

# **Bezpečnostní rizika v síti internet z pohledu poskytovatele internetových služeb**

Security risks on the internet from the perspective of internet service provider

Tomáš Krajča

---

Bakalářská práce  
2011



Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky

---

Univerzita Tomáše Bati ve Zlíně  
Fakulta aplikované informatiky  
akademický rok: 2010/2011

# ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení: **Tomáš KRAJČA**  
Osobní číslo: **A08709**  
Studijní program: **B 3902 Inženýrská informatika**  
Studijní obor: **Bezpečnostní technologie, systémy a management**

Téma práce: **Bezpečnostní rizika v síti internet z pohledu poskytovatele internetových služeb**

Zásady pro vypracování:

1. Provedte literární rešerši na zadané téma.
2. Stanovte a popište bezpečnostní rizika v síti internet.
3. Uvedte možnost ochrany vůči uvedeným bezpečnostním rizikům.
4. Prakticky navrhnete a popište vhodnou konfiguraci souboru restriktivních bezpečnostních opatření realizovaných na některé z vybraných platforem běžně používané poskytovateli internetových služeb.

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. THOMAS, Thomas M. Zabezpečení počítačových sítí – bez předchozích znalostí. Brno : Computer Press, 2009. 344 s. ISBN 80-251-0417-6.
2. Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick, Ronald W. Ritchey. Bezpečnost počítačových sítí: Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. Brno: Computer Press, 2005. 592 s. ISBN 80-251-0697-7.
3. WADLOW, Thomas A. The Process of Network Security: Designing and Managing a Safe Network. Reading, Massachusetts : Addison-Wesley Professional, 2000. 304 s. ISBN 978-0201433173.
4. MILLER, Michael. Absolute PC Security and Privacy. 1st edition. Hoboken, New Jersey : Sybex, 2002. 512 s. ISBN 978-0782141276.
5. SOSINSKY, Barrie. Mistrovství – počítačové sítě: vše, co potřebujete vědět o správě sítí. Vyd. 1. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.
6. Angela Orebaugh, Gilbert Ramirez, Josh Burke, Greg Morris, Larry Pesce, Joshua Wright. Wireshark a Ethereal. Brno : Computer Press, 2008. 448 s. ISBN 978-80-251-2048-4.
7. WENSTROM, Michael. Zabezpečení sítí Cisco: Autorizovaný výukový průvodce. Brno: Computer Press, 2003. 784 s. ISBN 80-7226-952-6.

Vedoucí bakalářské práce: **Ing. Petr Navrátil, Ph.D.**

Ústav řízení procesů

Datum zadání bakalářské práce: **25. února 2011**

Termín odevzdání bakalářské práce: **23. května 2011**

Ve Zlíně dne 25. února 2011

prof. Ing. Vladimír Vašek, CSc.  
*děkan*



doc. Mgr. Milan Adámek, Ph.D.  
*ředitel ústavu*

## **ABSTRAKT**

Tato bakalářská práce se věnuje obecnému stanovení rizik v síti internet z pohledu poskytovatele internetových služeb a její následné eliminaci pomocí vhodných bezpečnostních restričních opatření. Pojednává o aktivní obraně samotného uživatele internetu a stanovení pravidel, o kterých by měl být každý uživatel minimálně poučen. Dále analyzuje rizika spojená se správou serverových zařízení a hledá řešení, jak se jim účinně bránit. Praktická část demonstruje konkrétní návrh souboru restričních opatření proti běžným hrozbám napadení klienta či síťové infrastruktury na operační platformě Mikrotik – RouterOS založené na systému Linux.

Klíčová slova:

firewall, Mikrotik, zabezpečení, útok, RouterOS, internet, Linux, ISP

## **ABSTRACT**

This thesis deals with general determination of risk on internet network from perspective of internet service provider and its elimination via suitable security steps. It deals with defense of user of internet and settings rules which should know every internet customer. This thesis analyzes risks connected with administration of server equipment and it looks for solution how to resist them. The practical part of this essay demonstrate concept of restriction steps against common threats to attack client or network infrastructure on Mikrotik - RouterOS operating system based on Linux.

Key words:

firewall, Mikrotik, security, attack, RouterOS, internet, Linux, ISP

Rád bych poděkoval zejména vedoucímu své práce, panu Ing. Petru Navrátilovi, Ph.D., za příkladný a odpovědný přístup k jemu svěřeným úkolům. Dále bych chtěl vyzdvihnout ochotu jednatelů a techniků společnosti FOFRNET spol. s r.o., kteří si na mě udělali čas vždy, kdy jsem potřeboval, byli mi vždy ochotni odpovídat na mé dotazy a průběžně předávat tolik potřebné zkušenosti z praxe.

**Prohlašuji, že**

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

**Prohlašuji,**

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně

.....  
podpis diplomanta

**OBSAH**

<b>ÚVOD</b> .....	<b>9</b>
<b>I TEORETICKÁ ČÁST</b> .....	<b>11</b>
<b>1 AKTIVNÍ OBRANA Z HLEDISKA UŽIVATELE</b> .....	<b>12</b>
1.1 HROZBY ŠÍŘENÉ ELEKTRONICKOU POŠTOU .....	12
1.1.1 Viry, spyware, malware, keyloggery .....	12
1.1.2 Spam.....	13
1.1.3 Podvodné emaily .....	14
1.1.4 Hoax .....	15
1.2 RIZIKA SPOJENÁ S PROHLÍŽENÍM WEBU .....	15
1.2.1 Phishing a zneužití internetového bankovníctví .....	15
1.2.2 Rizika sociálních sítí .....	17
1.3 BEZPEČNOSTNÍ SOFTWARE .....	18
1.3.1 Antivirové programy .....	19
1.3.2 Antispyware .....	21
1.3.3 Firewall .....	22
<b>2 RIZIKA NAPADENÍ SÍTĚ Z HLEDISKA SYSTÉMOVÉHO ADMINISTRÁTORA</b> .....	<b>25</b>
2.1 MOŽNÁ RIZIKA NAPADENÍ SÍŤOVÉHO SERVERU .....	25
2.2 TYPY ÚTOČNÍKŮ .....	26
2.3 NEJČASTĚJŠÍ CHYBY DOVOLUJÍCÍ NAPADENÍ SERVEROVÉ INFRASTRUKTURY.....	28
<b>II PRAKTICKÁ ČÁST</b> .....	<b>32</b>
<b>3 KONFIGURACE FIREWALLU V PŘÍSTUPOVÉ SÍTI</b> .....	<b>33</b>
3.1 SEZNÁMENÍ S PLATFORMOU MIKROTIK – ROUTEROS.....	33
3.1.1 Příklady použití systému Mikrotik - RouterOS .....	34
3.1.2 Možnosti konfigurace.....	34
3.1.3 Potřebné vybavení .....	35
3.2 KONFIGURACE PRO ZAJIŠTĚNÍ FUNKCE INTERNETU .....	36
3.2.1 Přiřazení IP adres .....	36
3.2.2 Spuštění DHCP serveru.....	36
3.2.3 NAT překlad.....	37
3.2.4 Nastavení výchozí routy.....	38
3.2.5 Ostatní nastavení .....	38
3.3 OCHRANA VLASTNÍCH UŽIVATELŮ SLUŽEB .....	39
3.3.1 Eliminace peer-to-peer komunikace a přenosu dat mezi koncovými uživateli .....	40
3.3.2 Omezení výměnných sítí, šíření nelegálního obsahu a rizika přehlcení sítě .....	40
3.3.3 SMTP ochrana před skrytým odesíláním spamu .....	41
3.4 OCHRANA SÍŤOVÉHO PROVOZU .....	42
3.4.1 Script pro denní zaslání zálohy konfigurace na mail .....	43
3.4.2 Ochrana před neautorizovaným přístupem na server .....	44
3.4.3 Omezení přístupu ze vzdálených sítí.....	44
3.4.4 Sestavení šifrovaného VPN PPTP tunelu do sítě .....	46

---

<b>ZÁVĚR .....</b>	<b>47</b>
<b>ZÁVĚR V ANGLIČTINĚ.....</b>	<b>48</b>
<b>SEZNAM POUŽITÉ LITERATURY.....</b>	<b>50</b>
<b>SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....</b>	<b>51</b>
<b>SEZNAM OBRÁZKŮ .....</b>	<b>53</b>
<b>SEZNAM TABULEK.....</b>	<b>54</b>

## ÚVOD

Bezpečnost v síti internet je velmi široký pojem a zároveň důležitý problém jak pro běžné uživatele, tak administrátory rozlehlých komunikačních sítí. Ve své podstatě se jedná o soubor opatření, která mají za cíl znemožnit, nebo maximálně znesnadnit útočnickovi získání soukromých, či neveřejných dat, obsahu komunikace, zamezit převzetí vlády nad počítačem, případně celou sítí, nebo útoku s pokusem vyřadit server z činnosti. V širším smyslu do této oblasti náleží také ochrana před úniky nevhodných osobních informací, například na sociálních sítích, manipulace s lidmi na sociálních sítích, nebo zamezení zobrazení citlivých firemních dokumentů ve výsledcích vyhledávačů. Bezpečnost na internetu je v zájmu také států i mezinárodních organizací. Většinou se snaží zamezit provozu stránek s ilegálním obsahem, nebo zamezit samotné nelegální činnosti pomocí zákonů a nasazením policie. V některých státech však ochranu již lze přirovnat k cenzuře.

Obvykle útočníka zajímá informace, kterou může zpeněžit, případně zneužít k vydírání, nebo získání jiných cílů, případně omezení provozu serveru, či užití výpočetního výkonu k vytvoření tzv. botnetu. Botnet pracuje na obdobném principu jako distribuované výpočty, avšak s cílem rozesílat spam nebo koordinovat útok typu DoS. Útoky však též mohou probíhat z jiných důvodů, než je výdělek, např. útoky jsou prováděny jako upozornění na slabé zabezpečení s cílem proslavit své jméno, nebo otestovat svoje schopnosti. Nepeněžně motivovaní útočníci často své úspěchy zveřejňují. Pokusy prolomit zabezpečení též mohou být objednané samotným cílem jako penetrační test v rámci bezpečnostního auditu. [1]

Pronikat cíleně do vzdáleného počítače za účelem získání hesel, např. k internetovému bankovníctví, je dnes již relativně zřídka jevem. Hesla jsou hromadně a efektivněji sbírána k tomu vytvořenými programy, které se nazývají keyloggery, a poté jsou dražena na utajovaných aukcích jako celé "balíky" čítající až tisíce přístupových údajů, případně jsou rovnou zneužita. Keyloggery se mohou maskovat za užitečný software, například za program zprostředkující předpovědi počasí a podobně. Jsou řazeny mezi spyware (tj. programy sledující činnost počítače, případně připravující "zadní vrátka" pro útok). K průniku k citlivým datům lze také využít bezpečnostních chyb v běžných programech. Speciální kapitolou je tzv. phishing (z angl. rybaření). Útočník "uloví" heslo uživatele tak, že mu zobrazí falešnou stránku, která se vydává vzhledově za jinou, např. za stránku přihlášení do internetového bankovníctví. V praxi se to nejčastěji děje posláním falešného e-mailu, který dodržuje obvyklou vzhledovou strukturu e-mailů banky s žádostí o odeslání

hesla z důvodu např. poškození databáze. Zadá-li oběť svá přístupová hesla na danou stránku, jsou hesla okamžitě uložena a útočník tak získal možnost manipulovat s účtem. [1]

Cílem práce bude tedy všechna tato rizika stanovit, analyzovat a následně navrhnout opatření k jejich úspěšné eliminaci.

# **I. TEORETICKÁ ČÁST**

# 1 AKTIVNÍ OBRANA Z HLEDISKA UŽIVATELE

V dnešní době za nás hardwarové i softwarové vybavení počítače, nebo samotné zabezpečení sítě vyřeší velké množství rizikových situací ze své podstaty rezidentně. Ve většině případů dokonce s kvalitativně velmi obstojnými výsledky. Přes to všechno je to stále samotný uživatel a jeho konání, kdo jsou pro počítač největší bezpečnostní hrozbou. Ten sám však může fungovat mnohem lépe než všechny automatizované aplikace a svým mravním chováním v síti může při základních znalostech bezpečného chování ochránit svá data i svůj komfort.

Uživatel sám může narazit na řadu virových hrozeb přes botnety, malware, spyware, podvodné e-shopy, ale také na rizika ztráty soukromí na sociálních sítích, na rizika cloud computingu, pojistné podvody na internetu, rizika zneužití platebních karet či jiných platebních metod.

Zde svou roli sehraje i psychologie, zvědavost a možná ani vzdělání nemusí být vždy ku prospěchu věci. Mnoho pasivních uživatelů, často i samozvaných profesionálů, se nechají zmást podvodnými nabídkami na vyskakujících oknech, a aniž by četli obsah sdělení, kvitují ho. Nežřídko ani netuší, že tímto umožnili instalaci škodlivého kódu do svého počítače.

## 1.1 Hrozby šířené elektronickou poštou

Velké množství hrozeb, přichází do napadeného PC nejjednodušší cestou a to formou přílohy nebo aktivního obsahu v elektronické poště. Zde je rozhodující mít zejména instalovaný a spuštěný kvalitní aktualizovaný antivirový software, do poštovního klienta integrovaný antispamový filtr a zdravým rozumem usoudit a rozpoznat, zdali se jedná o zprávu očekávanou a žádoucí, nebo jde o nebezpečný materiál nebo spam. Uživatel se nesmí nechat zmást tím, že v záhlaví figuruje jméno, či emailová adresa jeho dobře známého, právě tohoto faktu využívají vývojáři škodlivého kódu k co nejglobálnějšímu rozšíření nákazy a spoléhají jen a pouze na lidské selhání.

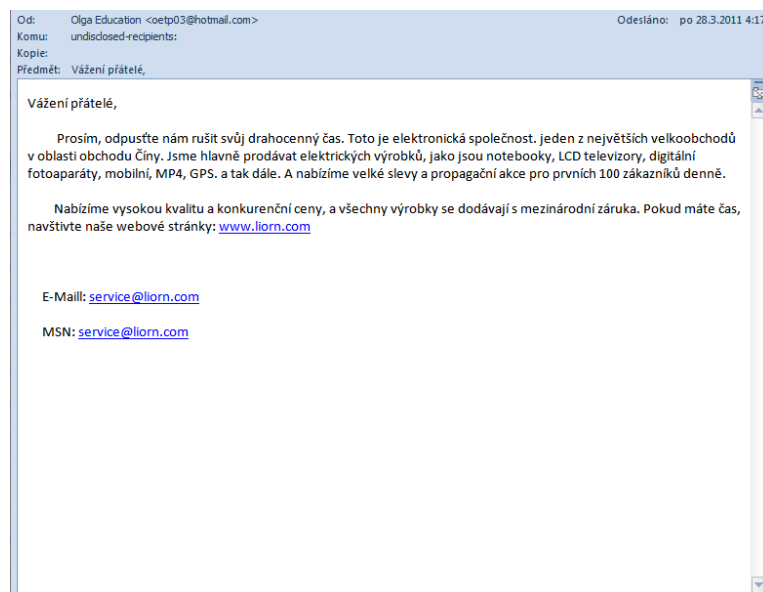
### 1.1.1 Viry, spyware, malware, keyloggery

Všeobecně jsou všechny tyto typy škodlivých kódů přeneseny do počítače prostřednictvím infikované přílohy emailové zprávy nebo odkazu na vzdálený webový obsah, který je nežřídko kdy klamavě označen velmi přitažlivým způsobem, například „nahá Pamela Anderson“ a podobně. Viry, spamy, malware a keyloggery lze obecně charakterizovat jako

škodlivý kód, který má za úkol sám sebe množit a skrytě přeposílat prostřednictvím našeho seznamu kontaktů své kopie našim jménem dál a zároveň různým způsobem zasáhnout do integrity systému, vytvořit do počítače backdoor, nebo sbírat citlivé informace a ty pravidelně odesílat vývojáři škodlivého kódu.

### 1.1.2 Spam

Spam je nevyžádaná zpráva doručená elektronickou poštou, většinou s komerčním reklamním obsahem. Spamming je vlastní činnost rozesílání spamových zpráv. Pokud má odesílatel souhlas adresáta se zasláním určitého druhu informací, může tak činit po dobu, po kterou tento souhlas bude platit. Adresát totiž může svůj souhlas kdykoliv odvolat. Pokud odesílatel souhlas nemá, je situace složitější. Zákon o ochraně osobních údajů umožňuje, aby správce nebo zpracovatel použil jméno, příjmení a adresu subjektu údajů pro zpracování těchto údajů za účelem nabízení obchodů nebo služeb. Ovšem v případě, že s takovým zpracováním subjekt údajů vyslovil nesouhlas, nelze uvedené údaje dále zpracovávat.



*Obr. 1. Typický příklad nevyžádané zprávy.*

Je třeba ovšem rozlišit spam od vyžádaných reklamních nabídek. Pokud se jedná o aktivitu, kdy subjekt údajů vysloví předchozí souhlas se zasláním komerčních nabídek a oznámení, je tato činnost legální a lze jí provozovat do doby, než subjekt vyjádří svůj nesouhlas s takovouto činností. [2]

### 1.1.3 Podvodné emaily

Poslední dobou velmi rozšířený způsob podvodného vymáhání osobních údajů pomocí elektronické pošty. Útočníci zašlou emailem důvěryhodně vypadající formulář jménem společnosti či organizace, u které využíváme některých služeb a žádá nás o ověření identity nebo k přístupu k bankovnímu účtu, platební kartě a podobně.

Útočník buď podvodné zprávy rozesílá všeobecně všem do internetu a žádá o vyplnění formuláře masově rozšířených finančních institucí jako PayPal a podobně. Může také záměrně zaslat podvodnou zprávu jménem společnosti, o které ví, že jejich služeb předem určená konkrétní oběť využívá. Toho může s výhodou využít ve svůj prospěch a například přidáním adresného oslovení do emailu přidá na důvěryhodnosti. Informaci o uživateli lze získat mnoha způsoby a to od prostého vyplnění dotazníku na ulici, přes odposlech komunikace s bankou. Email je nezabezpečený komunikační kanál a odposlech je možný i přesto, že komunikace s bankou je šifrovaná. Šifruje se totiž pouze tělo emailu, hlavička, ve které je obsaženo kdo s kým komunikuje, nikoliv.



Dear PayPal Customer

PayPal is currently performing regular maintenance of our security measures. Your account has been randomly selected for this maintenance, and placed on Limited Access status. Protecting the security of your PayPal account is our primary concern, and we apologize for any inconvenience this may cause.

To restore your account to its regular status, you must confirm your email address by logging in to your PayPal account using the form below:

<b>Email Address:</b>	<input type="text"/>
<b>Password:</b>	<input type="password"/>
<b>Bank Account</b>	
Enter Bank Account #:	<input type="text"/>
<b>Credit Card</b>	
Enter Credit Card #:	<input type="text"/>
Exp. date :	03 / 03

*Obr. 2. Podvodná žádost o vyplnění osobních údajů.*

Jakkoliv se zdá odposlech takovéto komunikace náročný, pro pokročilejšího útočníka je minimální problém obsadit některý z uzlů sítě a pomocí instalace packet snifferu, který provádí odposlechu paketů a jejich následnou hloubkovou analýzou zjistit kýžené informace. Tímto způsobem lze bez větších problémů odposlechnout komunikaci instant messengerů (například ICQ) a podobných chat služeb a také všechny údaje vkládaných do webových formulářů bez šifrovaného přístupu https.

### 1.1.4 Hoax

Hoaxem se rozumí zpráva se lživým obsahem. Zpráva uživatele varuje před virem, prosí o pomoc, informuje o nebezpečí, snaží se pobavit a podobně. Často nemá jiný účel, než se co nejvíce rozšířit a vyvolat důvěru mezi čtenáři takovýchto zpráv. Tito běžní uživatelé, kteří informaci obsaženou ve zprávě uvěří, jsou téměř vždy na konci vyzváni k přeposlání tohoto mailu ostatním přátelům. Právě toto však způsobí nekonečný řetězec a nekontrolovatelné šíření klamavých zpráv, o které původci hoaxu právě jde.

Mezi škodlivé vlivy hoaxu pak zejména patří:

- Obtěžování příjemců
- Nebezpečné rady
- Zbytečné zatěžování linek a serverů
- Ztráta důvěryhodnosti
- Prozrazení důvěrných informací

Typické formy hoaxových zpráv dle obsahu jsou:

- **Falešný poplach** – toto je původní význam slova hoax. Zpráva cíleně manipuluje s informacemi a snaží se přimět uživatele k dalšímu šíření nebo dokonce k destruktivnímu zásahu („*smažte jdbmgr.exe z C:\Windows – je to virus*“).
- **Zábavné zprávy** – tyto využívají uživatelovi touhy být vtipný a pobavit ostatní a využít lidské pověrčivosti a vyhrožují („*nepřepošleš-li, budeš mít 10 let smůlu*“).
- **Prosby** – zpravidla působí na city, prosí o darování krve, hledání ztracené osoby, poslání obnosu na cizí účet a podobně. [3]

## 1.2 Rizika spojená s prohlížením webu

Při prohlížení webu se můžeme setkat s celou řadou rizik. Nejběžnější a nejznámější je riziko napadení počítače virem či trojským koněm. Těmto rizikům obvykle zabrání instalovaný a řádně udržovaný antivirový systém. Díky němu není zpravidla další interakce od uživatele příliš potřeba. Když tedy pomineme riziko virové nákazy, jedná se zejména o rizika méně známá, ale o to nebezpečnější.

### 1.2.1 Phishing a zneužití internetového bankovníctví

Jedná se o podvodnou techniku používanou k získávání citlivých údajů od obětí útoku. Metodou rozesílání podvodných emailových zpráv oběť přeměrují na podvodnou

webovou stránku, která se vydává za oficiální žádost bankovní instituce, serveru mikroplatebních služeb a podobně. Ta vyzívá uživatele k zadání jeho údajů na odkazovanou stránku. Buď se vydává přímo za přihlašovací stránku dané společnosti a po zadání uživatelského jména a hesla odešlou tyto informace útočníkovi nebo se snaží pod jakoukoliv jinou záminkou (aktualizace databáze, přechod na vyšší stupeň zabezpečení,...) informace podvodně vymámit.

Existuje několik úrovní boje s phishingem. Na uživatelské úrovni zejména osvěta, dodržování bezpečnostních pravidel a především zdravý rozum. Na aplikační úrovni je možno použít specializované nástroje, které umožňují phishingové útoky rozeznat a upozorňovat na ně.

Dnes je již základní forma phishingové ochrany integrována do většiny nejběžnějších internetových prohlížečů minimálně pomocí specializovaného plug-inu. Ty jsou schopny podle jistých klíčových vlastností takovýchto stránek na pokus o útok upozornit a přístup zablokovat. [4]

Dalším krokem k ochraně proti phishingu může být tzv. „site-to-user“ autentizace. V tomto případě se sama přihlašovací stránka do internetového bankovníctví „autentikuje“ uživateli. Funguje to tak, že po zadání uživatelského jména systém zjistí, o jakého klienta se jedná, a na další stránce s požadavkem na zadání hesla mu prezentuje klientem dříve vybraný obrázek či text. Klient si tak může být jist, že své heslo nezadává do falešné phishingové stránky.

Dalším krokem je zavedení silnější autentizace uživatelů, a to buď již zmíněnými digitálními certifikáty, jednorázově generovanými a použitelnými hesly, nebo adaptivní autentizací. Protože je však správa životního cyklu digitálních certifikátů či generátorů jednorázových hesel pro velké množství klientů velmi nákladná, banky začínají víc a víc využívat právě metody adaptivní autentizace. Navíc dnes již ani digitální certifikát útočníka nezastaví.

Adaptivní autentizace je založena na risk-based multifaktorové autentizaci. To znamená, že způsob a síla autentizace uživatele se určuje až v momentě připojení uživatele k internetovému bankovníctví. Pokud se uživatel přihlašuje standardně (např. ze svého počítače, z běžné IP adresy, přes svého ISP, v běžnou denní dobu), systém vyhodnotí přihlášení jako minimálně rizikové a uživateli bude k přístupu na účet stačit jednofaktorová autentizace (jméno a heslo). Pokud však systém vyhodnotí v připojení uživatele nějakou

anomálii, vyhodnotí připojení jako rizikovější a požádá uživatele o dodatečnou autentizaci (např. zaslaným SMS kódem, položením několika osobních otázek, automatizovaným zavoláním na jeho mobilní telefon). V případě extrémních anomálií může systém připojení úplně odmítnout a věc dále řešit například pomocí call-centra. [4]

Žádná z bankovních institucí již nebere zabezpečení svého internetového bankovníctví na lehkou váhu, není ovšem bohužel výjimkou, že některým bankám stačí pro přístup k plnému ovládnání účtu pouze uživatelské jméno a heslo. Jiný stupeň ochrany nevyžadují. Na nás je, abychom vždy vyžadovali informaci o stupni a formách zabezpečení zneužití u svojí banky a v případě nevyhovujících podmínek internetového bankovníctví buď nevyužívali, nebo svou banku úplně změnili.

### **1.2.2 Rizika sociálních sítí**

Ještě před pár lety nebylo po sociálních sítích ani vidu ani slechu. Dnes jde ale o významný komunikační prostředek a komunitní centrum, které přináší kromě řady pozitiv relativně hodně nebezpečí. Je tedy třeba se silně zaměřit na rizika spojená s využíváním sociálních sítí a také na podvodné sociální sítě.

Mezi největší sociální sítě patří bezesporu Facebook a Twitter. V českých zemích má větší úspěch první ze jmenovaných. Dalo by se říci, že si Facebook získal přinejmenším stejnou popularitu jako ICQ - s tím rozdílem, že ICQ je ve světě minoritní, kdežto Facebook slaví stovky miliony uživatelů na celém světě a je tak celosvětovou jedničkou v oblasti sociálních sítí. V pozadí těchto všech aktivit, které můžeme na sociálních sítích provozovat, stojí skryté nebezpečí ztráty důležitých osobních dat.

Je nutné si položit otázku, k čemu tato data mohou být. Nejméně škodlivým důvodem je marketingová databáze potencionálních zákazníků. Za podobné databáze se dobře platí, firmy si je kupují, aby mohly nabízet své produkty a služby širšímu okruhu potencionálních zákazníků. Lidé si na Facebook dávají většinou jak e-mail, tak i telefon, případně město, odkud jsou či věkovou skupinu. Tato data jsou již pro firmy zajímavá a mohou tak oslovit přesně takové zákazníky, kteří by o jejich služby mohli mít zájem. Další důvody pro získání dat jsou různorodé. Od spamu, přes sledování určité skupiny osob až po ryze kriminální podtext. [5]

Můžeme argumentovat, že dbáme na svou bezpečnost a nemáme veřejný profil. Můžeme také omezit zobrazování fotografií a své příspěvky zobrazovat jen a pouze svým přátelům. To ale zdaleka nestačí. Pokud se chystáme na takovou drobnost jako vyplňovat kvíz či

spouštět hru na Facebooku, patrně budeme muset odsouhlasit přístup externí aplikace do vašeho profilu. Většina uživatelů toto upozornění bezmyšlenkovitě odklepne, bez toho aniž by si uvědomili, že tímto krokem předávají náhled do svého profilu jak aplikaci samotné, tak jejím tvůrcům, kteří si pak mohou s vašimi daty dělat, co chtějí. Jde tedy pouze o to, vytvořit aplikaci, o kterou budou mít lidé zájem a která bude dostatečně lákavá na to, aby si ji otevřelo co nejvíce lidí.

Dlužno podotknout, že jen málo lidí zpětně zamezuje přístup aplikacím, které povolili v minulosti. To má pak za následek situaci, že ač si uživatel již další aplikace do svého profilu nepřidává a začne se chovat tak, aby již neměly přístup k jeho datům, čerpají aplikace data z jeho profilu nadále. To vše na základě povolení udělených v minulosti. [5]

Bohužel na Facebooku většina lidí na soukromí nemyslí. Internet uživatele naučil, že je myšleno na jeho bezpečnost externě, lidé jsou zvyklí na zabezpečení z e-mailu nebo internetového bankovníctví, a tak předpokládají, že je bezpečný také Facebook či jiná sociální síť.

Používání sociálních sítí je velice populární a není záměrem, od této činnosti odrazovat. Jen je potřeba brát na zřetel bezpečnost a ochranu soukromí. Nikdy stoprocentně nevíte, jaké bezpečnostní složky mají k vašim datům přístup. U Facebooku se již několikrát kupříkladu hovořilo o propojení s FBI či CIA jakkoliv je to jistá či mylná informace, všechno jsou to osobní data, která leží a budou ležet v archivech společnosti možná navěky. [5]

### **1.3 Bezpečnostní software**

Přesto, že dnes již je bezpečnostní software na velmi vysoké úrovni a firmy zabývající se jejich vývojem jsou schopny reagovat na novou hrozbu v řádu hodin, je důležité si uvědomit, že vývojáři škodlivých kódů jsou stále o krok napřed před vývojáři bezpečnostních aplikací. Stejně tak bezpečnostní software pouze doplňuje obecné bezpečnostní základy, kterými se musí řídit každý uživatel, aby si udržel svá data a svůj komfort v bezpečí. Pro úplnost jsou jednotlivé typy softwaru rozděleny do kategorií podle účelu použití. Existují i jednoúčelové verze zaměřené přímo proti konkrétním virům či celým skupinám podobné rodiny nákaz v podobě různých aplikací k odstranění pouze trojských koní, virů skupiny Blaster, obtěžujících reklamních oken a bannerů adware, dialerů a podobně.

### 1.3.1 Antivirové programy

Všechny dnes dostupné antivirové systémy se skládají nejméně ze dvou základních částí – jádra antiviru a aplikační části antiviru. Úkolem jádra je po obdržení přístupu ke konkrétním souborům na základě virových signatur rozhodnout, jestli obsahem souboru je či není virus, pokud ano, tak jaký. Pokud je jádro vyhledává na základě jednotlivých řetězců, pak k němu nutně patří výše jmenovaná databáze virových signatur, která obsahuje definice, dle kterých lze s jistotou určit, zdali se jedná o infikovaný soubor či nikoliv. Tato databáze musí být pravidelně aktualizována, protože právě podle ní je antivirus schopen hrozbu správně a rychle identifikovat.

Aplikační část programu má na starost předkládání souborů jádru k analýze a k rozboru. Obvykle bývá složena ze dvou částí: [2]

- **On-demand skenování** se může také nazývat skenování na požádání či off-line skenování. Spočívá v kontrole vybraných souborů na přímou výzvu uživatele. Většina antivirových programů umožňuje definici úkolů pro toto skenování - např. skenování všech lokálních pevných disků nebo skenování diskety, kompaktního disku nebo USB flash disku. Po spuštění úkolu aplikační část prochází všechny soubory definované úkolem (například všechny soubory na lokálním pevném disku) jeden po druhém a předkládá je jádru antiviru. Ten rozhodne o tom, jestli obsahují virus nebo nikoli. Výsledky kontroly program předkládá uživateli. Prakticky všechny dnešní antivirové programy umožňují nastavování automatického spouštění definovaných úkolů, například po každém spuštění počítače, pravidelně jednou za týden nebo pokaždé po určité době nečinnosti počítače. Pokud antivirový program skenuje na základě řetězců, je vhodné nastavit on-demand skenování tak, aby se spustilo vždy po každé aktualizaci databáze virových signatur. Jedině tak je možné okamžitě odhalit nové viry, které přibyly od předchozí verze.
- **On-line skenování** se také nazývá rezidentní ochrana. Je založena na jednoduché myšlence, která předpokládá, že nejlepší okamžik pro antivirovou kontrolu je těsně před použitím podezřelého souboru. A proto tvůrci antivirových programů vytvářejí pro jednotlivé operační systémy ovladače, které se napojují přímo na souborový systém a mají ho plně pod kontrolou. Před každým požadavkem aplikace na otevření souboru předloží ovladač těsně před povolením jeho otevření soubor antivirovému jádru, který rozhodne o jeho čistotě. Pokud je soubor vyhodnocen jako čistý, je jeho otevření povoleno. Protože při běžné uživatelské práci se často otevírají obvykle stále

tytéž soubory (např. spuštění aplikace typu MS Word vyvolává otevírání desítek nezměněných souborů), snaží se antivirové programy kontrolovat pouze ty soubory, které se od poslední kontroly změnily. Tak se sníží zatížení systému způsobená zapnutím on-line antivirových mechanismů. [2]

Každý z vývojářů antivirových aplikací se snaží být tím nejlepším, o objektivní kvalitativní hodnocení se pravidelně starají autoři webu AV-Comparatives, kde jsou vždy k nalezení nejnovější srovnávací tabulky a hodnocení kvality detekce jednotlivých systémů. AV-Comparatives postupuje při testování velmi důkladně. Nejdůležitějším testem je tzv. ZOO test, ve kterém je jednotlivým antivirům předloženo obrovské množství infikovaných i neinfikovaných souborů. Na základě detekce je pak vyhodnocena procentuální úspěšnost, počet falešných detekcí a také je měřena rychlost scanování. Výsledky posledního testování této společnosti jsou uvedeny v *Tab. 1*. Jsou uvedeny záměrně pouze ty, které získaly více než 95% úspěšnosti.

<b>Antivirus</b>	<b>Úspěšnost</b>	<b>Hodnocení</b>	<b>Falešné detekce</b>	<b>Rychlost</b>
G DATA AntiVirus	99,6%	ADVANCED+	málo	průměrná
AVIRA AntiVir Premium	99,3%	ADVANCED+	málo	rychlá
Panda Antivirus Pro	99,2%	ADVANCED+	mnoho	rychlá
TrustPort AV	99,1%	ADVANCED+	málo	pomalá
McAfee VirusScan+	98,9%	ADVANCED+	mnoho	pomalá
PC Tools Spyware +AV	98,7%	ADVANCED+	málo	průměrná
Norton AntiVirus	98,6%	ADVANCED+	málo	rychlá
F-Secure Anti-Virus	97,8%	ADVANCED+	velmi málo	pomalá
NOD32 Antivirus	97,7%	ADVANCED+	velmi málo	průměrná
BitDefender AV	97,5%	ADVANCED+	velmi málo	pomalá
eScan Anti-Virus	97,5%	ADVANCED+	velmi málo	pomalá
avast! Professional	97,3%	ADVANCED+	málo	rychlá
Kaspersky AV	97,1%	ADVANCED+	málo	průměrná
K7 TotalSecurity	96,4%	STANDARD	velmi mnoho	průměrná
Microsoft Security Ess.	96,3%	ADVANCED	velmi málo	pomalá

*Tab. 1. Test antivirových programů z března 2011 zpracovaného společností AV-Comparatives.*

Z testu vítězně odcházejí antiviry, které získaly označení ADVANCED+. Obyčejně nabízejí vysokou detekci s minimem falešných poplachů. Uživatel by měl tedy vybírat přednostně z takto označených antivirů, a neřídít se jen dle procentuálního úspěchu.<sup>1</sup>

V obecné rovině tedy příliš nezáleží, který antivirus si vybereme, je pouze důležité, mít kterýkoliv z nich nainstalovaný a rezidentně spuštěný.

### 1.3.2 Antispyware

Spyware je obecný pojem používaný k popisu softwaru, který se chová určitým způsobem, například zobrazuje reklamu, shromažďuje osobní informace nebo mění konfiguraci počítače, obvykle bez získání vašeho předchozího souhlasu.

Spyware je často spojen se softwarem, který zobrazuje reklamy (nazývá se adware), nebo se softwarem sledujícím osobní či citlivé informace.

To neznamená, že veškerý software poskytující reklamu nebo sledující vaše aktivity online je špatný. Například se můžete zaregistrovat u bezplatné hudební služby, ale „zaplatit“ za to souhlasem k zobrazování cílených reklam. Pokud porozumíte podmínkám a souhlasíte s nimi, můžete se dojít k názoru, že to je spravedlivý obchod. Můžete také povolit společnosti sledovat vaše činnosti online, aby mohla vyhodnotit, kterou reklamu vám zobrazí.

Jiné druhy spywaru provádějí v počítači změny, které mohou být obtěžující a způsobit zpomalení nebo zhroucení počítače. [6]

Tyto programy mohou změnit domovskou či vyhledávací stránku vašeho prohlížeče nebo do něj přidat další součásti, které nepotřebujete či nechcete. Také výrazně ztěžují vrácení nastavení do původního stavu.

Klíčem ve všech případech je, zda (vy nebo jiná osoba používající počítač) chápete, co bude software dělat, a souhlasili jste s jeho nainstalováním do počítače.

Existuje mnoho způsobů, jakými se spyware nebo jiný nežádoucí software může dostat do počítače. Běžným trikem je tajná instalace tohoto softwaru během instalace jiného požadovaného softwaru, například programu pro sdílení souborů hudby či videa.

---

<sup>1</sup> Podrobné výsledky včetně metodiky testování dostupné na [www:  
http://www.av-comparatives.org/images/stories/test/ondret/avc\\_report25.pdf](http://www.av-comparatives.org/images/stories/test/ondret/avc_report25.pdf)

Při každé instalaci softwaru do počítače je nutné si pečlivě pročíst veškerou dokumentaci, včetně licenční smlouvy a prohlášení o zásadách ochrany osobních údajů. Někdy je zahrnutí nežádoucího softwaru do dané instalace uvedeno, ale může se zobrazovat na konci licenční smlouvy nebo prohlášení o zásadách ochrany osobních údajů. [6]

Antispyware je program, který právě tato rizika eliminuje a podle klíčových vlastností programů, je schopen určit, zdali se jedná o software chtěný či nikoliv. Prakticky se můžeme setkat s dvěma typy těchto programů – antispyware s rezidentní ochranou a bez rezidentní ochrany. Na rozdíl od antivirových programů není nutné, aby antispyware kontroloval soubory nepřetržitě na pozadí, pro běžné uživatele je ovšem více než vhodné užívat program právě s rezidentní ochranou, který dokáže detekovat a hlásit jednotlivé potenciálně nechtěné aplikace a odvrátit tak začas riziko nákazy. Všechno to ovšem za cenu vyššího čerpání systémových prostředků. Pro pokročilé uživatele naopak zpravidla stačí aplikace bez rezidentní ochrany. Tento uživatel ale musí dbát zvýšené opatrnosti při instalaci nejrůznějších programů a řekněme jednou měsíčně vykonat preventivní kontrolu disku proti nechtěným aplikacím.

### **1.3.3 Firewall**

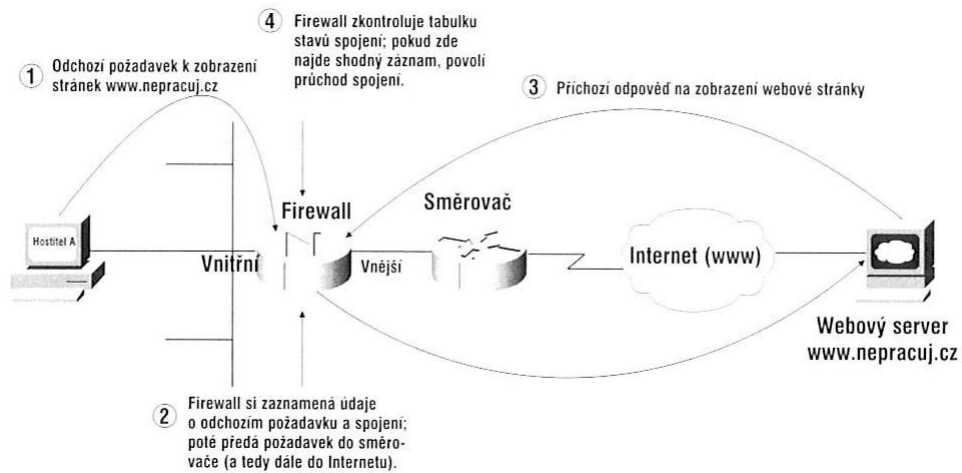
Firewall kompletně kontroluje síťový provoz, který vstupuje do některého z jeho rozhraní, a aplikuje na něj takzvaná pravidla. Na základě nich pak v podstatě daný provoz buďto povolí, nebo zamítne.

Firewall neustále kontroluje jak příchozí, tak i odchozí data. Je schopen filtrovat síťový provoz podle zdrojové a cílové IP adresy, podle protokolu a také podle stavu spojení. Jinými slovy, vstup provozu FTP přes firewall do vnitřní sítě normálně povolovat není nutné, ale pokud určitou komunikační relací navázal některý důvěryhodný uživatel vnitřní sítě, pak jí povolíme. Implicitně pak běžný firewall důvěřuje všem spojení z důvěryhodné vnitřní sítě do veřejné vnější sítě.

Jednou z možností firewallu je také zaznamenávat do svých protokolů pokusy o spojení, které se shodují s jistými pravidly a které v síti vedou k vyvolání výstrahy či poplachu. Firewall umožňuje také překlady síťových adres (tzv. NAT) z vnitřních privátních IP adres na veřejné IP adresy.

Většina firewallů provádí stavovou inspekci paketů, která sleduje všechny odchozí pakety a podle potřeby na ně reaguje. Kontroluje tedy veškerou komunikaci každého hostitele

s požadovaným cílem a ověřuje, jestli je příchozí odpověď namířená stejnému hostiteli, jenž celou konverzaci zahájil. Obr. 5 vysvětluje názorně činnost firewallu. [7]



Obr. 3. Funkce a zařazení systému firewall v rámci síťové infrastruktury. [7]

Firewall má tedy dvojí povinnost při práci s pakety – jejich inspekci a filtrování. K nejběžnějším pravidlům a jejich funkcím patří:

- **Blokování příchozího síťového provozu podle jeho zdroje nebo cíle.** Zablokování nežádoucího příchozího provozu je nejběžnější funkcí firewallu a je konec konců hlavním důvodem pro jeho instalaci - zabránit vstupu nežádoucího provozu do vnitřní sítě. Takovýto provoz obvykle pochází od útočníka, takže jej budeme chtít určitě rychle vykázat pryč.
- **Blokování odchozího síťového provozu podle jeho zdroje nebo cíle.** Řada firewallu dokáže sledovat také síťový provoz ve směru z vnitřní sítě do veřejného Internetu, takto můžeme například zaměstnancům vlastní firmy zabránit v přístupu k nevhodným webovým stránkám.
- **Blokování síťového provozu podle obsahu.** Vyspělejší firewally sledují v síťovém provozu také nepřipustný obsah. S firewallem může být například integrován antivirový program, který zabraňuje virům ve vstupu do vnitřní sítě; jiné firewally jsou integrovány s e-mailovými službami a monitorují a blokují průchod nežádoucí elektronické pošty.
- **Zpřístupnění zdrojů vnitřní sítě.** Primárním úkolem firewallu je sice zabránit v průchodech nežádoucího síťového provozu, u většiny z nich můžeme ale také nakonfigurovat selektivní povolení přístupu ke zdrojům (prostředkům) vnitřní sítě,

jako je například veřejný webový server; ostatní typy přístupu z Internetu do vnitřní sítě ponecháme zakázané. V řadě případů je možné tyto funkce zajistit pomocí takzvané demilitarizované zóny (DMZ), do níž umístíme mimo jiné i zmíněný veřejný webový server. Podrobněji viz část „Nejprve základy: život v demilitarizované zóně (DMZ)".

- **Povolení některých spojení do vnitřní sítě.** Zaměstnanci se do podnikové sítě běžně připojují také prostřednictvím virtuální privátní sítě (VPN). Tyto sítě umožňují bezpečné připojení z Internetu, například pro domácí pracovníky a pro obchodní cestující v terénu, nebo také pro vzájemné spojení vzdálených poboček firmy. Některé firewally přímo obsahují funkce sítě VPN a usnadňují tak zavádění popsaných spojení.
- **Oznamování průběhu síťového provozu a činnosti firewallu.** Při monitorování síťového provozu do a z Internetu je také důležité vědět, co všechno firewall dělá, kdo se pokouší „nabourat" do vnitřní sítě, a kdo se pokouší na Internetu přistupovat k nevhodnému materiálu. Většina firewallu obsahuje proto určitou formu mechanismu pro oznamování; dobrý firewall může také veškeré aktivity zaznamenávat do serveru syslog nebo do jiného záznamového zařízení. Zkoumání systémových protokolů firewallu po proběhlém útoku je jedním z důležitých a průkazných nástrojů, které máme k dispozici. [7]

## **2 RIZIKA NAPADENÍ SÍTĚ Z HLEDISKA SYSTÉMOVÉHO ADMINISTRÁTORA**

Napadení síťové infrastruktury se stává značným rizikem zejména v případě, že společnost či instituce uchovává na serverech strategicky důležitá či přísně soukromá data. Velmi přísné zabezpečení je zejména na místě v případě, kdy uchováváme citlivá data třetí osoby, která nám je s důvěrou svěřila.

### **2.1 Možná rizika napadení síťového serveru**

V prvé řadě je třeba důsledné stanovení a analýza možných rizik. Dá se říci, že základních typů útoků, proti nimž se budeme bránit je v podstatě pět: [8]

- **Útočník čte důvěrná data.**

Útočník se může dostat k důvěrným plánům na zavedení nového produktu, konkurenčním plánům do budoucnosti, ke jménům a adresám zákazníků, k informacím o kreditních kartách a bankovních účtech zákazníků, k číslům vašich bankovních účtů a jejich obsahu, a také k citlivým systémovým údajům, jako jsou telefonní čísla modemů, hesla atd.

K nejvyšší škodě dochází často tím, že útočník dá zjištěná data k dispozici ostatním. To, že se o záměru nového produktu dozví tento jeden útočník, ještě nemusí být nijak závažný problém. Pokud ale tyto plány zveřejní někde na internetu, kde se k nim dostane konkurence, to už je problém velice podstatný. A pokud dojde k vyzrazení čísel kreditních karet vašich zákazníků, přičemž tento útok vejde ve veřejnou známost (jako se stalo v nedávné době opakovaně společnosti Sony), budou se lidé zdráhat vůbec s takovouto firmou obchodovat.

- **Útočník provádí změny v datech**

Tento typ útoku je snad nejděsivější a znamená největší poškození. Útočník může změnit různé plány a data, aniž by si toho lidé jakkoli všimli. Změny v datech mohou způsobit jak ztráty na životech, tak i jiná závažná rizika. Představte si například, že se změní předpis pro výrobu nového léku ve farmaceutické společnosti, konstrukční plány nového automobilu nebo letadla, anebo dojde ke změně programu pro řízení továrny či lékařského přístroje, jako je rentgen nebo Gamma nůž. Mohou se změnit také záznamy o zdravotním stavu a léčbě pacienta. Každá z těchto situací může vést až ke smrti člověka - a také k vleklým soudním sporům.

Útočník si často dokonce ani nemusí uvědomit, že může takovouto škodu způsobit. V kalifornském Berkeley se crackeři dostali do systému pro řízení cyklotronu, který se někdy používal pro léčbu rakoviny. Crackeři také nabourali bankomaty, které vydávaly peníze jen tak bez zasunutí karty, a provedli nesmyslné změny na webových stránkách amerických vládních úřadů, včetně špionážní služby CIA.

- **Útočník maže data**

Zde je výsledné poškození zcela jasné, následky útoku omezuje dobrý záložní program, samozřejmě pokud na útok přijdeme.

- **Odepření služby**

Tento útok (anglicky denial of service, DoS) znamená, že počítač nebo síť jsou po útoku vetřelce „méně dostupné“, nebo dokonce zcela „nedostupné“. Snížení dostupnosti znamená, že se systém podstatně zpomalí kvůli zátěži nebo novému plánování úloh, vyvolanému vetřelcem, že je pro právoplatné uživatele k dispozici méně modemu nebo portů, nebo že někteří uživatelé musí být kvůli útoku (a následnému přetížení) odhlášeni apod. Nedostupnost pak znamená, že se vetřelci podařilo systém zcela vyřadit z provozu.

Útočník si může zkusit takto z dlouhé chvíle vyřadit z provozu například počítač, který řídí veřejnou telefonní ústřednu. Tím se ale bohužel zablokují zároveň volání na tísňové linky a přeruší se hlasové a radarové spojení v řízení letového provozu mezi řídicí věží a vzdálenými rádiovými anténami a dalšími řídicími věžemi. A to už může vést k přímé ztrátě na životech. Poznamenejme, že jakékoli narušení leteckého provozu ve Spojených státech, které způsobí ztrátu života, je těžký federální zločin a trestá se dokonce smrtí.

- **Útočník zneužívá vaše servery jako základnu k dalším útokům**

Při tomto útoku může dojít k odepření služby, a to jednak z důvodu ztráty přenosových kapacit, které využívá útočník, a jednak proto, že vás ostatní mohou zablokovat jako „crackerskou síť“. Tento útok může proto ve svém důsledku vést ke ztrátě veřejného mínění a může vést i k právnímu postihu.

## 2.2 Typy útočníků

- **Crackeři a hackeři**

Tito crackeři (piráti) považují často společnosti a úřady, do jejichž počítačů se vlámou, za zločinné nebo naopak jednoduše za nedůležité. Někdy třeba svou činností nic zhoubného

nevykonají (to znamená, že nepoškodí ani nezveřejní důvěrné údaje, ani nezpůsobí odepření služeb), „vykázat“ je ze systému stojí ovšem systémového administrátora čas a peníze. Jindy je ovšem jejich cílem způsobit co největší škody. Jejich útoky se objevují v podstatě nahodile, ale nejvíce tíhnou k „velkým jménům“, tedy typicky k různým velkým, nadnárodním, dobře známým společnostem a vládním úřadům. Polapit crackery je velice obtížné.

- **Konkurenti**

Konkurenci zpravidla jde o způsobení výpadku služeb oběti útoku. Takového stavu pak může s výhodou využít a zákazníky postižené společnosti přebírat pod záminkou kvalitnějších služeb. Toto nekalé jednání je bohužel velmi obvyklé a páchá celosvětově nemalé škody.

Konkurence se také často snaží získat plány nových produktů, seznamy zákazníků, záměry do budoucna atd. Tyto informace slouží často ke krádeži nápadů a přetahování zákazníků, ale někdy se takto dostanou nepříjemné věci i na veřejnost.

- **Kriminální živly**

Zatímco motivem crackerů jako takových zpravidla nejsou peníze, u kriminálních živlů a zločinců tomu bývá přesně naopak, takoví lidé se vlámou do systému pouze za účelem krádeže, vydírání a dalších kriminálně „výnosných“ aktivit. Do podobných útoků může být zapojen také organizovaný zločin.

- **Extremisté a teroristé**

Někteří jednotlivci a některé bohatě financované, pečlivě strukturované organizace se mohou do systému vloupat v rámci nějakého „morálního poslání“ nebo náboženské „křížové výpravy“. Existuje řada skupin, jejichž členové konali v minulosti kriminální činy proti počítačům nebo dokonce proti fyzickým objektům. Sem patří různé protivládní organizace, „aktivisté“, kteří bojují proti velkým nadnárodním společnostem nebo proti jistým průmyslovým oborům, političtí extremisté, nebo ti, kteří jsou pro tohle a proti tam tomu. Jestliže pracujete jako systémový administrátor ve firmě nebo úřadu, který by se mohl stát cílem útoku takovéto extremistické skupiny, musíte proti tomu přijmout příslušná opatření. Imunní není vůči těmto útokům prakticky nikdo.

- **Nespokojení současní i bývalý zaměstnanci**

Útoky současných zaměstnanců se dají předvídat poměrně obtížně, ale při správném auditu se dají pachatelé poměrně snadno chytit, strach z dopadení pak snižuje pravděpodobnost dalších útoků. Nelze než doporučit časté zálohy, které je navíc třeba ukládat takovým způsobem, aby žádný jednotlivec nemohl způsobit jejich ztrátu nebo nepoužitelnost.

Útoky bývalých zaměstnanců se již do jisté míry dají předpovídat - první věc, která nedobrovolně propuštěného zaměstnance napadne, bývá často poškození systému. Většina systémových administrátorů tak dostává smutný úkol, po vyhození zaměstnance šéfem nebo personálním pracovníkem zablokovat přístup tohoto člověka do systému. O zákazu přístupu je přirozeně nutné informovat všechny, kteří by bývalému zaměstnanci mohli nevědomky přístup poskytnout.

Čeho vůbec všichni tito lidé chtějí dosáhnout? Crackerům stačí, když v systému nechají nějakou svou značku, se kterou se pak pochlubí kamarádům a případně i vstoupí ve známost. Tichý cracker chce od vašeho počítače pouze strojový čas procesoru a síťovou komunikační kapacitu, kterou zneužije k útokům na jiné systémy. Nespokojení a vyhození zaměstnanci chtějí firmu samozřejmě poškodit, jejich cílem bývá obvykle smazání nebo změnění kriticky důležitých dat, případně zveřejnění důvěrných informací.

Konkurenti nejvíce touží po tom, jak zvýšit své vlastní zisky a tržní podíl, ale také po snížení vašich zisků a celkovém oslabení firmy jako konkurence. Zneužijí jakékoli informace, které se jim podaří získat. K nejběžnějším zcizovaným datům patří seznamy zákazníků a plány budoucích produktů nebo marketingových kampaní. [8]

### **2.3 Nejčastější chyby dovolující napadení serverové infrastruktury**

- **Nebezpečně slabá hesla**

Používání hesel pro autentizaci uživatelů IT je jedním z kritických míst bezpečnosti informační infrastruktury podniku. Pro bezpečné používání hesel bohužel existuje řada chybných, ale přitom velmi oblíbených doporučení a mýtů.

Heslo by nemělo vzniknout z nějakého údaje o nás či našem okolí, například:

- vlastní jméno či jméno někoho z rodiny, jméno psa, milenky apod.
- rodné číslo či datum narození
- č. domu, adresa, telefonní číslo...
- heslo, 1234...

Nejbezpečnější hesla jsou tedy „nesmyslné“ kombinace znaků. O to hůře si ale heslo zapamatujeme i my sami, a pokud ho pravidelně nepoužíváme, brzy ho zapomeneme. Napsat si heslo někam do poznámek určitě také není dobrý nápad. Vhodnější je vymyslet si k heslu nějakou mnemotechnickou pomůcku, podle které si ho snáze zapamatujeme (tato pomůcka ovšem musí zůstat stejně tajná jako heslo samotné).

Základním kritériem pro bezpečné heslo je obsah nejméně 8 znaků. V dobrém hesle by neměly být použité jen běžné znaky. Čím větší množinu znaků v hesle použijeme, tím je složitější heslo prolomit.

K dispozici máme 10 číslic, 26 základních písmen abecedy (a-z), které můžeme zdvojnásobit použitím velkých a malých písmen, dále můžeme přidat znaky s diakritikou a nakonec i interpunkční znaménka ( . , ; - ? ! ...). Výhodné je také využít speciálních znaků ( @ # & \$ ^ \_ \*). Dohromady tedy máme k dispozici přes 80 znaků relativně snadno použitelných na běžné klávesnici.

Nezapomínejme však, že na internetu některé servery nepodporují použití určitých speciálních znaků z bezpečnostních důvodů, stejně tak budeme mít problém při přístupu z počítače, kde není definováno české rozložení klávesnice. [9]

- **Otevřené síťové porty**

Stejně jako je každý účet v systému pro crackera potenciální cestou k vlámání, je každá síťová služba přímo silnicí. U do serverů se implicitně instaluje obrovské množství nejrůznějšího softwaru a služeb. Zcela záměrně preferují pohodlí před bezpečností, i když mnohé ze softwaru a služeb vůbec nejsou potřeba, ba dokonce ani nejsou žádoucí. Je třeba si tedy dát tu práci a odstranit veškerý software a služby, které nejsou nezbytně potřeba. Anebo ještě lépe - vůbec je neinstalovat.

Přehled spuštěných služeb spustíme například v Linuxu příkazem `netstat -a tu v`, případně s pomocí programu `ports`. Oběma postupy se vypíší všechny otevřené porty v systému. Takových otevřených portů může mít přitom i domácí systém několik desítek nebo stovek, rozsáhlý síťový server jich může mít ještě více.

Pokud se mezi výsledky nacházejí služby, které na tomto počítači nehodláte poskytovat, vyřadte je z činnosti. Mnohé z distribucí nabízejí vypínání služeb v ovládacím panelu, například Red Hat a Mandrake. Také je vhodné odstranit příslušné binární soubory z disku, nebo jim alespoň příkazem `chmod` změnit přístupová práva na 0, zejména pokud se jedná o programy s příznakem `set-UID` nebo `set-GID`.

Mezi nejoblíbenější služby, které se v mnoha distribucích Linuxu instalují implicitně, patří například NFS, finger, vzdálené „r\*” služby příkazového interpretu, provádění a přihlášení (rsh, rexec a rlogin), FTP, telnet, sendmail, DNS a linuxconf. Přinejmenším některé z nich by však na většině systému neměly být v provozu. Většinu těchto služeb ovládá konfigurační soubor v adresáři /etc/inetd.conf.

- **Staré verze softwaru**

Žádný serverový operační systém není dokonalý. Každý měsíc se v každém objevuje množství nových zranitelných míst. Netřeba ovšem propadat kvůli tomu beznaději. Rychlost, s jakou se problémy nacházejí a opravují, je (především v Linuxu) velmi rychlá. Administrátor musí tedy průběžně sledovat komunitní weby a informační báze a aktualizace doplňovat. Na Windows serverech takovéto aktualizace probíhají automaticky prostřednictvím služby Windows update.

Každá distribuce Linuxu má poštovní konferenci, do níž je možnost se přihlásit, vydává bezpečnostní dokumenty (bulletiny) a má k dispozici server FTP nebo WWW, na němž jsou k dispozici opravy. Existují také vynikající nezávislé poštovní konference věnované bezpečnosti, jako je například Bugtraq a X-Force Alert.

- **Nezabezpečené a chybně nakonfigurované programy**

Počet bezpečnostních chyb v běžně používaných linuxových programech i jejich závažnost se natolik podstatným způsobem snížily, že jsem ve výčtu nejčastějších bezpečnostních děr úplně vypustil téma nedostatečné fyzické bezpečnosti. Na jeho místo jsem zařadil provozování nebezpečných programů (jako je rsh, NFS, portmap a FTP) v jiných než přísně kontrolovaných situacích a provozování nesprávné konfigurace ostatních programů. Tyto „ostatní programy“ jsou schopny dobrého zabezpečení právě jen při správné konfiguraci.

Systémoví administrátoři by měli jistě dobře vědět, že protokoly POP a IMAP (pokud nejsou zapouzdřené v obálce SSL), telnet a FTP odesílají hesla v podobě prostého textu. Také, že služby NFS a portmap mají za sebou historii mnoha problémů a chyby v návrhu autentizace. Mnozí přesto uvedené nástroje používají a potom se diví, když jim do systému někdo pronikne. Lépe je tedy používat namísto nich raději spop, simap, SSH a scp nebo sftp z balíku SSH.

Mnohé z programů se dají považovat za bezpečné - jak jsem se již zmínil - jen při správné konfiguraci. Často jsou ale nakonfigurovány chybně. Někdy se za těmito chybami skrývá

chabé proškolení či nedostatečné pochopení možných rizik, zatímco jindy administrátoři používají nebezpečné funkce úmyslně protože je jednoduše systém nabízí. Nedávným případem jsou skriptové funkce jazyka PHP ve webovém serveru Apache. K tomuto jazyku se váže celá řada bezpečnostních problémů, které jsou dobře známé, hojně publikované, a stejně je hodně lidí používá nebezpečným způsobem a nedokáže k nim najít alternativu.

Než se rozhodneme uvést v systému do provozu jakoukoli službu (nebo než například změníme možnosti služby a způsob jejího provozování), je třeba si důkladně prověřit její bezpečnost nejlépe řízenou simulací napadení.

- **Nedostatečné prostředky a chybně stanovené priority**

V mnoha organizacích se stává, že nadřizení jednoduše neschválí dostatečné finanční prostředky, se kterými by systémoví administrátoři mohli vybudovat dobré zabezpečení. Je jasné, že dobrá bezpečnost systémů nepřichází jen tak náhodou, sama od sebe. Skutečně vyčerpávající bezpečnostní řešení se skládá z celé řady elementů. Pro zabezpečení systémů v dané organizaci je potřeba správné vzdělání administrátorů, návrh sítě, odpovídající implementace, školení uživatelů, údržba a také neustálá ostražitost. Pokud není bezpečnost v dané organizaci dostatečně podporována (jinými slovy financována), bývá často omezena jen na to, co se systémový administrátor rozhodne udělat sám ze svého rozhodnutí. A jestliže není ochoten věnovat bezpečnosti třeba i svůj volný čas, stejně bude vina za případné narušení bezpečnosti na něm. Díky tomuto se systémový administrátor dostává mezi problémy, za které ve skutečnosti není přímo odpovědný. Jinými slovy, vedení firmy mu nedovolí zavést takové změny, jaké jsou pro dobré zabezpečení sítě a pro správný chod podniku nezbytné.

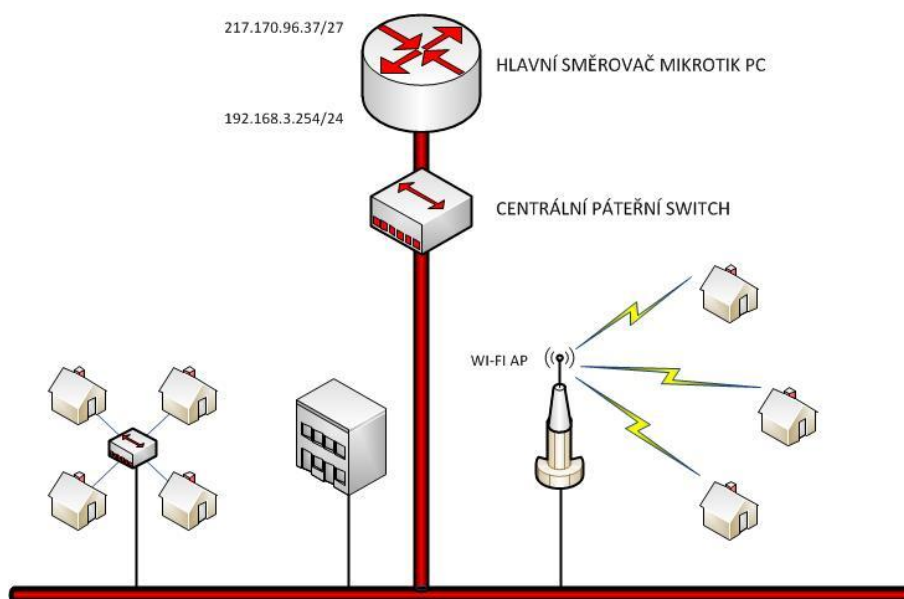
Tento nedostatek by neměl být žádným „technickým“ problémem, ale přesto bylo zjištěno, že je v mnoha organizacích skutečně příčinou průniku do systémů. [8]

## **II. PRAKTICKÁ ČÁST**

### 3 KONFIGURACE FIREWALLU V PŘÍSTUPOVÉ SÍTI

Vhodně konfigurovat hlavní směrovač v přístupové síti včetně všech bezpečnostních restričních opatření je náročný úkol i pro zkušeného systémového administrátora. Je třeba si zejména uvědomit, jaké služby bude chtít na síti provozovat, jaké klienty a s jakými požadavky lze na síti očekávat. Neexistuje tedy univerzální návod pro tuto aplikaci, zabezpečení každé sítě je totiž svým způsobem unikátní.

Pro praktickou ukázkou je vybrán jednoduchý případ sítě, kde centrální směrovač bude připojen do sítě internet a bude tvořit přístupový uzel pro větší množství klientů. Jednotliví klienti budou připojeni pomocí privátních adres v rozsahu 192.168.3.0/24. Na routeru bude probíhat jejich NAT překlad za adresu 217.170.96.37 a tím bude zajištěna funkčnost internetu. Na směrovači dále poběží služby firewall, queue, VPN a jiné. Praktická část bude zaměřena zejména na konfiguraci firewallu.



Obr. 4. Příklad sítě pro praktickou ukázkou.

#### 3.1 Seznámení s platformou Mikrotik – RouterOS

Vývoj MikroTik RouterOS sahá do roku 1995 kdy společnost MikroTik začala svou činnost vývojem a prodejem bezdrátových systémů zejména pro ISP. Původně byl tento OS vyvíjen v Lotyšsku pro dřívější Sovětský svaz. Následné zkušenosti s PC přivedly vývojáře k vybudování routovacího software MikroTik v2 PC, který přinesl výraznou stabilitu, ovladatelnost a flexibilitu pro všechny typy komunikačních periférií a kompatibilitu routovacích systémů založených na standardu PC.

MikroTik RouterOS je operační systém založený na bázi Linux OS, vhodný zejména pro náročné síťové servery, jako bezpečný HW firewall, pro řešení bezdrátových spojů popřípadě domácí router se snadnou GUI konfigurací.

Tento routerový operační systém je koncipován pro platformy: i386, mips, powerpc a je distribuován v podobě instalačních balíčků NPK pro embeded řešení, v podobě předinstalovaného systému na routerboardu<sup>2</sup> či v podobě klasického ISO souboru jako obrazu CD k vypálení a instalaci na PC.

### 3.1.1 Příklady použití systému Mikrotik - RouterOS

- Bezpečnostní Firewall (pravidla typu iptables)
- Omezující Firewall (QoS)
- VPN Server/Klient s podporou protokolů PPP, PPTP, L2TP, OVPN, EoIP, IPsec
- WiFi zařízení v režimech AP, Klient, WDS, N-streeme
- Kompletní hotspotové řešení pro hotely, letiště, kavárny včetně billingu
- Proxy server
- Bridge
- Router s podporou dynamických protokolů (RIP, OSPF, BGP, MME)
- Syslog
- TrafficMonitor Server

### 3.1.2 Možnosti konfigurace

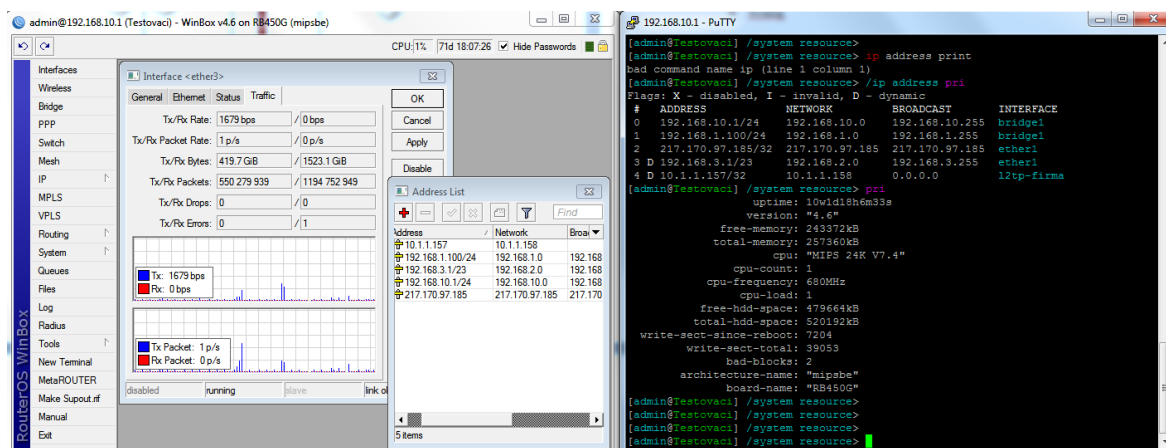
Komunikace s tímto OS se v současnosti provádí zejména přes GUI Winbox, ssh, telnet, sériovou konzoli, Mac-telnet (specifický protokol komunikující po 2. síťové vrstvě na správu OS bez zavedení IP adres).

Konfigurace přes webové rozhraní je značně omezená. V tomto lze konfigurovat pouze základní parametry a slouží výhradně pro začínající uživatele, kteří svůj Mikrotik nastavují

---

<sup>2</sup> Routerboard je embeded hardwarové řešení přímo společnosti Mikrotik. Jedná se zpravidla o nepříliš výkonné routery pro účely menších ISP sítí nebo jako domácí gateway. Kompletní přehled aktuálních typů nalezneme na [www.routerboard.com](http://www.routerboard.com)

jako klientské zařízení či domácí router bez větších systémových nároků. Ovšem v nejnovější stabilní verzi uvolněné v květnu 2011 je již možnost komplexního webového managementu nazvaného vývojáři WebFig (zatím ve verzi beta). To vše na základě požadavků administrátorů, pro které bylo klíčové svůj server jednoduše spravovat z vyspělých mobilních telefonů, tabletů či komunikátorů pouze pomocí webového prohlížeče.



Obr. 5. Srovnání konfigurace přes GUI WinBox a SSH přes terminál PuTTY.

### 3.1.3 Potřebné vybavení

Operační systém můžeme nainstalovat na takřka libovolný počítač. Pochopitelně je výhodné jej instalovat na tovární serverové platformy, které zaručí jistou stabilitu a jsou koncipovány na nepřetržitý provoz. Pro praktické předvedení je třeba mít alespoň dvě síťová rozhraní typu ethernet pro vstupní a výstupní část.

Obraz ISO instalačního disku je volně ke stažení na stránkách výrobce.<sup>3</sup> Obraz disku vypálíme na CD a naboťováním z něho spustíme instalaci. Instalace proběhne během pár minut bez nutnosti zásahu uživatele.

Jakmile je server připraven a nainstalován, zbývá se jen připojit pomocí RJ45 patchcordu<sup>4</sup> do libovolného síťového rozhraní a začít konfigurovat nejprve pomocí vrstvy L2 systémem mac-telnet.

<sup>3</sup> ke stažení na <http://www.mikrotik.com/download.html>. Mikrotik - RouterOS je licenční software, proto je nutné zakoupit licenci na základě vygenerovaného ID u výhradního zastoupení společnosti v ČR. Jednotlivé licenční modely jsou dopodrobna rozebrány na [http://wiki.mikrotik.com/wiki/Manual:License\\_levels](http://wiki.mikrotik.com/wiki/Manual:License_levels)

<sup>4</sup> krátký ethernetový propojovací UTP kabel, opatřen z výroby konektory RJ45 dle standardu T-658B

V čisté instalaci jsou spuštěny jen služby ftp (port 21), ssh (port 22), telnet (port 23) a www (port 80). Dále si můžeme všimnout, že se nám zobrazili jednotlivá síťová rozhraní v záložce interfaces včetně jejich názvů.

## **3.2 Konfigurace pro zajištění funkce internetu**

Základní nastavení směrovače pro funkčnost internetových služeb spočívá zejména v přiřazení jednotlivých IP adres odpovídajícím síťovým rozhráním, konfigurací a spuštěním DHCP serveru, definicí překladu privátních adres NAT masquerade a usměrnění odchozích paketů nastavením default gateway.

### **3.2.1 Přiřazení IP adres**

Od poskytovatele konektivity naší sítě jsme dostali informaci, že pro zařazení naší sítě do internetové hierarchie nám byla přidělena veřejná adresa 217.170.96.37/27. Tu přiřadíme na interface ether1, který označíme jako WAN. Ta nám bude sloužit pro připojení směrovače k externí síti. Na síťové rozhraní ether2, kde budou připojeni jednotliví klienti je vybrána síť 192.168.3.0/24. Obsloužit v této síti lze až 253 klientů a v případě nedostatku není problém adresní prostor rozšířit. IP adresa 192.168.3.254 v této síti je rezervována pro tento směrovač a bude sloužit jako výchozí brána pro jednotlivé klienty. Síťovému rozhraní ether2 přiřadíme také síť 192.168.2.0/24 zastoupenou IP adresou 192.168.2.254/24. V tomto rozsahu se nebude pohybovat žádný klient, bude sloužit pouze k přístupu na management ostatních zařízení v síti (switche, AP, ...).

Terminálový příkaz pro přiřazení IP adres je:

```
/ip address add address=217.170.96.37/27 interface=ether1
/ip address add address=192.168.3.254/24 interface=ether2
/ip address add address=192.168.2.254/24 interface=ether2
```

### **3.2.2 Spuštění DHCP serveru**

Protokol DHCP se používá k automatickému přidělování IP adres jednotlivým koncovým zařízením ve společné síti. Tento protokol umožňuje pomocí DHCP serveru nastavit všem stanicím kompletní sadu parametrů sloužících pro obousměrnou komunikaci v sítích.

Klienti žádají server o IP adresu, ten u každého klienta eviduje půjčenou IP adresu a čas, do kdy ji klient smí používat (doba zapůjčení, anglicky lease time). Poté co vyprší, smí server adresu přidělovat jiným klientům. Po připojení do sítě klient vyšle broadcastem DHCPDISCOVER paket. Na ten odpoví DHCP server paketem DHCPOFFER s nabídkou

IP adresy. Klient si vybere nabídnutou IP adresu a o tu požádá paketem DHCPREQUEST. Server mu ji vzápětí potvrdí odpovědí DHCPACK.

Jakmile klient obdrží DHCPACK, může už IP adresu a zbylá nastavení používat.

V našem serveru vytvoříme DHCP server pouze na ether2, který bude dynamicky přidělovat IP v rozsahu adres 192.168.3.1-253.

Série příkazů pro spuštění DHCP-serveru:

```
/ip dhcp-server setup
  dhcp server interface: ether2
  dhcp address space: 192.168.3.0/24
  gateway for dhcp network: 192.168.3.254
  addresses to give out: 192.168.3.1-192.168.3.253
  dns servers: 217.170.96.24,217.170.96.2
  Select lease time: 3d
```

### 3.2.3 NAT překlad

Překlad síťových adres NAT zavádíme ve třech případech:

- z důvodu nedostatku veřejných IP adres
- potřebujeme-li schovat síť za jednu IP adresu
- pokud máme přidělenou jen jednu veřejnou IP a je nutné připojit více PC

Překlad adres poskytuje metodu překladu adres počítačů protokolu IP v jedné síti na adresy IP počítačů v jiné síti. Směrovač IP s povoleným překladem adres NAT nasazený na hranici setkání privátní sítě s veřejnou sítí umožňuje pomocí této služby překladu přístup počítačů v privátní síti k počítačům ve veřejné síti.

Technologie překladu adres NAT byla vyvinuta k poskytování dočasného řešení problému vyčerpání adres IPv4. Počet dostupných globálně jedinečných (veřejných) adres IPv4 je příliš nízký, aby pojmul rychle rostoucí počet počítačů, které potřebují přístup k Internetu. I když již existuje dlouhodobé řešení – vývoj adres IPv6 (Internet Protocol version 6) – není tento protokol dosud rozšířen. Technologie překladu adres NAT umožňuje počítačům v libovolné síti využívat opakovaně použitelné privátní adresy pro připojení k počítačům s globálně jedinečnými veřejnými adresami v internetu.

Nesmíme zapomenout, že překlad adres sekundárně zajišťuje další stupeň zabezpečení pro naši síť, potažmo klienty. NAT útočníkovi výrazně ztěžuje:

- Mapování topologie sítě a zjišťování informací i konektivitě
- Zjištění počtu provozovaných systémů v síti
- Zjištění typu provozovaných počítačů a jejich operačních systémů
- Vedení různých útoků s odepřením služeb (DoS)

Překlady síťových adres NAT provozujeme tedy na vhodném zařízení v síti, zpravidla se jedná o firewall nebo směrovač, v našem případě Mikrotik server.

Příkaz pro zavedení NAT pravidla pro síť 192.168.3.0/24:

```
/ip firewall nat add action=masquerade chain=srcnat
src-address=192.168.3.0/24
```

### 3.2.4 Nastavení výchozí routy

Poslední, co je třeba ve směrovači definovat, je výchozí brána. Jak již název napovídá, hlavním úkolem routeru či jinak řečeno směrovače, je dle stanovených kritérií v routovací tabulce směrovat správným směrem příchozí i odchozí pakety.

Pravidla pro směr toku směrem z internetu ke klientům, jsou v routovací tabulce vytvořeny dynamicky DHCP serverem. Pokud nebudeme mít za již vytvořenou privátní síť další podsíť, do které chceme mít přístup a mít o ní kompletní přehled, není nutné další statické routy vytvářet. Toto neplatí pro opačný směr. Směr z vytvořené sítě do internetu je třeba jasně určit a to právě takzvanou výchozí routou. Zápis výchozí routy by se dal slovně vyjádřit jednoduše – veškerý provoz směrem do internetu směřuj na IP 217.170.96.33 přes ether1. Adresu výchozí brány opět dostaneme od našeho poskytovatele konektivity.

Zavedení výchozí routy provedeme takto:

```
/ip route add dst-address=0.0.0.0/0 gateway=217.170.96.33 distance=1
```

### 3.2.5 Ostatní nastavení

Teď je již směrovač kompletně připraven pro běžný provoz. Po připojení k internetu pomocí externího síťového rozhraní, je možno připojit přes datový přepínač jednotlivá koncová zařízení. V těch budou nadále veškeré internetové služby aktivní.

V operačním systému Mikrotik – RouterOS je ale vhodné konfiguraci doplnit o další neméně důležité parametry.

Na prvním místě je jistě nastavení hesla pro přístup ke konfiguraci směrovače. To by mělo bezesbytku splňovat již stanovená kritéria. O způsobu a doporučeních pro jeho vhodné nastavení bude pojednáno dále.

Pro případ, že v síti bude více podobných routerů, je nutno nastavit identitu serveru. Pokud totiž bude využívat kterýkoliv z klientů v síti podobné zařízení s operačním systémem RouterOS, je jediný identifikační znak, podle kterého je centrální směrovač dohledatelný, MAC adresa a právě tato identita. Tyto dva jediné identifikační údaje vysílá směrovač pomocí broadcast paketů na ISO/OSI vrstvě 2.

Nastavení identity je možno provést příkazem:

```
/system identity set name=PraktickaBC
```

V logu zařízení je možnost sledování změn či jiných událostí dle předem navolených kritérií. Aby události byly časově dohledatelné, nebo aby byla možnost využití skriptovacího modulu scheduleru, je třeba využít synchronizaci času pomocí protokolu NTP. Je možno využít veřejných NTP serverů sítě CESNET. Primárního tik.cesnet.cz a sekundárního tak.cesnet.cz. Při překladu na IP adresy tedy 195.113.144.201 respektive 195.113.144.238.

Zavedení synchronizace NTP serverů se provádí:

```
/set mode=unicast primary-ntp=195.113.144.201  
secondary-ntp=195.113.144.238
```

### **3.3 Ochrana vlastních uživatelů služeb**

Jednotliví klienti jsou z hlediska síťové infrastruktury nejlépe chráněni NAT překladem adres a důsledným uzavřením veškerých TCP portů, které nejsou pro provoz nutné. TCP porty jsou uzavřeny již ve výchozím nastavení směrovače a jejich otevření a směrování k jednotlivým klientům je nutné provádět pouze na vyžádání.

Z hlediska vnitřní sítě ovšem může dojít k útoku na počítač od klienta zapojeného ve stejném subnetu jako je počítač oběti. Jinak řečeno klient stejné společnosti, zapojený do společné sítě má možnost při slabém zabezpečení infrastruktury využít běžně sdílených prostředků kteréhokoliv jiného připojeného počítače třeba v sousedním domě.

### **3.3.1 Eliminace peer-to-peer komunikace a přenosu dat mezi koncovými uživateli**

Z bezpečnostního hlediska se jedná o jedno z největších rizik. Omezení peer-to-peer komunikace mezi klienty není standardně možné běžně řešit na úrovni směrovače. Ve firewallu by se však dala definovat pravidla na úrovni síťových rozhraní. Jedno by diktovalo, že pouze ty pakety, které vstupují do směrovače z ether2 a vycházejí přes ether1 nebo naopak vstupují přes ether1 a vystupují na ether2 jsou akceptována. Všechny ostatní pakety by padly pod třetí pravidlo, které by vykonalo jejich zahození. Tím zajistíme, aby nebylo možné směřovat provoz od klienta zpět přes stejné rozhraní k jinému klientovi a tím zamezit jejich nežádoucí sdílení. Toto řešení není však příliš využitelné v praxi, nabízejí se jiná, vhodnější.

Mnohem elegantnější řešení tedy je vše řešit na úrovni nastavitelných switchů. Ve většině z nich existuje funkce port isolation<sup>5</sup>. Ta jednoduchým způsobem eliminuje toto riziko a ochrání uživatelům jejich soukromá data.

Velmi vhodné je také klientům doporučit instalaci domácího směrovače za vstupní přípojku domácnosti či firmy. NAT překlad společně se správnou konfigurací routeru definitivně zamezí přístupu do sítě nižší úrovně zvenčí a sdílení mezi domácími nebo firemními počítači zůstává zachováno.

### **3.3.2 Omezení výměnných sítí, šíření nelegálního obsahu a rizika přehlcení sítě**

V praxi se poskytovatel internetových služeb často setkává s klienty, kteří formou peer to peer výměnných sítí šíří nelegální autorský obsah a musí následně čelit obsílkám policie a dohledáváním oněch šířitelů. Stejně tak je takový klient zdrojem průběžného zahlcování síťových kapacit tím, že generuje záplavy paketů mnohdy s navázanými až 200 spojeními. Tímto je schopno i pár klientů účastnících se výměny dat například pomocí torrentů zahltit síťový adaptér směrovače takovým způsobem, že dojde k výraznému poklesu kvality služeb zbytku zákazníků anebo k jejich úplnému přerušení. Ze strany poskytovatele služeb lze pomocí firewallových pravidel tomuto jednání zabránit několika způsoby.

---

<sup>5</sup> Port isolation je funkce na datových přepínačích, umožňující logické oddělení portů při zachování standardního provozu ostatních služeb. Každý výrobce označuje tuto funkcionalitu jinak, port isolation je pouze obecný název.

První z nich je omezení počtu spojení na zákazníka. Běžný klient rozdíl nepozná, i plné využívání v rámci jednoho PC generuje nejvýše 20 spojení. Optimální je tedy hodnota 100 spojení na jednu IP adresu. Toto pravidlo definujeme v konzolovém menu takto:

```
/ip firewall filter add action=drop chain=forward
connection-limit=100,32 protocol=tcp src-address=192.168.3.0/24
```

Druhý způsob je omezit funkce výměnných sítí úplně. RouterOS obsahuje vyspělé funkce detekce takových přenosů formou detailní analýzy paketu. Při odhalení jistých specifických znaků je spojení přidáno označení (connection mark) „p2p“ pomocí funkce mangle.

Funkce mangle je definována jako průchozí. Označení každého spojení pocházejícího z klientské aplikace výměnných sítí aktivujeme takto:

```
/ip firewall mangle add action=mark-connection chain=prerouting
new-connection-mark=p2p p2p=all-p2p passthrough=yes
```

S tímto označeným spojením je možno ve firewallu dále pracovat a provést drop každého z nich. O tomto kroku je ovšem nutné klienty informovat dříve, než dojde k jejich připojení. Dochází totiž k omezení obecných funkcí internetových služeb a mnohé klienty toto zabezpečení od nabídky může odradit, jiné naopak přilákat.

Pravidlo vylučující provoz výměnných sítí deklaruujeme tímto způsobem:

```
/ip firewall filter add action=drop chain=forward
connection-mark=p2p src-address=192.168.3.0/24
```

Posledním způsobem je omezit funkce výměnných sítí také, ovšem pouze v produktivní době. To znamená, že výměnné sítě budou neaktivní pouze po dobu pracovních dní od 7:00 do 23:00.

```
/ip firewall filter add action=drop chain=forward connection-mark=p2p
src-address=192.168.3.0/24 time=7h-23h,mon,tue,wed,thu,fri
```

Tyto pravidla lze libovolně kombinovat či editovat dle potřeb každého poskytovatele.

### **3.3.3 SMTP ochrana před skrytým odesláním spamu**

Další z případů, kdy v kooperaci s poskytovatelem připojení vstupuje do hry policie, nastává v případě, kdy si klient do svého PC připustí škodlivý kód, který skrytě rozesílá nevyžádanou poštu pomocí neautorizovaných SMTP serverů. Klient aniž cokoliv tuší, dochází prostřednictvím jeho osobního počítače k protiprávnímu jednání. Na poskytovateli

je poté pomocí syslogu a služby netflow nebo torch takového uživatele vyhledat a dalšímu šíření zabránit odpojením od sítě.

Elegantnější variantou je však pomocí firewallových pravidel zamezit odesílání z jiných, než zabezpečených a známých SMTP serverů na TCP portu 25.

Skupinu nejznámějších bezpečných SMTP serverů je třeba nejprve vymežit v sekci address-list. Tu lze na základě důkladného prověření operativně rozšiřovat podle požadavků klientů. Primárním serverem odchozí pošty ovšem bude server nejbližší, v tomto případě 217.170.96.3.

```
/ip firewall address-list add address=217.170.96.3 comment=nase_smtp
list=overene_smtp

/ip firewall address-list add address=77.75.76.48
comment=smtp.seznam.cz list=overene_smtp

/ip firewall address-list add address=90.183.38.22
comment=mail.centrum.cz list=overene_smtp

/ip firewall address-list add address=195.178.88.66
comment=smtp.utb.cz list=overene_smtp
```

Blokovat provoz na jiných, než ověřených SMTP serverech můžeme na TCP portu 25 tímto způsobem:

```
/add action=drop chain=forward dst-address-list=!overene_smtp
dst-port=25 protocol=tcp
```

### **3.4 Ochrana síťového provozu**

Pro ochranu kvality síťového provozu a kontinuální dostupnosti služeb zákazníkům je nutné nastolit řadu opatření.

Začít je třeba ve striktně definovaných režimových opatření týkajících se přístupu do serverové místnosti a datových rozvaděčů. Zajištěn přístup do centrální místnosti a podružných domovních rozvaděčů mohou mít jen ověřeni technici, kteří prošli technickými i bezpečnostními školeními a mají u podnikatele osobní důvěru.

Je třeba udržovat pravidelné minimálně denní automatizované zasilání nebo ukládání zálohy konfigurace směrovač. Stejně tak je vhodné, mít dle finančních možností v rozvaděči umístěn druhý, redundantní směrovač pro případ jeho náhlého selhání.

Každý, zejména pak centrální rozvaděč je nutné krýt nepřetržitě zdrojem náhradního napájení UPS pro případ výpadku síťového napětí. Tímto lze velmi levně zabránit nechtěnému výpadku jednotlivého segmentu či celé sítě.

Z hlediska konfigurace je třeba vyloučit proniknutí do správy směrovače. Vhodnou variantou je v tomto případě ochrana přístupu velmi silným heslem a omezení služeb telnet, SSH a WinBox pro přístup pouze z vnitřní sítě, nikoliv externě z internetu. Konfigurace se poté provádí po navázání šifrovaného VPN tunelu PPTP do privátní sítě.

### 3.4.1 Script pro denní zaslání zálohy konfigurace na mail

Mít vždy a za každých okolností zálohu posledních konfigurací je jedno z nejdůležitějších pravidel systémového administrátora. V operačním systému RouterOS lze toto vyřešit velmi elegantně pomocí jednoduchého skriptovacího jazyka. Tento skript se nám postará o vytvoření souboru s kompletní zálohou konfigurace a jeho následného odeslání emailem na zvolenou adresu.<sup>6</sup> V mailové schránce tedy máme vždy aktuální zálohu nanejvýš 24 hodin starou. Název výsledného souboru je pro přehlednost generován ve tvaru „identita-rrrrmmdd.backup“.

Skript pro pravidelné odesílání záloh zavedeme pomocí terminálu:

```
/tool e-mail set server=217.170.96.3 from="krajca@email.cz"

/system script add name=backup source={/system backup save
  name=([/system identity get name] . "-" . [:pick [/system clock get
  date] 7 11] . [:pick [/system clock get date] 0 3] . [:pick
  [/system clock get date] 4 6]);

/tool e-mail send to="krajca@email.cz" subject=([/system identity get
  name] . " zaloha " . [/system clock get date]) file=([/system
  identity get name] . "-" . [:pick [/system clock get date] 7 11] .
  [:pick [/system clock get date] 0 3] . [:pick [/system clock get
  date] 4 6] . ".backup");

:delay 10;

/file rem [/file find name=([/system identity get name] . "-" . [:pick
  [/system clock get date] 7 11] . [:pick [/system clock get date] 0
  3] . [:pick [/system clock get date] 4 6] . ".backup")];
```

---

<sup>6</sup> Tento skript není autorovým dílem, je volně přístupný v odpovídající sekci znalostní báze společnosti Mikrotik. Dostupný z [www: http://wiki.mikrotik.com/wiki/Send\\_Backup\\_email](http://wiki.mikrotik.com/wiki/Send_Backup_email)

```
:delay 10;

:log info message=Zaloha odeslana emailem prave ted!}

/system scheduler add name="automaticka_zaloha" on-event="backup"
    start-date=feb/18/2011 start-time=23:55:00 interval=1d
```

### 3.4.2 Ochrana před neautorizovaným přístupem na server

Nejjednodušší forma zamezení neautorizovanému přístupu do konfiguračního rozhraní serveru je ochrana pomocí velmi silného hesla. V továrním nastavení je uživatelské jméno admin a přístup je povolen bez hesla.

Uživatelské jméno admin nebo root se vyskytuje u většiny serverů a neopatrní administrátoři jej nezmění a zvyšují tak šanci nad ovládnutím sítě útočníkům. V ideálním případě je administrátorské uživatelské jméno i heslo s plnými právy naprosto jedinečné a znají jej pouze dva lidé pro případ selhání lidské paměti.

Heslo vygenerujeme nebo vymyslíme dle výše stanovených kritérií. Vytvoříme nového uživatele s jedinečným uživatelským jménem příkazem:

```
/user add name=krajca group=full
    password=hust0.d3monsky>krut0<pr1sn3*h3s10!
```

Ostatní ověřené uživatele můžeme pověřit třemi úrovněmi práv full-read-write. Uživatelské účty s patřičnými právy dle potřeby přiděluje administrátor jednotlivým pracovníkům především na základě předpokládané činnosti v síti, podle stupně technické erudice jednotlivce a v neposlední řadě také dle osobní důvěry.

### 3.4.3 Omezení přístupu ze vzdálených sítí

Jakékoliv síťové zařízení připojené do internetu prostřednictvím veřejné IP adresy je denně namáháno automatizovanými útočníky. Ti jsou schopni otestovat i několik kombinací uživatelských jmen i hesel do jedné sekundy. Na Obr. 4 vidíme syslog konfigurovaného směrovače, který byl do internetu připojen necelé dvě hodiny.

```
05:02:48 system,error,critical login failure for user administrator from 61.220.173.154 via ssh
05:02:52 system,error,critical login failure for user root from 61.220.173.154 via ssh
05:03:01 system,error,critical login failure for user alexandre from 61.220.173.154 via ssh
05:03:08 system,error,critical login failure for user joseluis from 61.220.173.154 via ssh
05:03:12 system,error,critical login failure for user ppazmino from 61.220.173.154 via ssh
05:03:16 system,error,critical login failure for user utilidades from 61.220.173.154 via ssh
05:03:20 system,error,critical login failure for user utilidad from 61.220.173.154 via ssh
05:03:23 system,error,critical login failure for user amstelecom from 61.220.173.154 via ssh
05:03:29 system,error,critical login failure for user dedlogistica from 61.220.173.154 via ssh
05:03:36 system,error,critical login failure for user dsantiago from 61.220.173.154 via ssh
05:03:44 system,error,critical login failure for user marcia from 61.220.173.154 via ssh
05:03:48 system,error,critical login failure for user consultoria from 61.220.173.154 via ssh
05:03:51 system,error,critical login failure for user primaveras from 61.220.173.154 via ssh
05:03:56 system,error,critical login failure for user salvatore from 61.220.173.154 via ssh
05:04:00 system,error,critical login failure for user comerciais from 61.220.173.154 via ssh
05:04:04 system,error,critical login failure for user cartas from 61.220.173.154 via ssh
05:04:08 system,error,critical login failure for user carta from 61.220.173.154 via ssh
05:04:11 system,error,critical login failure for user moralez from 61.220.173.154 via ssh
05:04:15 system,error,critical login failure for user nieves from 61.220.173.154 via ssh
05:04:19 system,error,critical login failure for user sol from 61.220.173.154 via ssh
05:04:24 system,error,critical login failure for user perla from 61.220.173.154 via ssh
05:04:27 system,error,critical login failure for user rocio from 61.220.173.154 via ssh
05:04:31 system,error,critical login failure for user simon from 61.220.173.154 via ssh
05:04:35 system,error,critical login failure for user sergio from 61.220.173.154 via ssh
05:20:38 system,info,account user admin logged in from 192.168.10.3 via winbox
```

*Obr. 6. Pokus o napadení směrovače metodou brutalforce.*

Terminálové služby SSH a telnet jsou nejčastějšími dveřmi do administrace, které se snaží útočníci překonat. Je tedy vhodné, přestože jsme nastavili velmi přísnou vstupní kombinaci uživatelského jména a hesla jim pokusy o tyto útoky odepřít. Nejlépe úplným zabráněním přístupu do administrace z externí sítě. Terminálové služby SSH a telnet fungují na TCP portech 22 respektive 23, grafické rozhraní WinBox na TCP portu 8291. Přístup po těchto portech můžeme pomocí pravidel specifikovat tak, že nám budou dostupné pouze z omezeného rozsahu IP adres nebo dokonce z jedné jediné.

Toho můžeme s výhodou využít a zabránit tak jakémukoli pokusu o prolomení hesla tím, že útočníka k pokusu jednoduše nepřipustíme pomocí vstupní restrikce:

```
/add action=drop chain=input dst-port=22 protocol=tcp
src-address=!192.168.2.0/23

/add action=drop chain=input dst-port=21 protocol=tcp
src-address=!192.168.2.0/23

/add action=drop chain=input dst-port=8291 protocol=tcp
src-address=!192.168.2.0/23
```

V této chvíli je směrovač dostupný přes terminálové služby i přes grafické rozhraní pouze z privátního rozsahu IP adres 192.168.2.0/23. Tento rozsah zahrnuje obě podsítě, které jsou zavedeny na vnitřním rozhraní směrovače. Pokud je třeba konfigurovat server vzdáleně, sestavíme do lokální sítě šifrovaný VPN PPTP tunel.

### 3.4.4 Sestavení šifrovaného VPN PPTP tunelu do sítě

Protokol PPTP pracuje na druhé vrstvě referenčního modelu OSI. Jedná se o standard pro dvoubodové vytáčené spojení mezi dvěma lokálními sítěmi. Při takovémto spojení se jednoduchým a efektivním způsobem dostaneme do vzdálené privátní sítě pomocí zabezpečeného šifrovaného tunelu.

V našem případě můžeme mít tedy přístup k administraci směrovače odkudkoli na světě bez obav z možných bezpečnostních rizik. Jeho výhoda spočívá také v tom, že náš počítač se prakticky nachází ve stejné síti jako ostatní klienti a my se tak můžeme v případě jeho závady jednodušší cestou dopátrat zdroje poruchy.

V systému RouterOS je možnost vytvořit celou řadu šifrovaných privátních spojení v případech kdy zvolený hardware obsahuje odpovídající čip i oblíbené zabezpečení IPSec. Z hlediska dostupnosti napříč všemi operačními systémy i jednoduššími VPN routery byl zvolen protokol PPTP, který nejen z bezpečnostního hlediska jistě dostačuje.

Jako první, je třeba službu aktivovat příkazem:

```
/ppp pptp-server enable
```

Po aktivaci služby je nutné definovat autentifikační údaje použité později při každém vytáčení spojení. Opět je třeba dbát na výběr velmi silného hesla.

```
/add local-address=192.168.2.1 remote-address=192.168.2.2 name=krajca  
password=sdVr!qf_6xW0 profile=default service=any
```

Adresy local a remote jsou spojovací adresy, pod kterými bude vystupovat jedna respektive druhá strana tunelu. Obě adresy se přidělí oběma stranám spojení dynamicky, jedinou podmínkou, je mít vždy ve firewallu vzdáleného počítače povolen provoz směrem do této sítě.

Nyní nám tedy bude při úspěšném navázání spojení z jakéhokoliv PC dynamicky přidělena privátní adresa 192.168.2.2 a výchozí brána 192.168.2.1. V tuto chvíli tedy obcházíme výše deklarovaná pravidla pro omezení vzdálené konfigurace a firewall nás k jinak zablokovaným službám propustí.

## ZÁVĚR

V bakalářské práci byla provedena komplexní a všeobecná analýza rizik v síti internet. Téma bylo pojato ve dvou obecných rovinách. V první byla stanovena známá i méně známá bezpečnostní rizika v síti internet, provedena jejich konkrétní analýza a stanoveny metody aktivní obrany a ochrany vůči nim. To vše z pohledu běžného konzumenta internetových služeb.

Ve druhé rovině byly podobným způsobem vyspecifikovány hrozby pohybující se v oblasti správy serverů a údržby síťové infrastruktury. Na základě načerpaných poznatků byly určeny jednotlivé cíle útoků a analyzován jejich dopad na běžný provoz. Hlubším rozborem problému bylo možno profilovat jednotlivé typy útočníků včetně výčtu situací, ve kterých můžeme jejich útok předpokládat a odhadnout škody jaké mohou svým jednáním napáchat. Byl také sestaven žebříček nejčastějších chyb správců síťové infrastruktury, které mohou vzniku rizikové situace účinně napomáhat.

Načerpané poznatky byly posléze aplikovány v praktické části práce. Jejím cílem bylo navrhnout komplexní řešení rozlehlejší síťové infrastruktury, zejména pak konfigurace centrálního směrovače, který řídí provoz celé sítě se silným důrazem na vhodné zabezpečení. Kompletní soubor restriktivních opatření implementovaný ve firewallu předem vybrané platformy Mikrotik – RouterOS byl navržen takovým způsobem, že nedovolí útočníkům běžným ani sofistikovaným způsobem omezit služby či převzít vládu nad centrálním směrovačem potažmo celou sítí.

Povedlo se najít hranici, kdy veškerá navržená bezpečnostní opatření nikterak nebrání jak běžnému tak i specifitějšímu užívání internetových služeb. Omezení či úplné znemožnění některých služeb by mohlo znamenat vyšší standard bezpečnosti, ovšem za cenu uživatelského komfortu.

Jakákoliv bezpečnostní pravidla v práci uvedená, lze jednoduchým způsobem modifikovat a nasadit dle potřeb a požadavků jednotlivých poskytovatelů internetových služeb. Stejně tak při požadavku klienta na vyšší stupeň zabezpečení pravidlo upravit a vztáhnout pouze k jeho IP adrese.

## ZÁVĚR V ANGLIČTINĚ

The purpose of my bachelor thesis has been to make a complex and general analysis of risks within the internet network. The topic was viewed from two general perspectives. The first one involved stating the well known and less known security risks within the internet network, making their specific analysis and stating methods of active protection against them. All the mentioned aspects were implemented from the viewpoint of a common user of internet services.

Concerning the second perspective, there were specified threats related to the sphere of server administration and maintenance of network infrastructure in a similar manner as within the above-mentioned one. On the basis of the knowledge obtained were determined the individual targets of invasion with the aim to analyze their influence on regular functioning. Thanks to more complex analysis of the problem, it was possible to shape the individual types of the invaders, including specification of the situations in which we are able to expect their invasion and also to estimate damages that can be caused by their activities. There was also assembled a list of the most common mistakes of the administrators of network infrastructure, which may effectively help the creation of a risk situation.

The information obtained was subsequently applied in the practical part of the thesis, the aim of which was to suggest a comprehensive solution of more extensive network infrastructure, in particular configuration of the central router, which manages functioning of the whole network with focus on suitable security. The complete set of restrictive measures implemented in firewall of the predefined platform Mikrotik – RouterOS has been designed in such way that it would not enable the invaders to eliminate services or take over administration related to central router or respectively the whole network neither in ordinary, nor in a sophisticated way.

I succeeded in finding the level in which all the suggested protective measures do not in any way restrict neither ordinary, nor specific use of internet services. Restriction or even restraint of some services could result in higher security standard but at the expense of user comfort.

Any security measures included in the thesis may be modified in a simple way and they may be adjusted to the needs of the specific needs and requirements of individual internet service providers, as well as to adjust the rule to fulfill the requirements of the client

concerning higher level of security by the means of limiting it exclusively to his IP address.

## SEZNAM POUŽITÉ LITERATURY

- [1] Bezpečnost na internetu. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 8.2.2010, last modified on 29.3.2011 [cit. 2011-05-19]. Dostupné z WWW:  
<[http://cs.wikipedia.org/wiki/Bezpe%C4%8Dnost\\_na\\_internetu](http://cs.wikipedia.org/wiki/Bezpe%C4%8Dnost_na_internetu)>.
- [2] FILIP, Radek. Bezpečnostní aspekty internetu. České Budějovice, 2003. 64 s. Bakalářská práce. Jihočeská Univerzita.
- [3] Hoax. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 29.1.2005, last modified on 16.3.2011 [cit. 2011-05-19]. Dostupné z WWW: <<http://cs.wikipedia.org/wiki/Hoax>>.
- [4] MAŤEJŮ, David. Lidovky.cz [online]. 2.9.2009 [cit. 2011-04-19]. Jak se bránit podvodům v internetovém bankovníctví. Dostupné z WWW:  
<<http://mateju.bigblogger.lidovky.cz/c/99648/Jak-se-branit-podvodum-v-internetovem-bankovnictvi.html>>.
- [5] PROCHÁZKA, David. DSL.cz [online]. 24.8.2010 [cit. 2011-04-19]. Rizika sociálních sítí jsou značná. Dostupné z WWW: <<http://www.dsl.cz/clanek/1929-rizika-socialnich-siti-jsou-znacna>>.
- [6] Microsoft security portal [online]. 2011 [cit. 2011-05-19]. Microsoft. Dostupné z WWW:  
<<http://www.microsoft.com/cze/athome/security/spyware/spywarewhat.msp>>.
- [7] THOMAS, Thomas M. Zabezpečení počítačových sítí : bez předchozích znalostí. Brno : Computer Press, 2005. 338 s. ISBN 80-251-0417-6.
- [8] THOMAS, Thomas M. Zabezpečení počítačových sítí : bez předchozích znalostí. Brno : Computer Press, 2005. 338 s. ISBN 80-251-0417-6.
- [9] Bezpečné heslo. In Wikipedia : the free encyclopedia [online]. St. Petersburg (Florida) : Wikipedia Foundation, 6.2.2008, last modified on 6.5.2011 [cit. 2011-05-19]. Dostupné z WWW:  
<[http://cs.wikipedia.org/wiki/Bezpe%C4%8Dn%C3%A9\\_heslo](http://cs.wikipedia.org/wiki/Bezpe%C4%8Dn%C3%A9_heslo)>.

## SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AP	Access Point.
BGP	Border Gateway Protocol.
CD	Compact Disc.
CIA	Central Intelligence Agency.
DMZ	Demilitarized Zone.
DNS	Domain Name Service.
DoS	Denial Of Service.
EoIP	Ethernet Over IP.
FBI	Federal Bureau Of Investigation.
FTP	File Transfer Protocol.
GID	Group Identification.
GUI	Graphical User Interface.
IMAP	Internet Message Access Control.
IP	Internet Protocol.
IPv4	Internet Protocol version 4.
IPv6	Internet Protocol version 5.
ISO	International Organization for Standardization.
ISP	Internet Service Provider.
L2TP	Layer 2 Transfer Protocol.
LAN	Local Area Network.
MAC	Media Access Control.
MME	Mesh Made Easy.
NAT	Network Address Translation.
NFS	Network File System.
NTP	Network Time Protocol.

OS	Operation Systém.
OSI	Open System Interconnection.
OSPF	Open Shortest Path First.
OVPN	Open Virtual Private Network.
P2P	Peer To Peer.
PC	Personal Computer.
PHP	Hypertext Preprocesor.
POP3	Post Office Protocol version 3.
PPP	Point To Point Protocol.
PPTP	Point To Point Tunneling Protocol.
QoS	Quality of Service.
RIP	Routing Information Protocol.
SMS	Small Message Service.
SMTP	Simple Mail Transfer Protocol.
SSH	Secure Shell Network.
SSL	Secure Sockets Layer.
TCP	Transmission Control Protocol.
UID	User Indentification.
USB	Universal Seríal Bus.
VPN	Virtual Private Network.
WAN	Wide Area Network.
WDS	Virtual Distribution Network.
WiFi	Wireless Fidelity.
WWW	World Wide Web.

## **SEZNAM OBRÁZKŮ**

Obr. 1. Typický příklad nevyžádané zprávy. ....	13
Obr. 2. Podvodná žádost o vyplnění osobních údajů. ....	14
Obr. 3. Funkce a zařazení systému firewall v rámci síťové infrastruktury. ....	23
Obr. 4. Příklad sítě pro praktickou ukázkou. ....	33
Obr. 5. Srovnání konfigurace přes GUI WinBox a SSH přes terminál PuTTY. ....	35

## **SEZNAM TABULEK**

Tab. 1. Test antivirových programů z března 2011 zpracovaného společností AV-Comparatives. ....	20
---	----