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)

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]

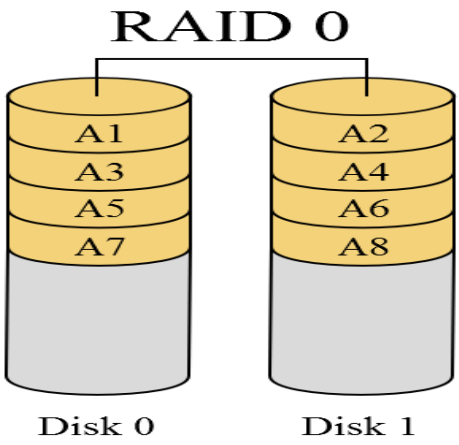
1.6 Bezpečné ukládání dat

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]

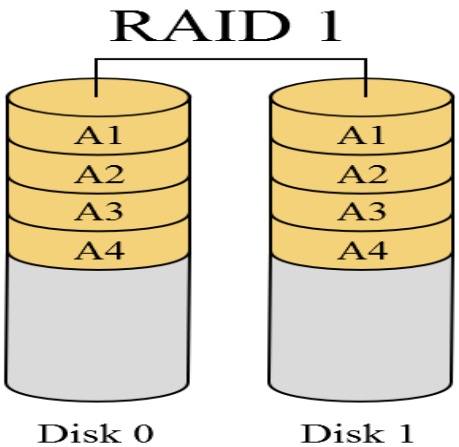


Obrázek 1: RAID 0

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]



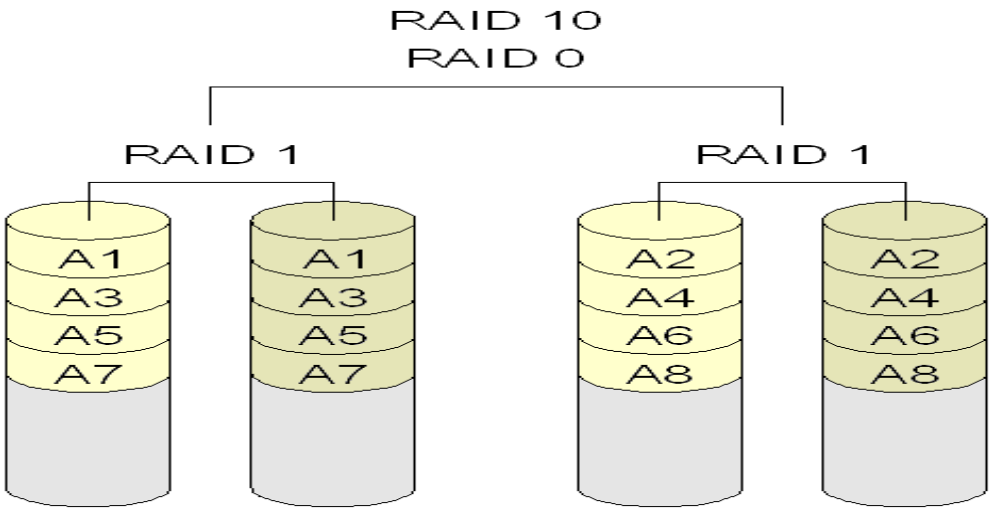
Obrázek 2: RAID 1

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]

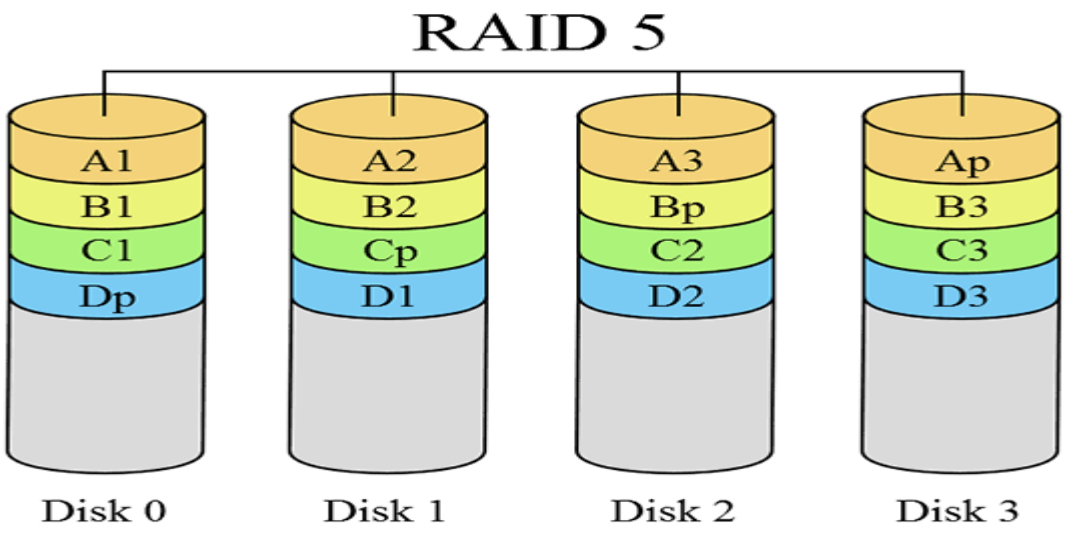


Obrázek 3: RAID 1+0

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.

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