte interpretery (interpreterem může být například PHP), je-li to možné. Pokud se však použití interpreteru nelze vyhnout, je

řešením použití určitého mezistupně v komunikaci mezi aplikací a samotným interpreterem – například vlastní rozhraní API (application programming interface), které bude mít vlastní velmi typizovanou syntaxi a přesně definovanou sadu příkazů, které pomocí něj budou moci být odeslány na server. [19]

Nyní víme, jaká existují rizika napadení a jaké máme možnosti těmto útokům předejít. V další části práce budou popsány utajované skutečnosti ve firmě, tedy jaké informace a data firma chce a musí chránit.

5 UTAJOVANÉ SKUTEČNOSTI VE FIRMĚ

Různé firmy utajují různé skutečnosti. Výrobní firmy utajují postupy výroby nových výrobků, banky utajují osobní a citlivé údaje svých klientů, firmy zabývající se obchodem utajují před konkurencí svoji strategii prodeje.

Prakticky každá firma musí dodržovat zákon o ochraně osobních údajů, takže se na něj také krátce zaměřím.

5.1 Klasifikace informací

Klasifikace informací je jedním ze základních pilířů systémů řízení informační bezpečnosti. Pokud chceme informace organizace účinně a přitom efektivně chránit, musíme nejen definovat kategorie a bezpečnostně-organizační pravidla pro zacházení s nimi, ale především musíme vědět, které konkrétní dokumenty chránit – tzn. zajistit, aby na všech dokumentech byla jejich klasifikace odpovídajícím způsobem vyznačena. [25]

Bezpečnostní standardy řady ISO/IEC 27000 definují následující opatření:

- „Informace by měly být klasifikovány, a to s ohledem na jejich hodnotu, právní požadavky, citlivost a kritičnost.“
- „Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“
- „Pro zabránění neautorizovanému přístupu nebo zneužití informací by měla být stanovena pravidla pro manipulaci s nimi a pro jejich ukládání.“ [25]

Stupně klasifikace informací

Firmy většinou klasifikují informace do třech stupňů: veřejné, interní a chráněné (konkrétní pojmenování kategorií se může lišit, případně jich může být i více). [25]

Do kategorie **veřejných** informací spadají všechny informace (dokumenty), které jsou ze své povahy primárně určeny ke zveřejnění. Typicky se jedná o reklamní a marketingové materiály a údaje na webových stránkách určené k prezentaci firmy a jejích služeb nebo zboží. Tyto informace nemusí být z pohledu důvěrnosti nijak chráněny. [25]

Do kategorie **interních** informací patří všechny informace, u kterých je žádoucí, aby zůstaly pouze v perimetru firmy, tj. jsou určeny pro zaměstnance, případně další subjekty nebo osoby, kteří jsou vázáni příslušnými dohodami o mlčenlivosti (NDA) a tyto informace potřebují např. ke splnění svých smluvních (dodavatelských) závazků. Pro tuto třídu

klasifikace již musí být nastavena bezpečnostní pravidla, která zajistí odpovídající ochranu při přenosu a ukládání. Je to například povinnost ukládání do úložišť s řízeným a monitorovaným přístupem, používání šifrování při zasílání vně organizace (e-mailem) nebo šifrování na discích notebooků či v jiných mobilních zařízeních. [25]

Do kategorie **chráněných** informací patří citlivé informace, u nichž není žádoucí šíření napříč celou organizací, protože jsou určeny jen pro vybraný okruh osob (např. management, vývojové oddělení, oddělení nákupu apod.). Pro tyto informace se již nastavují relativně přísná bezpečnostní opatření, která zahrnují povinná šifrování jak při uložení, tak i při různých formách přenosu, ukládání písemných dokumentů v trezorech, povinnou skartaci apod. [25]

5.2 Zákon o ochraně osobních údajů

V zákoně jsou uvedeny následující povinnosti osob při zabezpečení osobních údajů:

Ten kdo pracuje s osobními údaji (dále jen zpracovatel) je povinen přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, k jejich změně, zničení či ztrátě, neoprávněným přenosům, k jejich jinému neoprávněnému zpracování, jakož i k jinému zneužití osobních údajů. Tato povinnost platí i po ukončení zpracování osobních údajů. [26]

V rámci tohoto opatření zpracovatel posuzuje rizika týkající se:

- Plnění pokynů pro zpracování osobních údajů osobami, které mají bezprostřední přístup k osobním údajům.
- Zabránění neoprávněným osobám přistupovat k osobním údajům a k prostředkům pro jejich zpracování.
- Zabránění neoprávněnému čtení, vytváření, kopírování, přenosu, úpravě či vymazání záznamů obsahujících osobní údaje.
- Opatření, která umožní určit a ověřit, komu byly osobní údaje předány. [26]

Pokud se jedná o automatizované zpracování osobních údajů, je zpracovatel v rámci tohoto opatření povinen:

- Zajistit, aby systémy pro automatizovaná zpracování osobních údajů používaly pouze oprávněné osoby.

- Zajistit, aby fyzické osoby oprávněné k používání systémů pro automatizovaná zpracování osobních údajů měly přístup pouze k osobním údajům odpovídajícím oprávnění těchto osob, a to na základě zvláštních uživatelských oprávnění zřízených výlučně pro tyto osoby.
- Pořizovat elektronické záznamy, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly osobní údaje zaznamenány nebo jinak zpracovány.
- Zabránit neoprávněnému přístupu k datovým nosičům. [26]

Nyní už víme vše, co musíme znát před tím, než začneme navrhovat ochranu firemního informačního systému. Dále budou následovat dvě případové studie, které nám osvětlí postup tohoto návrhu zabezpečení.

6 PŘÍPADOVÉ STUDIE

V této kapitole uvedu dvě případové studie týkající se fiktivních firem. Jak již bylo řečeno v úvodu, fiktivní firmy jsou zde využity proto, že reálné firmy nechtějí a vlastně ani nemohou prezentovat, jak chrání svůj firemní informační systém.

První firma se zabývá tvorbou a prodejem výukových kurzů a má 20 zaměstnanců. Druhá firma se zabývá výrobou oken do autobusů, trolejbusů a dalších dopravních prostředků a má 60 zaměstnanců. Rozdílnost v počtu zaměstnanců není až tak markantní, ale první firma svoji veškerou činnost provádí přes internet a obchoduje vlastně pouze se službami, druhá firma vytváří fyzické výrobky a zaměstnává tedy i manuální pracovníky, kteří přístup k firemní síti prakticky nepotřebují.

V případových studiích tedy popíši, čím se firma zabývá, jak si firma klasifikuje informace a jaký používá informační systém. Poté provedu analýzu hrozeb a rizik, které firmám hrozí při přenosu a uchování dat. V návaznosti na tuto analýzu navrhnu řešení, která by měla hrozby a rizika snížit případně úplně vyloučit a v neposlední řadě uvedu pořizovací a provozní náklady na zvolená řešení.

6.1 Čím se firmy zabývají

V následující tabulce je znázorněno čím se firma zabývá, kolik má zaměstnanců a jakou má právní formu.

Tabulka 1: Druhy firem

	Firma Kurzy	**Firma Okna**
Čím se firma zabývá	Vytváření a prodej e-learningových kurzů	Výroba oken do dopravních prostředků
Počet zaměstnanců	20	60
Právní forma	Podnikající FO	s. r. o.

Zdroj: Vlastní zpracování

Firma Kurzy

Firma kurzy se zabývá tvorbou výukových kurzů, které nabízí na svých webových stránkách a zákazník si je pak může objednat na externím e-shopu. Zákazník má možnost si před nákupem jakéhokoliv kurzu vyzkoušet, zda mu bude daný kurz vyhovovat na malé ukázce, která je připravena ke každé tematické sekci.

Kurzy jsou koncipovány nejprve výkladem dané látky a poté následují různá cvičení na zapamatování dané látky. Firma také poskytuje lekce přes skype, po jejichž dokončení vám lektor zašle e-mail o výsledku vašeho snažení s návrhy co se je třeba ještě doučit.

Firma má 20 zaměstnanců, z tohoto počtu je 5 stálých zaměstnanců a 15 externistů, kteří se zabývají výhradně tvorbou výukových kurzů a samozřejmě skype lekcemi. V této firmě každý zaměstnanec potřebuje ke své práci počítač.

Zpětnou vazbu od klientů získává firma pomocí dotazníků, které klienti po absolvování kurzu vyplňují. Mají zde prostor vyjádřit své názory a firma má tak možnost své kurzy nadále vylepšovat.

Firma Okna

Firma Okna se zabývá výrobou oken do autobusů, trolejbusů a jiných dopravních prostředků. Jejími odběrateli tak jsou převážně velké firmy vyrábějící tyto dopravní prostředky.

Firma zaměstnává 60 zaměstnanců, 50 jich pracuje ve výrobě na různých úrovních (od manuálních pracovníků po vedoucí jednotlivých výrobních sekcí) a 10 zaměstnanců pracuje v kanceláři. Počítač tedy využívá 10 zaměstnanců kanceláře a dále vedoucí výroby jednotlivých sekcí případně mistři výroby.

6.2 Informační systémy v jednotlivých firmách

Jak již bylo řečeno, před návrhem zabezpečení informačního systému musíme přesně vědět, jak firma svůj informační systém využívá.

Firma Kurzy

Tato firma používá dva osobní počítače, které jsou nainstalovány v kanceláři firmy, dále využívá firemní notebooky, kterých má firma 20. Ve všech počítačích je nainstalován operační systém Windows 7. Jako souborový server firma používá server NAS (Network Attached Storage – „datové úložiště na síti“). Veškeré počítače jsou propojeny do místní sítě LAN.

Firma Okna

Firma využívá 10 osobních počítačů, které jsou nainstalovány v kanceláři firmy. Dále firma využívá tablety, které využívají vedoucí jednotlivých výrobních sekcí, tabletů má firma pět. Veškeré počítače a tablety mají nainstalovaný operační systém Windows 7. Dále firma využívá ERP systém, který zahrnuje účetní systém, vedení zásob a vedení výroby. ERP

systém je nainstalován na serveru a v počítačích v kanceláři fungují veškeré programy ERP systému, v tabletech funguje pouze vedení výroby. Data se sdílí ve všech počítačích, tak se tedy například určí které zásoby je potřeba na jakou objednávku a ERP systém upozorní na jejich případný nedostatek na skladu. Jako server firma používá dvouprocesorový rackový server. Veškeré počítače jsou propojeny do místní sítě LAN.

6.3 Klasifikace informací v jednotlivých firmách

V následující tabulce je uvedena klasifikace informací u jednotlivých firem. Informace jsou rozděleny do tří skupin, veřejné, interní a chráněné, podle nutnosti jejich utajení (vysvětleno v kapitole 5.1Klasifikace informací).

Firma Kurzy

Tabulka 2: Klasifikace informací u firmy Kurzy

Druh informací	Jaké informace to jsou
Veřejné	Informace na webových stránkách určené k prezentaci firmy a jejích produktů, e-learningové kurzy
Interní	Informace o zaměstnancích, jejich platy a náplň práce
Chráněné	Zdrojové kódy e-learningových kurzů, osobní údaje klientů

Zdroj:Vlastní zpracování

U firmy Kurzy jsou nejdůležitější data se zdrojovými kódy e-learningových kurzů a také osobní údaje klientů. Tyto informace je nejnutnější utajit a mohou s nimi nakládat pouze zaměstnanci, kteří k nim mají výslovně povolený přístup (přístup zaměstnanců k datům bude rozebrán později).

Firma Okna

Tabulka 3: Klasifikace informací u firmy Okna

Druh informací	Jaké informace to jsou
Veřejné	Informace o firmě na webových stránkách, reklamní a marketingové informace pro odběratele,
Interní	Informace o zaměstnancích, jejich platy a náplň práce
Chráněné	Informace o postupech výroby, osobní údaje klientů,

Zdroj:Vlastní zpracování

U firmy okna jsou opět důležité osobní údaje klientů a také informace o postupech výroby. S těmito daty mohou nakládat pouze zaměstnanci, kteří k nim mají výslovně povolený přístup (přístup zaměstnanců k datům bude rozebrán později).

6.4 Analýza rizik při přenosu a uchovávání dat u jednotlivých firem

Firma Kurzy

Tabulka 4: Analýza rizik firmy Kurzy

Typ rizika	Návrh řešení
Napadení počítačů hackerem	Ochrana Windows 7, Microsoft Security Essentials
Zneužití dat zaměstnancem	Řízení přístupu k IS, hesla
Ztráta znehodnocení dat na serveru	RAID 1, zálohování
Napadení komunikace se státní správou	Datová schránka
Napadení komunikace s ostatními firmami	Firemní e-mail chráněn SSL certifikátem Elektronický podpis
Injection flaw, XSS	Blacklist, odfiltrování nebezpečných znaků, CAPTCHA
Napadení stránek firmy hackery	SSL certifikát

Zdroj:Vlastní zpracování

U firmy Kurzy je největším rizikem napadení stránek firmy hackery a také Injection flaw a XSS. Firma získává zpětnou vazbu od klientů přes dotazníky, které zákazníci po absolvování kurzu vyplňují. Tyto dotazníky se zasílají na server do databáze MySQL. Zde hrozí, že dotazníky vyplní nějaký hacker případně spamovací robot a pokusí se tak do databáze proniknout.

Firma Okna

Tabulka 5: Analýza rizik firmy Okna

Typ rizika	Návrh řešení
Napadení počítačů hackerem	Ochrana Windows 7, Esset Secure Office+, zakázání některých webových stránek
Zneužití dat zaměstnancem	Řízení přístupu k IS pomocí ERP systému, hesla
Ztráta znehodnocení dat na serveru	RAID 1+0, zálohování
Napadení komunikace se státní správou	Datová schránka
Napadení komunikace s ostatními firmami	EID, Firemní e-mail chráněn SSL certifikátem, Elektronický podpis
Chybné zacházení s IS	Školení pro ERP systém
Chyby v software	Pravidelné aktualizace

Zdroj:Vlastní zpracování

U firmy Okna je riziko chybné zacházení s IS specifické pro ERP systém, protože tento systém je velice komplexní a obsahuje spoustu funkcí. Chyby v software jsou zde myšleny také pro ERP systém, protože aktualizace operačních systémů a dalších aplikací, které používáme pravidelně je snad v současné době už samozřejmostí.

6.5 Návrh ochrany jednotlivých firem

V této části uvedu pro jednotlivé firmy návrhy jak zabezpečit informační systém, před riziky, která firmám hrozí.

6.5.1 Firma Kurzy

V analýze rizik jsem uvedla, že největší riziko pro tuto firmu je **napadení firemních stránek hackery a Injection flaw a XSS**, proto začneme ochranou před těmito hrozbami.

Webové stránky si firma zabezpečí SSL certifikátem, který nejen zajišťuje bezpečnou komunikaci s klienty, ale také tím firma dává svým klientům najevo, že jí bezpečnost informací není lhostejná.

Ochrana před Injection flaw a XSS je poněkud složitější. Firma zavede takzvaný blacklist na kterém jsou uvedeny veškeré nežádoucí datové vstupy. Při validaci příchozích dat je tak zajištěno, že data uvedená na tomto seznamu budou odmítnuta. Pro jistotu ještě firma u políček, ve kterých bude uživatel vyplňovat text, definuje v PHP jazyce funkci htmlspecialchars, která převede „nebezpečné“ znaky (např. „<“, „>“, uvozovky a apostrofy) na příslušné HTML entity. Také zavede takzvaný CAPTCHA kód, který uživatel musí vyplnit před odesláním formuláře, měl by zamezit přístupu spamovacích robotů.

Ochranu počítačů před hackery si firma zajistí tím, že bude používat ochranu operačního systému Windows 7, který má firma nainstalovaný ve všech počítačích. Jedná se především o výchozí firewall a Windows defender, což je vestavěný antispywarový program. Vestavěný antivirový program zde bohužel není, musí se doinstalovat, ale Microsoft nabízí bezplatně antivirový program Microsoft Security Essentials.

Zneužití dat zaměstnancem se předejde řízením přístupu k informačnímu systému. Přístup k datům a počítačům bude ve firmě řešen takto:

- Administrátorská práva ke všem počítačům i firemním notebookům má pouze správce sítě. Ti kdo počítače používají, mají pouze uživatelská práva a veškeré potřebné aplikace a programy jsou v počítačích již nainstalovány. Pokud nastane nějaký problém je na všech počítačích nainstalován program TeamViewer, který umožňuje vzdálenou správu a případnou instalaci potřebných aplikací.
- Přístupy k počítačům jsou řízeny hesly, pouze správce sítě, ředitel firmy a další dva zaměstnanci mají přístup ke všem složkám a aplikacím. Ostatní zaměstnanci mají přístup pouze k tomu, co ke své práci potřebují.

- Důležité je také správně nastavit politiku hesel. Zaměstnancům je při příchodu do firmy dáno dočasné přihlašovací heslo, které si mají co nejdříve změnit na své heslo. Je jim doporučeno, aby heslo mělo minimální délku 8 znaků, minimální jedno malé písmeno a jedno velké písmeno, jedno číslo a jeden speciální znak. Hesla u jednotlivých zaměstnanců jsou v databázi hašované v bcrypt (Blowfish hashing).
- Dále jsou zde rozlišovány dva typy přístupů pro jednotlivé lektory. Jeden přístup je administrátor a druhý lektor. Administrátor může upravovat jakýkoliv kurz, včetně jeho smazání. Kurz se zatím pouze označí, jako smazaný a přímo v databázi ho může správce sítě opět označit jako aktivní, pokud by se snad administrátor spletl a chtěl smazat jiný kurz. Lektor může provádět úpravy pouze v kurzu, který založil.

Ztrátě nebo znehodnocení dat na serveru se předejde pravidelným zálohováním a také speciální metodou ukládání dat na server. U této firmy postačí, když bude používat metodu RAID 1 (1.6.2 RAID 1). Metoda RAID je však pouze zabezpečení proti selhání pevného disku, takže je špatně si myslet, že tato metoda nahradí zálohování. Firma bude provádět zálohování dat a zdrojových kódů k výukovým kurzům jednou denně na serveru metodou diferenciální zálohy. To je taková záloha, která obsahuje všechny soubory, které se změnily od poslední plné zálohy. Plné zálohy bude provádět jednou týdně na externí server a také jednou týdně na vlastní server. Jako externí server firma využívá

Pro **bezpečnou komunikaci se státní správou** si firma nechá zřídit datovou schránku, i když ji nemá ze zákona povinnou. Pro firmu bude toto řešení nejjednodušší, protože jakékoliv jiné řešení zahrnuje buď elektronický podpis od akreditovaného poskytovatele certifikačních služeb, nebo osobní dostavení se na pobočku úřadu.

Pro **bezpečnou komunikaci s ostatními firmami** si firma zřídí firemní e-mail. Protože ve firmě pracuje hodně externistů a je zde pouze 5 stálých zaměstnanců, firmě postačí firemní e-mail pouze pro stálé zaměstnance. Budou tak komunikovat nejen zaměstnanci mezi sebou ale také tak bude firma komunikovat s ostatními firmami. Pro komunikaci s externisty postačí jejich soukromý e-mail. Firma si zřídí firemní e-maily na Google Apps, zde probíhá komunikace chráněná SSL certifikátem. Jedná se zde především o předběžné dohody o spolupráci, pokud firma chce uzavřít s jinou firmou smlouvu o spolupráci, probíhají pak dohody osobně a smlouvy jsou již v papírové podobě. Tudíž si firma nemusí pořizovat elektronický podpis.

6.5.2 Firma Okna

Jak již bylo zmíněno, **chybné zacházení s IS** je typické pro ERP systém. Je tedy potřeba aby probíhala pravidelná školení zaměstnanců, kteří s tímto systémem pracují. Firmy, které ERP systémy nabízejí, většinou tato školení nabízejí automaticky a jsou tak například zahrnuta v pravidelných poplatcích za používání ERP systému.

Chyby v software jsou častým slabým místem, na které útočníci cílí. U této firmy je potřeba věnovat se nejen pravidelným aktualizacím operačního systému a veškerých dalších aplikací, které běžně používá, ale aby také nezapomínala na aktualizace ERP systému. Tyto aktualizace jsou většinou zahrnuty ve službách, které prodejce ERP systému nabízí svým zákazníkům.

Tato firma bude **chránit své počítače před hackery** také vestavěnou ochranou Windows 7 a antivirovým programem Esset Secure Office+.

Antivirový program zahrnuje základní sadu antivirových produktů pro ochranu koncových zařízení (včetně smartphonů a tabletů s OS Android) a souborového serveru. Všechny produkty je možné vzdáleně spravovat z jedné webové konzole a dále pokročilé vrstvy ochrany koncových zařízení jako je Firewall, Antispam, Vulnerability Shield, Ochrana proti botnetu a web kontrola.

Bylo by také vhodné zakázat přístup na některé webové stránky, které mohou být zdrojem hackerských útoků, jsou to samozřejmě různé nevhodné stránky z hlediska obsahu, a také například facebook a stránky s různými novinovými portály. Je to nejen z důvodu ochrany, ale také proto, aby zaměstnanci na těchto stránkách netrávili čas v pracovní době.

Zneužití dat zaměstnancem se v této firmě také předchází řízením přístupu k IS. Pravidla pro přístup k datům a počítačům jsou v této firmě následující:

- Administrátorská práva ke všem počítačům má pouze správce sítě, který se stará o správný chod sítě. Pokud tedy nastane nějaký problém a je třeba něco přeinstalovat nebo opravit má přístupová práva pouze správce sítě, ostatní uživatelé mají pouze uživatelská práva. Zabrání se tak tomu, že by uživatelé mohli nainstalovat nějaký program, který by pak mohl v síti škodit.
- Přístupová práva uživatelů jsou řešena pomocí ERP systému. Do celého systému má přístup pouze ředitel firmy a správce sítě. Účetní mají přístup do účetního systému, vedoucí výroby do vedení výroby a vedoucí skladu do vedení zásob. Účetní systém, vedení výroby a vedení zásob je propojeno do jednoho systému a sdílí se zde data.

Účetní potřebují vědět, co se vyrobilo, kolik se na to spotřebovalo zásob a kdo na tom pracoval. Vedoucí skladu potřebuje vědět kolik zásob je potřeba na určité výrobky. Vedoucí výroby potřebuje vědět, co se má vyrobit.

- Politika hesel je v této firmě řešena stejně jako u předchozí firmy.

Ztrátě nebo znehodnocení dat na serveru se zde také předejde pravidelným zálohováním a speciální metodou ukládání dat. Tato firma bude používat metodu RAID 1+0 (1.6.3 RAID 1+0). Firma bude také provádět zálohování dat jednou denně na serveru metodou diferenciální zálohy. Plné zálohy bude firma ukládat také jednou týdně na externí server a také jednou týdně na vlastní server.

Bezpečná komunikace se státní správou bude zajištěna datovou schránkou, kterou má tato firma povinnou ze zákona.

Bezpečná komunikace s ostatními firmami, které mají ERP systém je zajištěna pomocí EID (1.3.2 Nejčastěji používané služby). S firmami, které nemaní ERP systém bude firma komunikovat pomocí firemního e-mailu, také tak budou komunikovat jednotlivý zaměstnanci mezi sebou. e-mail bude zřízen na Google Apps. Pro větší důvěryhodnost komunikace s ostatními firmami si firma pořídí elektronický podpis.

6.6 Pořizovací a provozní náklady na zvolená řešení

V předchozí podkapitole jsou uvedena řešení, která by měla odstranit nebo zabránit rizikům, která byla určena v analýze rizik. Nyní zjistíme, jaké jsou náklady na tato řešení. Ceny v následujících tabulkách jsou uvedeny bez DPH.

6.6.1 Firma Kurzy

Tabulka 6:Pořizovací a provozní náklady pro firmu Kurzy

Druh ochrany	Pořizovací náklady	Provozní náklady
Ochrana Windows 7	0 Kč	0 Kč
Firemní e-mail	0 Kč	40€/rok
Zálohování	0 Kč	2 000 Kč/měsíc
Datová schránka	0 Kč	0 Kč
SSL certifikát	1047 Kč/3 roky	1047 Kč/3 roky
TeamViewer	11 739 Kč	0 Kč

Zdroj:Vlastní zpracování

Firma je velice malá, tudíž využívá ochranu od Windows 7, která je bezplatná. Firemní e-mail má firma zřízen pro 5 zaměstnanců takže provozní náklady na tyto e-maily budou 40€ za rok. Náklady na zálohování na externí server budou 2 000 Kč za měsíc. Jako SSL certifikát

využívá firma RapidSSL z důvodu hlavně nízké ceny. Náklady na pořízení programu TeamViewer jsou 11 739 Kč.

6.6.2 Firma Okna

Tabulka 7:Pořizovací a provozní náklady pro firmu Okna

Druh ochrany	Pořizovací náklady	Provozní náklady
Ochrana Windows 7	0 Kč	0 Kč
Esset Secure Office+	0 Kč	5 145 Kč/5 zařízení/rok
Firemní e-mail	0 Kč	40€/rok
Zálohování	0 Kč	3 000 Kč/měsíc
Datová schránka	0 Kč	0 Kč
Elektronický podpis	1047 Kč/3 roky	1047 Kč/3 roky

Zdroj:Vlastní zpracování

Tato firma využívá kromě základní ochrany Windows 7 také antivirový program Esset Secure Office+, který ji na všechny počítače bude stát 15 435 Kč za rok. Firemní e-maily jsou také na Google Apps a náklady na toto řešení budou pro všechny uživatele 40€ za rok. Náklady na zálohování dat na externí server jsou 3 000 Kč za měsíc. Jako SSL certifikát má tato firma také RapidSSL a cena zde také hraje významnou roli.

ZÁVĚR

V této bakalářské práci jsem se pokusila vytvořit návod, jak zabezpečit firemní informační systém. Před tím než se vůbec začnou nějaká zabezpečení vybírat a hlavně před tím než se začnou implementovat, musí podnikatel vědět spoustu věcí, které tento proces ovlivňují. To co musí podnikatel nebo lépe tvůrce ochrany informačního systému vědět je hlavně to co firma dělá, jaký informační systém využívá, jaké informace jsou pro firmu důležité, jaká rizika firmě hrozí při přenosu a uchovávání dat a v neposlední řadě kolik je majitel firmy zhruba ochoten investovat. V současné době se informační systémy a jejich ochrana tvoří zároveň přímo na míru jejich uživatelů. Může se ale stát, že absolvent bude chtít založit vlastní firmu a na zadání řešení jeho informačního systému prostě nebude mít peníze. Proto jsem vytvořila tento návod, který má uživatele, kteří už o informačních systémech něco málo tuší provést tím jak ho zabezpečit a na co si dát pozor.

V případových studiích jsem uvedla dvě firmy. Jedna se zabývá prodejem služeb a má 20 zaměstnanců, druhá se zabývá prodejem výrobků a má 60 zaměstnanců. V těchto případových studiích jsem poukázala na skutečnost, že každá firma vyžaduje individuální řešení a sestavit takový informační systém a hlavně tento informační systém zabezpečit není jednoduché řešení.

POUŽITÁ LITERATURA

[1] KÁLLAY, Fedor. Počítačové sítě LAN/MAN/WAN a jejich aplikace. 2. aktualiz. vyd. Praha: Grada, 2003, 356 s. ISBN 80-247-0545-1.

[2] SKLENÁŘ, Pavel. Co znamená ERP?: úvod do problematiky. E-komerce,cz: váš business na internetu[online]. 2002[cit. 2015-06-30]. Dostupné z: http://www.e-komerce.cz/ec/ec.nsf/0/bb3c13db9522519ac1256b79003104f2

[3] Chraňte svá cenná data. Svět hardware: vše ze světa počítačů [online]. 2012 [cit. 2015-08-11]. Dostupné z: http://www.svethardware.cz/chrante-sva-cenna-data/34573

[4] FIALA, Jan. Disková pole RAID: jejich výhody a nevýhody. Poradna.net: československá poradna [online]. 2007 [cit. 2015-08-11]. Dostupné z: http://pc.poradna.net/a/view/307945-diskova-pole-raid-jejich-vyhody-a-nevyhody

[5] Zákon o elektronickém podpisu. Sbírka zákonů. 2000. Dostupné také z: https://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=49532&recShow=1&nr=227~2F2000&rpp=100#parCnt

[6] Magazín o bezpečnosti: Microsoft aktualizuje seznam Root certifikátů a přidává nové autority [online]. [cit. 2015-06-21]. Dostupné z: http://www.blog.sslmarket.cz/ssl/microsoft-aktualizuje-seznam-root-certifikatu/

[7] LAPÁČEK, Jiří. Jak na datovou schránku a elektronickou komunikaci s úřady. 1. vyd. Brno: Computer Press, 2012, 197 s. ISBN 978-80-251-3680-5.

[8] Typy datových schránek. Datové schránky [online]. [cit. 2015-06-28]. Dostupné z: https://www.datoveschranky.info/zakladni-informace/typy-datovych-schranek

[9] Elektronická podání pro finanční správu. Finanční správa [online]. 2014 [cit. 2015-08-12]. Dostupné z: http://www.financnisprava.cz/cs/dane-elektronicky/danovy-portal/elektronicka-podani-pro-financni-spravu

[10] ING. PETLACHOVÁ, Petra. Vyzkoušejte EPO: pomůže vám bezchybně vyplnit daňové přiznání. Finanční správa [online]. 2014 [cit. 2015-08-12]. Dostupné z: http://www.financnisprava.cz/cs/financni-sprava/pro-media/tiskove-zpravy/tiskove-zpravy-2014/vyzkousejte-EPO-pomuze-vam-bezchybne-vyplnit-danove-priznani-4838

[11] Podmínky provozu elektronické podatelny Ministerstva zdravotnictví. Ministerstvo zdravotnictví České Republiky [online]. 2011, 7.1.2013 [cit. 2015-07-02]. Dostupné z:

http://www.mzcr.cz/obsah/podminky-provozu-elektronicke-podatelny-ministerstva-zdravotnictvi_2455_1.html

[12] SOSINSKY, Barrie A. Mistrovství – počítačové sítě. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.

[13] MARŤÁK, Pavel. Bezpečnost dat v praxi. SystemOnLine: S přehledem ve světě informačních technologií[online]. 2005, 2005(4) [cit. 2015-06-30]. Dostupné z: http://www.systemonline.cz/clanky/bezpecnost-dat-v-praxi.htm

[14] PŘÍBIL, Tomáš. Rootkity. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2007 [cit. 2015-07-01].Dostupné z: http://www.systemonline.cz/it-security/rootkity.htm

[15] SZOR, Peter. Počítačové viry: analýza útoku a obrana. Vyd. 1. Brno: Zoner Press. ISBN 80-86815-04-8.

[16] HOLUB, Petr. Jemný úvod do (anti)virové problematiky. Zpravodaj ÚVT MU [online]. 2002, 14.11.2011, XII(4) [cit. 2015-08-12]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/245.html

[17] MALINKA, Kamil a Radim PEŠTA. Zase ty viry. Zpravodaj ÚVT MU [online]. 2009, 14.11.2011, XIX(5) [cit. 2015-08-12]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/620.html#lit1

[18] PEŠTA, Radim. Počítačové viry. Zpravodaj ÚVT MU [online]. 1999, IX(5) [cit. 2015-07-01]. ISSN 1212-0901. Dostupné z: http://webserver.ics.muni.cz/bulletin/articles/160.html

[19] POMAZAL, Jiří. Hrozby pro bezpečnost webových aplikací a serverů. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2010 [cit. 2015-07-01]. Dostupné z: http://www.systemonline.cz/it-security/hrozby-pro-bezpecnost-webovych-aplikaci-a-serveru.htm

[20] LEZSKOW, Milan. Bezpečnost webových aplikací a portálů. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2013, (4) [cit. 2015-07-01]. Dostupné z: http://www.systemonline.cz/it-security/bezpecnost-webovych-aplikaci-a-portalu.htm

[21] ZECHMEISTER, Jindřich. Technologie zabezpečení webových stránek. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2013,

(5) [cit. 2015-07-01]. Dostupné z: http://www.systemonline.cz/it-security/technologie-zabezpeceni-webovych-stranek.htm

[22] Ministerstvo vnitra České republiky: eGovernment [online]. [cit. 2015-06-21]. Dostupné z: http://www.mvcr.cz/clanek/prehled-udelenych-akreditaci.aspx

[23] BARABAS, Maroš a Michal DROZD. Pokročilé formy útoků a jejich detekce. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2013 [cit. 2015-07-03]. Dostupné z: http://www.systemonline.cz/it-security/pokrocile-formy-utoku-a-jejich-detekce.htm

[24] Priority bezpečnostní politiky v malých a středních firmách. SystemOnLine: S přehledem ve světě informačních technologií [online].2013 [cit. 2015-06-26]. Dostupné z: http://www.systemonline.cz/it-security/priority-bezpecnostni-politiky-v-malych-a-strednich-firmach.htm

[25] Klasifikace informací a její prosazování v praxi. SystemOnLine: S přehledem ve světě informačních technologií [online]. 2015(3) [cit. 2015-06-24]. Dostupné z: http://www.systemonline.cz/sprava-dokumentu/klasifikace-informaci-a-jeji-prosazovani-v-praxi.htm

[26] Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění účinném od 1. ledna 2015. Sbírka zákonů. 2000. Dostupné z: https://www.uoou.cz/zakon-c-101-2000-sb-o-ochrane-osobnich-udaju-a-o-zmene-nekterych-zakonu-ve-zneni-ucinnem-od-1-ledna-2015/ds-3109/archiv=0&p1=1261