Návrh systému zabezpečení sítě poskytovatele internetových služeb

Design of Network Security Internet Service Provider

Bc. Tomáš Krajča

Diplomová práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Tomáš KRAJČA**
Osobní číslo:	**A11347**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Návrh systému zabezpečení sítě poskytovatele internetových služeb**

Zásady pro vypracování:

1. **Formou literární rešerše popište současný stav předmětné problematiky a úroveň jeho řešení v informačních zdrojích.**
2. **Vytvořte model pro zkoumání předmětné problematiky z hlediska bezpečnostních rizik z vnitřní i vnější perspektivy a následného hodnocení účinnosti protiopatření.**
3. **Vytvořte systém kriterií pro testování na modelu pro úroveň narušení provozuschopnosti; úroveň neoprávněného proniknutí do systému; úroveň neoprávněného získání informací; úroveň antivirové ochrany; úroveň antispamové ochrany, atd.**
4. **Naznačte přístupy možného řešení předmětné problematiky na různých platformách.**
5. **Prakticky navrhněte a popište vhodnou konfiguraci souboru restrikčních opatření realizovaných na vybrané platformě – zdůvodněte vámi navrhované řešení.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **TOXEN, Bob. Bezpečnost v Linuxu: prevence a odvracení napadení systému. Vyd. 1. Brno: Computer Press, 2003, 849 s. ISBN 80-722-6716-7.**
2. **THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, 338 s. ISBN 80-251-0417-6.**
3. **SELECKÝ, Matúš. Penetrační testy a exploitace: prevence a odvracení napadení systému. 1. vyd. Brno: Computer Press, 2012, 303 s. ISBN 978-80-251-3752-9.**
4. **SOSINSKY, Barrie. Mistrovství ? počítačové sítě: prevence a odvracení napadení systému. Vyd. 1. Brno: Computer Press, 2010, 840 s. Mistrovství (Computer Press). ISBN 978-80-251-3363-7.**
5. **JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. 1. vyd. Praha: Grada, 2007, 284 s. Mistrovství (Computer Press). ISBN 978-80-247-1561-2.**
6. **ENDORF, Carl. Detekce a prevence počítačového útoku. 1. vyd. Praha: Grada, 2005, 355 s. ISBN 80-247-1035-8.**
7. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Vyd. 1. Kralice na Hané: Computer Media, 2008, 98 s. ISBN 978-80-86686-35-6.**
8. **JAŠEK, Roman a Bohumír ŠTĚDROŇ. Informační a datová bezpečnost. Vyd. 1. Zlín: Univerzita Tomáše Bati ve Zlíně, 2006, 140 s. ISBN 80-731-8456-7.**

Vedoucí diplomové práce: **doc. Ing. Jiří Gajdošík, CSc.**
Ústav bezpečnostního inženýrství

Datum zadání diplomové práce: **8. února 2013**

Termín odevzdání diplomové práce: **3. června 2013**

Ve Zlíně dne 8. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Tato diplomová práce přibližuje čtenáři důležité poznatky o systému komplexního zabezpečení sítě poskytovatele internetových služeb a to zejména z pohledu síťového administrátora, nikoliv samotného uživatele. Řeší problematiku rizik hrozících jak z vnější tak z vnitřní části sítě a navrhuje proti nim účinná protiopatření. Zabývá se nejen riziky spojenými s neoprávněným ziskem citlivých informací nebo neoprávněného proniknutí do systému, ale i s rizikem narušení provozuschopnosti a kvality poskytovaných služeb. Rozšířenou formou následně prezentuje výsledky získané zkoumáním na vytvořeném modelu i v následném nasazení v reálném provozu.

Klíčová slova: zabezpečení, firewall, Mikrotik, internet, Linux,

ABSTRACT

This master's thesis brings readers important insights into the system of complex network security implemented by Internet service providers, especially from the perspective of network administrators rather than the users themselves. It addresses the issue of impending risks in the outer and inner environment, and proposes effective countermeasures to fight these risks. It deals not only with the risks associated with gaining unauthorized access to sensitive information and unauthorized entry into the system; it also addresses uptime and its disruptions as well as the quality of the services provided. This is followed by an extensive presentation of the results obtained by examination of the created model and the follow-up deployment and live operation.

Keywords: security, firewall, Mikrotik, internet, Linux

Chci poděkovat vedoucímu diplomové práce, panu doc. Ing. Jiřímu Gajdošíkovi, CSc., za příkladný pedagogický přístup, cenné konstruktivní připomínky a za ochotu věnovat mi svůj volný čas.

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/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 diplomová/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/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 diplomovou/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 – diplomovou/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 diplomové/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 diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/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 diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Internet se dnes řadí ke službám, bez které se již většina moderní populace neobejde. Jeho počátky se datují od šedesátých let minulého století, kdy v USA vznikla síť s názvem Arpanet. Tehdy stál největší mozkový trust tehdejší Ameriky, firma RAND Corporation[1], před nelehkým úkolem zadaným ministerstvem obrany, a to vymyslet, jak by jednotlivé orgány administrativy USA mohly komunikovat i po očekávané jaderné válce. Pokud by ona sama vůbec přestála devastující nukleární úder, velmi naléhavě by potřebovala fungující systém řízení a velení, který by dokázal spojit jednotlivé státy, jednotlivá města, vojenské základny a podobně. Systém fungující i přesto, že by některé z jeho částí mohly být nenávratně zničeny. Řešením se stalo propojení jednotlivých uzlů, které měli v zásadě rovnocenné postavení, a předem se počítalo s jejich potenciální nespolehlivostí. Právě decentralizovanost a kruhová topologie zajišťovala dostupnost služby i po částečném narušení. Postupným rozšířením komunikačních linek na evropský kontinent dala v sedmdesátých letech minulého století vzniknout něčemu, čemuž dnes říkáme internet.

V současné době se dá z podnikatelského hlediska hovořit o tom, že internet tvoří zásadní komoditu, pro kterou neexistuje odpovídající substitut a dá se jako cokoliv jiného nakoupit a prodat. Z toho důvodu zažil v devadesátých letech obchod „s internetem“ nebývalý rozvoj a velcí telekomunikační operátoři uvolnili své internetové kapacity mimo státní správu a akademickou půdu i pro firemní a domácí uživatele. Bohužel však pro manažerskou a obchodní neschopnost tehdejšího inkumbentu, firmy SPT Telecom (později Českého Telecomu, nyní Telefoniky O2) probíhal v našich zemích rozvoj domácího internetu velmi zvolna. To dalo na přelomu tisíciletí vzniknout velkému množství lokálních poskytovatelů internetových služeb. Jejich působnost byla zpravidla v radiusu obcí či měst. Ti dokázali využít neschopnosti monopolního poskytovatele a nabídli koncovým uživatelům srovnatelnou službu za mnohem výhodnějších podmínek. Právě drobní ISP se asi nejvyšší mírou zasloužili o prudký rozvoj domácího internetu v ČR. Někteří z těchto lokálních poskytovatelů se postupem času stali skutečnými telekomunikačními operátory a na trhu působí dodnes.

[1] Research And Development – je nezisková organizace usilující o interdisciplinární a kvantitativní řešení problému prostřednictvím překládání teoretických konceptů z formální ekonomie a exaktních věd do nových aplikací v jiných oblastech, zpočátku pro ozbrojené síly USA, postupně pro vlády ostatních zemí a další organizace.

V začátcích byly sítě lokálních poskytovatelů z hlediska technické vyspělosti na velmi nízké úrovni a výpadky byly na denním pořádku. Sítě vznikaly živelně, bez systémového přístupu, vzhledem k ceně se používali komponenty podřadné kvality, a technickým pracovníkům chyběla potřebná zkušenost. Dnes je situace jiná. S ohledem na požadavky zákazníků a dostupnosti velmi široké konkurence, musejí operátoři na kvalitu a bezpečnost svých služeb důkladně dbát. Hodnocení služby, jako celku, se díky tomu přesouvá z různých stupňů funkčnosti, na v zásadě dva režimy, a to funguje/nefunguje. Jako stav nefunguje, je uživatelem posuzováno i prosté snížení kvality nebo míry bezpečnosti. Například, i při krátkodobém omezení rychlosti bez přerušení dodávky služby, často zákazník požaduje po poskytovateli sankce ve smyslu krátkodobého odpuštění měsíčních poplatků za službu.

V liteře §98 zákona č. 127/2005 Sb., o elektronických komunikacích, je poskytovateli veřejných telekomunikačních služeb přímo uložena povinnost zajisti bezpečnost a integritu své sítě, propojených sítí a koncových uživatelů. Dnes si žádný z poskytovatelů nedovolí tento paragraf podcenit, v historii tomu tak ale zdaleka nebylo. Myšlenka na zabezpečení infrastruktury či snad na zabezpečení samotného uživatele byla často na posledním místě.

Každý operátor svůj štít nastavuje převážně na základě svých zkušeností a předvídatelných hrozeb. Publikací, které se zabývají otázkou obecné bezpečnosti informačních systémů, je celá řada, ovšem taková, věnující se potřebám samotných poskytovatelů internetových služeb, neexistuje. Správce proto musí skládat konfiguraci systému ze střípků informací získaných na internetu, konferencích a školeních a z nich tvořit a postupně zdokonalovat koncept pro nasazení v reálném provozu.

I. TEORETICKÁ ČÁST

1 ZABEZPEČENÍ SÍTĚ

Problematika zabezpečení svěřené sítě je pro operátory v jistém smyslu klíčová. Ve své podstatě se jedná o soubor opatření, která mají za cíl znemožnit, nebo maximálně znesnadnit útočníkovi 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 také v zájmu 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 lze však ochranu 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[2] pracuje na obdobném principu jako distribuované výpočty, avšak s cílem rozesílat spam nebo koordinovat útok typu DoS[3]. Útoky také 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 mohou být však objednané samotným cílem jako penetrační test v rámci bezpečnostního auditu. [1]

1.1 Specifika zabezpečení sítě z pohledu ISP

Systém zabezpečení poskytovatele internetových služeb je velmi odlišný od systému ochrany aplikačního serveru (například webového), nebo firemního informačního systému. U těchto jako správce víme, co koncový nebo vzdálený uživatel smí a co ne a jaké služby mu lze povolit nebo naopak zakázat. V roli správce sítě poskytovatele si dokonale restriktivní ochranný firewall nelze dovolit. V žádném případě totiž nesmí být omezena funkce jakýchkoliv i zřídka používaných síťových služeb směrem ke koncovému uživateli.

[2] Botnet – síť počítačů infikovaná škodlivým kódem, ta je centrálně řízena z jednoho místa a je možné pomocí ní vést koordinované útoky na vybraný cíl.
[3] Denial of Service – typ útoku na konkrétní cíl, kdy je cílem přehltit cíl falešnými požadavky a tím jej vyřadit z provozu.

Při počtech koncových uživatelů v řádu tisíců se vždy najde jisté množství takových, pro které je určitá, i potenciálně nebezpečná služba zásadní. Z hlediska administrátora se sice může jednat o bezpečnostní trhlinu, přesto ji nelze bez výjimky vyloučit. Typickým příkladem takovéto služby je například UPnP. Tato služba zajišťuje automatické otevírání síťových portů různými aplikacemi. Pokud zákazník hodlá využít připojení pro vzdálený dohled třeba nad kamerovým systémem a nemá k dispozici vlastní veřejnou IP adresu, neobejde se bez propagace síťových portů skrze síť.

Přesto je vhodné, aby zákazník nezůstal zcela nekrytý. Úkolem administrátora ISP je tedy neustále hledat rovnováhu mezi optimálním zabezpečením a umožnění provozu všech služeb. Takzvané „přezabezpečení“ sítě se tedy může stát v jistém ohledu parazitní.

2 RIZIKA NAPADENÍ SÍTĚ

Napadení síťové infrastruktury se stává značným rizikem zejména v případě, kdy společnost či instituce uchovává na serverech strategicky důležitá či přísně soukromá data. Velmi přísné zabezpečení je 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 možných rizik. Základních typů útoků, proti nimž se můžeme bránit je v podstatě pět:

2.1.1 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 poskytne zjištěná data k dispozici ostatním. To, že se o záměru nového produktu dozví tento jeden útočník, ještě nemusí být nijak závažný problém. Pokud ale dojde ke zveřejnění informace na internetu, kde se k nim dostane konkurence, to už je problém velice podstatný. Pokud dojde k vyzrazení čísel kreditních karet zákazníků, a tento útok vejde ve veřejnou známost (jako se stalo v nedávné době opakovaně společnosti Sony), budou se lidé zdráhat s takovouto firmou vůbec obchodovat. [2]

2.1.2 Útočník provádí změny v datech

Tento typ útoku je jeden z nejhorších možných variant a znamená největší poškození. Útočník může změnit různé plány a data, aniž by si toho kdokoliv všimli. Změny v datech mohou způsobit jak závažná rizika, tak i ztráty na životech. Lze si například představit, 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. [2]

Útočník si často ani nemusí uvědomit, že může takovouto škodu způsobit. V popsaných případech se v kalifornském Berkeley crackeři dostali do systému pro řízení cyklotronu, který se používal pro léčbu rakoviny. Jiní nabourali bankomaty, které vydávaly peníze bez zasunutí karty. Další pak provedli nesmyslné změny na webových stránkách amerických vládních úřadů, včetně špionážní služby CIA. [2]

2.1.3 Útočník maže data

Při tomto útoku je výsledek poškození zcela jasný, následky omezuje pouze dobrý záložní program, pokud se útok včas odhalí. [2]

2.1.4 Odepření služby

Denial of Service (DoS) útoky jsou síťové útoky, které brání přístupu ke službám. DoS útoky blokují služby sítě zaplavováním spojení, zhroucením serverů nebo programů běžících na serverech, vyčerpáváním zdrojů na serveru nebo jinak brání legitimním klientům v přístupu ke službám sítě.

DoS útoky mohou mít celou řadu podob, od útoku jednoho paketu (takzvaný single packet attack), který způsobí zhroucení serveru, až po koordinované záplavy paketů od mnoha manipulovaných útočníků. Při útoku jednoho paketu je poslán do sítě pečlivě přizpůsobený paket, který využívá známé zranitelnosti operačního systému nebo aplikace a zablokuje server, anebo některé služby jím poskytované. Například virus Slammer worm využívá jedné takové zranitelnosti starších verzí Microsoft SQL serverů.

Při záplavovém útoku jsou zdroje na serveru nebo na síti narušeny nebo vyčerpány záplavou paketů. Po napadení jednoho místa může být záplava celkem snadno identifikována a izolována. Mnohem sofistikovanější přístup, zvaný Distributed DoS (DDoS) útok, je nástroj pro mnoho záplavových útoků vedených k jedinému cíli.

Při DDoS útoku používá útočník k zasažení cíle velké množství počítačů. Některé útoky mají jednoduchý plán, jako poslání nekonečného proudu dat k zaplavení síťových spojení na serveru. Jiné útoky, jako třeba SYN záplavy, používají pečlivě upravené pakety k vyčerpání kritických zdrojů za účelem zabránit legitimním klientům v připojení k serveru. [3]

2.1.5 Útočník zneužívá vaše servery jako základnu k dalším útokům

Při tomto útoku může dojít k odepření služby, a to z důvodu ztráty přenosových kapacit, které využívá útočník, a také proto, že ostatní mohou zablokovat naši síť jako „crackerskou síť“. Tento útok může proto ve svém důsledku vést ke ztrátě veřejného mínění a může vést i k právnímu postihu. [2]

2.2 Typy útočníků

Potenciální útočníky lze shrnout do několika skupin. Jejich motivy pro narušení se liší v mnoha ohledech a dopady jejich činnosti jsou často katastrofální. Profily jednotlivých útočníků jsou v literatuře popsány takto: [4]

2.2.1 Crackeři a hackeři

Crackeři (piráti) považují často společnosti a úřady, na jejichž infrastrukturu útočí, za zločinné nebo naopak jednoduše za nedůležité. Někdy 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. Nejvíce tíhnou k „velkým jménům“, tedy typicky k různým velkým, nadnárodním, dobře známým společnostem a vládním úřadům. Eliminovat crackery je velice obtížné. [4]

2.2.2 Konkurenti

Konkurenci jde zpravidla o způsobení výpadku služeb oběti útoku. Takového stavu pak mohou s výhodou využít a zákazníky postižené společnosti přebrat 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 a podobně. Tyto informace slouží ke krádeži nápadů a přetahování zákazníků, ale někdy se takto dostanou na veřejnost i nepříjemné kompromitující materiály. [4]

2.2.3 Kriminální živly

Zatímco motivem crackerů zpravidla nejsou peníze, u kriminálních živlů a zločinců tomu bývá přesně naopak. Takoví lidé se proniknou do systému pouze za účelem krádeže,

vydírání a dalších kriminálně „výnosných“ aktivit. Do podobných útoku může být zapojen také organizovaný zločin. [4]

2.2.4 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 průmyslovým oborům, političtí extremisté a jim podobní. Systémový administrátor, pracující ve firmě nebo úřadu, který by se mohl stát cílem útoku extremistické skupiny, musí proti tomu přijmout příslušná opatření. Imunní není vůči těmto útokům prakticky nikdo. [4]

2.2.5 Nespokojení současní i bývalí 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 útoku. Nelze než doporučit časté zálohy, které je navíc třeba ukládat takovým způsobem, aby kterýkoliv jednotlivec nemohl způsobit jejich ztrátu nebo nepoužitelnost.

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

2.2.6 Motivy potenciálních útočníků

Crackerům postačí, když v systému nechají nějakou svou značku, se kterou se pak chlubí 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 poškodit, jejich cílem bývá obvykle smazání nebo změna kriticky důležitých dat, případně zveřejnění důvěrných informací.

Konkurenti nejvíce touží po tom, jak zvýšit své vlastní zisky a tržní podíl, ale také po celkovém oslabení konkurenční firmy a snížení jejich zisků. Zneužijí jakékoli informace, které se jim podaří získat. K nejběžnějším zcizovaným datům patří seznamy zákazníků a plány budoucích produktů nebo marketingových kampaní. [4]

2.3 Nejčastější chyby dovolující napadení serverové infrastruktury

2.3.1 Nebezpečně slabá hesla

Používání hesel pro autentizaci uživatelů IT je jedním z kritických míst bezpečnosti informační infrastruktury. 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, manželky apod.
- rodné číslo či datum narození
- č. domu, adresa, telefonní číslo…
- heslo, 1234…

Nejbezpečnější hesla jsou tedy náhodné kombinace znaků. O to hůře si však heslo zapamatujeme i my sami, a pokud ho pravidelně nepoužíváme, brzy ho zapomeneme. Napsat si heslo do poznámek určitě také není vhodné řešení. Nabízí se vymyslet si k heslu nějakou mnemotechnickou pomůcku, podle které si ho snáze zapamatujeme (tato pomůcka ovšem musí zůstat stejně tajná stejně 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 je v hesle použito, tím je složitější ho prolomit. [5]

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 je tedy k dispozici přes 80 znaků relativně snadno použitelných na běžné klávesnici.

Je nutné podotknout, že některé servery na internetu nepodporují použití určitých speciálních znaků z bezpečnostních důvodů. Stejně tak nastane problém při přístupu z počítače, kde není definováno české rozložení klávesnice. [5]

2.3.2 Otevřené síťové porty

Stejně jako je každý uživatelský účet v systému pro crackera potenciální cestou k průniku, je každá síťová služba přímo silnicí. 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. Nejlepší variantou je, vůbec je neinstalovat. [6]

Přehled spuštěných služeb lze spustit 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 muže mít ještě více. [6]

Pokud se mezi výsledky nacházejí služby, které na tomto počítači není třeba poskytovat, musejí se vyřadit je z činnosti. Mnohé z distribucí Linuxu 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*. [6]

Mezi nejoblíbenější služby, které se v mnoha distribucích Linuxu instalují implicitně, patří například NFS, finger, vzdálené „remote“ 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*. [6]

2.3.3 Staré verze softwaru

Žádný serverový operační systém není dokonalý. Každý měsíc se objevuje množství nových zranitelných míst. Rychlost, s jakou se problémy nacházejí a opravují, je ale často 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. [6]

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. [6]

2.3.4 Nezabezpečené a chybně nakonfigurované programy

Počet bezpečnostních chyb v běžně používaných programech i jejich závažnost se podstatným způsobem snížily, že si lze dovolit ve výčtu nejčastějších bezpečnostních děr vypustit téma nedostatečné fyzické bezpečnosti. Na jeho místo je vhodnější zařadit provoz nebezpečných programů (jako je rsh, NFS, portmap a FTP) v jiných, než přísně kontrolovaných situací, a provozování nesprávné konfigurace ostatních programu. Tyto „ostatní programy“ jsou schopny dobrého zabezpečení právě jen při správné konfiguraci. [6]

Systémový administrátor by měl také myslet na to, že protokoly POP a IMAP (pokud nejsou zapouzdřené v obálce SSL[4]), telnet a FTP odesílají hesla v podobě prostého textu. Také, že služby NFS a portmap mají za sebou historii mnoha problému a chyb v návrhu autentizace. Mnozí přesto uvedené nástroje používají. Lépe je tedy používat namísto nich raději spop, simap, SSH a scp nebo sftp z balíku SSH. [6]

Mnohé z programů se dají považovat za bezpečné, ovšem jen při správné konfiguraci. Často jsou konfigurovány 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 mnoho správců používá nebezpečným způsobem a nedokáží k nim najít alternativu. [6]

Než uvedeme v systému do provozu jakoukoli službu (nebo než například dojde ke změně možnosti služby a způsob jejího provozování), je třeba si důkladně prověřit její bezpečnost nejlépe řízenou simulací napadení. [6]

2.3.5 Nedostatečné prostředky a chybně stanovené priority

V mnoha organizacích se stává, že nadřízení jednoduše neschválí dostatečné finanční prostředky, se kterými by systémoví administrátoři mohli vybudovat dobré zabezpečení. Skutečně vyčerpávající bezpečnostní řešení se skládá z celé řady elementů. Pro

[4] SSL (Secure Socket Layer) – Protokol SSL se nejčastěji využívá pro bezpečnou komunikaci s internetovými servery pomocí HTTPS, což je zabezpečená verze protokolu HTTP. Po vytvoření SSL spojení je komunikace mezi serverem a klientem kryptograficky šifrovaná, a tedy zabezpečená.

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, 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. [6]

Tento nedostatek není žádným technickým problémem, ale přesto bylo zjištěno, že je v mnoha organizacích skutečně příčinou průniku do systémů. [6]

3 PROSTŘEDKY ZAMEZENÍ INFILTRACE DO SYSTÉMU

Do systému lze proniknout několika způsoby. Ty se liší podle pozice útočníka a způsobu jeho nežádoucího přístupu. Může jít o přímý fyzický nebo falešně legitimní průnik, kde se lze nejlépe bránit nastolením organizačních a režimových opatření. Vzdálený útok vedený z internetu i ze strany klientských stanic pak lze odvrátit pomocí důsledně konfigurované brány firewall.

3.1 Organizační a režimová opatření

Většina režimových i organizačních opatření byla specifikována v předchozích kapitolách. Lze shrnout, že se jedná zejména o stanovení odpovědných pracovníků a nastavení bezpečnostních směrnic jednotlivých procesů, včetně zpětné kontroly jejich naplňování. Důležité je dbát personálních doporučení (viz. kapitola 2.2.5), velmi častými útočníky jsou současní a bývalí zaměstnanci těžící ze znalosti infrastruktury a přístupových údajů. Technicky je nutné zachovat přísnou autentifikaci, identifikaci a záznam přístupu do uživatelských i konfiguračních rozhraní jednotlivých prvků infrastruktury.

V další rovině je třeba vyloučit přímý, fyzický kontakt s klíčovými prvky infrastruktury. Komponenty je třeba chránit proti neoprávněnému přístupu, který může mít mnohem vážnější následky než průnik softwarový. Zde totiž útočník využívá přímý kontakt se systémem a citlivá data získává například krádeží pevných disků.

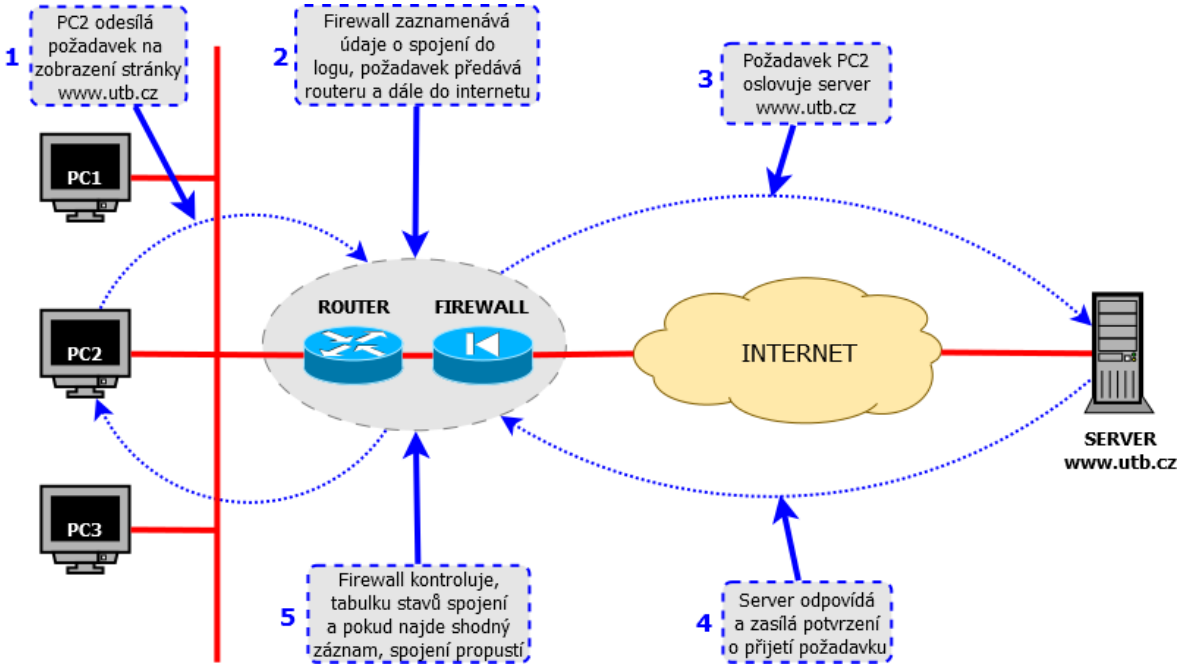
3.2 Brána firewall

Firewall kompletně kontroluje síťový provoz, který prochází přes jeho rozhraní. Na tento provoz následně aplikuje takzvaná pravidla, na základě kterých daný provoz buďto povolí, nebo zamítne.

3.2.1 Charakteristika brány firewall

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



Obr. 1 – Funkce a zařazení systému firewall v rámci síťové infrastruktury. (autor)

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, který celou konverzaci zahájil. Obrázek 1 vysvětluje názorně činnost firewallu.

3.2.2 Základní funkce brány firewall

Firewall má tedy dvojí povinnost při práci s pakety – jejich inspekci a filtrování. K nejběžnějším pravidlům a jejich funkcím patří: [7]

- **Blokování příchozího síťového provozu podle jeho zdroje nebo cíle.** Zablokování nežádoucího příchozího provozu je nejběžnější funkcí firewallu a je hlavním důvodem pro jeho instalaci - zabránit vstupu nežádoucího provozu do vnitřní sítě. Takový provoz obvykle pochází od útočníka, takže jej budeme chtít určitě rychle vykázat pryč. [7]
- **Blokování odchozího síťového provozu podle jeho zdroje nebo cíle.** Řada firewallu dokáže sledovat také sítový provoz ve směru z vnitřní sítě do veřejného

internetu, tímto způsobem můžeme například zaměstnancům vlastní firmy zabránit v přístupu k nevhodným webovým stránkám. [7]

- **Blokování síťového provozu podle obsahu.** Vyspělejší firewally sledují v síťovém provozu také nepřípustný 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. [7]
- **Zpřístupnění zdrojů vnitřní sítě.** Primárním úkolem firewallu je sice zabránit v průchodech nežádoucího síťového provozu z vnější sítě. U většiny z nich je možné nakonfigurovat také selektivní povolení přístupu ke zdrojům (prostředkům) vnitřní sítě, jako je například veřejný webový server. Ostatní typy přístupu z internetu do vnitřní sítě lze ponechat zakázané. V řadě případů je možnost tyto funkce zajistit pomocí takzvané demilitarizované zóny (DMZ), do níž lze umístit mimo jiné i zmíněný veřejný webový server. [7]
- **Povolení některých spojení do vnitřní sítě.** Zaměstnanci se do podnikové sítě běžně připojují 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. [7]
- **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 obsahu. Většina firewallu obsahuje určitou formu mechanismu pro oznamování. Dobrý firewall muže také veškeré aktivity zaznamenávat do systémového logu nebo na jiné záznamové zařízení. Zkoumání systémových protokolů firewallu po uskutečněném útoku je jedním z důležitých a průkazných nástrojů, které máme k dispozici. [7]

4 PENETRAČNÍ TESTOVÁNÍ

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí i zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému.

Penetrační testy jsou v podstatě napodobení útoku hackera. Útok může být směrován jak z vnější sítě (typicky z internetu) na servery umístěné v DMZ nebo na vnější rozhraní firewallu, tak i zevnitř na síťovou infrastrukturu nebo zranitelné servery. Průnik zevnitř do systému může být veden fyzicky přítomným hackerem, kterému se podařilo připojit vlastní počítač do interní sítě nebo získat fyzický přístup k počítači v chráněné síti. Průnik může být veden i metodou tzv. "sociálního inženýrství průniku", kdy hacker zneužije důvěřivosti uživatele nebo použije jinou netechnickou metodu a tím získá přístup, který mu samozřejmě nenáleží, nachytá běžného uživatele a podsune mu spustitelný kód, pomocí kterého převezme vládu nad jeho počítačem nebo celým systémem. [8]

Penetrační testy tvoří důležitou součást bezpečnostní analýzy. Za použití různých nástrojů jsou prováděny pokusy proniknout do různých částí informačního systému zvenčí či zevnitř. Výsledkem těchto testů je odhalení slabých míst v ochraně informačního systému, uložených dat a infrastruktury testovaného subjektu. Následuje definice existujících rizik. Penetrační testy ve své podstatě vyhledávají a aplikují metody pro napadení informačního systému tak, jak by k tomu mohlo potenciálně dojít při projevech počítačové kriminality. Tyto aktivity mají za účel prověřit zabezpečení informačního systému vůči napadení a současně ukázat analyzované organizaci, kde existují slabá místa a jak může být informační systém napaden. Slabá místa v informačním systému jsou hackery trvale vyhledávána a používané systémy jsou testovány na možnosti napadení. Aby bylo možno čelit jejich útokům, je nutné velmi podrobně sledovat a testovat informační technologie podobným způsobem. [8]

Při bezpečnostních testech infrastruktury je potřeba se zaměřit zejména na:

- penetrační testy vnitřní i vnější (scanning, sniffing, redirecting)
- zkušební útoky
- analýzu zranitelnosti firewallů
- kontrolu bezpečnostních pravidel mezi zónami firewallů
- analýzu zranitelnosti aktivních prvků
- analýzu zranitelnosti operačních systémů na serverech a stanicích

- analýzu systému zálohování [8]

Testy se provádějí na základě expertních zkušeností metodou "etického hackingu" a ve shodě s normami ČSN ISO/IEC TR 13335 a ČSN ISO/IEC 17799.

Při penetračních testech jsou především prováděny následující zkoušky:

- firewally - DoS útoky, změny směrování, zranitelnost
- Backdoory - programy umožňující získání kontroly nad počítačem
- CGI scripty - získání plné kontroly www nad serverem
- DNS systémy - předstíráním identity síťového zařízení
- mailové systémy – spam
- FTP systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem
- LDAP systémy - zneužití adresářové služby LDAP (Lightweight Directory Access Protocol)
- síťové odposlouchávání - špatná konfigurace aktivních prvků či nevhodný design infrastruktury umožní síťové odposlouchávání
- NFS systémy - neautorizovaný přístup k souborovému systému a převzetí kontroly nad serverem (Network File System)
- systémy založené na RPC -vzdálené volání procedur (Remote Procedure Call)
- systémy se sdílením zdrojů - získání neautorizovaného přístupu (Samba, SMB)
- SNMP systémy - bezpečnostních díry v implementaci Simple Network Management Protocolu v aktivních prvcích sítě [8]

Získané znalosti mají další využití pro sledování, testování a výběr nástrojů ochranu před neoprávněným přístupem (Firewall) a pro automatizovanou detekci a zabránění pokusu o napadení informačního systému (Intrusion Prevention System). [8]

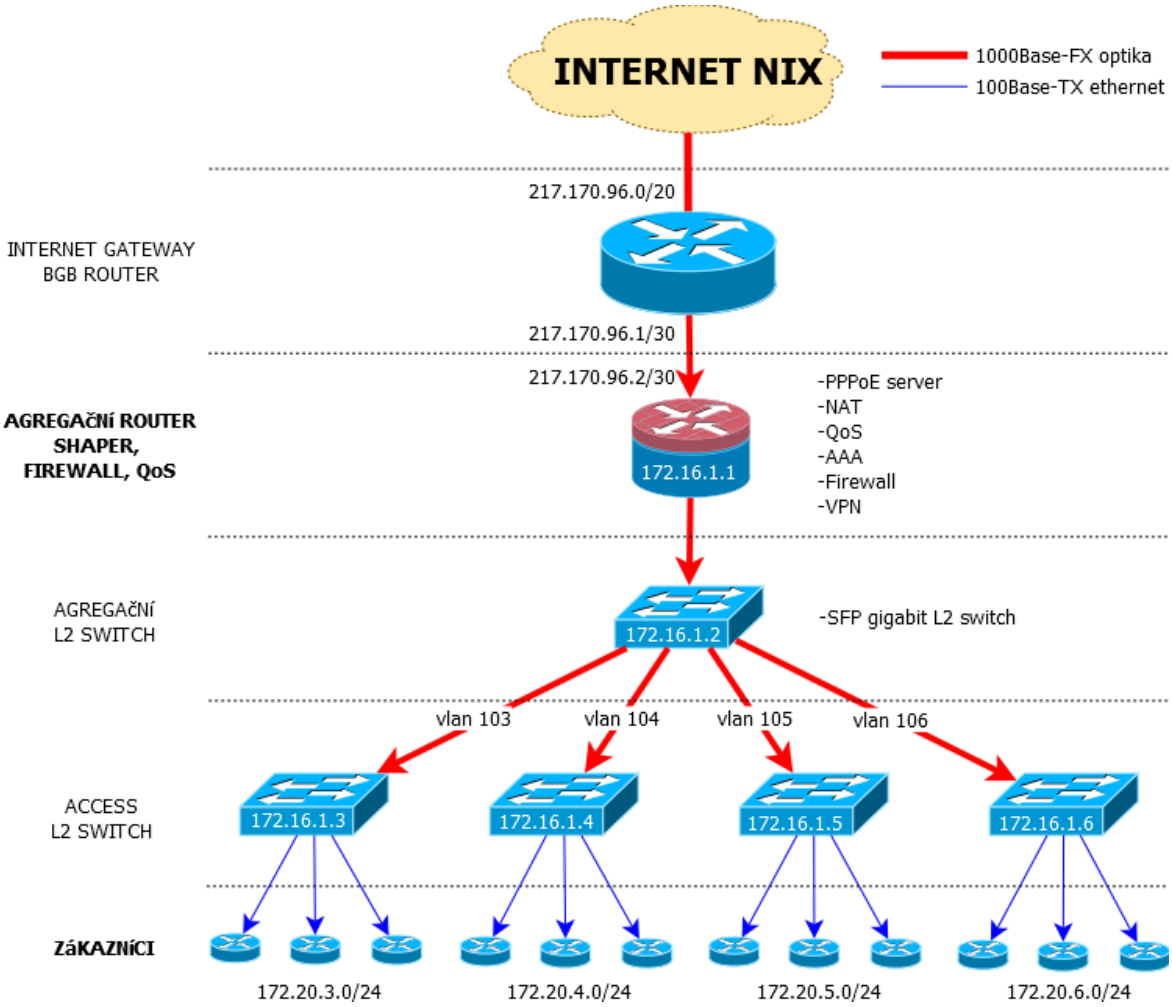
Složitým rozhodnutím bývá správný okamžik pro penetrační testy. Řada společností penetrační testy odkládá pod záminkami ve smyslu: „až bude nový firewall, máme webovou prezentaci hostovanou a do sítě nám přichází pouze emaily, máme čerstvě vybudovaný systém, a ten je přeci v pořádku, máme pravidelně aktualizovaný antivir“ a podobně. To jsou velmi naivní tvrzení, na penetrační testy je čas kdykoliv a je více než vhodné je pravidelně opakovat. Vždyť napadení počítačů a odepření jejich služby může nastat kdykoliv, třeba jen lavinovým rozšířením infikovaného emailu. Nebo třeba zprávou skype s linkem na kliknutí. Ta přijde od známé a důvěryhodné osoby, a protože

komunikace skype je šifrována, tak nedojde k její kontrole antivirovým programem a hromadné nakažení počítačů je dílem okamžiku. Toto je však možné jen díky neexistenci, či flagrantnímu porušování bezpečnostní politiky. I takovéto situace lze technicky ošetřit, ale bohužel to není běžné. [8]

II. PRAKTICKÁ ČÁST

5 MODEL TOPOLOGIE ZKOUMANÉ SÍTĚ

Pro studium předmětné problematiky je třeba předem vytvořit obecný model struktury zkoumané sítě. Na níže uvedeném diagramu (Obr. 2) je naznačena část sítě, odpovídající jednomu funkčnímu segmentu běžné poskytovatelské sítě. Dle získaných informací obecně odpovídá strukturám sítí největších českých FTTx[5] operátorů typu UPC, Netbox nebo O2.



Obr. 2 – Model zkoumané sítě. (autor)

[5] FTTx je zkratka systému připojení Fiber To The x, písmeno x zde reprezentuje různé typy ukončení optického vláka. Písmeno H označuje Home, to znamená, že vlákno je ukončeno přímo v bytě účastníka, analogicky je B – Building, C – Curb, A – Anttena, O – Office, …

5.1 Hladiny modelu sítě

Jednotlivé komponenty lze kategorizovat do jednotlivých hladin podle jejich funkční závislosti. Základním stavebním prvkem bude širokopásmový směrovač kombinovaný s bránou firewall (v modelu nazván agregační router). Zde bude docházet k aplikaci navržených bezpečnostních opatření a zkoumána jejich účinnost.

5.1.1 Internet NIX

NIX.CZ je zájmové sdružení právnických osob (založeno roku 1996), které sdružuje poskytovatele internetových služeb v České republice za účelem vzájemného propojení jejich počítačových sítí (tzv. peering). Telekomunikační společnosti působící v ČR tvoří toto sdružení, protože mají společný zájem na tom, aby byly jejich počítačové sítě vzájemně kvalitně propojeny a jejich zákazníci mohli rychle komunikovat v počítačové síti internet v rámci ČR. Členové společně přispívají na provoz a na technologie, které tvoří neutrální výměnný uzel. Dá se říci, že se jedná o centrální bod českého internetu. [9]

Zde získává navržená síť internetovou konektivitu, kterou dále distribuuje do sítě.

5.1.2 Internet gateway

Hlavní směrovač v síti odděluje veřejný internet od vnitřní části sítě. Díky protokolu BGP[6] a vlastnímu číslu AS[7] obsahuje vlastní rozsahy veřejných IP adres. Evropským správcem přidělování těchto rozsahů je společenství RIPE sídlící v Holandsku. Úkolem tohoto routeru je pouze distribuce vlastních adresních rozsahů dále do internetu a načtení IP adres ostatních AS do své routovací tabulky. Lokálně směruje vnitřní adresní rozsahy sítě. Nejčastěji se jedná o tovární jednoúčelové routery výrobců Cisco nebo Juniper.

5.1.3 Agregační router

Agregační směrovač patří funkčně k srdci poskytovatelské sítě. Koncentrují se v něm nejpodstatnější funkce pro zajištění konektivity zákazníkovi a kvality služby. S kvalitou služby úzce souvisí účinnost restrikčních opatření bezpečnostní brány firewall, která je ve většině případů do lokálního směrovače přímo implementována. Jakékoliv narušení

[6] Border Gateway Protocol (BGP) je dynamický směrovací protokol používaný pro směrování mezi autonomními systémy. Je základem propojení sítí různých ISP v peeringových uzlech.
[7] AS množina IP sítí a routerů pod společnou technickou správou, která reprezentuje vůči Internetu společnou routovací politiku. Pro routování mezi AS se používá Border Gateway Protocol (BGP).

provozu, ať už systematickým útokem nebo náhodným poškozením, má za následek omezení kvality služby nebo její úplné přerušení.

Router může mít řadu provedení. Nejběžnější je použití standardního PC určeného pro serverový provoz. Výhodou je v tomto případě volná volba softwarového vybavení, které věnuje routeru požadované funkce. Subjektivně vhodnějším řešením se ovšem jeví směrování pomocí továrního routeru s jednoúčelovým operačním systémem pro řízení sítě. Již z výroby obsahuje vše potřebné pro zajištění běžných i rozšířených funkcí. Jádro operačního systému (firmwaru) je zkompilováno přesně pro nasazený hardware a je schopno jej využít bezezbytku.

Kritéria pro výběr vhodného typu pro aplikaci v předeslaném modelu je třeba stanovit zejména dle plánovaného nasazení. Z hardwarového hlediska je pro univerzální použití základem dispozice minimálně dvou rozhraní ethernet 1000Base-TX. Důležitý je také ověřený výkon pro řízení datového toku dosahujícího špičkově až do saturace kapacity vstupního rozhraní, a to bez zjevného zhoršení přenosových parametrů linky. Klíčové služby na softwarové úrovni jsou zejména schopnost přijmout a ověřit PPPoE[8] spojení, komplexní brána firewall, schopnost řídit přidělenou šířku pásma jednotlivých klientů (traffic shaping), modul VPN[9], schopnost pracovat s VLAN[10] a další služby pro směrovač běžné.

5.1.4 Agregační switch

Distribuce internetových služeb z lokálního směrovače pokračuje dál směrem k zařízení zákazníka výhradně na linkové vrstvě modelu ISO/OSI. První datový přepínač (switch) zařazený za routerem je tzv. agregační. Aplikačně neslouží pro připojení koncových klientů. Jeho úkolem je sdružit všechna podřízená zařízení (odtud název agregační). Z každého portu je linkové spojení na podřízené přístupové switche. Dle modelu komunikuje ve zpětném směru s routerem a v dopředném směru s přístupovými přepínači

[8] PPPoE umožňuje vytvářet spoje typu bod-bod (peer-to-peer) na přepínaných ethernetových sítích. Klienti jsou připojeni k přístupovému bodu, každý klient má své vlastní spojení a jeví se jako nezávislý interface.

[9] VPN je zkratka pro virtuální privátní síť. VPN slouží k virtuálnímu spojení více fyzicky vzdálených počítačů, takže se chovají, jako by byly přímo propojené jednou sítí.

[10] VLAN je zkratka pro Virtuální LAN. Je logicky nezávislá síť v rámci jednoho nebo několika zařízení. Virtuální sítě mají cíl učinit logickou organizaci sítě nezávislou na fyzické vrstvě, čímž lze usnadnit správu sítě, zvýšit její výkon a podpořit bezpečnost.

pomocí VLAN. Požadavky na vhodný typ jsou zejména plný L2[11] management, schopnost obsluhovat VLAN, porty v provedení šachet pro umístění optometalických konvertorů SFP[12] standardu 1000 Base-FX.

Obr. 3 – Agregační switch Juniper EX4200 plně obsazený SFP moduly. [10]

5.1.5 Přístupový switch

Přístupový switch topologicky navazuje na výše jmenovaný a jeho umístění je zpravidla situováno přímo v objektu s koncovými klienty. Vstupní port (uplink) má přímé spojení pomocí optického vlákna a jednotlivý klienti jsou již připojeni datovým UTP kabelem. Uplink port je tedy nastaven v módu trunk[13] a přísluší přidělené VLAN, která v reálné situaci odpovídá například jednomu bytovému domu. Ostatní metalické porty jsou v módu access.

Vhodný switch je tedy podobně jako agregační s plným L2 managementem, podporou VLAN, vhodná konfigurace portů je ovšem 2-4 SFP a 8-48 RJ45.

Obr. 4 – Přístupový switch TP-LINK JetStream. [11]

[11] L2 (Layer2) – označení druhé síťové vrstvy ISO/OSI, analogicky L3 je označení třetí vrstvy.
[12] SFP (small form-factor pluggable) je konvertor signámů z optického vlákna na signály elektrické. Zapojuje se do kompatibilních síťových prvků.
[13] Porty příslušící VLAN dle IEEE 802.1q mají dva základní režimy provozu access a trunk. Access znamená, že odchozí rámce z portu budou zbaveny informace o VLAN. Trunk si informaci zachová, používá se na propojení s dalšími zařízeními co VLAN tagy podporují.

5.1.6 Zákazníci

Klientské zařízení umístěné přímo u klienta není vhodné podcenit. Jeho bezpečnostní funkce je podobně významná jako u všech ostatních komponent poskytovatele. Velmi často totiž dochází k útokům přímo v rámci lokální sítě. Motivací může být i prostá sousedská zvědavost. Poskytovatel má možnost tento jev v rámci lokální sítě jen částečně eliminovat. Pokud jsou zákazníci v jednom přístupovém switchi, není úplně jednoduché komunikaci zákazníků mezi sebou vyloučit. Pro zachování systémového přístupu je tedy nanejvýš vhodné volit nejjednodušší řešení a delegovat bezpečnostní opatření na zákazníka. Jako vhodná varianta se nabízí použití domácího routeru, který spolehlivě oddělí domácí síť od sítě poskytovatele.

5.1.7 Přenosové trasy

Spojení mezi jednotlivými prvky přenosového řetězce je realizováno pomocí optických vláken. Volba jejich typu záleží zejména na lokálních podmínkách oblasti. Páteřní propoje mají základní kapacitu 1 Gbps a v případě nutnosti v hustě saturovaných oblastech není problém kapacitu jednoduše navýšit na 10 Gbps.

Koncové linky realizují metalické propoje v rámci objektu. Jsou tvořeny kabeláží UTP[14] minimálně kategorie 5e. Jejich propustnost může být 100 Mbps nebo 1 Gbps a je dána použitým přístupovým switchem a koncovým zařízením zákazníka.

[14] UTP kabeláž je tvořena čtyřmi páry kroucené dvoulinky. Kategorie určuje šířku přenášeného pásma, cat5e je schopna přenést 1 Gbps, cat6 přenese 10 Gbps na omezenou vzdálenost, cat7 přenese 10 Gbps již na plnou vzdálenost 100m.

6 VÝBĚR VHODNÉ PLATFORMY

Při výběru vhodných komponent sítě je nutné zaměřit se zejména na prvek, ve kterém se koncentruje většina bezpečnostních opatření. Ve stanoveném modelu topologie se o toto stará lokální router. V kapitole 5.1.3 byly popsány technické parametry, které by měl pro danou funkci splňovat. Stranou ovšem zůstaly ostatní, neméně důležité parametry jako zejména MTBF[15], přívětivost uživatelského rozhraní, nároky na erudici obsluhy, dostupnost podpory, a to jak ze strany výrobce nebo dodavatele, tak komunitní podpory, která mnohdy reaguje lépe, rychleji a kvalitněji než servis výrobce. V dnešní době drahých energií se výrobci také čím dál více zabývají otázkou energetické úspornosti a s tím související miniaturizace komponent při zachování srovnatelného nebo vyššího výkonu. Posledním, parametrem, který je ve většině případů u lokálních poskytovatelů internetových služeb rozhodující, je pochopitelně cena.

6.1 Routery předních světových výrobců

6.1.1 Charakteristika

Předními světovými výrobci jsou zejména značky Cisco, Juniper, NETGEAR, Nortel a podobní. Tyto směrovače se vyskytují v sítích největších poskytovatelů s počtem zákazníků 20 000 a více. Jejich technologické hranice určují směr vývoje a ve všech parametrech předčí jakékoliv jiné řešení. Jediným značně diskvalifikujícím prvkem je jejich cena. U nejnižší řady routerů Juniper MX-10 přesahuje částku 250 tisíc korun. Za tuto cenu je sice možné mít v síti mimořádně kvalitní router, který bez navýšení latence přenese až 10 Gbps, ovšem pro potřeby lokálního routeru pro tisíc zákazníků s agregovanými tarify 50-100 Mbps s rezervou stačí takový, který je schopen v nejvyšší špičce odbavit 2 Gbps.

Obr. 5 – Router Juniper MX-10. [12]

[15] Střední doba mezi poruchami - anglicky Mean Time Between Failures.

6.1.2 Hodnocení

Jejich konfigurace probíhá v řádkovém terminálu a vyžadují hluboké znalosti obsluhy. Podpora (zejména u nejpoužívanější značky Cisco) je příkladná. Pro jakýkoliv problém či funkcionalitu existuje množství popsaných řešení.

Tento router si tedy lze představit buď v sítích obrovských rozsahů, nebo v menších sítích, kde ho lze výhodně zařadit jako hraniční BGP router.

6.2 Linux PC server

6.2.1 Charakteristika

V době začátků firem poskytujících internetové připojení byla jedinou dostupnou formou řízení sítě stavba vlastního PC s operačním systémem linux různých distribucí. Někteří ISP používají Linuxové servery dosud a nedají na ně dopustit. Je pravdou, že pokud je administrátor schopný (a ochotný) strávit dny, někdy i týdny kompilací jádra, spouštěním a laděním služeb, řešením problémů s nekompatibilním hardware, získá velmi výkonný směrovač za minimální cenu. Málokdo (i s linuxových nadšenců) je ovšem zastáncem all-in-one serverů, kde jsou všechny nutné i pomocné služby pro provoz na jednom „stroji“. Riziko nekonečného řešení drobných problémů, které se na serveru v plném provozu velmi složitě identifikují, je velmi náročná práce.

K těmto serverům je bezpodmínečně nutná vždy aktuální dokumentace vedená administrátorem. Pokud se z jakéhokoliv důvodu stane, že „otec“ serveru není v okamžiku poruchy dostupný, stává se z routeru typický black-box. Množství změn v jádru OS, úpravy hluboce skrytých konfiguračních souborů, spuštěné desítky sladěných služeb jsou pro jiného administrátora přesto, že má práva root[16], komplikace, která prodlužuje řešení problému na dny.

6.2.2 Hodnocení

Z uvedených důvodů se stále více administrátorů přiklání k továrním routerům nebo k těm, které jsou jednoúčelově založené. Ladění koexistence jednotlivých služeb mají na starost

[16] Nejvyšší úroveň uživatelských práv v OS linux.

vývojáři systému. Také přehled o funkcích, službách a konfiguraci trvá i průměrně graduovanému správci řádově minuty.

6.3 Mikrotik – RouterOS

Operační systém Mikrotik RouterOS je jednoúčelově založený operační systém s využitím linuxového jádra. Je určený správcům domácích, středních i rozlehlých sítí. Svůj původ má v Lotyšsku a vývoj je datován od roku 1995. Svým rozsahem s logickou strukturou plně vyhovuje většině administrátorů a jeho konfigurační rozhraní umožňuje v krátkém čase nastavit komplexní souhrn všech funkčních i bezpečnostních parametrů.

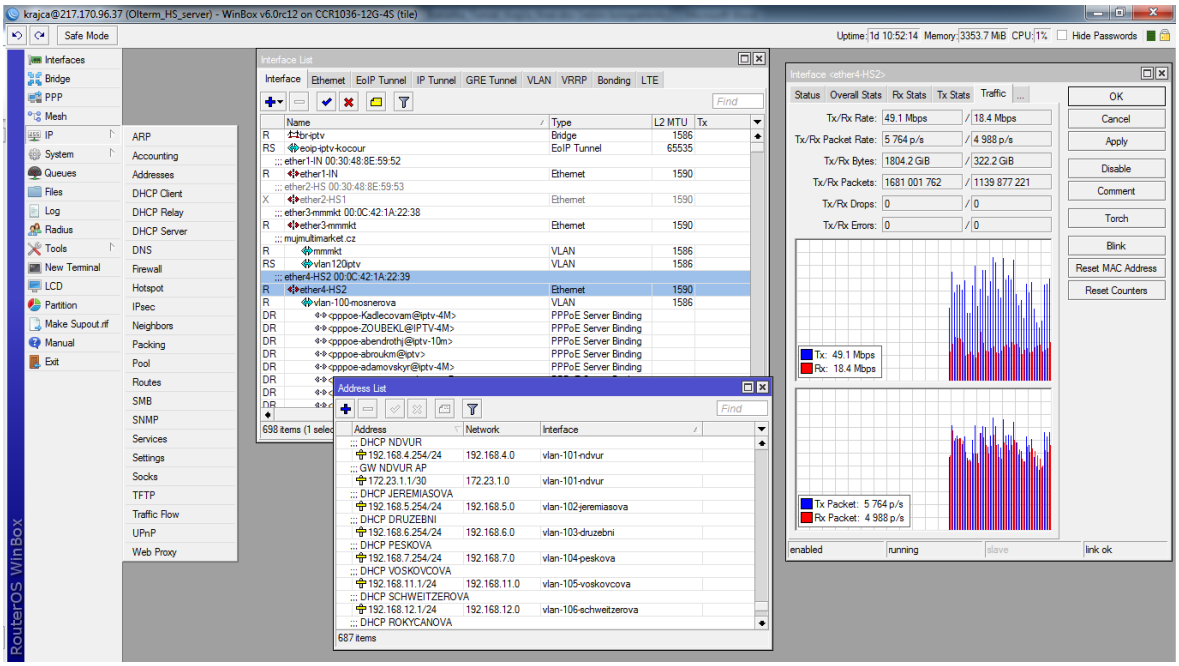
6.3.1 Software RouterOS

Tento systém je koncipován pro platformy Intel x86, mips, PowerPC a od verze 6 už i v 64 bitové verzi pro mnoha jádrové procesory architektury Tile. Systém lze instalovat jak do běžných serverových PC, tak do vlastních hardwarových řešení společnosti Mikrotik nazvané Routerboard.

Mezi nejdůležitější funkce patří:

- Bezpečnostní Firewall (pravidla typu iptables)
- Omezující Firewall (QoS)
- Pokročilý scripting
- 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
- a mnoho dalších…

Konfiguraci je možno provádět řadou nástrojů. První, nejrozšířenější je SSH, kde je možné pomocí textových příkazů v CLI nastavovat všechny i v jiných režimech skryté funkce. Další variantou je i nezabezpečený telnet, který je syntaxí totožný, ten se však kvůli přenosu příkazů v prostém textu (snadný odposlech) nedoporučuje. Výjimkou je MAC-telnet, zde se jedná o specifický protokol komunikující na druhé síťové vrstvě pro konfiguraci bez spojení přes IP adresu. Lze jej využít pro vyhledání routeru pomocí broadcastu a následného spojení s ním aniž bychom znali jeho nastavení. Velmi pozitivně lze také hodnotit konfiguraci v GUI s přístupem přes utilitu WinBox. Zde lze získat velmi přehledný a ucelený přehled o konfiguraci rozčleněné do příslušných sekcí.



Obr. 6 – Příklad konfigurace WinBox. (autor)

6.3.2 Hardware RouterBoard

Routerboard je vlastní hardwarové řešení směrovačů firmy Mikrotik. V tuto chvíli je na trhu kolem dvaceti různých typů lišících se ve vlastním výkonu a počtu použitelných rozhraní. To vychází zejména z původního směru vývoje těchto stanic pro řízení WiFi sítí a bezdrátových spojů. RouterBoard je tedy univerzální platforma na výstavbu routerů nebo WiFi přístupových bodů. Jednotky s typovým označením RB4xx a RB7xx lze použít především pro klientské instalace a přístupové body. Řada RB1xxx a RB2xxx je pak určena pro firemní a páteřní routery. Výjimku z číselných řad tvoří router CCR1036-12G-4S. To je nevídaně výkonné řešení, tvoří významný milník ve směru vývoje firmy. Jeho procesor architektury Tile s počtem 36 jader zvládne bez větších problémů přenést až 16

Gbps. Toto posouvá hardware firmy Mikrotik do skutečně profesionální úrovně za více než příznivou cenu.

Označení	RB433AH	RB411AH	RB450G	RB800	RB1100AH	RB1200	RB750GL	CCR 1036
Porty	3x Fast Ethernet	1x Fast Ethernet	5x Gigabit Ethernet	3x Gigabit Ethernet	13x Gigabit Ethernet	10x Gigabit Ethernet	5x Gigabit Ethernet	12x Gigabit Ethernet 4x SFP
Rozhraní	LAN, WiFI	LAN, WiFI	LAN	LAN, WiFI	LAN	LAN	LAN	LAN, SFP
Procesor	Atheros AR7130 680MHz	Atheros AR7130 680 MHz	AR7161 680MHz	MPC8544 800MHz	PowerPC P2020 dual core 1066MHz	PowerPC PPC460GT (až 1200 MHz)	Atheros AR7242 400MHz	Tile GX 1200MHz 36 core
RAM	128 MB DDR SDRAM	64 MB DDR SDRAM	256 MB DDR SDRAM	256MB DDR SDRAM	2 GB DDR SODIMM	512 MB	64 MB SDRAM	4 GB DDR3
NAND	64MB	64 MB	512 MB	512 - 1000 MB		64 MB	64MB	4 GB
Sloty	3x miniPCI	1x miniPCI	-	4x miniPCI, 1 miniPCI-e	-	-	-	-
I/O	RS-232	RS-232	RS-232	RS-232	RS-232	RS-232	nemá	USB
OS	RouterOS L5	RouterOS L4	RouterOS L4	RouterOS L5	RouterOS L6	RouterOS L6	RouterOS L4	RouterOS L6

Tab. 1 – Přehled typů RouterBoardů

V praxi se vždy volí takový hardware, který odpovídá dané aplikaci. Velká výhoda je v tom, že i v základní variantě typu RB711 za pár stovek korun, i ve vysoce výkonné jednotce CCR má RouterOS naprosto stejnou funkcionalitu a omezena je pouze propustnost mezi jednotlivými rozhraními a množství záznamů ve filtrovacích pravidlech firewallu.

6.3.3 Hodnocení

Po stránce funkcí softwaru, přívětivosti ovládání a uživatelské podpory je na velmi vysoké úrovni, dalo by se říci, že se rychle přibližuje profesionálním řešením světových výrobců. To dokazuje sílící uživatelská základna a zvyšující se tržní podíl ve světové ekonomice.

6.4 Závěrečné srovnání platforem

Pokud shrneme jednotlivé vlastnosti jmenovaných typů routerů, je možné je konkrétně posuzovat ze dvou klíčových rovin, a to z hlediska hardwarových a poté softwarových vlastností.

Pro posouzení každé skupiny je třeba vybrat vhodného reprezentanta, vhodného danému účelu. Základními kritérii výběru jsou:

- Přenosová kapacita při plné konfiguraci aspoň 1 Gbps
- Komplexní L3 funkční vybavenost
- Co nejvyšší čas mezi poruchami MTBF
- Kvalitní HW i SW podpora
- Přehlednost uživatelského prostředí
- Nízké nároky na obsluhu
- Zpracovaná uživatelská dokumentace
- Vysoká úroveň bezpečnosti
- Redundance napájení ze dvou nezávislých zdrojů
- Energetická nenáročnost
- Nízká cena

Výběr konkrétních typů proběhne na základě hardwarových vlastností, základem je schopnost přenosu a řízení toku 1 Gbps. Na základě zkušeností jsou zvoleny tyto modely:

- **Tovární router** – router Juniper MX-10, operační systém *JunOS*
- **Linux PC** – server HP ProLiant ML330, Xeon E5603, 8GB RAM, *OS Linux*
- **Mikrotik** – router CCR 1036-12G-4S, operační systém *RouterOS*

Nyní je možné konkrétní porovnání uvedených klíčových parametrů. Hodnocení ve většině případů vychází z hodnot uvedených výrobcem. V neměřitelných případech je subjektivní, a stanovuje se na základě zkušeností s jednotlivými platformami. Číselná hodnota uvedená u posuzovaného parametru odpovídá školnímu známkování: 1 – nejlepší, 5 – nejhorší. Každá vlastnost má svou váhu v celkovém hodnocení, ta je stanovena na základě požadavků pro výběr typu v síti poskytovatele internetových služeb.

Prvním důležitým parametrem je výkon zařízení. Posuzuje se množství spotřebovaných systémových prostředků při plném nasazení v reálném provozu. Vyzdvihnout lze router Juniper, který nevykazuje do hodnoty přenosu 10 Gbps ani minimální zhoršení přenosových vlastností.

Čas mezi poruchami MTBF je u Juniperu také nejvyšší, výrobcem uvedená dostupnost činí 99,99784%. U ostatních dvou výrobců je nutné se spokojit se stanovenou hodnotou dostupnosti 99,99%.

Hardwarové servisní služby má v ČR nejlépe pokryty společnost Mikrotik. Ta disponuje velkým množstvím lokálních distributorů. Náhradní kus stejného HW není při poruše problém získat v řádu hodin. U HP je servis zajištěn do následujícího pracovního dne pouze při zakoupení balíčku CarePack[17]. Při poruše zařízení Juniper se může (podle zkušenosti) stát, že náhradní kus není v ČR dostupný a proto získává nejhorší hodnocení. Reálná spotřeba elektrické energie je u CCR 1036 50W, HP ML330 80W a Juniper MX-10 85W.

Poslední určeným parametrem je cena. Ta se stává rozhodujícím parametrem, CCR 1036 lze pořídit za 15 000 Kč, HP ProLiant ML330 za 23 500 Kč. Juniper MX10 je k dispozici za ceny převyšující 250 000 Kč.

HW VLASTNOSTI				
parametr	*váha*	**Juniper MX-10**	**HP ProLiant ML330**	**CCR 1036-12G-4S**
VÝKON	25%	**1**	2	2
MTBF	20%	**1**	2	2
HW SERVIS	15%	4	2	**1**
SPOTŘEBA ENERGIE	10%	3	3	**1**
CENA	30%	5	2	**1**

Tab. 2 – Porovnání hardwarových vlastností routerů

Softwarové vlastnosti jsou posouzeny zpravidla subjektivně. V přehlednosti konfigurace lze vyzdvihnout jednoúčelové OS. U nich je možnost projít a pochopit kompletní nastavení v krátkém čase, jinak tomu je u OS Linux, kde poznání kompletní konfigurace vyžaduje hlubší studium.

Nárok na erudici obsluhy je u všech platforem vysoký, přesto se RouterOS díky GUI více blíží ideálnímu stavu. Z hlediska funkční vybavenosti ovšem zaostává. Jeho rozšiřitelnost je na rozdíl od ostatních minimální.

Bezpečnost je posuzována jako nejdůležitější kritérium, zde zaostává OS Linux. Jakákoliv neověřená služba či proces může znamenat potenciální riziko. Minimální chyba administrátora pak může vyústit v závažné ohrožení integrity systému.

[17] CarePack je služba, která za poplatek zajišťuje nadstandardní servisní plnění společnosti HP vůči zákazníkovi.

Softwarovou podporu lze hodnotit ve všech případech velmi dobře. U JunOS a RouterOS existuje množství tréninkových programů vedených certifikovanými školiteli. U OS Linux se lze oproti tomu v každém případě spolehnout na vyspělou komunitní podporu. Uživatelská dokumentace existuje u všech srovnávaných systémů zpravidla v cizím jazyce, nejucelenější formu však výrobce dodává k systému JunOS.

SW VLASTNOSTI				
parametr	*váha*	JunOS	Linux	RouterOS
PŘEHLEDNOST KONFIGURACE	15%	1	2	1
NÁROKY NA ERUDICI OBSLUHY	10%	4	4	3
FUNKČNÍ VYBAVENOST	20%	1	1	2
BEZPEČNOST	30%	1	2	1
SW PODPORA	10%	1	1	1
UŽIVATELSKÁ DOKUMENTACE	15%	2	3	3

Tab. 3 – Porovnání softwarových vlastností routerů

Celkové hodnocení (viz. Tab. 4) shrnuje uvedené parametry a současně zohledňuje váhu jednotlivých kritérií. Přestože se Juniper MX-10 jeví funkčně na nejvyšší úrovni, jeho cena jej pro použití v síti ISP jako agregačního routeru jednoznačně diskvalifikuje. Nejvhodnějším reprezentantem se tedy stává Mikrotik CCR 1036-12G-4S s operačním systémem RouterOS s výsledným hodnocením 1,58.

CELKOVÉ HODNOCENÍ			
parametr	Tovární router	Linux PC	Mikrotik
HW VLASTNOSTI	2,85	2,25	1,45
SW VLASTNOSTI	1,45	2,05	1,70
VÝSLEDNÁ ZNÁMKA	2,15	2,15	**1,58**

Tab. 4 – Celkové hodnocení vlastností routerů

Další konfigurace bude probíhat na nejlépe hodnocené platformě a zdrojové kódy budou odpovídat syntaxi systému RouterOS. Struktura a klíčové funkce jsou si u všech platforem velmi podobné, proto je lze pro případ potřeby přepracovat i pro použití v ostatních systémech.

7 KRITÉRIA BEZPEČNOSTI

Pro posuzování bezpečnosti informačních systémů je předepsána celá řada standardů platných napříč různými státy. Nejběžnější z nich jsou TCSEC (Trusted Computer System Evaluation Criteria), TTAP (Trust Technology Assesment Program), ITSEC (Information Technology Evaluation Criteria) a nejnovější společná Common Criteria. Tyto standardy jsou využívány pro stanovení konkrétní úrovně zabezpečení, na základě které lze informační systém určitým způsobem kategorizovat.

V uvedeném modelu sítě poskytovatele internetových služeb však není zcela účelné rizika nejrůznějším způsobem hodnotit, jak z hlediska možného výskytu, tak z hlediska úrovně zabezpečení proti nim. Stupeň ochrany zde nelze škálovat. Stanoveny jsou pouze dvě úrovně a to, jestli riziko je/není vyloučeno. Hlavním kritériem bezpečnosti posuzovaného modelu je veškeré zde stanovené způsoby narušení úspěšně a bezezbytku eliminovat.

Povinnost zajistit bezpečnost a integritu své sítě a služeb, nařizuje poskytovateli zákon č. 127/2005 Sb., o elektronických komunikacích. Stejně tak nařizuje vytvořit takovou úroveň bezpečnosti, která odpovídá míře existujícího rizika s cílem předejít nebo minimalizovat dopad událostí na uživatele nebo vzájemně propojené sítě. Bezpečností sítě a služby se tedy rozumí jejich schopnost odolávat náhodným incidentům nebo neoprávněným či svévolným zásahům, které závažně narušují dostupnost nebo interoperabilitu služeb a integritu sítí. [13]

Pro stanovení kritérií bezpečnosti zkoumané síťové infrastruktury je nutné nejprve konkrétně analyzovat veškerá běžná rizika, která mohou bezprostředně omezit či ohrozit její integritu.

7.1 Popis možných způsobů narušení integrity sítě

V daném typu sítě se lze setkat s těmito druhy rizik:

Fyzické vnější faktory – do této oblasti spadá zejména zabezpečení výpadku elektrické energie a vyloučení neoprávněného přístupu k technologiím. Dále živelná rizika jako požár nebo povodeň. Tyto faktory mohou způsobit částečné nebo úplné omezení služby a v případě neoprávněného přístupu i krádež dat nebo průnik do administrace systému. Pro eliminaci těchto rizik je třeba nastavit důkladná technická a režimová opatření.

Fyzické vnitřní faktory – nedostupnost je způsobena vlastním provozem nebo poruchou síťové technologie. Může být způsobena výrobní vadou, mechanickou závadou nebo

vysokou teplotou. Tato rizika nelze zcela ošetřit, pouze jim předcházet nebo se na ně připravit.

Neoprávněný přístup do konfigurace – tomuto případu je nutné se striktně vyhnout veškerými dostupnými metodami. Po průniku získá útočník nad sítí plnou vládu. Může odcizit data, měnit je, celou síť zneužít nebo úplně vyřadit z provozu. Pokud není odhalen, může tak činit opakovaně po dlouhou dobu. Jako protiopatření je třeba stanovit kritéria přístupových práv a technicky zabránit použití běžných typů penetračních metod.

Provoz neautorizovaného uživatele – neautorizovaní uživatelé mohou čerpat službu bez platné smlouvy a mohou v internetu anonymně působit nekalou činnost. Zákon v určitých případech ukládá nutnost dohledání konkrétního uživatele, která je v tomto případě nemožná. Pomocí vhodných technických opatření a nastavení ochrany sítě je nutné zabránit průniku neautorizovaného uživatele ke službě.

Odepření služby – je nutné se bránit proti systematickým útokům s účelem odepření služby. Typicky se jedná o DoS nebo DDoS útoky. Ty však nelze eliminovat bezezbytku, lze jim jen vhodným způsobem předcházet a pro případ trvajícího útoku stanovit plán pro minimalizaci jeho následků.

Zneužití sítě pro šíření virů a spamu – směrem od koncových uživatelů nebo k nim může docházet k šíření škodlivého kódu nebo spamu. Účinným protiopatřením je nutné toto jednání vyloučit nebo aspoň minimalizovat.

8 FYZICKÁ BEZPEČNOST INFRASTRUKTURY

Velmi často opomíjenou problematikou z hlediska zabezpečení IT systémů je jejich fyzická bezpečnost. Často je do jisté míry zanedbávána kvůli přílišné fixaci na ostatní prvky bezpečného IT systému, jako je ochrana před vnějšími útočníky, ochrana před viry a dalšími druhy škodlivého softwaru, nebo využití hesel či jiných autentizačních prostředků pro identifikaci uživatelů. Fyzické ohrožení systému se tak dostává do ústraní. [14]

Zanedbání fyzické bezpečnosti má zpravidla vliv na udržení kontinuity provozu, při jejím velkém podcenění hrozí i převzetí vlády nad systémem bez předchozí znalosti přístupových údajů.

8.1 Kontrola fyzického přístupu k technologiím

Pokud se potenciální narušitel fyzicky dostane k aktivní technologii, už není mnoho možností pro odvrácení útoku. V krátkém čase lze ze serveru vyjmout pevné disky a dostat se tak k jejich obsahu nebo router vypnout či mechanicky poškodit.

Z hlediska mechanického zabezpečení je nutné klíčové serverové místnosti vždy vybavit technickými prostředky pro omezení vstupu neautorizovaných osob. Základní ochrany lze dosáhnout pomocí plášťového mechanického zabezpečení. Případná okna do technologické místnosti je vhodné vybavit mřížemi, nebo pokud to vnější plášť budovy nedovoluje, bezpečnostními foliemi a dveře bezpečnostním zámkem s chráněným profilem nebo zámkem elektronickým. Doporučují se bezpečnostní prachotěsné dveře, a pro případ dispozice v místě s častým pohybem osob, i zvukotěsné. Klíč má potom technický personál, majitel a správce objektu.

Důsledná režimová opatření kontrolují veškerý přístup do serverovny, která by měla být vytrvale monitorována jak kamerovým systémem se záznamem, tak systémem kontroly přístupu s osobní identifikací vstupující osoby, která zanechává otisk jakéhokoliv přístupu do elektronické databáze včetně času a data. Tyto přístupy pak mohou být porovnány s provozním deníkem, kde by měl být vždy specifikován i účel vstupu. Informace o přístupu také může být odeslána v reálném čase na operační středisko sítě, kde může odpovědný pracovník postup dohledovat.

8.2 Eliminace působení ostatních vlivů

Na kontinuitu provozu, mohou působit i jiné vlivy technického i netechnického charakteru. Lze se jim účinně bránit a trvale zachovat kvalitu poskytovaných služeb na vysoké úrovni.

Nejčastějším rizikem technického charakteru je výpadek dodávky elektrické energie. Ten lze v omezeném čase pokrýt vhodně dimenzovaným zdrojem záložního napájení UPS. Jeho kapacita je stanovena na základě předchozí důsledné analýzy. V té je prvořadě zohledněn předpokládaný výkonový odběr jednotlivých technologií a to i s rezervou pro umístění dalších předpokládaných zařízení v budoucnosti (doporučená rezerva je 30%), a také předpokládanou dobu chodu nutnou k pokrytí výpadku.

Obr. 7 – Záložní zdroje UPS různé kapacity. [15]

Pro bezchybnou funkci systémů je třeba v serverové místnosti vyloučit nebo monitorovat ostatní nežádoucí vlivy prostředí. Jakékoliv změny mimo rozsah stanovený výrobcem systému neprospívá. V místnosti je nutné držet optimální vnitřní teplotu v rozmezí 20-24°C. Tyto parametry zabezpečí vhodně dimenzovaná klimatizační jednotka, která obstará i žádoucí odvlhčení vnitřní atmosféry.

Ostatní vnější vlivy, zejména pak živelné (požár, povodeň) je vhodné elektronicky monitorovat a tím zajistit vždy včasné varování. V případě vyhlášení environmentálního poplachu probíhá likvidace mimořádné události v souladu s předem stanoveným plánem, zhotoveným speciálně pro každý z těchto případů. Pro eliminaci těchto rizik jsou důležitá preventivní opatření v podobě vhodně zvoleného umístění serverovny a také pravidelných revizí elektroinstalace a hasicích přístrojů.

9 NÁVRH KONFIGURACE

Před řešením konkrétních příkladů konfigurace, je třeba stanovit několik základních poznatků a kritérií. Zavedením funkce provozu služeb internetu se práce v plném rozsahu nezabývá, pozornost je směřována spíše k vlastní bezpečnosti směrovače, uživatele a eliminace omezení nebo odepření provozu služeb. Konfigurační příkazy jsou psány neproporcionálním písmem s číslováním jednotlivých kroků, na které je v textu průběžně odkazováno.

9.1 Zajištění funkce provozu internetu, základní nastavení

V první fázi před sebou máme router bez jakékoliv konfigurace. Nejdříve definujeme obecné parametry jako identita *(1),* NTP server *(2),* vytvoření interface vlan103-106 *(3)* a zavedení dostatečně silného hesla pro administraci a odstranění původního účtu *(4).*

1) `/system identity set name=PraktickaDP`
2) `/system ntp set mode=unicast primary-ntp=195.113.144.201 secondary-ntp=195.113.144.238`
3) `/interface vlan add arp=enabled disabled=no interface=ether2 l2mtu=1516 mtu=1500 name=vlan103 use-service-tag=no vlan-id=103`

   `add arp=enabled disabled=no interface=ether2 l2mtu=1516 mtu=1500 name=vlan104 use-service-tag=no vlan-id=104`

   `add arp=enabled disabled=no interface=ether2 l2mtu=1516 mtu=1500 name=vlan104 use-service-tag=no vlan-id=105`

   `add arp=enabled disabled=no interface=ether2 l2mtu=1516 mtu=1500 name=vlan104 use-service-tag=no vlan-id=105`
4) `/user add name=krajca group=full password=hust0.d3monsky>krut0<pr1sn3*h3sl0!`

   `/user remove name=admin`

Z nadřazeného routeru (podle modelu) vyplývá, že na vstupní interface má být zavedena adresa 217.170.96.2/30 *(5)* a výchozí brána *default gateway (7),* kterou je druhá volná adresa v dané síti a je zavedena na odpovídajícím rozhraní hlavního routeru. Na rozhraní *ether3* nastavíme servisní rozsah pro správu směrovače 192.168.100.1/24 *(6)* s aktivním DHCP serverem *(8).* Ten bude přidělovat adresy v rozsahu 192.168.100.2 až 192.168.100.20. Díky němu bude možné směrovač lokálně pohodlně konfigurovat.

```
5) /ip address add address=217.170.96.2/30 interface=ether1
6) /ip address add address=192.168.100.1/24 interface=ether3
7) /ip route add dst-address=0.0.0.0/0 gateway=217.170.96.1
8) /ip dhcp-server setup dhcp server interface: ether3
   dhcp address space: 192.168.100.0/24
   gateway for dhcp network: 192.168.100.1
   addresses to give out: 192.168.100.2-192.168.100.20
   dns servers: 217.170.96.24,217.170.96.2
   Select lease time: 3d
```

V tuto chvíli je v routeru dostupný internet a lze pokračovat v další konfiguraci.

9.2 Odepření služeb neautorizovaným uživatelům

Vniknutí neautorizovaného zákazníka je velmi častým jevem, se kterým se poskytovatelé setkávají. Způsobů jak tomuto zamezit velké množství. Nejjednodušším řešením je omezení na MAC adresu a přidělenou IP, to je ovšem jak pro zákazníka, tak pro poskytovatele komplikované řešení jak z hlediska správy, tak z hlediska pohodlí. Odposlechnout IP a MAC je pro potenciálního narušitele velmi jednoduché, proto se nejedná o skutečně bezpečnou metodu.

Jednou z méně využívaných avšak maximálně bezpečných autentifikačních metod je přímé PPPoE vytáčené spojení proti koncovému zařízení klienta. V něm je uloženo unikátní uživatelské jméno a heslo, pomocí kterého se u serveru zákazník identifikuje. V případě autorizovaného přístupu mu pak umožní další spojení.

9.2.1 PPPoE server

Pro každý VLAN interface, kde lze dle modelu očekávat připojení koncových uživatelů je vytvořen samostatný PPPoE server *(11)*, ten po ověření uživatelského jména a hesla přidělí na základě PPP profilu *(10)* IP adresu z odpovídajícího adresního rozsahu *(9)* a vytvoří pro každého uživatele samostatný *Server Binding interface*. V profilu PPP je nastaven šifrovaný přenos hesla pomocí CHAP.

```
9) /ip pool add name=pppoe_103 ranges=172.20.3.2-172.20.3.254
   add name=pppoe_104 ranges=172.20.4.2-172.20.4.254
   add name=pppoe_105 ranges=172.20.5.2-172.20.5.254
   add name=pppoe_106 ranges=172.20.6.2-172.20.6.254
```

```
10) /ppp profile add change-tcp-mss=yes dns-server=217.170.96.24,
   217.170.96.2 local-address=172.20.3.1 name=pppoe103 remote-
   address=pppoe_103

   add change-tcp-mss=yes dns-server=217.170.96.24, 217.170.96.2
   local-address=172.20.4.1 name=pppoe104 remote-address=pppoe_104

   add change-tcp-mss=yes dns-server=217.170.96.24, 217.170.96.2
   local-address=172.20.5.1 name=pppoe105 remote-address=pppoe_105

   add change-tcp-mss=yes dns-server=217.170.96.24, 217.170.96.2
   local-address=172.20.6.1 name=pppoe106 remote-address=pppoe_106

11) /interface pppoe-server add authentication=chap default-
   profile=pppoe103 disabled=no interface=vlan103 service-name=service

   add authentication=chap default-profile=pppoe104 disabled=no
   interface=vlan104 service-name=service

   add authentication=chap default-profile=pppoe105 disabled=no
   interface=vlan105 service-name=service

   add authentication=chap default-profile=pppoe106 disabled=no
   interface=vlan106 service-name=service
```

9.2.2 Správa autorizovaných koncových uživatelů

Autentifikace klienta probíhá na základě přiděleného uživatelského jména a hesla. Tyto údaje je třeba někde v přehledné podobě koncentrovat. Nabízejí se dvě metody ověření. Buď přes centrální server radius[18], nebo přes tabulku umístěnou lokálně v routeru (*/PPP/secrets*). Konfigurace vhodnější varianty, serveru radius, se vymyká rozsahu práce, proto bude demonstrována druhá varianta.

Pro uživatelské jméno zvolíme jednoznačný identifikátor, například jméno nebo lépe číslo smlouvy o poskytování datových služeb *(12)*.

```
12) name="cislosmlouvy" password=dka58sE4 disabled=no
   profile=pppoe103 service=pppoe
```

Pokud se v této chvíli na síti VLAN 103 objeví router s příslušným nastavením WAN rozhraní, dostane IP adresu z příslušného adresního rozsahu *(9)*.

[18] RADIUS (Remote Authentication Dial In User Service, česky Uživatelská vytáčená služba pro vzdálenou autentizaci) je AAA protokol (authentication, authorization and accounting, česky autentizace, autorizace a účtování) používaný pro přístup k síti nebo pro IP mobilitu. Může pracovat jak lokálně tak i v roamingu.

9.3 Konfigurace firewall

Alfou a omegou bezpečnosti síťového provozu je odborně definovaný a kvalitně odladěný firewall. Systém RouterOS disponuje velmi pokročilým systémem širokého rozsahu. Jeho funkce začínají na standardním paketovém filtru a končí u Layer7 filtrů s možností hloubkové analýzy obsahu paketů v reálném čase.

9.3.1 Části systému firewall

V systému RouterOS je firewall rozdělen do několika částí:

9.3.1.1 Filter Rules

Je nejdůležitější součástí brány, kde se zadávají samotná pravidla paketového filtru, která se vykonávají chronologicky na základě pořadí. Pro úsporu systémových prostředků routeru, je nepsaným pravidlem, že se jako první vykonají pravidla, která umožní volný průchod největšímu množství paketů. Poté se postupně pravidla zpřísňují. Kontrolovat lze pakety firewallem průchozí, do něj příchozí nebo z něj odchozí. Žádoucí směr kontrolovaných paketů se definuje pomocí volby *chain*, u které lze zvolit hodnotu *forward* pro průchozí pakety, *input* pro směr příchozí a *output* pro odchozí. Dalšími zadanými hodnotami se už pouze zpřesňuje, pro které pakety bude pravidlo určené.

Pokud paket určenému filtru odpovídá, je třeba nastavit akci, jakým způsobem ho firewall zpracuje.

Definovaných akcí je deset:

- ***accept*** – paket je akceptován, není kontrolován dalšími pravidly
- ***add src to address list*** – zdrojová adresa je zařazena do address listu
- ***add dst to address list*** – cílová adresa je zařazena do address listu
- ***drop*** – paket je blokován
- ***jump*** – paket je samostatně kontrolován v uživatelsky definovaném *chain*
- ***log*** – spojení je zaznamenáno do syslogu
- ***passthrough*** – bez určené funkce, použitelné pro statistiku
- ***reject*** – paket blokován, zdroji odeslána ICMP reject zpráva
- ***return*** – předá kontrolu zpět k řetězci, odkud paket přišel (přes *jump*)
- ***tarpit*** – zachytí a drží TCP spojení

9.3.1.2 NAT

Zde se nastavuje síťový překlad adres, hraje nejdůležitější roli v ochraně koncového uživatele. Je to funkce, která umožňuje překlad adres z veřejných na privátní a naopak. To znamená, že adresy z lokální sítě přeloží na jedinečnou adresu, která slouží pro vstup do jiné sítě. Adresu překládanou si uloží do tabulky pod náhodným portem a při odpovědi si v tabulce vyhledá port a pošle pakety na IP adresu přiřazenou k danému portu. Díky němu se klient stává pro externí síť svým způsobem neviditelný a bez speciálních technik nebo využití škodlivých kódů se útočník nedostane přímo k jeho PC.

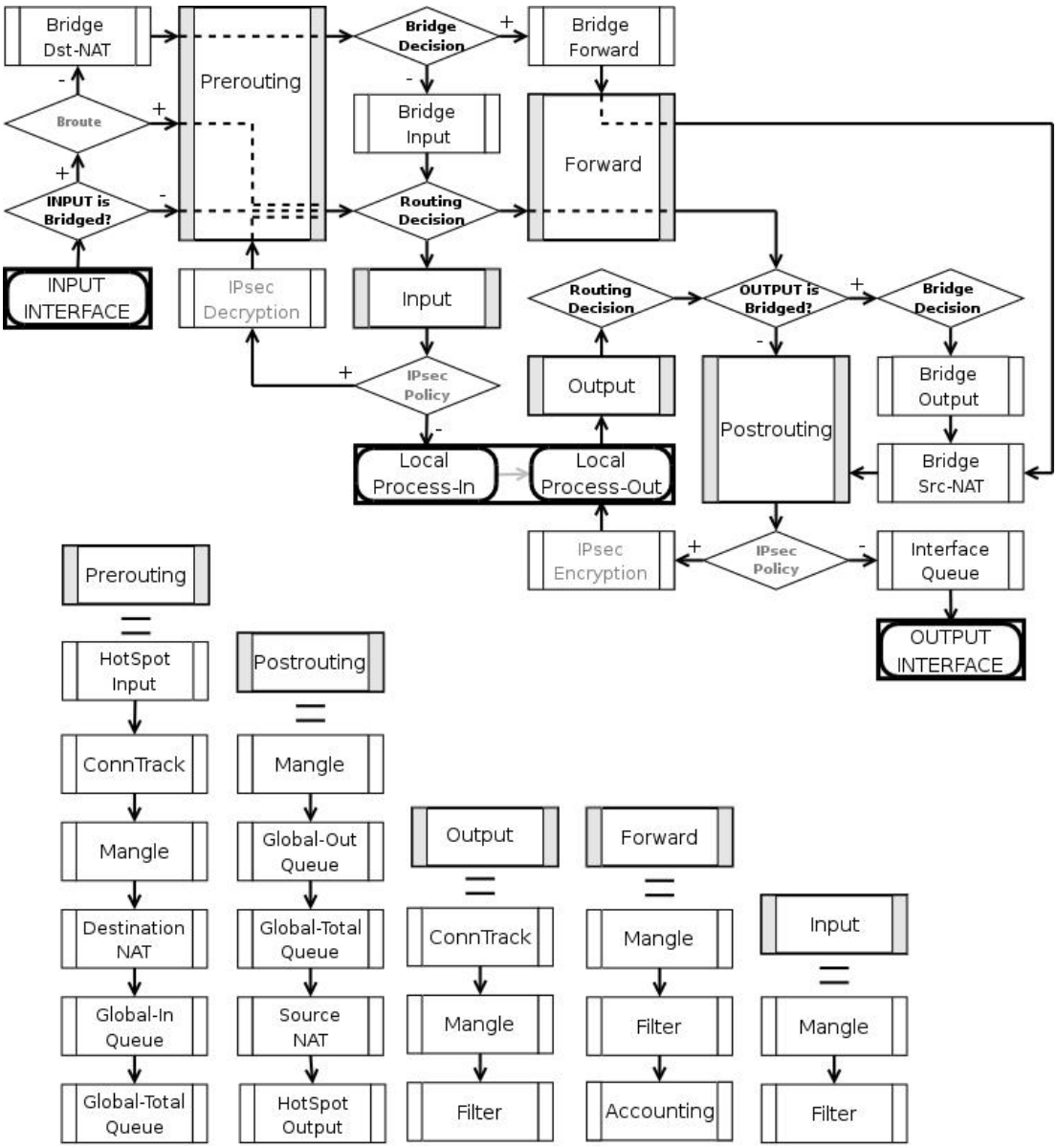
9.3.1.3 Mangle

Funkce používající se nejčastěji k značení paketů nebo spojení. S takto „označkovanými" pakety lze dále pracovat pomocí jiných funkcí zcela nezávisle. Je například možné značkovat pakety patřící do provozu sítí peer-to-peer pro sdílení nelegálního obsahu a ty pak pomocí filtrů omezovat. Také lze označit spojení od určitého uživatele jako prioritní a umožnit jim rychlejší přenos skrz infrastrukturu (typicky pro hlasové služby VoIP).

9.3.1.4 Address Lists

Obsahuje seznam adres a adresních rozsahů seskupených do skupin. Se skupinami se dá dále pracovat a zadávat je jako upřesnění do filtračních pravidel. Ve filtrech je také funkce *add-src(dst)-to-address-list,* která uloží dynamicky adresu zdroje nebo cíle a tu lze potom pomocí dalších pravidel dočasně nebo trvale z komunikace vyloučit.

Na následujícím diagramu (Obr. 8) je detailně popsán průchod paketu přes router od vstupního k výstupnímu interface.



Obr. 8 – Diagram průchodu paketu skrz Mikrotik RouterOS. [16]

9.3.2 Obecná pravidla

V nastavení části firewall v sekci *connections* jsou řazena všechna navázaná spojení procházející přes zařízení. Jejich zapsaný stav může nabývat čtyř hodnot: *new*, *established*, *related* a *invalid*. Firewall odbavuje pakety jednotlivými filtry chronologicky podle pořadí, v jakém jsou pravidla zapsána. Pokud první zapsané pravidlo vyhodnotí pakety jako akceptovatelné, jsou propuštěny a dalšími pravidly neprochází. Aby tedy firewall zbytečně nekontroloval již jednou zkontrolovaná a tedy navázaná spojení ve stavu *established* a *related*, tak se prvními dvěma filtry akceptují *(13, 14, 15, 16)*. Stav spojení *invalid* je nežádoucí a je dobré takové spojení v každém případě odmítnout *(17, 18)*.

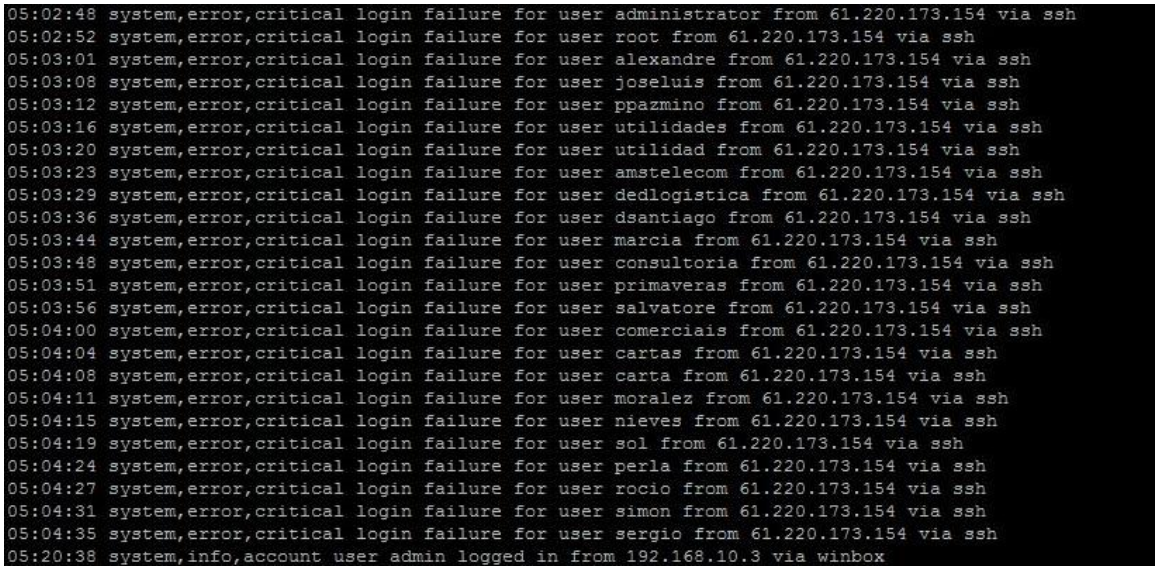
```
13) /ip firewall filter add chain=forward connection-state=established
    comment="Povolena pruchozi navazana spojeni"
14) /ip firewall filter add chain=input connection-state=established
    comment="Povolena prichozi navazana spojeni"
15) /ip firewall filter add chain=forward connection-state=related
    comment="Povolena pruchozi souvisejici spojeni"
16) /ip firewall filter add chain=input connection-state=related
    comment="Povolena prichozi souvisejici spojeni"
17) /ip firewall filter add chain=forward connection-state=invalid
    action=drop comment="Odmitnuta pruchozi neplatna spojeni"
18) /ip firewall filter add chain=input connection-state=invalid
    action=drop comment="Odmitnuta prichozi neplatna spojeni"
```

Výše uvedená pravidla jsou zapsána jako první v pořadí. Tím je zabezpečena hlubší kontrola pomocí následujících zapsaných pravidel pouze u nových spojení. To má za následek zásadní úsporu systémových prostředků. Pokud by přesto bylo potřeba kontrolovat některá již navázaná spojení, je možné odpovídající filtr je zapsat nad pravidlo č. *13*.

9.3.3 Neoprávněný přístup, bruteforce attack

Nejvíce rozšířenou metodou útoku na síťová zařízení je lámání hesel pomocí metody bruteforce. Často stačí připojit do internetu nezabezpečený router s veřejnou IP adresou a otevřenými porty a v krátkém čase jsou systémové logy zaplněny záznamy o neúspěšných pokusech o přihlášení. Útoky pochází z nejrůznějších částí světa (převládají však asijské země). Za těmito pokusy o proniknutí stojí roboti a automatizované systémy, které jsou schopny v průběhu minuty otestovat stovky kombinací uživatelských jmen a hesel. Na obrázku 9 je znázorněn systémový log nezabezpečeného směrovače po půl hodině od připojení do sítě.

Roboti procházejí postupně všechny dostupné veřejné IP adresy, a v případě, že se jim na žádaném portu otevře spojení, začínají útočit. Obvykle se lze setkat s pokusy pomocí nejběžnějších kombinací uživatelských jmen a hesel typu admin/1234 a podobně. Pokud však mají vysokou motivaci k proniknutí, zahájí na výpočetní výkon mnohem náročnější slovníkový útok, který může trvat i dny.



Obr. 9 – Systémový log v průběhu bruteforce napadení. (autor)

Z praxe je známo, že nejčastějším terčem průniku je TCP port 22. Zde běží funkce SSH, která je obvyklou vstupní branou do administrace systému. Elementárním základem je ochrana uživatelských účtů pomocí velmi přísně nastavené kombinace uživatelského jména a hesla. Další obrana není náročná, nelze však komunikaci na portu 22 bezezbytku vyloučit. Služba SSH je jednou z nejdůležitějších a často se k ní váže množství jiných funkcí systému.

Z těchto důvodů byla vyvinuta trojstupňová metoda odepření. Ta zajistí vždy a odkudkoliv bezproblémový provoz v případě oprávněného přístupu do systému. Pokud však budou během nastaveného času navázána tří nová, neúspěšná spojení, dojde k blokaci zdrojové IP adresy na 10 dní. Pokud se potenciální útočník pokusí přihlásit do administrace poprvé pomocí nesprávného jména a hesla, je jeho zdrojová adresa uložena do *address-listu* pod prefixem „SSHdrop1min“ *(23)*. Záznam má dobu platnosti (*timeout*) pouze jednu minutu, jestliže se do té doby nepokusí o další průnik tak se záznam smaže a útočník je na stejné úrovni jako na začátku. V případě, že se v časovém limitu jedné minuty pokusí o další spojení, dostane se do kompetencí vyššího filtračního pravidla *(22)*. Pokud bude i tento přístup opět neúspěšný, dojde k záznamu s příznakem „SSHdrop2min“. Situace se opakuje a v případě dalších neúspěšných spojení je zařazen do nejvyšší, avšak stále akceptované hladiny s dobou platnosti záznamu v tabulce *address-listu* 5 minut *(21)*. Poslední instancí je pravidlo přiřazující IP adrese příznak „SSHdrop10dni“ *(20)*. Zde již dochází k úplnému vyloučení provozu směrem do routeru na dobu deseti dní *(19)*.

```
19) /ip firewall filter add chain=input protocol=tcp src-address-
    list=SSHdrop10dni action=drop comment="Blokovani louskaci SSH"
    disabled=no

20) /ip firewall filter add chain=input protocol=tcp dst-port=22
    connection-state=new src-address-list=SSHdrop5min action=add-src-
    to-address-list address-list=SSHdrop10dni address-list-timeout=10d
    comment="Blokace SSH na 10 dni" disabled=no

21) /ip firewall filter add chain=input protocol=tcp dst-port=22
    connection-state=new src-address-list=SSHdrop2min action=add-src-
    to-address-list address-list=SSHdrop5min address-list-timeout=5m
    comment="Blokace SSH na 5 minut" disabled=no

22) /ip firewall filter add chain=input protocol=tcp dst-port=22
    connection-state=new src-address-list=SSHdrop1min action=add-src-
    to-address-list address-list=SSHdrop2min address-list-timeout=2m
    comment="Blokace SSH na dvě minuty" disabled=no

23) /ip firewall filter add chain=input protocol=tcp dst-port=22
    connection-state=new action=add-src-to-address-list address-
    list=SSHdrop1min address-list-timeout=1m comment="Blokace SSH na
    jednu minutu" disabled=no
```

Tato konfigurace může selhat v jediném případě, a to ve chvíli, kdy se podaří útočníkovi odhalit heslo během prvních třech spojení. Stanovení přísného hesla dle kritérií uvedených v kapitole 2.3.1 se dá tato situace vyloučit.

Jednoduchou modifikací cílových portů v jednotlivých krocích lze uvedený postup analogicky aplikovat pro kteroukoliv další, roboty potenciálně ohroženou službu. Těmi jsou zpravidla FTP fungující na portu TCP 21, telnet na portu TCP 23 nebo rlogin na portu TCP 513.

9.3.4 Odepření služby DoS

Cílem tohoto typu útoku je záměr narušitele vyřadit služby z provozu. V posuzovaném případě to většinou znamená odepření přístupu uživatelů na internet, přerušení nějaké konkrétní služby nebo zahlcení celé vnitřní sítě. V případě poskytovatele internetových služeb to vede k nemalým finančním ztrátám a množství nespokojených zákazníků.

Je nutné myslet i na to, že útok DoS může sloužit pouze jako zástěrka klasického hackerského útoku, kdy útočník využívá zaneprázdnění administrátora řešením obranných povinností. Takový útok je jen částečně agresivní a hacker čeká na chybnou reakci

správce, který může v jistou chvíli nechat otevřená některá slabá místa a tehdy útočník proniká do systému, který může jakkoliv kompromitovat.

Bohužel však z podstaty DoS útoku, který využívá známých slabin TCP komunikace neexistuje účinný způsob jak se bránit. Je popsáno několik metod, ty však mohou ochránit pouze před určitým typem DoS a nelze pomocí nich pokrýt celé riziko. Na útok je možné se připravit a celý proces ochrany lze rozdělit do tří částí:

- **Prevence před útokem**
- **Detekce útoku**
- **Reakce na útok**

9.3.4.1 Prevence před útokem

DoS útokům se velmi těžko brání, základem je proto technická a organizační připravenost. Prvním krokem je sestavení zodpovědného havarijního týmu, ten nastoupí v okamžiku zjištění vedení útoku. Nejkritičtějším faktorem je v tomto případě časové hledisko. Proto čím více času je ztraceno rozhodováním o tom, kdo bude co a jak dělat, tím déle bude síť a uživatelé odříznuti od poskytovaných služeb. Tento tým má odpovědnost za sestavení krizového plánu, kde jsou jasně definovány role každého člena týmu, jejich úlohy a za ně zodpovědné osoby.

Vycházíme-li ze známých vlastností vedení útoků, můžeme pomocí pokročilého firewallu omezit aspoň některé typy útoků. Prvním charakteristickým znakem je velké množství otevřených spojení z jedné zdrojové adresy. Pro nezbytný záznam o provedení blokace v systémovém logu je nutné provést mezikrok pomocí *address-listu* s přiřazením prefixu „DoS_max_100_spojeni“ s dobou platnosti jeden den. Pokud do routeru vstupuje více jak sto spojení z jedné zdrojové adresy, zařadí se do *address-listu* s uvedeným příznakem *(25)*. Další pokusy o vyšší množství spojení jsou odmítnuty pomocí funkce *tarpit*. Ta funguje jiným způsobem než prostý *drop*, který pakety odmítá bez jakékoliv akce. Akce *tarpit* je využitelná speciálně pro pokusy o přehlcení. Jestliže tedy v *address-listu* zdrojová adresa uvedena, je povoleno pouze pět legitimních spojení, ostatní zůstávají nezpracovány *(24)*.

```
24) /ip firewall filter add chain=input protocol=tcp connection-
   limit=100,32 action=add-src-to-address-list  address-
   list=DoS_max_100_spojeni address-list-timeout=1d

25) /ip firewall filter add chain=input protocol=tcp src-address-
   list=DoS_max_100_spojeni connection-limit=5,32 action=tarpit
```

Další známou vlastností, které útočníci využívají, je podvržení zdrojové adresy v hlavičce paketu, takzvaný spoofing. V RouterOS existuje funkce *rp_filter*, která prozkoumá původ každého paketu. Funguje tím způsobem, že pokud zdrojová adresa nevede ke stejnému interface, od kterého přišla, nebo pokud adresa vůbec neexistuje, pak takový paket odmítne. Je možné nastavit dva scénáře průběhu, přísný (strict) a volný (loose). Oba scénáře jsou popsány v doporučení RFC3704[19]. Striktně odmítá každé podezřelé spojení a je vhodný v sítích s prostým routováním. Volný režim lze využít, pokud síť využívá pokročilé routování (například MPLS nebo OSPF). Paket v tomto případě může díky kruhové topologii přijít jiným rozhraním, než je uvedeno v jeho zdroji. Filtr ho poté chybně vyhodnotí jako podvržený. V uvedeném modelu sítě pokročilého routování není využito, proto je zvolen striktní mód *(26)*. V továrním nastavení je funkce vypnuta.

```
26) /ip settings set rp-filter=scrict
```

Dalším klíčovým prvkem obrany proti DoS útoku zaplavením pakety protokolu TCP s příznakem SYN je takzvaná syncookie. Pro útok pomocí přehlcení těmito pakety se používá anglické označení SYN flood. Funkce je definována jako částečný výběr počátečního čísla sekvence paketu TCP. Použití syncookies dovoluje serveru snížit počet zahozených žádostí o spojení při naplnění fronty připravovaných spojení, což je právě cílem útočníka. Server se chová, jakoby se fronta zvětšila. Pokud server obdrží žádost o spojení (paket s příznakem SYN), pošle zdroji kladnou odpověď, tedy paket s příznaky SYN a ACK. Nicméně na rozdíl od obvyklého způsobu pak žádost odstraní z fronty. Když přijde od klienta paket s příznakem ACK, server podle čísla sekvence pozná, o kterou žádost se jednalo. To problém se zaplavením žádostmi o spojení řeší, neboť server si v paměti nic neukládá. [17]

Funkci zpracování syncookie RouterOS obsahuje, její funkci ve firewall lze aktivovat prostým povolením *(27)*.

```
27) /ip firewall connection tracking set tcp-syncookie=yes
```

Těmito funkcemi je zajištěna ochrana samotného směrovače před útokem vedeným z vnější nebo vnitřní sítě. Nelze opomenout, že distribuce záplavových paketů může naší

[19] RFC je zkratka anglického výrazu Request For Comments (žádost o komentáře), která se používá pro označení řady standardů a dalších dokumentů popisujících Internetové protokoly, systémy apod. RFC jsou oficiálně považovány spíše za doporučení než normy v tradičním smyslu, přesto se podle nich řídí drtivá většina Internetu.

sítí pouze procházet od koncového uživatele nakaženého malwarem, který je zneužit pro distribuovaný DoS (DDoS) útok. Může se tedy stát, že naše infrastruktura bude chybně vyhodnocena jako potenciálně nebezpečná. V modelovém případě, kdy je pomocí DoS napadán web www.seznam.cz a jeden z uživatelů spadající do naší sítě je k útoku zneužit, mohou inteligentní IDS/IPS filtry seznamu odříznout provoz z celé naší sítě směrem k napadenému webu a znemožnit tak všem ostatním přístup na něj.

Tomu se lze bránit. TCP SYN pakety jsou nedílnou součástí provozu internetu, lze však účinně hlídat jejich množství a při překročení určité úrovně počtu spojení je nepropustit dále do internetu. Akci tarpit zde není možné využít, protože nežádoucí provoz nepřichází do routeru, ale pouze přes něj prochází. Využije se tedy akce drop, nelze totiž předpokládat, že výkon a kapacita konektivity je u klienta vyšší než u směrovače. Přetížení směrovače v tom případě nehrozí.

Nejprve je třeba oddělit veškerou SYN komunikaci firewallem do samostatného řetězce (*chain*). Všechna nová spojení procházející přes směrovač v libovolném směru s příznakem SYN jsou zpracovávána samostatnými pravidly s názvem řetězce „SYNdrop“ *(28)*. Všechny SYN pakety jsou odděleny a zpracovávány dvěma pravidly, která je rozřadí a vyhodnotí jejich nebezpečnost. Maximální povolená měřená úroveň počtu těchto paketů je 500 za sekundu. Úroveň nižší než 10 paketů za sekundu není měřena a je považována za normální stav *(29)*. Pokud počet paketů nepřesáhne uvedenou úroveň, jsou spojení propuštěna. Pokud je počet SYN paketů vyšší než v předchozím pravidle, lze se důvodně domnívat, že jde o útok a pakety jsou v průchodu blokovány *(30)*.

```
28) /ip firewall filter add chain=forward protocol=tcp tcp-flags=syn
    connection-state=new action=jump jump-target=SYNdrop comment="SYN
    Flood ochrana" disabled=no

29) /ip firewall filter add chain=SYNdrop protocol=tcp tcp-flags=syn
    limit=500,10 connection-state=new action=accept comment="SYN OK"
    disabled=no

30) /ip firewall filter add chain=SYNdrop protocol=tcp tcp-flags=syn
    connection-state=new action=drop comment="SYN KO" disabled=no
```

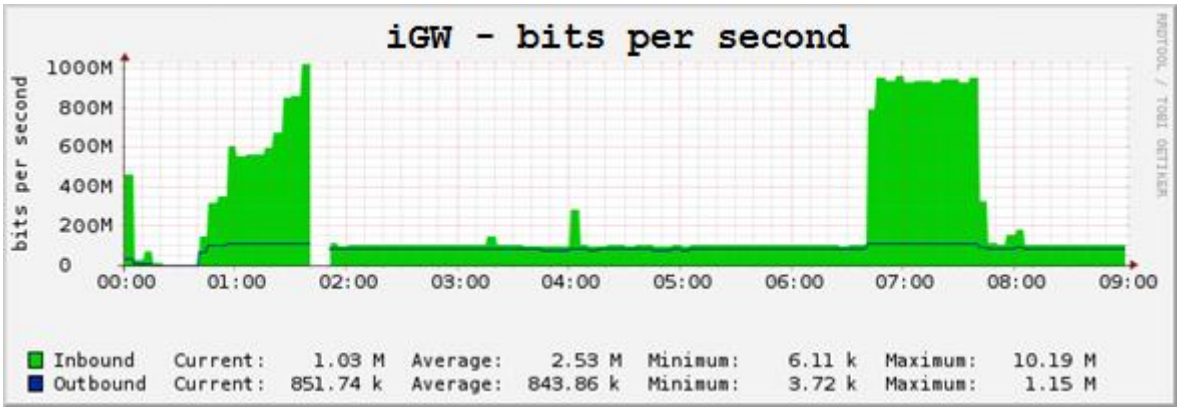
Modifikace hodnot uvedených pravidel umožňuje přizpůsobit ochranu konkrétním požadavkům různých sítí. Hodnoty uvedené v textu jsou odpovídající zvolenému modelu.

9.3.4.2 Detekce útoku

Útok lze detekovat mnohými způsoby. Základem je mít dokonale zvládnutý vzdálený monitoring, který na probíhající útok okamžitě upozorní. Existují symptomy, které i přesto, že router odpovídá, a navenek se hlásí jako dostupný, napovídají tomu, že je na něj útok veden. Mezi typické příznaky patří:

- Netypicky mnoho navázaných spojení
- Skokově zvýšený datový tok
- Vysoké využití procesoru
- Neobvykle vysoká úroveň počtu průchozích paketů za sekundu
- Nedostupnost zařízení

Pokud všechny uvedené údaje z celé sítě sbíráme, jsme schopni je i vyhodnocovat. Hodnoty je ovšem obtížné kontrolovat jednotlivě, proto je vhodné využít centrální monitorovací systém, který hodnoty zpracovává a při překročení určité prahové hodnoty vysílá varovné signály.

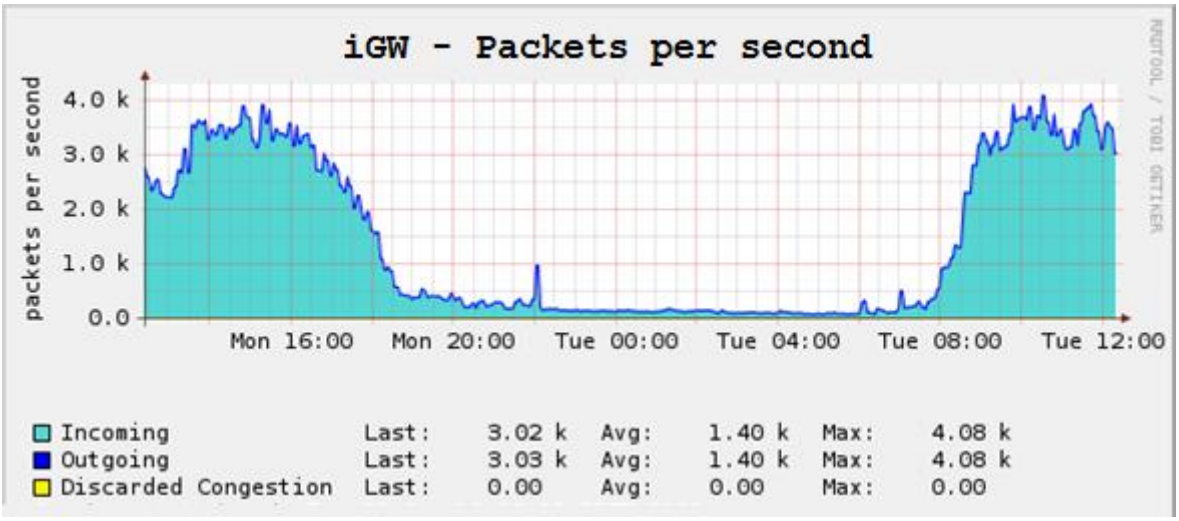


Obr. 10 – Graf skokově zvýšeného datového toku na vstupním rozhraní. (autor)

Jedním s nekomerčních produktů, šířený pod svobodnou licencí, je například monitorovací systém Zabbix. Ten je schopen číst veškeré hodnoty z jakéhokoliv zařízení pomocí SNMP[20] a v případě neobvyklé události reportovat správci. Mnohem pokročilejší nástroje jsou komerční produkty známých výrobců. Mezi které patří například HP OpenView

[20] SNMP (Simple Network Management Protocol) – je součástí sady internetových protokolů. Slouží potřebám správy sítí. Umožňuje průběžný sběr nejrůznějších dat pro potřeby správy sítě, a jejich následné vyhodnocování. Na tomto protokolu je dnes založena většina prostředků a nástrojů pro správu sítě.

VantagePoint, ten umožňuje také vzájemnou korelaci zjištěných údajů, a tím i přesnější určení příčiny. Tak ušetří správci cenné desítky minut při řešení nenadálého problému.



Obr. 11 – Graf neobvykle vysokého počtu odbavených paketů za vteřinu. (autor)

Nejlepší variantou pro detekci útoku jsou systémy nazývané IDS nebo IPS (Intrusion Prevention System nebo Intrusion Detection System). Tato zařízení se vřadí do sítě a prochází přes ně veškerý provoz. Jejich úkolem je pečlivá detekce a kontrola každého přeneseného paketu, zdali nehledá zranitelné místo systému, a nelze jej tak označit za podezřelý. Jestliže zařízení vyhodnotí nežádoucí provoz, je schopno velmi rychle reagovat a pomocí komunikace s firewallem útok v reálném čase odvrátit. Vyhodnocovací algoritmy a definice jsou pečlivě střeženým know-how výrobců systémů a jejich kvalita odpovídá ceně. Pořízení IDS špičkových výrobců typu RealSecure nebo Allot vyjde majitele sítě přinejmenším na stovky tisíc korun.

9.3.4.3 Reakce na útok

Pokud se DoS rozvinul a monitorovací systém na něj upozorní, není možné již útok jednoduše odvrátit, lze pouze zmírnit jeho následky.

Nejprve je zapotřebí informovat havarijní tým, který by měl zahrnovat vnitřní administrátory, bezpečnostního správce a odpovědné techniky. Postup se pak řídí podle předem stanoveného plánu. Pokud útok přichází z vnitřní sítě, u které je administrace v naší moci, je třeba postupovat hlouběji do infrastruktury a původce eliminovat nejlépe fyzicky přerušením datové cesty. Při útocích vedených z vnější sítě je situace mnohem složitější. Je nezbytné kontaktovat nadřazeného dodavatele konektivity a s ním postupně procházet hierarchicky jeho strukturu až k původci útoku, dokud jej nenalezneme.

Dalším poměrně jednoduchým způsobem, který lze v sítích poskytovatelů internetových služeb aplikovat, je změnit IP adresu napadeného směrovače. Administrátora změní několik málo řádků v routovací tabulce a tím dokáže problém dočasně vyřešit. Jedná se o provizorní řešení, protože narušitel je schopen tuto změnu zjistit, a zahájit útok na novou IP adresu.

Závěrem lze říci, že pro řešení nastalého útoku neexistuje univerzální návod, vždy je třeba postupovat zejména podle jeho charakteru pomocí předem připravených scénářů v havarijním plánu. Zároveň není žádoucí pro řešení využít varianty úplného zákazu služeb, přesně toho chce útočník dosáhnout. Řešením je omezování s postupným zpřesňováním s ohledem na zdroj.

9.3.5 Zneužití sítě – spam

Další případ, kdy může být síť prostřednictvím koncového uživatele zneužita k protiprávnímu jednání je rozesílání spamu. V nechráněné síti se této skutečnosti dozví nezodpovědný administrátor v lepším případě z veřejně dostupných blacklistů, kde jsou uvedeny IP adresy, ze kterých bylo již v minulosti rozesílání spamových zpráv zaznamenáno, v horším případě přímo od policie. Od 7.9.2004 platí zákon č. 480/2004 Sb., který takové jednání bez prokazatelného souhlasu příjemce zakazuje.

Vhodnou konfigurací brány firewall je možné zneužití sítě předejít. Je známo, že SMTP komunikace při odesílání emailových zpráv probíhá na portu TCP 25. Lze tedy stanovit přípustný počet spojení navázaných v časovém intervalu, a pokud dojde k překročení limitu, je další komunikace omezena. V případě, že směrovačem prochází nadlimitní množství spojení z jedné zdrojové IP adresy, v tomto případě 30 během jedné vteřiny, je odesílatel zařazen na 5 dní do *address-listu* s příznakem „spammer“ *(32)*. Pomocí předcházejícího pravidla *(31)* je veškerá další nadlimitní komunikace omezena.

```
31) /ip firewall filter add chain=forward protocol=tcp dst-port=25 src-
    address-list=spammer action=drop comment="Blokovani spammeru"

32) /ip firewall filter add chain=forward protocol=tcp dst-port=25
    connection-limit=30,32 limit=30,5 action=add-src-to-address-list
    address-list=spammer address-list-timeout=5d comment="Detekce
    spammeru"
```

9.3.6 Antivirová ochrana zákazníků

Antivirová ochrana koncových uživatelů je pomocí RouterOS a jeho firewallu také možná. Při konstrukci restrikčních omezení pro tento typ ochrany vychází z charakteristických vlastností komunikace těchto škodlivých kódů s internetem. Z dokumentace k různým druhům virů, která je ve velkém množství dostupná na internetu, je možné zjistit, které porty jaké služby pro své šíření využívají[21]. Komunikaci a šíření nejrozšířenějších typů virů lze pak účinně filtrovat.

Aby nedocházelo ke zbytečné kontrole všech průchozích paketů, je pro pakety vytvořen samostatný řetězec s názvem „viry“. Pravidlo pro skok do tohoto řetězce je umístěno na konci všech filtračních definic a do řetězce „viry“ směruje všechny zbylé pakety, které nezpracovala předchozí pravidla *(34)*. Následně se vyřazuje komunikace na viry ovládaných portech TCP nebo UDP a to postupně, pro každý zvlášť *(33 a dále)*.

```
33) /ip firewall filter add chain=viry protocol=tcp dst-port=1080
    action=drop comment="MyDoom.B"

    /ip firewall filter add chain=viry protocol=tcp dst-port=1377
    action=drop comment="Cichlid"

    /ip firewall filter add chain=viry protocol=tcp dst-port=1433-1434
    action=drop comment="Worm"

    /ip firewall filter add chain=viry protocol=tcp dst-port=2283
    action=drop comment="Dumaru.Y"

    /ip firewall filter add chain=viry protocol=tcp dst-port=2535
    action=drop comment="Beagle.W"

    /ip firewall filter add chain=viry protocol=tcp dst-port=2745
    action=drop comment="Beagle.C"

    /ip firewall filter add chain=viry protocol=tcp dst-port=3127-3128
    action=drop comment="MyDoom.A.B"

    /ip firewall filter add chain=viry protocol=tcp dst-port=3410
    action=drop comment="Backdoor OptixPro"

    /ip firewall filter add chain=viry protocol=tcp dst-port=5554
    action=drop comment="Sasser"
```

[21] Návrh filtračních pravidel vychází z tabulky: http://www.chebucto.ns.ca/~rakerman/trojan-port-table.html

```
/ip firewall filter add chain=viry protocol=tcp dst-port=8866
action=drop comment="Beagle.B"

/ip firewall filter add chain=viry protocol=tcp dst-port=9898
action=drop comment="Dabber.A"

/ip firewall filter add chain=viry protocol=tcp dst-port=10000
action=drop comment="Dumaru.Y"

/ip firewall filter add chain=viry protocol=tcp dst-port=10080
action=drop comment="MyDoom.B"

/ip firewall filter add chain=viry protocol=tcp dst-port=17300
action=drop comment="Kuang2"

/ip firewall filter add chain=viry protocol=tcp dst-port=27374
action=drop comment="SubSeven"

/ip firewall filter add chain=viry protocol=tcp dst-port=65506
action=drop comment="PhatBot, AgoBot, GaoBot"

…

34) /ip firewall filter add chain=forward action=jump jump-target=viry
    comment="KONTROLOVAT CHAIN VIRY"
```

Definice pro vyloučení zbylé komunikace na viry ovládaných portech není zdaleka kompletní. Na základě aktuálních potřeb a zjištěných hrozeb je možné definice kdykoliv operativně doplňovat a tím zajistit aspoň základní ochranu nezodpovědným uživatelům s nezabezpečenými počítači. Bohužel některé viry pro své šíření využívají porty, které jsou sdílené s žádoucími službami a tak je nelze vyloučit. Jako názorný příklad lze uvést Blade Runner. Ten se šíří portem TCP 21 určenému pro FTP přenos. Při jeho vyloučení by sice nehrozilo nakažení tímto virem, ale koncovým uživatelům by však byly zároveň eliminovány služby FTP, což je v každém případě nežádoucí.

Je nezbytné si uvědomit, že tato ochrana je jen ochranou doplňkovou a nesplňuje plnohodnotnou antivirovou funkci. Za opravdový komplexní štít proti škodlivým kódům lze prosazovat vždy pouze kvalitní softwarové antiviry známých výrobců.

9.4 Pomocné skripty

Systém Mikrotik RouterOS disponuje pokročilými možnostmi uživatelského skriptování. Obecné vlastnosti definice proměnných, matematické a logické operace, práce s cyklickými funkcemi, hledání v řetězcích, atp. umožňují přidávat a programovat další funkce na základě speciálních požadavků. Vytvořené uživatelské skripty jsou uloženy

v repositářích a je možné je spouštět ručně nebo periodicky pomocí vestavěného plánovače.

9.4.1 Pravidelné zasílání zálohy konfigurace na FTP

Jedno z důležitých pravidel síťového správce je mít kdykoliv k dispozici zálohu aktuální konfigurace prvků svěřené síťové infrastruktury pro zabezpečení kontinuity provozu. V systému RouterOS dosud paradoxně chybí nativní funkce pro pokročilou práci se zálohami. V průběhu času bylo vývojáři postupně ohlášeno několik doporučených postupů pro zasílání záloh vzdálenému serveru. Nikoliv však na FTP server a jiné běžně používané metody. Nejpřijatelnější z nich bylo její zasílání na email.

Od verze 5 vývojáři v tichosti rozšířili skrytou funkci *fetch* o možnost komunikace s FTP serverem. Tato funkce dovolila navrhnout dosud nedokumentovaný skript, který uloží zálohu jak v binárním formátu .backup tak v sadě skriptů .rsc.

Nejprve vytvoříme nový skript s názvem „zaloha-ftp“ *(35)*. Průběh posloupnosti řešení jednotlivých definovaných úkolů skriptu je tisknut do systémového logu serveru *(36, 43, 46, 50, 51)*. To umožňuje velmi rychle ověřit, zdali celý proces proběhl korektně. Pro funkci zálohy jsou definovány tři globální proměnné *(37, 38, 39)* zastupující komplikovaný název výstupního souboru a identitu routeru. Příkazy pro vytvoření dvou samostatných souborů záloh *(40, 41)* vytvoří soubory připravené k přenosu na dočasný diskový prostor směrovače. Při úvodním ladění skriptu docházelo k situaci, kdy přenos na FTP server proběhl nekompletně a výsledný soubor dorazil v poškozeném tvaru. Testováním bylo zjištěno, že korektnímu přenosu brání velmi rychlé vykonání funkce *fetch*, která odesílá ještě nedokončené soubory záloh. Proto bylo do posloupnosti vřazeno 20 vteřin přerušení *(42)*. Následuje stěžejní funkce *fetch (44, 45)*, ta v lokálním úložišti najde soubory příslušných názvů a odešle je na definovaný FTP server, kde se zálohy hromadí. Po ohlášení konce přenosu jsou soubory z lokálního úložiště smazány *(48, 49)*.

```
35) /system script add name="zaloha-ftp" source={
36) :log warning "*Zaloha na FTP zacina>"
   ;
37) :global identity [/system identity get name];
38) :global backup ([/system identity get name] . "-" . [/system
   resource get board-name] . "-" . \[:pick [/system clock get date] 7
   11] . [:pick [/system clock get date] 4 6] . ".backup");
```

```
39) :global rsc ([/system identity get name] . "-" . [/system resource
   get board-name] . "-" . \[:pick [/system clock get date] 7 11] .
   [:pick [/system clock get date] 4 6] . ".rsc");

   ;

40) /system backup save name="$backup";

41) /export file="$rsc";

   ;

42) :delay 20;

   ;

43) :log warning "*Zaloha ulozena, zacina prenos>"

   ;

44) /tool fetch address=217.170.96.3 user=zalohy password=Za10hyMTK
   mode=ftp upload=yes src-path="$backup" dst-path="mtbackup/$backup";

45) /tool fetch address=217.170.96.3 user=zalohy password=Za10hyMTK
   mode=ftp upload=yes src-path="$rsc" dst-path="mtbackup/$rsc";

   ;

46) :log warning "*Prenos dokoncen>"

   ;

47) :delay 20;

   ;

48) /file rem [/file find name="$backup"];

49) /file rem [/file find name="$rsc"];

   ;

50) :log warning "*Soubory smazany>"

51) :log warning ("*Zaloha uspesne odeslana na FTP :) " . [/sys cl get
   time] . " " . [/sys cl get date])
```

Tímto je skript kompletně definovaný a při jeho ručním spuštění jsou soubory aktuálních záloh uloženy na FTP. Aby byla zajištěna periodicita samočinného spouštění v nastaveném intervalu, lze funkci pravidelně volat pomocí integrovaného plánovače (*scheduler*). Pro běžné účely stačí uložení zálohy 1x denně *(52)*.

```
52) /system scheduler add interval=1d name=zaloha-ftp

   on-event=zaloha-ftp
```

9.4.2 Vzdálená hromadná změna konfigurace

Pokud má operátor v síti desítky až stovky zařízení, potýká se často s problémem nutných hromadných změn konfigurace. K tomuto je možnost znovu využít funkci *fetch*, která ale tentokrát pracuje v opačném režimu. To znamená, že si stáhne soubor v prostém textu (formát .txt nejlépe kódování UTF-8), ten přečte a vykoná to, co je v jeho těle uvedené, respektive to, co správce do souboru definoval.

Jako první příklad je možné uvést právě hromadnou změnu hesla do administrace. Ta je často potřebná z důvodu jeho nechtěného prozrazení nebo také propuštění zaměstnance.

Na FTP server umístíme soubor v uvedeném formátu s názvem heslo.txt. Jeho obsahem bude řetězec, který chceme nastavit jako nové heslo. V první fázi založíme script s názvem „změna-hesla“ *(29)*. Funkcí fetch se program připojí v klientském režimu na definované FTP a vyhledá zdrojový soubor „heslo.txt“ (*30)*. Do globální proměnné uloží obsah nalezený v těle souboru *(31)*, ten pak nastaví jako heslo pro uživatele admin.

```
53) /system script add name="zmena-hesla" source={
54) /tool fetch address=217.170.96.3 user=config password=c0nf1G
    src-path=heslo.txt
    ;
    :delay 10;
    ;
55) :global heslo [/file get heslo.txt contents];
56) /user set admin password=$password ;
    :log warning "*Probehla naplanovana zmena hesla"
    }
```

Opět je nutné funkci pravidelně spouštět pomocí plánovače úloh, ideální interval spuštění, vzhledem k důležité povaze typu změny, je tentokrát jedna hodina. Reálné testování odhalilo slabinu koexistence více naplánovaných úloh, při kterých se kryje čas spuštění. Pokud existuje další plánovaná akce, která je spuštěna ve shodný čas s úlohou předchozí nemusí obě proběhnout korektně. Tomuto se lze vyhnut, pokud je nastaven interval periodického spuštění 1 hodina, 1 minuta *(57)*.

```
57) /system scheduler add interval=1h1m name=zmena-hesla
    on-event=zmena-hesla
```

Občas je také nutné urychleně reagovat na jiné hrozby šířící se sítí. Mnohdy se stane, že administrátor odhalí v síti nebezpečný provoz, kterému je potřeba pro bezpečnost uživatelů nebo infrastruktury zabránit pomocí nových restrikčních pravidel. Postupná ruční úprava každého z routerů by trvala hodiny, proto je třeba hledat pohodlnější řešení.

Nyní umístíme do kmenového adresáře na FTP soubor sady skriptů .rsc, v jehož těle je uložena posloupnost příkazů, které se po spuštění vykonají. Když dojde v reálném případě k situaci, že se internetem šíří nový, nebezpečně agresivní virus a je známo, že pro svou komunikaci a šíření využívá port TCP a UDP 12345 můžeme ho jednoduše eliminovat (viz kapitola 9.3.5). Zde však záleží na rychlosti zavedení restrikčního pravidla. Omezení provozu je nutné zařadit do řetězce „viry“ a průchozím paketům na uvedených portech nastavit akci *drop (58, 59).*

```
58) /ip firewall filter add chain=viry protocol=tcp dst-port=12345
    action=drop comment="Novy vir"
59) /ip firewall filter add chain=viry protocol=udp dst-port=12345
    action=drop comment="Novy vir"
```

Tuto posloupnost uložíme do souboru s názvem config.rsc a umístíme do kmenového adresáře FTP serveru. Nový skript bude mít název „zmena-konfigurace“ a pomocí funkce *fetch* se připojí na zvolené FTP a pokud nalezne soubor config.rsc uloží jej na svůj disk *(57)*. Následuje pauza 10 vteřin pro zajištění kompletního přenosu souboru *(58)* a příkaz obsažený v souboru se vykoná *(59).*

```
60) /system script add name="zmena-konfigurace" source={
    /tool fetch address=217.170.96.3 user=config password=c0nf1G
    src-path=config.rsc
    ;
61) :delay 10;
    ;
62) import file-name=config.rsc
63) :log warning "*Probehla naplanovana zmena konfigurace"
64) }
```

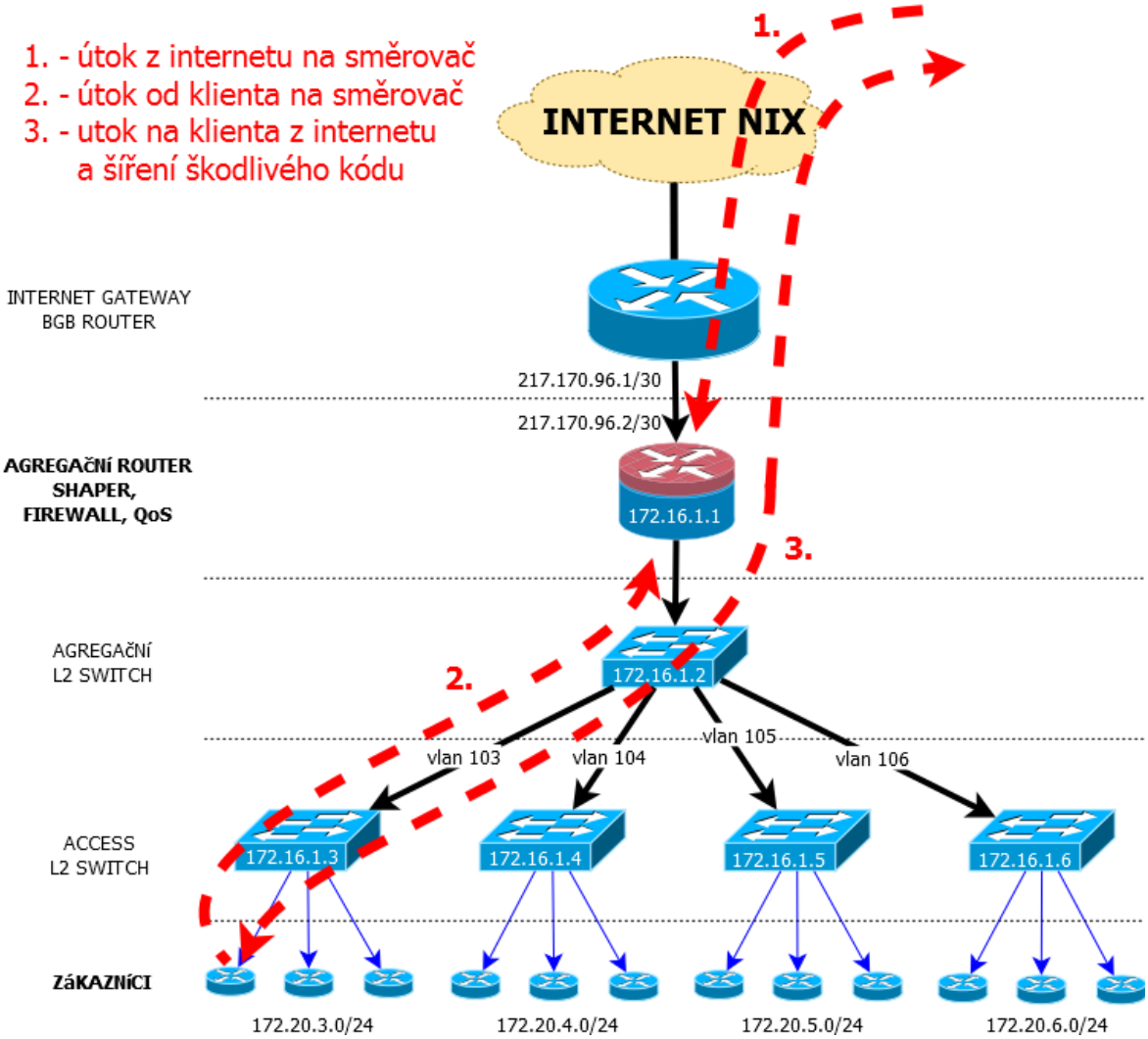
Funkci je opět nutné pravidelně spouštět. V tomto případě se může jednat o skutečně kritickou změnu konfigurace, proto je zvolen krátký interval pouze 12 minut *(65).*

```
65) /system scheduler add interval=12m name=zmena-konfigurace
    on-event=zmena-konfigurace
```

Pomocí skriptovacího jazyka je možné systém průběžně rozšiřovat. Na základě požadavku spolupracujícího poskytovatele byly cíleně vytvořeny další funkce pro monitorování dostupnosti jiných zařízení, sledování využití systémových prostředku a reporting důležitých událostí pomocí emailu.

10 TEST FUNKCÍ A ÚČINNOSTI PROTIOPATŘENÍ

Pro výchozí test návrhu bude nejprve ověřena funkce nebezpečnostních prvků konfigurace, následně bude provedena zkouška odolnosti definovaných protiopatření. Proběhne simulace útoků z vnější i vnitřní strany sítě a její výsledky budou porovnány s požadavky, které vycházejí z analýzy rizik.



Obr. 12 – Směry útoku znázorněné na modelu sítě. (autor)

10.1 Metodika testování

Pro ověření jednotlivých funkcí byl použit notebook se systémem MS Windows 7 PRO a domácí router TP-LINK TL-WR740WR. Počítač byl podle charakteru testované funkce připojen do síťové topologie buď jako koncový uživatel (Obr. 12 – hladina zákazníci), nebo do externí sítě z pozice vzdáleného útočníka. Specifikace uvedených IP adres odpovídá modelu. Cílem útoku je agregační router nebo zákazník.

10.2 Test obecných funkcí

Nejprve dojde k ověření funkce internetových služeb (kapitola 9.1). Testovací počítač byl připojen ethernetovým kabelem do rozhraní *ether3* agregačního směrovače. Pomocí DHCP serveru obdržel IP adresu ze síťového rozsahu 192.168.100.0/24 a to konkrétně 192.168.100.2/24. V tu chvíli byly internetové služby dostupné.

10.3 Test bezpečnostních funkcí

10.3.1 Odepření služeb neautorizovaným uživatelům (kapitola 9.2)

Zde existují čtyři scénáře pokusu o podvrženou autorizaci:

- Prosté připojení počítače do sítě
- Připojení přes router v továrním nastavení
- Připojení přes router se smyšleným přihlašovacím jménem a heslem
- Připojení přes router s legitimně přiděleným jménem a heslem

V případě připojení počítače do sítě přes přístupový switch bez specifikace IP adresy nebo s adresou smyšlenou, k provozu služeb nedojde, topologie a nastavení toto neumožňuje.

Pokud je připojen domácí router v tovární konfiguraci (interface WAN nastaven jako DHCP klient), je situace stejná a provoz služeb je z principu nemožný.

Připojíme-li router s nastavením WAN interface v módu PPPoE s vyplněnými smyšlenými přístupovými údaji, je už možné spatřit pokusy o navázání spojení v systémovém logu. V případě, že se přístupové údaje neshodují se záznamy v tabulce uživatelů, není přístup umožněn.

Pokud dojde ke změně přístupových údajů na údaje shodné se záznamem v tabulce uživatelů, je po připojení navázáno legitimní PPPoE spojení, přiřazena byla IP adresa 172.20.3.2 a internetové služby jsou dostupné.

Tato autentifikační metoda tedy obstála a je **plně funkční.**

10.3.2 Neoprávněný přístup, bruteforce attack (kapitola 9.3.3)

Testování proběhne z lokální i vzdálené sítě a bude ověřena funkčnost třístupňové ochrany. Pokud po vícenásobném zadání nesprávných přihlašovacích údajů bude zdrojová IP z další komunikace vyloučena a filtr je možné prohlásit za funkční.

V první fázi je testovací počítač připojen přes PPPoE do vnitřní sítě a pomocí terminálové aplikace PuTTY vytvoří první pokusné spojení na směrovač pomocí služby SSH. Po zadání korektních přihlašovacích údajů je umožněn volný přístup do konfigurace.

Po opuštění konfiguračního rozhraní je test zopakován, tentokrát však se smyšlenými přihlašovacími údaji. Po prvním pokusu je zdrojová adresa správně zařazena do address-listu s příznakem „SSHdrop1min“, po druhém pokusu do vyšší skupiny s časem platnosti 2 minuty a po dalších dvou pokusech je další komunikace vyloučena a služba SSH není dále dostupná. Zdrojovou adresu je možné v tuto chvíli nalézt v tabulce s prefixem „SSHdrop10dni“.

K testování z vnější strany bylo využito připojení od společnosti UPC a opakovala se stejná situace odepření přístupu po třech neúspěšných pokusech.

Třístupňové omezení přístupu je tedy **plně funkční** i z vnitřní i z vnější sítě.

10.3.3 Ostatní bezpečnostní funkce

Ochrana proti útokům DoS, antivirová ochrana zákazníků a ochrana proti zneužití sítě pro rozesílání spamu nebyla explicitně testována. Metodiky určené pro testování těchto rizik jsou svým rozsahem nebo nutným vybavením mimo rámec této práce.

Tyto funkce ovšem byly nasazeny v reálném provozu a z výpisů čítačů blokovaných paketů je patrné, že určitý **provoz filtrují.**

10.4 Test doplňkových funkcí

Pro zkoušku doplňkových funkcí musel být nejdříve spuštěn FTP server s příslušnými přihlašovacími údaji. Byla mu přiřazena IP adresa 217.170.98.177, a proto musely být odpovídající údaje ve skriptech účelově změněny.

10.4.1 Zasílání zálohy konfigurace na FTP (kapitola 9.4.1)

Po zavedení skriptu do konfigurace došlo k jeho ručnímu spuštění. Průběh bylo možné sledovat v systémovém logu a po potvrzení úspěšného přenosu se záložní soubory v žádoucím formátu skutečně nacházeli v příslušném adresáři FTP serveru.

Funkce plánovače byla ověřena týdenním testovacím provozem. Podle očekávání zde skript zanechal každý den aktuální zálohu konfigurace.

Uvedený skript lze tedy označit jako **plně funkční.**

10.4.2 Hromadná změna konfigurace (kapitola 9.4.2)

Pro zkoušku této funkce byly připraveny dva soubory s totožným obsahem uvedeným v kapitole 9.4.2. Skripty byly uvedeny do provozu a na FTP server byl umístěn nejprve soubor „heslo.txt“. Po jedné hodině byl ověřen stav a ke změně hesla do konfiguračního rozhraní skutečně došlo.

Následně byl na stejné místo uložen soubor „config.rsc“ s pravidly dle uvedeného zdrojového kódu *(58, 59)*. Po patnácti minutách uvedené dva filtry skutečně nalézali sekci *Filter Rules*. Kontrolou systémového logu bylo zjištěno, že uvedené funkce s žádnou jinou funkcí nekolidovaly a vždy proběhly korektně až do konce.

Skript pro hromadnou změnu konfigurace je tedy rovněž **plně funkční.**

ZÁVĚR

Tato diplomová práce přinesla čtenáři důležité poznatky z oboru bezpečnosti počítačových sítí. Cílovou skupinou jsou především administrátoři rozlehlých kabelových sítí poskytovatelů internetových služeb. Práce navazuje na bakalářskou práci autora, kde se z větší části zabýval ochranou bezpečnosti z hlediska koncového uživatele.

V úvodu teoretické části se práce věnuje stručnému popisu historie internetu v České Republice i ve světě, a všímá si souvislostí, které dali vzniknout lokálním poskytovatelům internetových služeb. Následně byly formou literární rešerše podobným způsobem specifikovány hrozby pohybující se v oblasti správy serverů a údržby síťové infrastruktury. Na základě načerpaných poznatků byly vyhledány jednotlivé cíle útoků a analyzován dopad jejich napadení 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.

Protože je pro studium předmětné problematiky klíčové získat všeobecný náhled na zařazení centrálního agregačního zařízení v přenosovém řetězci, bylo jej v praktické části nutné nejprve hierarchicky zasadit do kompletního modelu topologie zkoumané sítě. Od tohoto návrhu se následně odvíjely všechny následující části práce. Jako konkrétní typ zařízení pro aplikaci restrikčních opatření, byl podle všeobecného hodnocení tří funkčně si odpovídajících reprezentantů, vybrán Mikrotik – RouterOS.

Na základě určených kritérií bezpečnosti a popisu možných způsobů narušení integrity sítě byla vytvořena pokročilá konfigurace filtračních řetězců a bezpečnostních definic. Ta přísným způsobem brání průniku neautorizovaného klienta do sítě, neoprávněnému přístupu do konfigurace zařízení, odepření služby DoS a DDoS a zneužití síťové infrastruktury pro šíření spamu a je doplněna o antivirovou ochranu zákazníků.

Nastavené funkce byly nejprve úspěšně testovány pomocí nejrůznějších simulací v lokálním prostředí a následně průběžně experimentálně nasazovány do reálného provozu ve funkční síti, která strukturou i počtem uživatelů odpovídá stanovenému modelu. Reálným provozem byla sekundárně ověřena funkčnost jednotlivých struktur brány firewall a doplňkové funkce byly doplněny o některé další vlastnosti, které se projevili až v průběhu reálného testování.

Důsledným laděním funkcí tedy vznikl konkrétní model obecné i bezpečnostní konfigurace, který může být po změně hodnot odpovídajících konkrétní síti úspěšně nasazen do samostatného provozu, bez nutnosti dalších úprav.

ZÁVĚR V ANGLIČTINĚ

This master' thesis has brought readers important insights from the field of computer network security, being targeted primarily at the administrators of large cable networks of internet service providers. The thesis follows the author's bachelor's thesis, which largely dealt with protection and security from the perspective of end users.

At the beginning of the theoretical part, the thesis provides a brief description of the history of the Internet in the Czech Republic and abroad, elaborating on the context that gave rise to local Internet service providers. As the next step, the threats existing in server management and network infrastructure maintenance are defined in a similar manner, in the form of a literary review. Based on the knowledge gained, the individual targets attacked were identified and the impact of these attacks on normal operation was analyzed. A deeper analysis of the problem allowed for identification of the profiles of the different types of attackers, including a list of situations in which their attacks may be anticipated; the damage potentially inflicted by their actions could also be assessed. A ranking was compiled of the most common mistakes committed by network infrastructure managers that can effectively help risk situations to arise.

When studying the issue at hand, it is crucial to have a general view of the incorporation of the central aggregation device in the transmission chain; therefore, in the practical part, the device had to be first incorporated into the hierarchy of the complete topological model of the examined network. The rest of the thesis unfolds from such a design. The specific type of device chosen for the application of measures, based on a general evaluation of three functionally identical representative samples, was Mikrotik – RouterOS.

Based on the determination of the safety criteria and the description of possible ways of network integrity disruption, an advanced configuration of filter chains was created that would adequately prevent the entry of unauthorized clients into the network, prevent unauthorized access to the device configuration, deny the use of the DoS and DDoS services and prevent spamming; the configuration is complemented by a anti-virus protection of customers.

The functions configured were continually subjected to local testing by means of a variety of simulation experiments and then gradually deployed into live operation in a functional network, the structure of which corresponded to the model determined. Live operation was an additional means to verify the functionality of the individual firewall structures, and

additional features were complemented with certain logical characteristics the need for which had not arisen until the testing in live operation.

Consistent tuning up of the functionalities therefore gave rise to a configuration model to be independently deployed, once the values have been adjusted to the given network, without the need for additional modifications.

SEZNAM POUŽITÉ LITERATURY

[1] Bezpečnost na internetu. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-05-10]. Dostupné z: http://cs.wikipedia.org/wiki/Bezpečnost_na_internetu

[2] TOXEN, Bob. Bezpečnost v Linuxu: prevence a odvracení napadení systému. Vyd. 1. Brno: Computer Press, 2003, s. 8-10. ISBN 80-7226-716-7.

[3] WEBER, Filip. DoS a DDoS útoky a ochrana proti nim (1). Svět sítí [online]. [cit. 2013-05-10]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=DoS-a-DDoS-utoky-a-ochrana-proti-nim-1-742008

[4] TOXEN, Bob. Bezpečnost v Linuxu: prevence a odvracení napadení systému. Vyd. 1. Brno: Computer Press, 2003, s. 10-12. ISBN 80-7226-716-7.Bezpečné heslo. In:

[5] Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-05-10]. Dostupné z: http://cs.wikipedia.org/wiki/Bezpečné_heslo

[6] TOXEN, Bob. Bezpečnost v Linuxu: prevence a odvracení napadení systému. Vyd. 1. Brno: Computer Press, 2003, s. 31-38. ISBN 80-7226-716-7.

[7] THOMAS, Thomas M. Zabezpečení počítačových sítí bez předchozích znalostí. Vyd. 1. Brno: CP Books, 2005, s. 140-141. ISBN 80-251-0417-6.

[8] WEBER, Filip. Penetrační testy v bezpečnostní analýze informačního systému. [online]. 2007 [cit. 2013-05-10]. Dostupné z: http://www.svetsiti.cz/clanek.asp?cid=Penetracni-testy-v-bezpecnostni-analyze-informacniho-systemu-28102007

[9] NIX. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): Wikimedia Foundation, 2001- [cit. 2013-05-10]. Dostupné z: http://cs.wikipedia.org/wiki/NIX

[10] Juniper networks [online]. 2013 [cit. 2013-05-02]. Dostupné z: http://www.juniper.net/us/en/products-services/switching/ex-series/ex4200/

[11] TP-LINK [online]. [2013] [cit. 2013-05-10]. Dostupné z: http://cz.tp-link.com/products/details/?categoryid=222&model=TL-SG5428

[12] Juniper networks [online]. 2013 [cit. 2013-05-02]. Dostupné z: http://www.juniper.net/us/en/products-services/routing/mx-series/mx80/

[13] Česká Republika. § 98 127/2005 Sb. o elektronických komunikacích. In: http://portal.gov.cz/app/zakony/zakonPar.jsp?page=7&idBiblio=59921&recShow=114&nr=127~2F2005&rpp=15#. 2005.

[14] MALANÍK, Ing. David. Význam fyzického zabezpečení IT systémů. Security Revue [online]. 2010 [cit. 2013-05-03]. Dostupné z: http://www.securityrevue.com/article/2010/09/vyznam-fyzickeho-zabezpeceni-it-systemu/

[15] APC [online]. [2013] [cit. 2013-05-30]. Dostupné z: http://www.apc.com/products/family/index.cfm?id=165

[16] Packet Flow. In: Mikrotik testdocs [online]. 2006 [cit. 2013-04-22]. Dostupné z: http://www.mikrotik.com/testdocs/ros/2.9/ip/flow.php

[17] About: SYN cookies. In: Dbpedia [online]. [2013] [cit. 2013-05-01]. Dostupné z: http://dbpedia.org/page/SYN_cookies

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AAA	Authentication, Authorization And Accounting
AP	Access Point
AS	Autonomní Systém
BGP	Border Gateway Protocol
CCR	Cloud Core Router
CIA	Central Intelligence Agency
CLI	Command Line Interface (Příkazový Řádek)
DDoS	Distributed Denial Of Services
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarizovaná Zóna
DNS	Domain Name Systém
DoS	Denial Of Service
EoIP	Ethernet Over IP
FTP	File Transfer Protocol
FTTx	Fiber To The X
GUI	Grafical User Interface
HW	Hardware
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IMAP	Internet Message Access Protocol
IP	Internet Protocol
IPS	Intrusion Prevention System
IPsec	Internet Protocol Security
ISO/OSI	International Org. for Standardization/ Open Systems Interconn.

ISP	Internet Service Provider
ITSEC	Information Technology Evaluation Criteria
L2	Layer 2 (druhá vrstva ISO/OSI)
L2TP	Layer 2 Tunneling Protocol
L3	Layer 3 (třetí vrstva ISO/OSI)
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
Mbps	Megabit per second (megabit za sekundu)
MPLS	Multiprotocol Label Switching
MTBF	Mean Time Between Failures
NAT	Network Address Translation
NFS	Network File System
NTP	Network Time Protocol
OS	Operační Systém
OSPF	Open Shortest Path First
OVPN	Open Virtual Private Network
POP3	Post Office Protocol 3
PPP	Point-To-Point Protocol
PPPoE	Point-To-Point Protocol Over Ethernet
PPTP	Point-To-Point Tunneling Protocol
QoS	Quality Of Service
RB	RouterBoard
RIP	Routing Information Protocol
RPC	Remote Procedure Call
SFP	Small Form-Factor Pluggable Transceiver

SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
SW	Software
TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TTAP	Trust Technology Assesment Program
UDP	User Datagram Protocol
UPnP	Universal Plug-and-Play
UTP	Unshielded Twisted Pair
VLAN	Virtual Local Area Network
VoIP	Voice Over IP
VPN	Virtual Private Network
WAN	Wide Area Network
WDS	Virtual Distribution System
WiFi	Wireless-Fidelity

SEZNAM OBRÁZKŮ

SEZNAM TABULEK