VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT

INSTITUTE OF INFORMATICS

# NÁVRH ZABEZPEČENÍ POČÍTAČOVÉ SÍTĚ MALÉ SOFTWAROVÉ FIRMY

PROPOSAL OF COMPUTER NETWORK SECURITY IN A SMALL SOFTWARE COMPANY

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE — JAN ŠPIČÁK

AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.

SUPERVISOR

BRNO 2010

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2009/2010
Ústav informatiky

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

**Špičák Jan**

Manažerská informatika (6209R021)

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

**Návrh zabezpečení počítačové sítě malé softwarové firmy**

v anglickém jazyce:

**Proposal of Computer Network Security in a Small Software Company**

Pokyny pro vypracování:

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

Seznam odborné literatury:

NORTHCUTT, S.[et al.] (2005): Bezpečnost sítí: velká kniha. 1.vydání. CP Books, Brno. 589 stran. ISBN 80-251-0697-7.
THOMAS, M. T. (2005): Zabezpečení počítačových sítí bez předchozích znalostí. 1.vydání. CP Books, Brno. 338 stran. ISBN 80-251-0417-6.
DOSTÁLEK, L.(2003): Velký průvodce protokoly TCP/IP. 1.vydání. Computer Press, Praha. 571 stran. ISBN 80-7226-849-X.
DOSEDĚL, T.(2004): Počítačová bezpečnost a ochrana dat, 1.vydání. Computer Press, Brno. 190 stran. ISBN 80-251-0106-1.
BOTT, E., SIECHERT, C.(2004): Mistrovství v zabezpečení Windows 2000 a XP. Computer Press, Brno. 696 stran ISBN 80-7226-878-3

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

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2009/2010.

L.S.

| | |
|---|---|
| Ing. Jiří Kříž, Ph.D.<br>Ředitel ústavu | doc. RNDr. Anna Putnová, Ph.D., MBA |

V Brně, dne 03.06.2010

Abstrakt:
Bakalářská práce předkládá analýzu stavu současného zabezpečení počítačové sítě a následné optimalizaci v malé softwarové firmě. Předkládá návrhy jak zlepšit zabezpečení, které mohou zabránit útokům z internetu a ztrátě důležitých informací.

Abstract:
The bachelor thesis is concerned with the analysis of the current conditions of computer network security and its optimalization in a small software company. The thesis presents solutions how to improve the security of the computer network. The solutions are supposed to prevent the computer network from the Internet attacks and thus avoid losing important data and information.

Klíčová slova:
zabezpečení sítě, zabezpečení webové služby, zabezpečení dat, zabezpečení databáze, zabezpečení systémů, antivirová ochrana, firewallová ochrana, ochrana proti přetížení sítě, antivir, firewall, malware, vir, IP, DoS, DDoS, IDS, IPS, NOD32, Windows, server, klient, XSS, RCE, SFTP, PPTP, VPN, L2TP, SQL Injection, WPA, AES

Keywords:
network security, security of web service, security of stored data, security of database, security of operating system, antivirus defense, firewall defense, DoS defense, antivirus, firewall, malware, virus, IP, DoS, DDoS, IDS, IPS, NOD32, Windows, server, client, XSS, RCE, SFTP, PPTP, VPN, L2TP, SQL Injection, WPA, AES

Bibliografická citace mé práce:
ŠPIČÁK, J. Návrh zabezpečení počítačové sítě malé softwarové firmy. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2010. 47 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

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

V Brně dne 3. června 2010

---

Podpis

Chtěl bych poděkovat panu Ing. Viktoru Ondrákovi, PhD. za cenné rady a vedení této bakalářské práce.

Společnost, která souhlasila s účastí na projektu této bakalářské práce, si přeje zůstat v anonymitě. Proto je na ni v následujícím textu odkazováno pod fiktivním názvem DREAM SOFTWARE.

## Obsah

# 1. Úvod

Tato bakalářská práce se zabývá zhodnocením původního stavu zabezpečení počítačové sítě v malé softwarové firmě, návrhem realizace řešení a vlastním řešením, jak zlepšit zabezpečení místní sítě s připojením k internetu se spuštěnou webovou službou a vzájemným propojením několika externích zařízení přes místní bezdrátové a také virtuální privátní sítě v malé softwarové firmě.

Jelikož je internet v současné době nejistým prostředím, zejména z důvodu zneužívání zranitelností nastavení využívaných operačních systémů, aplikací, služeb a vybraných politik, stává se oblast ochrany a zabezpečení legitimity využívaných zařízení stále větší prioritou. Současné trendy v oblasti zabezpečení počítačových sítí malých firem naznačují, že vkládané prostředky do vylepšování bezpečnostních řešení se v budoucnu projeví jako ekonomicky výhodné.

Světové servery informují o vzrůstajícím počtu zneužití osobních informací a následné finanční škodě způsobené špatným či nedostatečným zabezpečením počítačových systémů, a/nebo selháním lidských zdrojů. Z těchto důvodů je nutné zabránit co největšímu množství bezpečnostních nedostatků a snižovat případná rizika.

Tato bakalářská práce popisuje možné i reálné řešení těchto rizik a třídí je dle priority a nutnosti časové i finanční realizace. Je překvapivé, jak se lze pro malou společnost nevelkou investicí vyhnout velkým ztrátám.

Po realizaci desítek penetračních testování a zjišťování zranitelností počítačových systémů a k nim připojitelných zařízení ve firmě Dream Software přináší tato práce několik závěrů, jak lze systém ve firmě zabezpečit.

Po celou dobu realizace projektu této bakalářské práce přistupovalo vedení firmy k samotnému projektu velmi ochotně, ať už ve formě nákupu nových zařízení a software, nebo ve formě ceny času stráveného účastí na realizaci.

S rostoucími riziky v oblasti zabezpečení sítí se zvyšuje i jeho kvalita, zejména díky tomu, že jsou lépe dostupné znalosti této problematiky v návaznosti na studiu nově vznikajících zranitelností a následného promptního řešení.

V průběhu realizace projektu této bakalářské práce se ve firmě Dream Software začala implementovat nová hardwarová zařízení s dokonalejšími nastaveními, týkající se nastavení firewallu, ochran proti přetížení, obecně známým typům útoků, odstranění

zranitelnosti webové služby. Vedení firmy investovalo do velice kvalitního software s důrazem kladeným na co nejefektivnější nastavení pro vybrané situace.
Provedenými kroky se ve firmě dosáhlo snížení rizik, zvýšení rychlosti odvracení případných budoucích hrozeb a celkového zlepšení zabezpečení v celém počítačovém ekosystému firmy, což se může projevit jak na finanční, tak kvalitativní stránce budoucího vývoje.
Technologie, které se v současnosti ve firmě testují, s velkou pravděpodobností přinesou další zlepšení v celém systému zabezpečení a očekávají se další ekonomické výhody.

Poznámka: Teoretická část práce byla napsána před realizací samotného projektu, praktická část během jeho realizace a z části po ní.

# 2. Vymezení problému a cíle práce

Cílem mé bakalářské práce je navrhnout účinný systém zabezpečení ICT malé softwarové firmy a podílet se na implementaci kvalitnějšího a komplexnějšího řešení, zahrnujícího především ochranu místní sítě, pracovních stanic a webové služby před hrozbami plynoucími z neoprávněného prostředí.

V teoretické části popisuji, jak jednotlivé prvky související se zabezpečením fungují a pracují a jaké výhody mohou pro firmu Dream Software z inovací těchto prvků plynout.

Praktickou část představuje vlastní realizace projektu bakalářské práce, tedy inovace systému zabezpečení počítačové sítě ve firmě Dream Software.

# 3. Analýza současného stavu

## 3.1. Charakteristika firmy

Firma Dream Software, spol. s.r.o. (dále jen Dream Software) byla založena v roce 1993, v období, kdy společnost a ekonomika procházela od „Sametové revoluce“ významnými ekonomickými a institucionálními změnami. Od té doby prošla firma Dream Software řadou změn v organizaci, struktuře a předmětu podnikání až do současné podoby, kdy v jejím čele stojí ředitel a firma zaměstnává 16 zaměstnanců.

Průměrný roční obrat firmy se pohybuje okolo 20 mil. Kč,- a přibližný čistý zisk převyšuje 2 mil. Kč.

Společnost Dream Software začínala svou podnikatelskou aktivitu v oblasti vývoje a distribuce programů, zejména daňového a účetního (ekonomického) software.

Mezi uživatele programů firmy Dream Software patří převážně auditoři, daňoví poradci, účetní firmy, velké organizace i menší firmy, podnikatelé i soukromé osoby.

V současnosti se společnost Dream Software zabývá především službami pro uživatele dříve vyvinutých programů a neustálým vývojem nových verzí a dalších aplikací. Svým uživatelům společnost nabízí telefonickou a e-mailovou technickou podporu, aktualizace s legislativními změnami, týkající se nabízených produktů, a e-mailový zpravodaj o změnách nebo novinkách v oblasti nabízených produktů. Noví zákazníci získají s pořízením jakéhokoliv ekonomického software firmy Dream Software výše zmíněné služby zdarma.

Cílem firmy Dream Software je poskytovat takový software, který uživatelům poskytuje komfort obsluhy, možnost přizpůsobení a který šetří práci. Při vývoji software využívá společnost moderních technologií, nástrojů a programů, umožňujících importy a exporty dat v mnoha formátech. Výhodou software vyvinutého firmou Dream Software je skutečnost, že tento software nevyžaduje servis přímo u zákazníka, ale dotazy zpracovává technické oddělení telefonicky nebo pomocí e-mailu.

V současné době nabízí firma Dream Software tři základní druhy ekonomického software; software na vedení účetnictví a daňové evidence, software na správu osobních financí a na hospodaření v domácnosti a v neposlední řadě software na vyplňování a elektronické podání formulářů.

### 3.2. HARDWARE A SOFTWARE

Ve firmě Dream Software se nachází 13 moderních a kvalitně vybavených osobních počítačů.

Počítače určené k vývoji a programování nových verzí a aplikací disponují 64 bitovými dvou jádrovými, či čtyř jádrovými procesory AMD nebo Intel, disky SATA, pamětí RAM o velikosti 4GB až 8GB a LCD monitory o velikosti úhlopříček 24“.

Využívanými operačními systémy jsou Microsoft Windows 7 64 bit a Microsoft Windows XP Professional 32 bit, skrze XP mód. Vývojovými nástroji pro tvorbu software jsou aplikace Visual Studio od firmy Microsoft a Delphi od firmy Borland.

Počítače obchodního oddělení jsou osazeny 64 bitovými dvou jádrovými procesory AMD, disky SATA, pamětí RAM o velikosti 2 GB a 22“ a 24“ LCD monitory, které jsou pro potřeby tohoto oddělení dostačující. Operačním systémem těchto počítačů je Microsoft Windows XP Professional 64 bit. Mezi další využívaný software patří poštovní klient Microsoft Outlook a firmou vlastně vyvinutý software, který slouží k evidenci objednávek.

Počítače na oddělení technické podpory jsou osazeny dvou jádrovými 64 bitovými procesory AMD, paměti RAM o velikosti 4 GB a 24“ LCD monitory. Operačními systémy, které jsou využívané na těchto počítačích, jsou Microsoft Windows 7 64 bit a Microsoft Windows XP Professional 32 bit, skrze XP mód. Pro e-mailovou komunikaci slouží poštovní klient The Bat!.

Počítače na testovacím oddělení jsou vybaveny jak staršími komponenty, tak i staršími operačními systémy (např. Microsoft Windows 2000), a to z důvodu testování funkčnosti vyvíjeného software.

Na obchodním oddělení se uskutečňuje také vypalování software na média. Počítače k tomuto určené jsou vybaveny 64 bitovými dvou-jádrovými procesory AMD, disky SATA, pamětí RAM o velikosti 1 GB, sdílenými monitory a vypalovacími CD/DVD mechanikami. Tyto počítače pracují na operačním systému Microsoft Windows XP Home Edition.

Servery společnost Dream Software jsou vybaveny 64 bitovými, dvou jádrovými a čtyř jádrovými procesory firmy AMD. Paměť RAM těchto serverů je o velikosti 2 GB a 4 GB. Pevné disky mají kapacitu od 500 GB po 2 TB. Využívanými operační systémy jsou Windows Server 2003 a Windows Server 2008.

Několik vývojových pracovníků působí externě a komunikují se společností přes internet. Technická specifikace hardware i software osobních počítačů je plně dostačující pro vývoj software v nástroji Visual Studio nebo Borland Delphi. V neposlední řadě je zde zabezpečená telefonní ústředna, zajišťující VOIP telefonii pro potřeby obchodního oddělení, např. pro vyřizování objednávek a pro potřeby technické podpory, kdy je třeba řešit problém interaktivně, pracující na Unixovém systému.

### 3.3. Počítačová síť a aktivní prvky

Jádro počítačové sítě tvoří 4 výkonné servery, které spojují všech 15 počítačů a vytváří mezi nimi interní síť s maximální přenosovou rychlostí 1 Gbit. Na těchto serverech běží Microsoft Windows Server 2003 a 2008. Připojené počítače mají různá oprávnění pro čtení či zápis souborů. Ředitel, správce sítě a programátoři mají neomezené oprávnění. Funguje zde sdílení laserových či inkoustových tiskáren pro potřebu jakéhokoliv uživatele.

První dva servery fungují jako zálohové a jsou pravidelně zásobovány důležitými daty. Pracují pod operačním systémem Microsoft Windows Server 2003. Nejvyužívanější úložiště dat představuje další server běžící pod operačním systémem Windows Server 2008, který disponuje přes 2 TB diskového prostoru a slouží pro sdílení dat v rámci firemní sítě. Další server běží také pod operačním systémem Microsoft Windows Server 2008. slouží k potřebám webové služby.

Mezi další síťové prvky patří telefonní ústředna pro zajišťování VOIP telefonie. Je využívaná pro zákaznickou podporu od 8 do 16 hodin, zajišťovanou dvěma operátory a zároveň pro přijímání a vyřizování objednávek, které zajišťují současně dvě operátorky. Telefonní ústředna běží pod Unixovým systémem s velmi dobrým stupněm zabezpečení.

Veškeré počítače mají možnost přistupovat k internetu přes linky, které dostatečně vyhovují potřebám pracovníků, např. stahování a nahrávání velkých množství dat na FTP servery, VOIP telefonie, čtení a posílání e-mailů, instant messaging, čtení potřebných informací z internetu a nebo stáhnutí velkého množství dat. Jedná se o linky 16 Mbit pro download a 512 Kbit pro upload a také vyhrazenou linku se zaručenou rychlostí 4 Mbit pro download a 4 Mbit pro upload.

Dále je zde bezdrátový router, který zprostředkovává připojení k internetu pomocí bezdrátového signálu pro případnou potřebu připojení pomocí WiFi.
Na střeše budovy je rozmístěná trojice AP, které umožňují připojení z externích lokalit, jež využívají externí programátoři, metodik, školitel a majitelé firmy.

### 3.4. Zabezpečení přístupového bodu uvnitř firmy pro potřeby interních zaměstnanců

V objektu je umístěn přístupový bod, který má vytvořenou bezdrátovou sít na frekvenci 2,4 GHz, na níž není nastaveno heslo pro přístup, je viditelné jméno vytvořené sítě (SSID) a není nastaveno šifrování bezdrátového přenosu. Je nastaveno přidělení IP adresy z DHCP serveru, ve stejném segmentu jako místní síť a je povolena možnost sdílení připojení k internetu.

### 3.5. Zabezpečení přístupových bodů pro potřeby externích spolupracovníků

Jedná se o 4 přístupové body (AP – Acces Point), které nemají splněny jedny ze základních bezpečnostních doporučení. Jedná se např. o prosté skrytí vysílaného názvu bezdrátové sítě, či nastavení hesla kombinací alfanumerických znaků včetně ostatních znaků, jeden z nich dokonce obsahuje zastaralé šifrování WEP. Další dvě AP obsahují standardní šifrování WPA2.

### 3.6. Zabezpečení ADSL modemu

Zabezpečení ADSL modemu je podceněno, je sice nastaveno maskování vnitřní sítě, ale je vypnut firewall a nejsou nastavena pravidla pro příchozí a odchozí komunikaci. Není spuštěna ochrana proti DoS a DDoS útokům (SYN flood, UDP flood, ICMP flood, Smurf, Ping of Death, Land, Teardrop atd.).

### 3.7. Zabezpečení SHDSL modemu

Zabezpečení SHDSL modemu je řešeno jen vzdáleně u poskytovatele, a tudíž není transparentní.

### 3.8. Připojené počítače nepatřící zaměstnancům

Vzhledem k velké oblibě a rozšířenosti bezdrátových sítí se mohou i uživatelé připojení prostřednictvím legitimně se připojujících zařízení externistů dostat až do samotného segmentu místní sítě. Ze vzniklé situace vyplývá, že z počítačů nepřímo souvisejících se samotným chodem firmy (tedy zařízeními připojenými k vlastním soukromým přístupovým bodům externistů) je možné vidět strukturu interní místní sítě firmy Dream Software.

### 3.9. Antivirová ochrana

Antivirová ochrana je zprostředkovávána antivirem AVG 7.5, který zpomaluje testováním metodou heuristické analýzy práci na počítači na nevhodnou míru.

### 3.10. Zabezpečení pomocí firewallu dodávaného s Microsoft Windows XP, 2003, Vista, 2008 a 7

Je využit Firewall dodávaný s Windows XP a 2003, kde je zapnutá možnost filtrace pouze příchozí komunikace, nikoliv odchozí. Na dalších stanicích je použit Firewall dodávaný s Windows Vista, 2008 a 7, kde je již možné filtrování pro odchozí komunikaci zapnout, ale není tak učiněno. Nastavení je tedy výhodné jenom jednostranně, za předpokladu normálního provozu, ovšem není možné zablokovat program u kterého hrozí nevyžádaný odchozí datový tok.

### 3.11. Neaktuálnost verzí používaného software

Obecně se nenazírá na potřebu mít aktuální verze aplikací jako na důležitý prvek. Není zajištěna kontrola, zda jsou staženy a nainstalovány potřebné aktualizace Microsoft Windows, Microsoft Office. Hrozí tedy zneužití bezpečnostních zranitelností. U dvou

klientských stanic a jednoho serveru je diagnostikován problém se stahováním automatických aktualizací samotného operačního systému, takže nejsou instalovány aktuální záplaty. Není zajištěna kontrola aktualizací Microsoft SQL Serveru, nejsou nainstalovány aktuální záplaty ani servisní balíčky a existuje zde velké množství zranitelností. Není prováděna kontrola na aktuálnost webových prohlížečů, e-mailových klientů, komunikačních aplikací pro chat a konferenční hovory, a aplikace od firmy Adobe, s názvy Professional, Acrobat a Flash player. Ostatní využívané aplikace nejsou z hlediska rizikovosti zranitelnosti podstatné.

### 3.12. Rizika spojená s funkcí autorun

Na většině počítačů je povolená funkce autorun pro výměnná media, tedy CD, DVD, či externí úložiště.

### 3.13. Rizika spojená s možností vypnutí serverové stanice bez nutnosti přihlášení

Na serverových stanicích je povolená možnost vypnutí dané stanice bez nutnosti přihlášení.

### 3.14. Autentizace pomocí LM

Na serverových stanicích je povolená možnost autentizace pomocí zastaralé metody LM.

### 3.15. Zranitelnosti v aplikaci Adobe Reader

Na serverových stanicích je zastaralá verze aplikace Adobe Reader, která umožňuje zranitelnosti typu DoS, vzdáleného vsunutí kódu, Cross Site Scripting - XSS, přetečení zásobníku – buffer overflow a další problémy s úniky paměti.

### 3.16. Ostatní rizika

Ostatní rizika jsou spojena se zápisem zdrojového kódu na webových stránkách firmy, kde je možné zneužít zranitelnosti XSS a provedení útoku typu SQL Injection.

### 3.17. Směrnice

Firma disponuje pouze dvěma typy základních směrnic, které existují v písemné podobě. Při podpisu pracovní smlouvy podepisuje zaměstnanec dva dodatky. Podpisem dodatku č. 1 přebírá zaměstnanec hmotnou zodpovědnost za škodu způsobenou vinou nedostatečného zabezpečení objektu firmy při odchodu posledního zaměstnance, tj. např. zanechání pootevřených dveří od samotného objektu, případně nezapnutí zabezpečovacího zařízení svěřeným heslem a opuštění pracoviště. Podpisem dodatku č. 2 stvrzuje zaměstnanec zodpovědnost za legálnost aplikací a obsahu dat na úložných médiích, tj. především pevných discích na své pracovní stanici. Veškeré další směrnice jsou řešeny ústní domluvou a nemají formální podobu. Dají se stručně charakterizovat následujícími výroky.

O veškerou funkčnost hardware a software firmy Dream Software se stará správce či jeho zástupce. K jeho povinnostem patří mimo jiné správa síťové infrastruktury a ochrana dat zálohováním. Jakékoliv zásahy nekompetentní osobou jsou zakázány. Jeho ohodnocení probíhá individuálně na základě délky trvání řešení problému.

Vždycky pokud si někdo není jistý, jak má pokračovat při nestandardní akci, je doporučeno zeptat se správce, či jeho zástupce.

Nákup nového zařízení, systémů a aplikací se předem důkladně projednává a řeší v kruhu kompetentních osob.

Pro svou činnost využívá společnost Dream Software vlastní komplex nemovitostí. Hlavní odpovědnost za péči o nemovitosti, výrobní zařízení a vybavení pracovních prostor nesou majitelé firmy.

Hlavním důvodem pro nevypracování podrobných směrnic v oficiální textové podobě je dle majitele firmy velmi dobrý vzájemný vztah mezi vedením a zaměstnanci, i mezi zaměstnanci samotnými. Firma se dlouhodobě a úspěšně snaží o odbourání bariér typu „zaměstnavatel – zaměstnanec“, „zaměstnanec - zaměstnanec“ a o přechod na vztah

přátelský, ve kterém panuje větší míra důvěry, vzájemné pomoci a tolerance při řešení různých situací.

# 4. Teoretická východiska řešení

## 4.1. Politiky a procedury

Jedná se většinou o nejzákladnější obraz, jak konkrétní společnost nazírá na otázku zabezpečení. Jako příklad se dá uvést procedura, jak postupovat při zapomenutí důležitého hesla. Pokud není přesně definována, lze ji negativní manipulací zneužít a tak obejít všechny další úrovně zabezpečení. (BITTO 2006: 30)

## 4.2. Fyzická bezpečnost

Je pochopitelné, že pokud není dobře chráněno datové centrum nebo celá společnost, např. zámky, kamerovými systémy nebo například HSM a TPM moduly, lze dosáhnout snadného zneužití. Je potřeba nadefinovat oprávněné osoby, kterým je umožněn přístup, popř. předány oprávnění. Také je potřeba centrum zabezpečit proti přírodním katastrofám. (EISENKOLB 2003: 5)

## 4.3. Autentizace a řízení přístupu

Samotný proces autentizace probíhá v jakémkoliv informačním či operačním systému, kde je potřeba sdělit informace o své identitě a určit tím, jak má systém entitu identifikovat. Následně je třeba potvrdit vhodným způsobem pravdivost předchozího tvrzení. Autentizace může probíhat třemi přístupy. První nejrozšířenější je na základě nějaké znalosti, např. heslo, či PIN. Druhý přístup je na základě vlastnictví nějakého předmětu, např. čipové karty nebo USB klíče. Zde je třeba myslet na možnost zneužití ztraceného zařízení, což se provádí nutným doplněním autentizace o jednoduché heslo. Třetí přístup je na základě biometrických údajů, např. otisk prstů nebo obrazu oční sítnice.

Řízení přístupu probíhá na základě přidělení přístupových práv, což rozhoduje administrátor podle potřeby a rizik jednotlivého uživatele pracovat s povolením přístupu k daným datům či službám. Tento proces se nazývá autorizace.

DOSEDĚL (2004: 77) doplňuje, že žádný uživatel nebo proces nemůže vyčerpat prostředky systému natolik, aby znemožnil jejich využívání ostatním procesům nebo uživatelům.

### 4.4. Bezpečná síť - firewall

Pokud se počítač připojí k internetu nebo jiné počítačové síti, vzroste velmi značně množství možného nebezpečí, proti kterému je třeba počítač chránit. Jako velmi dobrý sluha se jeví kvalitně nakonfigurovaný firewall. Jedná se ve skutečnosti o počáteční obrannou linii každé jednotlivé počítačové sítě a právě proto je zabezpečení velice důležité a velmi obtížné. Jedná se o nejpoužívanější technologii, která by měla blokovat patřičné porty, bránit se nejrozšířenějším druhům útoků a kontrolovat veškerý síťový provoz na aplikační vrstvě. (BITTO 2006: 31)

Firewall umožňuje řízení a zabezpečování provozu v síti, mezi jednotlivými počítači připojenými přímo do sítě s různým stupněm důvěryhodnosti a zabezpečení.

Nejstarší a nejjednodušší forma je technologie paketových filtrů. Kontrola probíhá na 3. a 4. vrstvě modelu OSI. Je přesně dáno odkud (IP adresa, port) a kam (IP adresa, port) by měl být paket doručen. Největší výhodou je velmi svižná doba zpracování a hlavně proto se i dnes používají firewally s paketovými filtry tam, kde není potřebná důkladnější analýza procházejících paketů, ale kde je žádaná vysoká rychlost přenosu velkých objemů dat. Největší nevýhodou je velmi nízká úroveň kontroly vzniklých spojení a podle DOSEDĚLA (2004: 117) také nemožnost analyzovat procházející data a povolovat či zakazovat jejich průchod podle jejich významu.

Další generací, i když ne o moc starší, je technologie aplikačních bran, jinak nazývaná technologie proxy firewallů. Kontrola probíhá na 7. vrstvě modelu OSI. Tato technologie dokáže prozkoumat aplikace nebo protokoly (např. FTP, DNS, prohlížení internetu) a umí rozpoznat a zastavit nechtěný protokol, který může ohrozit systém. V tomto případě by to znamenalo, že pokud uživatel vyšle někam do internetu požadavek, tak je povoleno, aby se mu vrátila odpověď, ale již se nemůže stát, že by například nějaký FTP server sám inicializoval a snažil se navázat připojení k uživateli z internetu.

Firewally bývají často doplňovány o funkci tzv. překladu adres (Network Address Translation). Bezpečnostní výhoda spočívá ve skrytí několika soukromých IP adres umístěných v místní síti (LAN) a vystupování každé z nich pod jedinou, internetovým poskytovatelem (ISP) přidělenou, veřejnou adresou. Proto nehrozí riziko zahájení komunikace s počítačem skrytým za routerem, za předpokladu, že se používá moderní router, který se nenechá přesvědčit neoprávněnou aplikací, aby mu sdělila adresy vnitřní sítě.

Podle DOSTÁLKA (2001: 193) je možné NAT využít pro řešení i zcela odlišného problému, a to rozložení zátěže výkonu serveru s aktivovanou komponentou TCP Load Distribution.

IDS (Intrusion Detection System), nebo-li systém na detekci útoků, obecně detekuje nechtěné manipulace se systémem, většinou skrze internet. IDS se používá pro detekci některých škodlivých prostředí, která mohou zneškodnit zabezpečení počítačového systému. Zabraňuje taktéž útokům na zranitelné služby a data, útokům na aplikace, neautorizovaným přístupům a přístupu k citlivým datům. Samozřejmě brání všem známým druhům malware. Jedná se o nejkvalitnější zařízení současnosti, které si ovšem vyžádá mnoho času pro správné nastavení, ale výhodou je možnost si některé IDS pořídit i zdarma a v licenci GNU/GPL, takže je možné si zdrojové kódy upravovat přímo na míru vlastní situaci, např. ve formě aplikace Snort. Stejně tak existují i placené varianty, ve kterých jsou zadarmo služby technické podpory. THOMAS (2005: 253) trefně uvádí, že tajemství správné konfigurace a zprovoznění detekčního systému IDS je „pohrát“ si s ním a jemně ho doladit.

Zajímavá technologie, která má jisté podobnosti s firewallem a je velmi výhodná ve spojení s IDS, se nazývá Intrusion Prevention System (IPS), tzv. systém pro prevenci narušení. Jedná se o bezpečnostní zařízení monitorující síť nebo systémové aktivity, které zaznamenává škodlivé nebo nevhodné činnosti a dokáže je v reálném čase zablokovat nebo jim dokonce předcházet. Tato technologie monitoruje probíhající datový tok a umí si z něj vybrat jen špatné pakety, ty vyřadit a zbytek nechat volně pokračovat. IPS je v současnosti na špici technologie zabezpečení počítačových systémů a souvisejících zařízení, ale jejímu výhodnému a žádanému nasazení do běžnějšího provozu menší firmy brání vcelku velké vstupní a průběžné náklady spojené s údržbou systému a zakupováním pravidelných aktualizací instrukcí a databází škodlivých kódů pro skenovací software samotného zařízení. Limitující může být i propustnost kontrolovaných dat, jejíž velikost také hraje podstatnou roli v celkové ceně zařízení.

Kvalitní nastavení firewallu umožňuje zabránit výše zmíněným DoS a DDoS útokům.

## 4.5. Škodlivý software

V následujících odstavcích práce popisuje, s jakými hrozbami se společnost, či jednotlivec při nedokonalém zabezpečení počítačové sítě, či počítače může setkat.

Existuje mnoho druhů škodlivého software, obecně označovaného jako malware a mnoho způsobů, jakými škodí. Obecně nejrozšířenější formou infiltrace je virus. (WOLFE et al. 2004: 353)

Jako první lze uvést tzv. souborové viry, které napadají spustitelné soubory nebo ovladače, a při jejich spuštění se snaží o rozmnožení. Jedná se především o soubory typu COM, EXE, BAT nebo SYS. V současnosti souborové viry napadají nejvíce 32-bitové Windows, konkrétně se šíří pomocí WIN32 API (Application Program Interface), tedy množinou funkcí Windows 9x a NT (NT, 2000, XP, 2003, Vista, 2008, 7).

Nejstarším typem virů jsou tzv. boot sektorové viry, které napadají systémovou oblast disku nebo médií, tzv. Master Boot Sector, a tím si zajišťují spuštění pří startu čtení z tohoto oddílu vnějších pamětí.

Mezi další nebezpečí se řadí červi (worms), kteří se šíří pomocí elektronické pošty, ale častěji přímo v síťových paketech. Pracují na nižší úrovni než klasické viry. Jejich výskyt závisí na zneužití bezpečnostních děr v operačním systému a šíření na množství rozšířenosti bezpečnostních děr v software. Vedlejším efektem může být zahlcení sítě - jak místní, tak vnější. (HLAVENKA 2002: 271)

Mezi nepříjemné, špatně analyzovatelné a téměř heuristickou analýzou nemožně zjistitelné viry jsou tzv. High Level Language viry. Jsou vytvořené ve vyšších programovacích jazycích, např. C++, Delphi nebo Basic. Šíří se především elektronickou poštou.

Mezi méně nebezpečné hrozby, které se dají považovat někdy pouze za špatný vtip, patří tzv. hoax, což je poplašná zpráva, která obvykle varuje před neexistujícím nebezpečím. Ono nebezpečí může vést k šíření poplašné zprávy, a tak se lavinovitě šíří.

Dalším nebezpečným druhem malware jsou makroviry. Jak již název napovídá, jedná se o viry napadající makra vytvořená v balících Office, např. Word nebo Excel.

Mezi další hrozby patří tzv. parazitické viry, jejichž tělo se připojí na začátek, střed nebo nejčastěji konec souboru a při jeho spuštění se aktivují.

Zřejmě nejjednodušší formou infekce, při níž dojde k přepsání a tím pádem i zničení původní části kódu programu, jsou tzv. přepisující viry. Původní část je tak nenávratně

ztracena a spuštěním souboru dojde pouze k aktivaci viru, snažícího se o vlastní replikaci, nikoliv ke spuštění vlastního programu.

Další možnou nákazou jsou tzv. retroviry, snažící se vypnout nebo dokonce vymazat antivirové programy. Pokud pomineme jednoduché pokusy skriptovacích virů v podobě dávkových souborů, mohou nás reálně ohrozit pouze škodlivé kódy obsažené ve Visual Basic Scriptech nebo Java Scriptech.

Trošku mimo stojí adware, který obtěžuje uživatele reklamou, např. v podobě pop-up oken a BITTO (2006: 161) tvrdí, že si může najít cestu do každého počítače a zaskočit tak uživatele náhlým přívalem obtěžujících reklamních oken. Může však mít i výhody, kdy aplikace, která je distribuována s reklamou uvnitř, má více pokročilejších vlastností, než aplikace která je jenom volně dostupná, ale reklamu vloženou nemá.

Omezující a na hranici legálnosti stojící je spyware, který skrze internet odesílá data bez poskytnutí souhlasu oprávněného uživatele. Může se jednat narozdíl od backdooru o data, jako je např. historie navštívených stránek nebo názvy používaných programů. Jeden z lepších důvodů pro tvorbu spyware je snaha o zjištění zájmů oprávněného uživatele, který může být využit pro lepší nabídku služeb. Nebezpečné je ovšem to, že se neví, kdy může být tato činnost zneužita. WOLFE et al. (2004: 345) upozorňuje, že jakmile je spyware v systému, může získat naši emailovou adresu spolu se všemi adresami z našeho adresáře.

Poměrně nebezpečným typem malware je trojský kůň, který se tváří jako užitečný program. Ve skutečnosti je to ovšem jenom škodlivý kód, který není schopen replikace ani napadání souborů, ale jeho nebezpečí se skrývá v jeho schopnosti umožnit přístup do PC zvenčí. Odstranit lze jednoduchým smazáním dotyčného souboru. ( ... citace ... )

Dynamické mutace klasických virů, které je čím dál tím těžší rozpoznat, se nazývají "oligomorfní", "polymorfní" a stále častěji "metamorfní" viry, které šifrují část sebe sama, nebo jinak upravují vlastní kód jako metodu zamaskování před rozpoznáním virovými databázemi.

V poslední době patří mezi často zmiňovaný problém phising (český slangový výraz je rhybaření). Jako příklad lze uvést e-mail, který přijde, a v něm je odkaz na webovou stránku, která je většinou velmi podobná oficiálnímu vzhledu webové stránky nějaké důvěryhodné organizace, ve většině případů banky, a vyžádá si informace, že vznikla nová verze internetového bankovnictví a že je třeba do nové databáze zadat přístupové

jméno a heslo. Většinou je e-mail psán s kladením tlaku na psychiku uživatele, protože ve stresu se zvyšuje tendence dělat neuvážené činnosti. Uživatel tak může např. pod pohrůžkou zrušení internetového bankovnictví relativně jednoduše poskytnout jméno a heslo a odeslat je na podvrženou adresu. Pak už hrozí zneužití uživatelova internetového bankovnictví a neoprávněná osoba může s účtem nakládat dle nastavených oprávnění. Stránka může být k nerozpoznání stejná jako originální vzhled původního důvěryhodného webu, s jednou změnou, a to, že má v adresním řádku prohlížeče jinou adresu než obvykle. Pokud uživatel nepoužívá alespoň u elektronického bankovnictví dvojí autorizaci, např. přihlašovací jméno a heslo a následné upozornění formou SMS na mobilní telefon, vystavuje se velkému riziku, ztrátě vložených financí, či přinejmenším cenných informací. Mnohdy než si oprávněný uživatel uvědomí, co se mu stalo, může být na nápravu pozdě.

## 4.6. ANTIMALWARE

Proti výše zmíněných hrozbám lze počítač bránit pomocí antivirového programu. Antivirový software se snaží identifikovat, zastavit přístup, léčit, popř. vymazat škodlivý software snažící se dostat k počítači a jeho aplikacím nebo systému. Název vznikl na základě dřívějších příkladů bojů s počítačovými viry, ovšem moderní antivirový software je nyní naprogramován na boj proti mnoha druhům hrozeb. Např. červy, phising, rootkit, trojani a další druhy malware. Obvyklý průměrný antivir klasicky používá několik rozdílných metod obrany.

Jedna metoda spočívá ve skenování souborů proti známým virům, které vyhovují definicím ve virové databázi a hledají podezřelé prostředí v jakémkoliv programu spuštěném v počítači, který může indikovat infekci. Další metoda se nazývá heuristická analýza. Její pomocí lze analyzovat využívaná data a na základě pokročilých metod odhalovat škodlivé části kódu. Existují i další rozšířené vlastnosti testování.

Většina antivirů používá metody s důrazem na skenování souborů a vyhodnocování na základě známých definic.

Antivirus zpracovává soubory a porovnává je se známými příznaky ve své virové databázi. Jestli se část kódu shoduje, antivirus udělá některý z následujících postupů:

a) pokusí se vyléčit soubor odstraněním škodlivého kódu viru

b) uloží soubor do virové karantény, takže virus není přístupný a nemůže se dále šířit.

c) smaže zavirovaný soubor

K dosažení dlouhodobějšího stavu bez infekce viru je nutné co nejrychleji nainstalovat nové bezpečnostní aktualizace. Vše samozřejmě probíhá online. Pokud se někde najde soubor s virem, který ještě není ve virové databázi, může být zaslán do antivirového centra, kde se většinou velmi rychle prozkoumá a případně zahrne do virové databáze pro pozdější snadnější identifikaci, a nebo se zjistí, že jde o neškodný program, který např. heuristická analýza chybně označila za škodlivý. BITTO (2006: 140) dodává, že ve většině antivirových programů je volba nastavení citlivosti heuristické analýzy, kde při příliš nízké úrovni mohou některé viry testem projít, a opačně.

Antivirový software typicky může hledat viry za jakékoliv běžné práce s operačním systémem a nainstalovanými aplikacemi, většinou kontroluje soubory, které jsou právě vyžadovány pro práci.

Bohužel se čím dál tím častěji objevují různé dynamické mutace jako jsou oligomorfní, polymorfní nebo metamorfní viry, které modifikují sebe sama nebo se zašifrují, a tak oklamou známé signatury v databázích.

Metodu, kterou používá stále více antivirových programů, je tzv. whitelisting. Jedná se o udělování povolení pro spuštění důvěryhodným programům a automatickou blokaci malware. White listy jsou především vytvářeny administrátory.

Moderní metoda používaná některými antiviry se nazývá heuristická analýza. Její činnost se dá vyjádřit charakterizovat jako pokus o napodobování začátku kódu, každého spouštěného souboru, kterou antivir provede před skutečným spuštěním. Pokud spuštěný program projeví prvky sebe modifikujícího kódu nebo se pokusí najít další spustitelné soubory (což je klasické chování viru), antivirus soubor označí jak zavirovaný. Bohužel má tato metoda i nevýhody, protože někdy hlásí i o nezavirovaném souboru, že je napadený.

Další metodou je používání tzv. sandboxu. Snaží se napodobovat operační systém a spouští v této virtualizaci spustitelné podezřelé soubory. Po ukončení software analyzuje sandbox, jestli nějaké změny neindikují virus. Protože je ovšem tato metoda náročná na systémové prostředky, je spouštěna na požádání. Neúspěchy se vyskytují u případů, kde pokračování programu má více variant, jež vyúsťují do rozdílných situací. Některé virové skenery varují, pokud určitý typ souboru obsahuje obvykle častěji virus než jiný.

Velmi nebezpečné viry jsou viry s příznačným označením Zero Day, což je vir rozšiřující se ještě před zjištěním, že existuje, a tedy před uvolněním antivirové záplaty, a proto jej lze najít jen pomocí heuristiky používaného antimalwarového řešení.
Obecně lze říct, že nejlepší antiviry mají v testech úspěšnost vyhledání a vyléčení malware blížící se sto procentům. Obzvláště úspěšné jsou antiviry, které používají současně více skenovacích jader a mají velmi dobře propracovanou heuristickou analýzu testování a efektivně provádějící behaviorální analýzu, ovšem úspěšnost léčení se někdy zvětšuje taktéž s vyšší zátěží systému a nárocích na obsluhu a následném zpomalení potřebné činnosti. Důležitá je včasnost stažení aktualizací samotného řešení. (THOMAS 2005: 289)

### 4.6.1. ANTIVIRUS NOD32

Jako nejlepší antimalwarové řešení se dle dostupných informací projevil NOD32. Byl již 50krát testován světově uznávaným serverem Virus Bulettin a z toho 47krát oceněn jako nejlepší testovaný produkt. Antivir vytváří slovenská společnost Eset Software, která začala působit na trhu v 90. letech 20. století, kdy se malware začal čím dál tím běžněji šířit. Vytváří jak klientské tak serverové verze. Serverové verze lze používat na Microsoft Windows a Unixových systémech. Eset vytváří kompletní balíky obsahující antivir, antispaware, firewall se systémem IDS, antispam filtrující nevyžádanou poštu, včetně phishingu a např. funkcí správy vzdálené plochy. Bude popsána verze NOD32 Antivirus Business Edition obsahující antivirus, antispyware a možnost sledování a ovládání vzdáleně. Antivir se skládá z několika částí a to skeneru, který prohledává oblasti, které si zvolí uživatel, a čtyřech monitorovacích zařízení, které pracují v reálném čase. Otestování skenerem může povolit uživatel a může si vybrat důkladnost testu, umístění zdrojů apod. Další součásti monitorují různé vstupy umožňující vznik hrozby. Jednotlivě to pak jsou tzv.:
AMON což je Antivirus Monitor zajišťuje skenování souboru před viry v takovém pořadí, jaké si určuje systém pro splnění požadavků uživatele.
DMON - Document Monitor zajišťuje skenování dokumentů např. z kancelářského balíku Office proti makrovirům.

IMON - Internet Monitor zajišťuje kontrolu a případné přerušení průběhu výměny dat s HTTP nebo např. POP3, či SMTP servery, a zabránění vniknutí malware na disk počítače společně se stahovanými daty.
EMON - E-mail Monitor zajišťuje pomoc při skenování příchozích nebo odchozích e-mailů přes rozhraní MAPI používané např. v Microsoft Outlook nebo Microsoft Exchange Client.
(BITTO 2006: 147)
Jedna z vlastností, kterou NOD32 vyniká nad ostatními, je schopnost využít pokročilé technologie pro-aktivní ochrany, formy heuristické analýzy tzv. ThreatSense, a zachytit škodlivý kód, který ještě není obsažen ve virové databázi.
NOD32 je naprogramovaný z velké části v jazyce symbolických adres, což přispívá k velmi nízkému využití systémových prostředků a k velmi příznivé rychlosti vyhledávání, kterou přesahuje všechny ostatní antivirové produkty jiných známých a srovnatelných výrobců. Dokáže přibližně zpracovat více než 23 MB za vteřinu na počítači s procesorem Intel Pentium 4 nebo jeho výkonnostní obdobou Athlonu od AMD, a v průměru využívá necelých 20 MB paměti.
Podle renomovaného internetového časopisu, který testoval NOD32 v roce 2005, pracuje až pětkrát rychleji než jiné antivirové programy.
Mezi nezbytné funkce patří velmi častá aktualizace nových virových bází z centrálního serveru Esetu pro nejaktuálnější možnou ochranu, v průměru přibližně jednou za 2 hodiny.
Další výhodou je možnost centrální správy, a s tím související vzdálenou instalací nových verzí programu, sledování aktuálního stavu, vzdáleného spouštění testů, import nastavení samotného programu. Vše lze provádět hromadně a vzniká tak velmi výrazná úspora času a potažmo peněz za mzdu pracovníka, a odpadají starosti ostatních zaměstnanců se starostí o zabezpečení, jelikož se stav každou minutu obnovuje, případný problém lze velmi rychle zjistit a řešit.
Instalace antiviru NOD32 je velice snadná a intuitivní. Velmi dobrá konfigurace je standardně nastavena. Za zmínku stojí nastavit aktualizaci virové databáze ihned po jejím zveřejnění. V pokročilejších volbách nastavení, které se objeví po stisku klávesy F5, je dobré nastavit v záložce „antivirus a antispyware“ a v její podsložce „rezidentní ochrana souborového systému“ a v další podsložce s názvem „nastavení skenovacího

jádra ThreatSense“ volbu „rozšířená heuristika“ a „detekci potenciálně zneužitelných aplikací“. V nabídce léčení je vhodné nastavit volbu „přísné léčení“ a v nabídce „ostatní“ je výhodné nastavit volbu „zapisovat všechny objekty do protokolu“, pro případné čtení a analýzy. Vše ostatní je velmi dobře nastaveno standardně.
Typickou možností síťových antivirových řešení je zrcadlení aktualizací.
Programové aktualizace včetně aktualizace virové báze jsou staženy od výrobce AV systému z internetu pouze dedikovaným počítačem a následně jsou nabídnuty ostatním stanicím a serverům v lokální síti. Přínosem tohoto řešení je významné snížení zátěže internetové linky, jelikož ostatní stanice a servery provádějí aktualizaci v rámci lokální sítě.
Řešení bývá realizováno nejčastěji prostřednictvím protokolu HTTP či HTTPS,
k vidění jsou řešení na bázi síťově sdíleného adresáře, odkud si jednotlivé stanice požadované aktualizace stahují.

### 4.7. Zodpovědná osoba

Vždy by měla být vytvořena funkce pro člověka, který se bude o zabezpečení starat a kdo bude za chyby přebírat zodpovědnost. V průběhu času se vžilo označení CISO, tedy Chief Information Security Officer. Takovýto člověk by měl v písemné podobě vypracovat vizi, kam se bude zabezpečení firmy dále vyvíjet. Tato osoba by měla také vypracovávat analýzy rizik a vytvářet krizové plány. Samozřejmostí je vypracování směrnic, se kterými je potřeba seznámit stávající zaměstnance a hlavně nově příchozí. Tato osoba by měla číst a analyzovat uložené logy zařízení. Například logy routerů, firewallů a antivirů.

### 4.8. Zálohování dat

Mělo by fungovat kvalitní a časté zálohování vytvořené práce na jiné médium, než na které se práce pravidelně ukládá, pro případ havárie zařízení a následné ztráty dat. Vždy by měla být vytvořena funkce pro člověka, který se bude o proces zálohování starat a přebírat zodpovědnost za případné nedostatky. Stejně tak by měla pověřená osoba analyzovat vznikající situace a následně upravovat časový harmonogram zálohování a zvažovat systém záloh. HORÁK (2001: 89-91)

### 4.9. FTP vs SecureFTP

Vzhledem k potřebě nahrávat na server poskytovatele hostujícího webové stránky data, která by si mohl stáhnout uživatel, je vhodné využití SecureFTP přenosu. Při běžném přenosu přes FTP veškerá data, včetně přihlašovacích údajů, tečou nezabezpečeně. Je poté velmi snadné data a přihlašovací údaje odposlechnout a zneužít.

### 4.10. Počítače

Jak klientské, tak serverové stanice musí být dobře zabezpečeny. Dá se tak učinit např. pravidelným stahováním a instalací bezpečnostních aktualizací od výrobce operačního systému, zesílením bezpečnostní konfigurace, vylepšeným a do hloubky propracovaným nastavením firewallu, instalací a používáním antimalwarového řešení obsahující antivirovou, antispywarovou, antirootkitovou a antibotovou ochranu a celý nástroj je pravidelně zásobován nejaktuálnějšími definicemi staženými z aktualizačního serveru výrobce.

### 4.11. Aplikace

Řešení na aplikační vrstvě je jedinečné pro každou konkrétní aplikaci, která má být zabezpečována. Základním principem zabezpečení je pokaždé její vyladěná konfigurace zajišťující správné fungování. Veškeré ostatní komponenty, jež nejsou využívány, se doporučují odstranit, což snižuje prostor pro případný neoprávněný průnik.

### 4.12. Útoky odmítnutí služby (DoS)

Mezi síťové útoky patří i Denial of Service (DoS), útok tzv. odmítnutí služby. Jedná se o útok na internetové služby nebo webové stránky, způsobem přehlcení nelegitimními požadavky a dočasným pádem nebo nedostupností služby pro legitimní požadavky.

Všechny typy DoS a DDoS útoků se vyznačují několika společnými charakteristikami:

1) Zahlcení provozu na síti nelegitimními požadavky, které brání protékání požadavků legitimních.
2) Zabránění nebo přerušení oprávněnému zařízení v přístupu k požadované službě.
3) Možné narušení správného konfiguračního nastavení.

4) Extrémní zatížení procesoru cílového serveru.

5) Vsunutí nesprávných hlášení do sekvence instrukcí v programu, které mohou způsobit pád databáze.

6) Pád samotného operačního systému.

THOMAS (2005: 279) tvrdí, že uvedený typ útoků je z pohledu obrany jedním z nejobtížnějších, protože mnohé útoky zneužívají normální provoz, který se v sítích běžně vyskytuje.

Protože má společnost neustále spuštěnu webovou službu, je potřeba ji proti těmto útokům bránit. V nastavení routeru je několik možností, které brání nejrozšířenějším útokům.

Jedná se o:

a) SYN flood

b) UDP flood

c) ICMP flood

Například princip útoku SYN Flood je předstírání, že se chce neoprávněný počítač propojit s počítačem legitimním. Když legitimní strana odpoví, nelegitimní už neodpoví nazpět. To počítač oběti zmate a pošle odpověď znovu. Než se spojení ukončí kvůli vypršení času na odezvu tzv. timeout, což mohou být i desítky vteřin.

### 4.13. Operační systém

Je známo, že Microsoft Windows patří mezi nejméně bezpečné operační systémy, což vychází z jeho samotného návrhu a koncepce přístupu k zabezpečení, a také částečně z jeho obrovské popularity, potřeby být maximálně použitelný a jednoduše ovladatelný. Samozřejmě existují i speciální systémy specializující se primárně na zabezpečení proti neoprávněné manipulaci, jako je např. OpenBSD, či speciálně vytvořené linuxové distribuce, ovšem jejich uplatnění a rozšíření je limitující nesrovnatelně menším počtem využitelných, vytvořených a volně dostupných aplikací. Pozitivní na takových systémech je i vlastnost šíření velké většiny aplikací zdarma, a s otevřeným zdrojovým kódem, pro možnou úpravu a vylepšení při znalosti programovacího jazyka, ve kterém je aplikace či systém napsán.

Nabízí se možnost uplatnit některý speciální operační systém zaměřený na bezpečnost, jako např. webový či poštovní server, ale je potřeba počítat se zaškolením administrátora, či placením specialisty, který vše potřebné již umí.

Při zaměření na operační systém Microsoft Windows je potřebné vědět, že v něm existují chyby staré i několik let, které ještě nejsou opraveny, a jsou tedy za podmínek znalosti zranitelnosti a souvisejících informací zneužitelné vždy, pokud se tomu nezabrání na předchozí vrstvě zabezpečení. Lze s mírnou nadsázkou říci, že v administrátorských právech tkví 2/3 všech zranitelností samotného operačního systému Microsoft Windows. Pokud by se využívala standardně pouze práva standardního uživatele, nebylo by možné bez práv správce instalovat aplikace, což by sice na jedné straně razantně zvýšilo zabezpečení počítače, ale na druhé straně by omezilo rychlost běžné práce a přidělalo práci při administrování prováděném pod vyšším uživatelským oprávněním v souvislosti s instalací potřebných a využívaných aplikací.

### 4.14. Funkce Autorun

Jedná se o funkci, která automaticky po připojení externího disku či vložení CD nebo DVD vyvolá možnost automatického spuštění. Již dlouhou dobu se zneužitím této funkce šíří malware, kdy se po vložení či připojení externího média automaticky spustí dávkový soubor, který se pokusí malware nainstalovat. Proto je lepší ji standardně vypnout.

### 4.15. Útok typu CSRF

Celý útok spočívá v přimění uživatele, aby navštívil stránku s napadenou aplikací, ve které se provádí procedura, o které uživatel neví, např. při přihlášení k legitimní webové aplikaci. Po té již mohou být data legitimního uživatele kompromitována. Tato zranitelnost je např. v Adobe Flash přehrávači ve verzi 8.0.34.0 a dřívější.

### 4.16. Zamezení možnosti vypnutí systému bez přihlášení

V nastavení Windows je možné zamezit vypnutí systému z přihlašovací obrazovky bez samotného přihlášení se k uživatelskému účtu. Je to doporučená volba a na druhé straně potenciální zranitelnost.

### 4.17. Využití autentizace pomocí NTLM oproti LM

V nastavení Windows je možné nastavit kvalitnější autentizační proces, při kterém se eliminují zranitelnosti typu odposlouchávání komunikace.

### 4.18. Zranitelnosti operačního systému

Jedná se o soubor nepodchycených vlastností operačních systémů, který v návrhu nebyl ošetřen proti neoprávněnému průniku. Systém může být sice funkční, použitelný, odpovídající potřebám, ale málokterý je dokonalý z hlediska zamezení neoprávněného přístupu. Pokud se včasně neaktualizuje, zvyšuje se riziko nelegitimních operací.

### 4.19. Zranitelnosti prvků síťové infrastruktury

Stejně jako operační systém potřebuje nové instrukce pro lepší, bezpečnější a spolehlivější provoz aktualizace, prvky síťové infrastruktury potřebují aktualizovat firmware. Ten se dá stahovat ze stránek výrobce.

### 4.20. Aktivní prvky síťové infrastruktury

Je velmi důležité samotné nastavení prvků jako jsou modemy, přístupové body, routery, rozbočovače nebo různé kombinace předchozích zařízení. Už jejich koncepce a správné nastavení dokáže velmi výrazně zabezpečit celou počítačovou síť a velmi ulehčit následující práci a snížit rizika hrozeb. Existuje velmi mnoho nastavení zabezpečení síťové infrastruktury. Mezi nejzákladnější patří filtrování firewallem, ochrana proti DoS útokům, filtrování přístupu na základě předem daných kritérií, šifrování, skrývání samotných zařízení proti neoprávněnému zjištění, volba přístupu k těmto zařízením a samozřejmě volba hesel k různým nastavením a samotným přístupům do sítě.

## 4.21. Síťové útoky

Řadí se sem útoky na přístupové body pomocí zjišťování hesla pro povolení přístupu. Pokud je zabezpečení řešeno starým typem zabezpečení typu WEP, je zjištění hesla při relativně mírném datovém toku otázkou několika dnů, ovšem při relativně vyšším datovém toku může odhalení hesla trvat jen pár hodin.

Dalším síťovým útokem se dá nazvat skenování sítě, zjišťování její struktury a následného připojování do okruhu, který je vyhrazen pro legitimní zařízení.

Následně se dá pokoušet o využívání zranitelností jednotlivých zařízení.

## 4.22. Cross site scripting - XSS

XSS je jednou z metod, při které se naruší správná funkčnost webových stránek, zneužije se neošetřeného vstupu pro vkládání údajů a pro podstrčení nelegitimního javascriptového kódu, což může vést ke změně vhledu, nefunkčnosti, získání citlivých údajů návštěvníků nebo také phisingu.

## 4.23. SQL Injection

SQL Injection je útok na samotnou databázovou aplikaci, vsunutím nelegitimního kódu. Následně probíhá vykonání vlastního SQL dotazu. Zabránit útoku se dá ošetřením vstupu, před vykonáním transakce.

## 4.24. VPN

VPN, neboli Virtual Private Network, tedy virtuální privátní síť, funguje jako zabezpečený most (většinou s 40-256 bitovým šifrováním přenášených dat) mezi dvěma síťovým rozhraními, který umožňuje zabezpečenou komunikaci po síťovém protokolu, který může být zprostředkován buď na lokální, nebo globální úrovni. Např. přímým dosahem WIFI připojení k cíli, nebo pomocí internetu odkudkoliv na světě. Rychlost spoje se pak analogicky odvíjí od rychlosti daného spojení. (THOMAS 2005: 192)

# 5. Vlastní návrhy metod řešení

Na základě výše popsaného stavu zabezpečení počítačové sítě ve firmě Dream Software a s využitím teoretických znalostí jsem firmě navrhl varianty, které popisují možnosti zlepšení systému ochrany počítačové sítě v několika krocích, jejich finanční stránku a časový harmonogram. Vše z návrhu se mně s pomocí specialisty z externí firmy podařilo přenést do reálné podoby a implementovat.

Návrh, který jsem firmě předložil, se skládal z několika kroků, jejichž kompletní realizace by v budoucnu měla výrazně zvýšit obranyschopnost všech prvků počítačového vybavení firmy.

Návrh byl sestaven jednoduše tak, aby kladl pokud možno co nejnižší nároky na obsluhu a údržbu používaného software a hardware.

Důležitým parametrem byla i snaha o minimalizaci nákladů při realizaci a pro funkčnost návrhu.

## 5.1. Zabezpečení vnitřního přístupového bodu

Po realizaci mého návrhu byla nastaveno silné heslo přístupového bodu, skládající se z alfanumerických a diakritických znaků. Dále bylo nastaveno šifrování WPA2, skrytí vysíláni názvu sítě – SSID, a s tím vším související odpojení aktivního nelegálního připojení, které na přístupovém bodě bylo aktivní. Zmíněné změny do budoucna přinesou vyhnutí se velkému aktivnímu riziku, které by mohlo způsobit rozsáhlé škody.

## 5.2. Nákup nového antivirového řešení

Jelikož podstatné množství možných rizik způsobuje malware, navrhl jsem firmě zvážit možnost nákupu kvalitnějšího antivirového řešení, které by odpovídalo současným požadavkům zaměstnanců a zaměstnavatele. Antivirový produkt jsem vybral na základě pěti hlavních kritérií v porovnávání jednotlivých řešení různých antivirových firem. Těmito kritérii byla rychlost a kvalita testování, možnost vzdálené správy, podložená dlouhodobá kvalita a stabilita produktu a přijatelnost ceny. Dle zmíněných parametrů jsem navrhl a zvolil NOD 32 Bussines Edition s funkcí vzdálené správy. Produkt byl implementován a je nyní využíván na všech stanicích. Monitorován a spravován je

vzdáleně administrátorem, který takto přebírá zodpovědnost za případné nedokonalosti. Zřídil jsem funkci zrcadlení aktualizací, a tak ulehčil internetové konektivitě.

### 5.3. Nákup nového routeru s nastavením firewallu

Dalším bodem návrhu bylo nakoupení velice kvalitního routeru Mikrotik, na kterém byla nastavena pravidla pro adresování datových toků. Společně s překladem adres se do tohoto routeru nasměrovala všechna další zařízení, tj. 4 AP, SHDSL, ADSL a ostatní routery. Zde se nastavila pravidla ve firewallu. Nejdříve se povolila komunikace v místní síti, kde nebyla nastavena žádná omezení. Dalším krokem se definovala komunikace týkající se vnějšího prostředí, tedy internetu, kde byla nastavena neomezená pravidla pro odchozí provoz. Pro příchozí provoz byla však pravidla stanovena pouze pro data legitimní. To znamená, že mohou přitéci pouze ta data, která dávají odpověď na požadavek oprávněné osoby z vnitřní sítě vůči vnějšímu prostředí. Jedná se o naprosto běžné situace, jako je hledání na webu, přijímání a odesílání pošty, stahování aktualizací nebo textové a audiovizuální komunikace. V následujícím kroku byla povolena možnost pro oprávněného uživatele administrovat nebo prohlížet nastavení samotného routeru. Tato možnost je vázána na znalosti uživatelského jména a hesla. Přenos probíhá šifrovaně a byl zabezpečen šifrou RSA. Taktéž byla povolena možnost přistupovat k webové službě z internetu, zejména za účelem odeslání objednávek některého z nabízených produktů nebo při potřebě zaslání elektronického daňového dokladu k nákupu vyvíjeného produktu. Mezi další povolené protokoly patří FTP kvůli stahování informačních letáků. Nově bylo také umožněno přistupovat k virtuální privátní síti na základě znalosti určitých údajů, tj. znalost IP adresy, uživatelského jména a hesla. Kvůli umožnění vzdáleného přístupu byl povolen protokol PPTP. V neposlední řadě byl povolen zabezpečený příkazový řádek SSH pro vzdálenou administraci telefonní ústředny využívané pro poskytování zákaznické podpory. Veškerá další komunikace byla nastavena pro odmítnutí.

## 5.4. Vytvoření VPN pro umožnění přístupu externím entitám do místní sítě

Návrh dále obsahoval podnět k vytvoření několika VPN pro možnost zabezpečeného přístupu do místní sítě z libovolného umístění, kde je dostupný internet, proto nebylo nastaveno omezení na IP adresu či MAC adresu. Po připojení k VPN byla nově vytvořena možnost využití sdílených dat či funkce vzdálené plochy pro externisty či pro práci z domova pro interní zaměstnance. Tímto řešením byly odstraněny problémy se zabezpečením přístupu nevyžádaných externích zařízení. Vytvoření možnosti připojení k VPN se pro jednotlivého uživatele nově řeší zápisem příslušného pravidla do nastavení routeru s operačním systémem Mikrotik RouterOS. Výsledkem realizace návrhu je snadný a zabezpečený přístup k režimu vzdálené plochy na stanici, pro niž má uživatel autentizační oprávnění, skládající se ze znalosti přihlašovacího jména, hesla a IP adresy na kterou se zařízení má připojit. Proces přenosu je po realizaci návrhu zabezpečen 128 bitovým šifrováním. Navrhl jsem přechod na L2TP pro využití šifrování IPSec s algoritmem AES a 256 bitovým klíčem, hlavně kvůli náhodnému generování klíče na základě kryptografického protokolu Diffie-Hellman. Jedná se o lepší bezpečnostní řešení než u PPTP, protože u PPTP se šifrovací klíče odvozují přímo dle hesla uživatele.

## 5.5. Zabezpečení webové služby

Zjištěné zranitelnosti jsem vyřešil aktualizací servisních balíčků databáze a další zranitelnosti budou průběžně hledány testováním kódu webových stránek s webovou službou. Výsledkem aktualizace SP bude zabránění DoS a XSS útokům. Do budoucna jsem firmě navrhl zvážit optimalizaci zápisu programovacího kódu ASP.NET, v němž je webová stránka, přes kterou se přistupuje k webové službě, napsaná. Samotná optimalizace spočívá v kontrole a následné úpravě vstupních dat, před vytvořením samotného dotazu. Výsledkem tohoto vylepšení bude zabránění útoku typu SQL Injection.

### 5.6. Častá kontrola a testování aktuálnosti software

Provedl jsem aktualizaci samotných zranitelných operačních systémů ve verzích klientských i serverových. Aktualizoval jsem balíky Office, prohlížeče, aplikace od firmy Adobe, aplikace pro komunikaci a aktualizoval jsem samotné databáze. Využil jsem řadu nástrojů pro testování zranitelností systémů a databází a využil jsem doporučených postupů při řešení vzniklých komplikací. Současně jsem zavedl novou směrnici s názvem „aktualizace software“, která popisuje nutnost využívat nejaktuálnější dostupné stabilní verze software. Směrnice doporučuje možnost nechat si vysvětlit, jak aktualizace najít, nastavit automatické hledání nebo manuálně nainstalovat vyhledané aktualizace. Případná odpovědnost je uložena oprávněnému uživateli pracovní klientské stanice. Směrnice dále popisuje nutnost správy serverových stanic administrátorem, který souhlasem se směrnicí přebírá zodpovědnost za případné nedostatky na serverových stanicích.

### 5.7. Vytvoření směrnic pro zabezpečení zařízení

Také jsem vytvořil směrnici popisující nezahrnuté nestandardní akce a jejich řešení. Směrnice se týká samotného procesu nejistoty při nestandardní akci a doporučuje požádat o pomoc správce. Při takové akci může nezkušený uživatel podlehnout síle okamžiku a ve kvalitně chráněném systému zabezpečení proti útoku z vnějšku způsobit chybou lidského faktoru zranitelnost zevnitř. Zmíněná možnost by mohla být posléze zneužitelná i z vnějšího prostředí.

### 5.8. Nastavení a využívání firewallu třetí strany

Na vybrané testovací stroje jsem nainstaloval aplikaci Comodo Firewall Pro z důvodu porovnání firewallu samotných Windows. Firewall Windows nelze ovládat interaktivně, zatímco firewall Comodo to umožňuje. Dle testů odborných serverů samotný firewall Windows zachytí přibližně 4% škodlivých akcí oproti 99% škodlivých akcí zachycených aplikací Comodo. Vyhodnotil jsem efektivitu využívání obou firewallů a doporučil jsem používání firewallu Comodo pouze zkušeným uživatelům, u kterých je vyšší úroveň zabezpečení a kontroly nezbytná. Příjemná je licenční politika, jelikož je tento skvělý firewall poskytován zdarma.

### 5.9. Nastavení a využívání antimalware řešení třetí strany

Na vybrané testovací stroje jsem nainstaloval antimalwarové řešení s behaviorálním analyzátorem od firmy EmsiSoft, které se v internetových testech jeví jako vhodný doplněk zlepšující výsledky i renomovaných řešení s velkou úspěšností odhalení malware, např. od společností Eset, Kaspersky, Avira či Gdata. Doporučení pro využívání lze předat opět jen zkušeným uživatelům, u kterých bude vyšší úroveň antivirové kontroly nutná. Je důležité zaplatit licenční poplatek blížící se 500,- Kč, za licenci programu s roční aktualizací.

### 5.10. Návrh k nákupu testovacího software

Předložil jsem návrh k nákupu testovacího a penetračního nástroje v proprietární licenci. Z aktuální nabídky trhu lze pořídit velice kvalitní skener zranitelností od firmy GFI, který lze bezplatně využívat pro skenování až pěti IP na jednu licenci zdarma. Za každou další IP se platí 120,- Kč. Při realizaci mého návrhu byl skener využit, stejně tak byla použita speciálně vytvořená linuxová distribuce pro penetrační testování a hledání zranitelností, která není zpoplatněna a je možné si jí libovolně upravovat pro danou situaci. Všechny použité nástroje jsou poskytovány zdarma, a proto celé výdaje pro testování se rovnaly ceně stráveného času. Průběžně byly využívány i proprietární aplikace, ale vždy jenom v testovacím režimu, kdy je aplikace plně funkční obvykle po dobu několika dnů, či týdnů. Před uplynutím této doby byly ze systému proprietární aplikace odinstalovány, aby nedošlo k porušení licenčních ujednání. Po implementaci daných testovacích zařízení jsem zjistil mnoho zranitelností. Zranitelnosti s nejvyšší prioritou se podařilo zabezpečit. V současnosti se dále pracuje na odstranění zbylých méně závažnějších zranitelností. S jistou mírou nadsázky lze říci, že se jedná o nikdy nekončící proces.

### 5.11. Návrh k využívání šifrovacího nástroje k zabezpečení dat

Předložil jsem návrh na využívání šifrovacího nástroje pro šifrování dat jak na přenosných, tak i na pevných discích. Nejlepší z nabídky na webu se ukázala být aplikace TrueCrypt, protože má velmi kvalitní algoritmy šifrování a podporuje paralelismus procesů. Implementoval jsem aplikaci TrueCrypt na některé počítače s

vícejádrovými procesory. Tuto aplikaci jsem zvolil i kvůli jejím dalším výhodám, zejména kvůli možnosti přihlášení se k systému pomocí USB klíče a možnosti užívání aplikace zdarma. Implementací jsem zajistil vyšší úroveň soukromí a bezpečí uložených dat na vybraných systémech.

### 5.12. Aktualizace firmware aktivních prvků sítě

Předložil jsem návrh na pravidelně se opakující 3 měsíční aktualizování firmware, přístupových bodů, ADSL a SHDSL modemů a routerů. Zároveň jsem provedl aktualizace na nejnovější verze firmware. Přínosem je několik menších vylepšení ve formě nových instrukcích poskytnutých výrobcem.

### 5.13. Zakázání funkce autorun

Předložil jsem návrh na zakázání funkce autorun na serverových stanicích. Implementace probíhala vypnutím volbu automatického spouštění vyměnitelných médií v zásadách místního zabezpečení. Výsledkem je mírné vylepšení zabezpečení, protože už se nemůže ihned po zapojení výměnného média do počítače automaticky nahrát virus zneužívající tuto vlastnost operačního systému.

### 5.14. Zakázání možnosti vypnutí serverových systémů z přihlašovacího okna bez nutnosti přihlášení

Předložil jsem návrh o zakázání možnosti vypnutí systému bez nutnosti autentizace na serverových systémech. Realizaci jsem provedl přes nastavení v zásadách místního zabezpečení, a zamezil tak neoprávněnému vypnutí nepřihlášenou osobou a případné ztrátě dat.

### 5.15 Návrh a implementace využívání SecureFTP přenosu

Součástí mého návrhu byla i implementace zabezpečeného FTP přenosu pro komunikaci se serverhostingem. Jelikož obsah a autentizační údaje byly před realizací pomocí protokolu FTP skrze internet lehce zneužitelné (zde se setkala teorie s praxí a na firemní webové stránky byl po přenosu přes FTP připsán škodlivý kód), navrhl jsem

využívání právě zmíněného zabezpečeného FTP přenosu, abych dalšímu nebezpečí zamezil. Jelikož firma dlouhodobě využívá aplikaci Filezilla, která SFTP přenos podporuje, stačilo jen požádat u poskytovatele o změnu přístupové adresy a vyřízení formalit s SFTP. Samotná aplikace je šířena zdarma, navíc pod licencí open source a je plně vyhovují ve všech ohledech. Není proto třeba hledat jinou alternativu. Výsledkem je zabezpečení autentizace a šifrování přenosu 256 bitovou šifrou.

# 6. ZHODNOCENÍ A ZÁVĚR

Cílem mé bakalářské práce bylo navrhnout účinný systém zabezpečení ICT malé softwarové firmy, která vystupuje pod fiktivním názvem Dream Software. I když jsem navrhl řešení pro tuto konkrétní firmu, může být jeho koncepce podkladem a inspirací firmám jiným, které s inovací otálejí, až už z důvodů finančních, koncepčních nebo organizačních. Vývoj jde v oblasti ochrany počítačových sítí natolik kupředu, že každá firma by měla věnovat dostatečné množství času a lidských zdrojů na to, aby se pokusila být v těsném závěsu za moderními trendy zabývajícími se zranitelnostmi software.

Realizace projektu mé bakalářské práce proběhla v časovém pásmu přibližně jednoho roku. V této době se podařilo dostát cílům, které jsem si stanovil, tj. podílet se na implementaci kvalitnějšího a komplexnějšího řešení zabezpečení ICT ve firmě Dream Software. Realizace projektu probíhala podle předpokladů, jejím výsledkem je zjednodušení práce zaměstnanců i majitele firmy, zrychlení antivirové kontroly a komplexní práce s počítačem. Především se realizací projektu podařilo zdokonalit ochranu místní sítě, pracovních stanic a webové služby a chránit je tak před hrozbami plynoucími z neoprávněného prostředí.

Celkové náklady na realizaci projektu se odhadují na 15 000,- Kč investovaných do antivirového řešení ESET NOD32 Antivirus 4 s roční aktualizací, 10 000,- Kč investovaných do routeru Mikrotik a přibližně 20 000,- Kč investovaných do času věnovaného implementaci zabezpečení. Výrazně se ušetřilo na penetračních a testovacích nástrojích, které se využívaly zdarma - ať už jako testovací proprietární licence, nebo licence poskytované zdarma i pro komerční užití. Vzhledem ke ztrátám, které mohl přinést nelegální přístup zvenčí zachycený na nezabezpečeném AP, jsou investice opodstatněné. Pokud bych teoreticky vyčíslil hodnoty zdrojových kódů vyvíjených aplikací, uložených licenčních údajů vlastních i nakoupených aplikací, důvěrných informací o zákaznících a zaměstnancích, uložených heslech k poštovním aplikacím, k internetovým bankovnictvím a soukromým datům každého zaměstnance, jednalo by se o velké ztráty ať už po stránce finanční, nebo morální.

Porovnám-li stav před realizací projektu, kdy bylo reálných možností zneužití z venkovního prostředí velmi mnoho, se stavem po realizaci projektu, je zneužití z venkovního prostředí vyloučeno. Jediné možné zneužití může tedy vzejít na základě

chyby některého zaměstnance, který by inicializoval spojení s nebezpečnou částí vnější sítě jako první.

Roční obrat firmy Dream Software činí přibližně 20 mil. Kč a čistý zisk přes 2 mil. Kč, a tak se mnou navržený a realizovaný projekt ukázal být i po finanční stránce pro firmu vyhovující.

## Seznam použité literatury


BITTO, Ondřej. *Jak zabezpečit domácí a malou síť Windows XP.* Brno: Computer Press, 2006. 216 s. ISBN 80-251-1098-2.

BOTT, Ed, SIECHERT, Carl. *Mistrovství v zabezpečení Windows 2000 a XP.* Brno: Computer Press, 2004. 696 s. ISBN 80-7226-878-3.

DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat.* Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

DOSTÁLEK, Libor. *Připojujeme se k Internetu.* Praha: Computer Press, 2003a. 179s. ISBN 80-7226-800-*7.*

DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP.* Praha: Computer Press, 2003b. 571 s. ISBN 80-7226-849-X.

EISENKOLB, Kerstin; GÖKHAN, Mehmet; WEICKARDT, Helge. *Bezpečnost Windows 2000/XP.* Praha: Computer Press, 2003. 501 s. ISBN 80-7226-789-2

HLAVENKA, Jiří. *Používáme, využíváme (a zneužíváme) e-mail.* Praha: Computer Press, 2002. 280s. ISBN 80-7226-606-3

HORÁK, Jaroslav; KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce.* Praha: Computer Press, 2001. 165 s. ISBN 80-7226-566-0.

KOCMAN, Rostislav; LOHNINSKÝ, Jakub. *Jak se bránit virům, spamu a spyware.* Brno: Computer Press, 2005. 148 s. ISBN 80-251-0793-0.

MATĚJKA, Michal. *Počítačová kriminalita.* Praha: Computer Press, 2002. 106s. ISBN 80-7226-419-2.

MYKISKA, Antonín. *Spolehlivost technických systémů*. Praha: ČVUT, 2000. 177 s. Fakulta strojní. ISBN 80-01-02079-7.

NORTHCUTT, Stephen.[et al.] *Bezpečnost počítačových sítí.* Brno: Computer Press, 2005. 589 s. ISBN 80-251-0697-7.

STŘIHAVKA, Marek. *Vaše bezpečnost a anonymita na Internetu.* Praha: Computer Press, 2001. 87 s. ISBN 80-7226-586-5.

THOMAS, M. Thomas. *Zabezpečení počítačových sítí bez předchozích znalostí*. Brno: Computer Press, 2005. 338 s. ISBN 80-251-0417-6.

TŮMA, Pavel. *Freeware: jak zdarma vybavit počítač softwarem.* Praha: Grada Publishing, 2006. 264 s. ISBN 80-247-1332-2.

WOLFE, Paul. [et al.] *Antispam.* Brno: Computer Press, 2004. 375 s. ISBN 80-251-0479-6.

ZEMÁNEK, Jakub. *Slabá místa Windows aneb jak se bránit hackerům.* Kralice na Hané: Computer Media, 2004a. 156 s. ISBN 80-86686-11-6.

ZEMÁNEK, Jakub. *Stavba a správa sítě aneb cesta do hlubin internetu.* Kralice na Hané: Computer Media, 2004b. 204 s. ISBN 80-86686-26-4.