Univerzita Pardubice
Fakulta ekonomicko-správní

Bezpečnost počítačových sítí – firewally

Bc. Michal Sedláček

DIPLOMOVÁ PRÁCE

2009

Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky
Akademický rok: **2008/2009**

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michal SEDLÁČEK**
Studijní program:	**N6209 Systémové inženýrství a informatika**
Studijní obor:	**Regionální a informační management - Informačn management**
Název tématu:	**Bezpečnost počítačových sítí - firewally**

Zásady pro vypracování:

1. Úvod
2. Síťová bezpečnost
3. Bezpečnostní síťová zařízení
4. Návrh řešení - praktický příklad
5. Závěr

Rozsah grafických prací:

Rozsah pracovní zprávy:

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

Seznam odborné literatury:

Thomas T.: Zabezpečení počítačových sítí. Brno 2005. ISBN 80-251-0417-6

Wiliam Ch., Steven B.: Firewalls and Internet Security. Reading 1994. ISBN 0-201-63357-4

Jirkovský V.: Kybernetická kriminalita. Praha 2007 ISBN 978-80-247-1561-2

Dostálek, L. a kol.: Velký průvodce protokoly TCP/IP: Bezpečnost - 2.aktualizované vydání. Computer Press, Brno ISBN: 80-7226-849-X

Vedoucí diplomové práce: **prof. Ing. Jan Čapek, CSc.**
Ústav systémového inženýrství a informatiky

Datum zadání diplomové práce: **6. října 2008**

Termín odevzdání diplomové práce: **1. května 2009**

L.S.

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

doc. Ing. Jiří Křupka, Ph.D.
vedoucí ústavu

V Pardubicích dne 6. října 2008

Prohlašuji:
Tuto práci jsem vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 14. 8. 2009

Michal Sedláček

SOUHRN

Diplomové práce se zabývá problematikou profilu ochrany se zaměřením na firewally v rámci projektu Společných kritérií pro hodnocení informační bezpečnosti. První část diplomové práce popisuje firewally, jejich funkce a možnosti aplikace. V druhé části jsou vysvětleny obecné principy bezpečnosti počítačových sítí. Další kapitola je věnována kritériím pro hodnocení informační bezpečnosti a podrobně je rozebrán profil ochrany pro firewally. V závěrečné části je zpracován vlastní průzkum, do jaké míry organizace v České republice splňují bezpečností požadavky definované v tomto profilu.

KLÍČOVÁ SLOVA

firewall; bezpečnost IT; Společná kritéria, Profil ochrany

TITLE

Network Security – Firewalls

ABSTRACT

The diploma thesis deals with the Firewall Protection Profile within the scope of the Common Criteria for Information Technology Security Evaluation. In the first part of the thesis, firewalls, their function and possibilities of their application are described. General principles of network security are presented in the second part. The next chapter describes criteria for evaluation of information security, focusing particularly on the Firewall Protection Profile. In the final part of the thesis, conclusion of my own investigation how and to which extent organization in the Czech Republic comply with the security requirements defined in the Common Criteria are presented.

KEYWORDS

Firewall, IT security, Common Criteria, Protection profile

Poděkování

Rád bych na tomto místě vyjádřil své poděkování vedoucímu diplomové práce panu prof. Ing. Janu Čapkovi, CSc. za jeho podnětné připomínky a cenné rady při vedení mé diplomové práce, které mi umožnily problematiku lépe odborně formulovat a ve svém důsledku tak celou práci zkvalitnit. Dále děkuji svým rodičům za podporu po celou dobu mého studia.

OBSAH

Úvod 9
1 Firewally 10
1.1 Historie 10
1.1.1 První generace firewallů 10
1.1.2 Druhá generace firewallů 10
1.1.3 Třetí generace firewallů 11
1.2 Základní pojmy 11
1.2.1 Detekční systémy 13
1.2.2 Referenční modely počítačových sítí 14
1.3 Funkce firewallů 15
1.3.1 Omezení firewallu 16
1.4 Typy firewallů 16
1.4.1 Paketový filtr 16
1.4.2 Stavové paketové filtry 17
1.4.3 Aplikační proxy 18
1.4.4 Firewall jako součást operačního systému 19
1.4.5 Firewall – samostatné zařízení 20
1.5 Umístění firewallu v síti 21
1.5.1 Model sítě s jedním firewallem 21
1.5.2 Model sítě s jedním firewallem a bastion host 22
1.5.3 Model sítě s jedním firewallem a demilitarizovanou zónou 23
1.5.4 Model sítě se dvěma firewally a DMZ 24
1.6 Datový provoz 25
2 Síťová bezpečnost 29
2.1 Bezpečnostní principy 29
2.1.1 Princip (AAA) Autentizace, Autorizace a Audit 29
2.1.2 Princip (CIA) Důvěrnost, integrita a dostupnost dat 29
2.1.3 Princip minimálních oprávnění (least privilege) 30
2.2 Ochrana Informací 30
2.3 Síťová bezpečnost a Internet 31
2.4 Útoky na počítačové sítě 33
2.4.1 Nestrukturované útoky 33
2.4.2 Strukturované útoky 33
3 Kritéria hodnocení informační bezpečnosti 34
3.1 TSEC (Trusted Computer System Evaluation Criteria) 35
3.1.1 Struktura TSEC 35
3.2 Common Criteria 35
3.2.1 Struktura Common Criterií 35
3.2.2 Profily ochrany a cíle bezpečnosti 36
3.3 Profil ochrany 36
3.3.1 Popis částí Profilu ochrany 36
4 Profil ochrany pro firewally verze 2.0 39
4.1 Popis TOE 39
4.2 Provozní prostředí TOE 39

4.3 Bezpečností prostředí TOE ... 40
4.3.1 HROZBY ... 40
4.4 Organizační bezpečnostní politiky ... 41
4.4.1 Předpoklady ... 41
4.5 Bezpečností cíle ... 42
4.5.1 Bezpečnostní cíle TOE ... 42
4.5.2 Bezpečnostní cíle prostředí ... 42
5 Výsledky dotazníkového šetření a řízených rozhovorů ... 44
5.1 Cíl průzkumu ... 44
5.2 Vzorek respondentů ... 44
5.3 Sběr dat ... 45
5.4 Analýza dat a výsledků průzkumu ... 45
6 Návrh zabezpečení – praktický příklad ... 66
Závěr ... 72
Použitá literatura ... 75
Seznam obrázků ... 78
Seznam tabulek ... 78
Seznam grafů ... 78
Seznam příloh ... 79

Úvod

Síťová bezpečnost se dnes dostává do popředí zájmu všech velkých, středních i menších organizací i jednotlivců. Důvod je prostý. Dnes již každý ví, že na síti není bezpečno, a to zejména na síti veřejné. S dynamickým rozvojem Internetu se objevilo velké množství bezpečnostních rizik, kterým je potřeba aktivně čelit, a to jak softwarovými, tak hardwarovými prostředky. Mezi nejsofistikovanější prostředky pro ochranu dat a zabezpečení počítačových sítí patří firewally. Firewally jsou zařízení, která umožňují bezpečný přechod dat mezi důvěryhodnou (např. interní podniková síť) a nedůvěryhodnou (např. veřejná síť Internet) sítí. Umožňují účinně eliminovat nežádoucí síťový provoz, a to zejména ze strany nedůvěryhodné sítě.

V důsledku rozvoje firewallů a ostatních bezpečnostních technologií vznikla potřeba vytvářet referenční kritéria, podle kterých lze jednotlivé produkty a systémy porovnávat. V oblasti bezpečnosti informačních technologií je vhodné při vyhodnocování kritérií postupovat podle předem daných a ověřených postupů. Důležité je, aby referenční kritéria bylo možné používat univerzálně a jednotně. Za tímto účelem vznikly různé mezinárodní normy. Jednou z těchto norem jsou Společná kritéria (Common Criteria), kterými se tato práce zabývá.

Cílem této diplomové práce je poukázat na existenci profilu ochrany zabývající se výhradně problematikou firewallů v rámci projektu Společných kritérií a přiblížení této problematiky českým uživatelům. Dále pak na základě průzkumu zmapovat a vyhodnotit, do jaké míry organizace v České republice splňují bezpečností požadavky definované v tomto profilu ochrany. První část diplomové práce popisuje firewally, jejich funkce a možnosti aplikace. V druhé části jsou vysvětleny obecné principy bezpečnosti počítačových sítí. Další kapitola je věnována kritériím pro hodnocení informační bezpečnosti a podrobně je rozebrán profil ochrany pro firewally. V závěrečné části je zpracován vlastní průzkum. V poslední kapitole je uveden praktický příklad.

1 Firewally

Ochrana dat a zabezpečení počítačových sítí je technologickým trendem současnosti. Proces ochrany počítačových sítí je stále náročnější a složitější díky obrovskému rozvoji v této oblasti. Přitom pro mnoho organizací tvoří výdaje na ochranu dat a informací méně než jedno procento z celkového rozpočtu [1]. Při nákupu nebo správě technologií pro zabezpečení podnikové sítě jsou klíčovým produktem firewally. Firewally samozřejmě nepředstavují jediný nástroj pro zabezpečení počítačové sítě, ale při efektivním využití mohou značnou měrou snížit riziko zneužití nebo ztráty dat. Současně s integrovanými technologiemi, jakými jsou antivirový software, hloubková analýza paketů, filtrování Uniform Resource Locator (URL) a virtuální privátní sítě (VPNs), mohou firewally poskytnout velké množství zabezpečovacích technologií v rámci jednoho systému.

1.1 Historie

Firewally jsou ve světě výpočetní techniky poměrně mladým odvětvím. První firewally se objevily v polovině osmdesátých let minulého století, v laboratořích výrobce síťových komponentů Cisco Systems. V roce 1988 vyšla vůbec první kniha zabývající se technologií firewallů. Jejím autorem je Jeff Mogul z firmy Digital Equipment Digital Corporation (DEC).

1.1.1 První generace firewallů

První firewally sloužily pouze k oddělení jednotlivých privátních sítí LAN. Jednalo se o bezstavové paketové firewally. Jedním z prvních byl firewall vyvinutý v softwarové divizi společnosti Cisco Systems.

Bezpečnostní politika firewallu byla prostá: Povol všem „uvnitř“ přístup „ven“ a zabraň komukoliv „zvenku“ přístup „dovnitř“. Jednalo se o velmi účinný, ale limitovaný bezpečnostní systém. [11]

1.1.2 Druhá generace firewallů

Následovala druhá generace firewallů vyvíjená společností AT&T Bell Laboratories od roku 1990. Jednalo o firewally založené na filtrování paketů s kontrolou stavu (State full packet inspection). [11]

1.1.3 Třetí generace firewallů

Za otce třetí generace firewallů jsou považováni Marcus Ranum a Bill Cheswick. Právě díky jejich práci firma DEC uvolnila první komerční firewall s názvem SEAL v roce 1991. Tento typ firewallů je známý pod pojmem aplikační proxy (application proxy firewall). [2]

1.2 Základní pojmy

Pro pochopení principů a možností firewallů a bezpečnosti počítačových sítí je vhodné znát základní pojmy, které mají s touto problematikou přímou souvislost.

Paket je formátovaný blok dat, který se přenáší v počítačové síti. O paketech se mluví v souvislosti se síťovou vrstvou. Paket se skládá ze tří základních prvků, a to hlavičky, datové oblasti a traileru. Hlavička obsahuje informace potřebné pro doručení paketu do místa určení. Paket obsahuje IP adresu, další atributy a data. Zabalí se do rámce a následně putuje sítí. [2]

IP adresa – slouží k jednoznačné identifikace fyzického připojení k síti. Data zasílaná v počítačové síti ve formě paketů vždy obsahují IP adresu. IP adresy je možné rozdělit podle verze protokolu IPv4 nebo IPv6. V současné době je stále nejvyužívanější verze IPv4. Tato 32-bitová adresa je tvořena čtyřmi osmi bitovými čísly, z nichž každé může nabývat hodnoty od 0 do 255. Existují 3 základní třídy IP adres: A, B a C. Rozdělení do tříd se provádí na základě prvních tří bitů adresy. Nejnovější prognózy hovoří o tom, že adresní prostor protokolu IPv4 bude vyčerpán mezi lety 2011 až 2012. Tento problém řeší protokol IPv6.

Adresa protokolu IPv6 je 128-bitová. Zapisuje se jako osm skupin po čtyřech hexadecimálních číslicích. Kromě mnohem většího adresního prostoru, má protokol IPv6 některé nové vlastnosti reagující na vývoj počítačových sítí. Například design odpovídající vysokorychlostním sítím, bezpečnostní mechanismy přímo v IP, podporu mobilních zařízení, automatickou konfiguraci, kooperaci IPv4 a co nejhladší přechod ze stávajícího protokolu na nový. [13]

Port je logická přípojka k síti určená šestnácti bitovým číslem, které TCP i UDP užívají k dodávce dat k příslušné aplikaci. K portu může být připojena jen jedna aplikace. Porty

jsou očíslovány 0 – 65535, přičemž rezervované porty mají čísla. [4] Přehled nejznámějších TCP a UDP portů uvádí tabulka 1.

Tabulka 1: TCP a UDP porty

Nejznámější TCP a UDP porty	
TCP	**UDP**
FTP 21	DNS 53
SSH 22	DHCP-Relay 67
Telnet 23	TFTP 69
SMTP 25	NTP 123
HTTP 80	IKE 500
IMAP 143	Syslog 514

Internet protokol (IP) společně s protokolem TCP tvoří základ dnešního internetu. Jedná se o protokol sloužící k přenosu dat v síti. Přenos je rozdělen do bloků zvaných datagramy. Každý datagram je přenášen samostatně a nezávisle na ostatních. Nejčastěji používaná verze protokolu je IPv4. Nástupcem je verze IPv6. Verze protokolu úzce souvisí s adresací (viz pojem IP adresa). [2]

IP-protokol je tvořen několika dílčími protokoly:

- Vlastním protokolem IP.
- Služebním protokolem ICMP sloužícím zejména k signalizaci mimořádných stavů.
- Služebním protokolem IGMP sloužícím pro dopravu adresných oběžníků.
- Služební protokoly ARP a RARP, které jsou často vyčleňovány jako samostatné na IP nezávislé protokoly, protože jejich rámce nejsou předcházeny IP-záhlavím[2,3].

User Data Protocol (UDP) je protokol určený pro aplikační protokoly a procesy, které požadují rychlý a nezabezpečený přenos paketů bez potvrzování příjmu a opakování přenosu. Protokol se přenáší v datové části IP paketů. Protokol obsahuje mechanismus adresování koncových procesů, aby mohl vykonávat multiplex a demultiplex dat mezi koncovými procesy a sítí. [14]

Transmission Control Protocol (TCP) je spojovanou službou, tj. službou, která mezi dvěma aplikacemi naváže spojení – vytvoří na dobu spojení virtuální okruh. Tento okruh je

plně duplexní (data se přenášejí současně na sobě nezávisle oběma směry). Přenášené bajty jsou číslovány. Ztracená nebo poškozená data jsou znovu vyžádána. Integrita přenášených dat je zabezpečena kontrolním součtem. [2]

Bastion host je v české odborné literatuře překládán jako bašta. V původním významu se baštou rozumí silně opevněná část středověkého hradu, která slouží k ochraně před útočníky. V souvislosti s firewally a síťovou bezpečností se jedná o systém, který spravuje administrátor firewallu. Typicky jde o počítač, který má jako jediný nebo jeden z mála přístup do vnitřní i vnější sítě. To z něj činí kritický bod zabezpečení. V současnosti se používá obvykle jen v kombinaci s jinými způsoby zabezpečení. Typické nasazení bastion je v případě, že organizace spravuje veřejně dostupný webový nebo FTP server.

Demilitarizovaná zóna (DMZ) je síťový segment, který je pod správou administrátora sítě, ale fyzicky je oddělen od vnitřní chráněné sítě [4].

Target of evaluation (TOE) znamená předmět hodnocení. Tento pojem se vyskytuje v souvislosti s Common Criterii a profily ochrany viz kapitola 4.3. V této diplomové práci je TOE většinou firewall nebo bezpečnostní politika organizace.

Virtual Private Network (VPN) je virtuální privátní síť. VPN slouží k virtuálnímu spojení více fyzicky vzdálených počítačů, takže se chovají, jako by byly přímo propojené jednou sítí. Umožňuje například spojení sítí dvou poboček jedné firmy do sítě, která se chová jako jeden celek. [15]

1.2.1 Detekční systémy

Intrusion Detection Systém (IDS) nebo též Intrusion Detection and Prevention System (IPS) jsou v podstatě stejné systémy, které různí výrobci označují různými způsoby V tomto případě se jedná spíše o marketing. Jde o systémy pasivní i aktivní bezpečnosti podle typu nastavení. Tyto technické prvky poskytují ochranu na aplikační vrstvě modelu TCP/IP, tj. provádějí filtraci nikoliv jen hlaviček TCP paketů, ale i samotných dat, která jsou pakety přenášena. Filtrace je prováděna na základě analýzy anomálií (signatur). Anomálie je v podstatě reprezentativní vzorek vadného kódu, například viru apod. Databáze signatur jsou pravidelně aktualizovány ze strany výrobců.

Detekční systém může být nastaven ve dvou režimech, tyto režimy se nazývají aktivní a pasivní: Aktivní režim v případě, že systém detekuje anomálii v probíhajícím spojení, zruší probíhající spojení a je vytvořen záznam (log o tomto bezpečnostním incidentu).

V případě aktivního režimu je firewall společně s detekčním prvkem zapojen sériově.

V případě pasivního režimu je přicházející provoz kopírován pomocí hardwarového členu replikátoru. Pokud je detekována anomálie, není probíhající spojení nijak dotčeno, ale pouze se vytváří log o takové události. Výhodou pasivního režimu je, že nedochází ke zpomalení síťového provozu.

1.2.2 Referenční modely počítačových sítí

ISO/OSI model je referenční komunikační model označený zkratkou slovního spojení "International Standards Organization / Open System Interconnection" (Mezinárodní organizace pro normalizaci / propojení otevřených systémů)

Referenční model, stejně tak jako celá rodina protokolů ISO/OSI, obsahuje některé důležité principy a mechanismy v oblasti síťové komunikace. Jako celek je však poněkud teoretický a zbytečně složitý. ISO/OSI model je založen na sedmivrstvé síťové architektuře. Jednotlivé vrstvy se nazývají fyzická, spojová, síťová, transportní, relační, prezentační a aplikační.

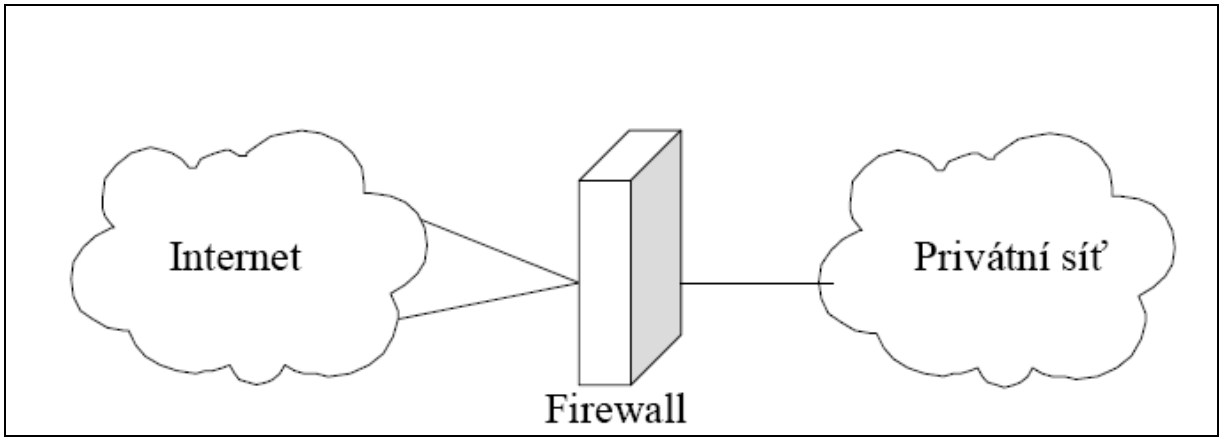
Podle ISO/OSI je vždy možno komunikovat pouze s vrstvou nad nebo pod. A všechny vrstvy musí být v komunikaci obsaženy, což v řadě praktických úloh přináší zbytečnou zátěž. Přesto je ISO/OSI model dobrý pro výklad a teoretický popis sítí. [16]

TCP/IP pochází ze zkratky anglického Transmission Control Protocol/Internet Protocol. Referenční model TCP/IP je pojmenován podle nejpoužívanějších internetových protokolů, jimiž jsou TCP/IP.

Referenční model TCP/IP se skládá ze čtyř vrstev, a to vrstvy síťového rozhraní, internetové vrstvy, transportní vrstvy a aplikační vrstvy. Někdy je mezi fyzickou a internetovou vrstvu uváděna vrstva spojová. [16]

1.3 Funkce firewallů

Firewall je zařízení či software sloužící k „bezpečnému“ oddělení, zabezpečení a řízení komunikace mezi sítěmi s různou důvěryhodností [9]. Brání před neoprávněnými průniky do sítě a odesílání dat ze sítě bez vědomí a souhlasu uživatele.



Obrázek 1: Firewall jako kontrolní bod mezi veřejnou a privátní sítí podle [10]

Moderní firewally v dnešní době již neslouží pouze pro ochranu před únikem dat a napadením lokální sítě, ale stávají se spíše komplexními nástroji pro ochranu počítače a lokální sítě při připojení k síti. Mezi jejich funkce patří:

- **Filtrování paketů:** Firewally provádějí kontrolu na úrovni paketů protokolů TCP/IP. Odmítají pakety od neautorizovaných uživatelů a pokusy o připojení k neautorizovaným službám. Jsou založeny na znalosti z jaké adresy a portu na jakou adresu a port paket prochází. Fungují na třetí a čtvrté vrstvě modelu OSI. [3]
- **Přístupová práva:** Správce sítě může pomocí firewallu omezovat některé síťové služby, například blokování určitého obsahu na Internetu, zákaz používání chatovacích programů či třeba stahování pomocí P2P sítí, atd.
- **Intrusion detection system (IDS):** Obecně slouží jako detektory rozpoznávající napadání či pokusy o napadení koncových stanic. Součástí služby jsou zpravidla záznamy do logovacích souborů.
- **Antivirová ochrana:** Některé firewally umožňují využití antivirových programů k nalezení a identifikaci virů. Výhoda spočívá v rychlosti a centralizaci takového řešení v síti.
- **Překládání síťových adres (NAT):** Překládá IP adresy hostů v interní síti a odstiňuje a skrývá je tak před monitorováním zvenčí. Vytváří tak účinnou bariéru mezi jednotlivými sítěmi. Používá se také při řešení problému s přiřazováním jedinečných IP adres, proto firewall může všechny IP adresy před bránou pomocí maškarády zaonačit tak, že si vystačí firma s jednou jedinečnou IP adresou, která je poskytovatelem přidělena. [12]
- **Šifrovaná autentizace:** Povoluje vstup do interní sítě na základě autentizace uživatelů webových stránek vztahujících se k určité kategorii.

1.3.1 Omezení firewallu

Jak již bylo uvedeno v úvodu této kapitoly, firewall není schopen sám o sobě ochránit počítačovou síť před útokem. Má samozřejmě svá omezení. Mezi nejdůležitější patří:

- Firewall nemůže poskytnout ochranu proti útokům, které nejsou směrovány přes něj samotný.
- Firewall odráží celkovou úroveň zabezpečení sítě. Pokud je architektura sítě závislá pouze na jednom bezpečnostním mechanismu, je zde riziko jeho selhání a proniknutí útočníka zvenčí.
- Pokud je firewall špatně nakonfigurován, není schopen plnit svou funkci. Konfigurace je v rukou školených administrátorů, kteří využívají svých zkušeností k minimalizaci rizika napadení sítě.
- Pokud útočník použije maškarády jako důvěryhodný uživatel nebo zaměstnanec, je pro firewall takový útok velmi těžko identifikovatelný.
- Firewally nešifrují emaily ani důvěrné dokumenty, které jsou posílány uvnitř nebo mimo organizaci.
- Firewall nemůže zaručit 100% ochranu pro systém nebo organizaci.
- Firewall neumí najít další slabá místa, která umožňují případnému útočníkovi prolomení do vnitřní sítě.

1.4 Typy firewallů

Jednotlivé typy firewallů vycházejí z jejich historického vývoje. V této podkapitole budou postupně popsány principy jejich fungování a případně jejich modifikace.

1.4.1 Paketový filtr

Je nejjednodušší a nejstarší typ firewallu, kde jsou pakety řízeny pravidly, která uvádějí, z jaké IP adresy a portu na jakou IP adresu a port může být doručen procházející paket. Tyto informace jsou získány z hlaviček paketů. Paketový filtr pracuje na síťové vrstvě ISO/OSI modelu. Nejčastější použití slouží k omezení komunikace. Typickou bezpečnostní politikou je povolení webu a e-mailové komunikace, především těchto vzdálených portů:

- 80 (HTTP tedy nešifrovaný web)
- 443 (HTTPS tedy šifrovaný web)
- 25 (SMTP tedy nešifrované odesílání pošty)
- 465 (SMTP-SSL tedy šifrované odesílání pošty)
- 110 (POP3 tedy nešifrované přijímání pošty)
- 995 (POP3-SSL tedy šifrované přijímání pošty)

Tyto čistě paketové filtry jsou účinné pouze při omezování komunikací, které musí mít pevný vzdálený port. Např. www servery komunikují obvykle na portu 80, a lze tedy velmi snadno zakázat web v interní síti. Problematické je ovšem blokování decentralizované komunikace typicky P2P sítí, kdy vysílač není nadřazen přijímači a obecně přijímač je zároveň vysílačem.

1.4.1.1 *Výhody paketového filtru*

Řešení firewallu jako paketového filtru se vyznačuje jednoduchostí a transparentností, což se projevuje vysokou rychlostí. Z toho důvodu je toto řešení hojně využíváno v místech, kde není potřeba důkladnější analýza toku dat.

1.4.1.2 *Nevýhody paketového filtru*

Nevýhodou je nízká úroveň kontroly procházejícího spojení. To je způsobeno schopností sledovat pouze jednotlivé pakety bez možnosti hledání závislostí mezi nimi.

1.4.2 Stavové paketové filtry

Stavové paketové filtry umožňují totéž jako paketové filtry a navíc umožňují ukládání informací o povolených spojeních, která lze používat při rozhodování o budoucnosti paketů. Tato informace urychluje funkci firewallu, protože u vytvořených spojení již není nutné ověřovat pakety. Dále dochází ke zvýšení bezpečnosti, jelikož lze nastavit, která strana může otevřít spojení, a firewall bude povolovat i pakety jdoucí z druhé strany jako odpovědi na požadavky.

Spojení je ve stavové tabulce udržováno buď do jeho ukončení (obě strany pošlou postupně pakety), nebo do doby tzv. time-out. K time-outu dojde, pokud není určitou (na firewallu definovanou) dobu spojení používáno – tedy pokud po danou dobu nepřijde na rozhraní firewallu žádný paket souhlasící s tímto řádkem v tabulce stavů. [10]

1.4.2.1 *Výhody stavových paketových filtrů*

Mezi výhody patří stejně jako u paketových filtrů vysoká rychlost zpracování požadavků a současně lepší možnost zabezpečení než u paketových filtrů. Další výhodou je jednoduchá konfigurace minimalizující škody způsobené například překrýváním některých pravidel.

1.4.2.2 *Nevýhody stavových paketových filtrů*

Nevýhodou je nižší úroveň zabezpečení oproti aplikační proxy.

1.4.3 Aplikační proxy

Aplikační brána (proxy firewall, proxy server, aplikační proxy) je ochrana na aplikační vrstvě modelu ISO/OSI. Zde dochází k úplnému oddělení sítí.

1.4.3.1 *Netransparentní proxy*

Spojení probíhá tak, že klient pošle proxy serveru požadavek na otevření spojení s nějakou službou v jiné síti a aplikační brána toto spojení otevře. Uživatel se pak nepřipojuje přímo na službu, kterou požaduje (např. na web-server 146.102.16.4), ale připojí se na web-server běžící na tomto firewallu. (Samotný firewall je pro uživatele serverem spuštěný program, na který se připojuje pro získání dat). Následně web-server na firewallu předá požadavek klientovi (webovému prohlížeči na firewallu) a ten si vyžádá požadovanou stránku ze serveru 146.102.16.4. Po té ji předá web serveru běžícímu na firewallu a ten ji poskytne uživateli jako jakýkoliv jiný web-server [10].

Všechna data jdou vždy přes proxy server, který rozhodne o jejich osudu. Jinými slovy, proxy server slouží jako prostředník mezi klientem v jedné síti a službou v síti druhé. Vedlejším efektem tohoto způsobu komunikace je skrytí zdrojové adresy klienta, protože jako klient vždy slouží aplikační brána.

1.4.3.2 *Transparentní proxy*

Zde je nutné uvést, že existuje ještě koncept, kdy firewall nenavazuje spojení přímo. V literatuře je tato konfigurace označována jako transparentní proxy. Klient navazuje spojení přímo se serverem, ale proxy zasahuje do všech paketů. Kromě standardního filtrování povolit zamítnout zahodit mění i jejich obsah, a to obvykle bez možnosti zjištění klientem. Nejčastěji jde o využití ve formě cache, kdy má proxy danou stránku uloženu, dál IP paket nepustí, a jménem dotazovaného serveru vytvoří odpověď, jako by přišla přímo ze serveru.

Transparentní proxy bývají často kritizovány za zasahování do obsahu paketů, kterému nemůže klient ani (webový) server nijak zabránit. Většinou ho nemůže ani detekovat.

1.4.3.3 *Výhody aplikační proxy*

Obecně výhoda řešení firewallu pomocí aplikační proxy představuje možnost kontroly obsahu přenášených paketů (např. antivirová kontrola, filtrování nevhodného obsahu), autentizaci uživatelů, možnost skrytí zdrojové adresy klienta.

1.4.3.4 *Nevýhody aplikační proxy*

Proti tomuto řešení hovoří především vyšší hardwarové nároky zejména na CPU a netransparentnost, kdy musí každá aplikace podporovat připojení pomocí proxy, a tyto aplikace musí být správně nastaveny.

1.4.4 Firewall jako součást operačního systému

Základem pro firewall je právě samotný operační systém (OS), který běží na standardním počítači. Operační systém není výhradně zaměstnán firewallovou aplikací a nadále poskytuje veškeré ostatní funkce. Použitým operačním systémem může být některý z operačních systémů, jako jsou Microsoft Windows, Linux, nebo Solaris. Software firewallu je součástí operačního systému, tak aby OS byl schopen provádět běžné operace pro jiné systémy nebo uživatele.

1.4.4.1 *Výhody firewallu jako součást OS*

Toto řešení má své výhody. Zařízení není využíváno pouze za jedním účelem. Mohou být nainstalovány aplikace třetích stran. Tedy aplikace vytvořené za účelem spolupráce s operačním systémem. Díky silné systémové podpoře umožňuje využívat další pokročilé funkce. Například je-li třeba přidat do zařízení nové rozhraní, lze jednoduše hardware upgradovat a firewallovou aplikaci přeinstalovat, takže dojde k upgradu celého systému.

1.4.4.2 *Nevýhody firewallu jako součást OS*

Bohužel současné komerční i volně distribuovatelné operační systémy, jako jsou například MS Windows XP, Microsoft Windows 2003 Server i různé distribuce operačního systému Linux, trpí skrytými vadami (chyby v kódu). Pokud se skrytá vada odhalí, vývojáři (výrobci) na to reagují vydáváním aktualizačních balíčků. Tvorba aktualizačního balíčku však zabere určitý čas, řádově dny. Tato skutečnost vytváří velké riziko napadení určitých funkcí operačního systému. Jádro operačního systému není v tomto případě firewallem.

Samotný software realizující firewall je automaticky spouštěn jako uživatelská aplikace po startu operačního systému.

1.4.5 Firewall – samostatné zařízení

Zde je firewall fyzicky samostatné zařízení, které má za úkol posílat pakety mezi sítěmi jak je to nejrychleji možné a ještě je kontrolovat v závislosti na zvolené bezpečnostní politice. V tomto případě není operační systém využit pro nic jiného než běh firewallové aplikace. Hardware takovéhoto zařízení je specializován na pouze jednu aplikaci a zahrnuje v sobě procesor, paměť a flash paměť pro ukládání dat.

1.4.5.1 *Výhody firewallu jako samostatného zařízení*

Tyto firewally používají specifický typ hardwaru, který zajišťuje vyšší stabilitu, propustnost a celkovou účinnost takového zařízení. Tyto firewally jsou tvořeny několika vrstvami kontroly. První vrstvou je vrstva hardwarová programovatelných hradlových polí. Druhou vrstvou je vrstva zákaznických obvodů tzv. ASIC obvodů, které umožní aplikaci uživatelsky zvolených filtrů (pravidel firewallu). Třetí vrstvou, která rozhoduje, pokud nejsou schopny rozhodnout první ani druhá vrstva, je vrstva specifického operačního systému firewallu (firmware). Až ve třetí vrstvě je nucen se do rozhodování o spojení nebo jiné události zapojit procesor.

1.4.5.2 *Nevýhody firewallu jako samostatného zařízení*

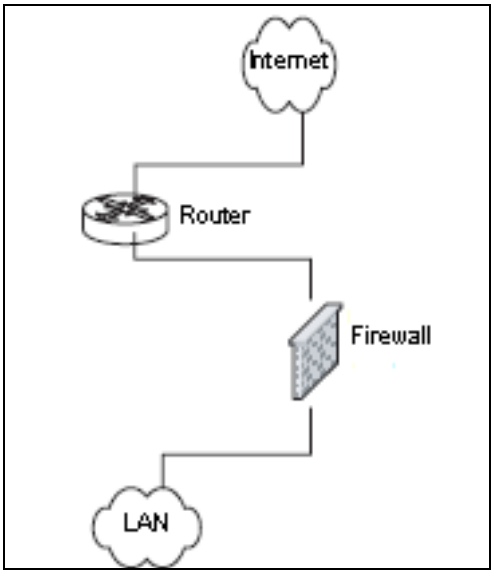
K nevýhodám těchto firewallů patří nemožnost instalace aplikací třetích stran a dále řada specifických limitací, jako omezená paměť nebo počet fyzických rozhraní. Pokud je třeba firewall upgradovat, je většinou nutné vyměnit celé zařízení. Mezi další nevýhody lze zařadit i vyšší finanční nároky na pořízení takového zařízení, které se mohou pohybovat řádově ve statisících i miliónech korun.

1.5 Umístění firewallu v síti

Nehledě na zvolený typ firewallu je další klíčovou otázkou především umístění samotného zařízení. To znamená, kde nejefektivněji umístit firewall a maximalizovat tak jeho účinnost. V literatuře např. [3,6] je ukázána celá řada možností. Zde budou nastíněny pouze čtyři základní varianty.

1.5.1 Model sítě s jedním firewallem

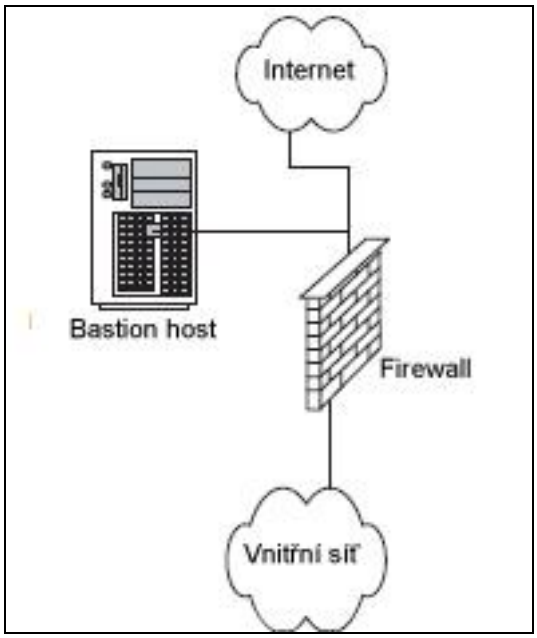
Na obrázku 2 je znázorněna základní konfigurace, která se používá především u sítí s jednoduchou topologií, a kde organizace neposkytuje služby mimo interní síť. Typické uplatnění tohoto modelu je u malých firem, případně pro podsítě, které musí být odděleny od hlavní sítě. Může se jednat například o mzdové nebo vývojové oddělení.



Obrázek 2: Ochrana vnitřní sítě jedním firewallem podle [9]

1.5.2 Model sítě s jedním firewallem a bastion host

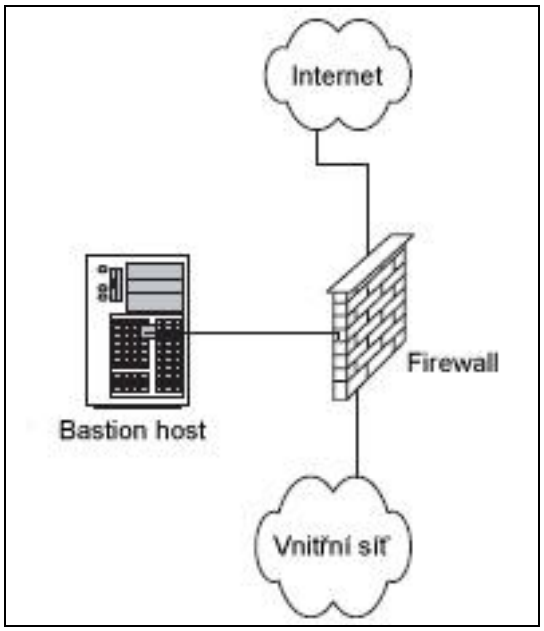
Obrázek 3 znázorňuje situaci, která umožňuje implementaci a zajištění služeb vně chráněné sítě. V tomto modelu jsou nastavena pravidla na firewallu tak, aby nedovolovala přístup z Internetu do vnitřní sítě. Pouze minimální a absolutně nezbytné množství služeb bude instalováno na počítači mající roli bastion host. Nasazení tohoto modelu je vhodné tam, kde je poskytována webová prezentace nezahrnující e-komerci vyžadující dynamické aktualizace obsahu stránek. Naopak tato architektura není vhodná pro VPN sítě, FTP služby vyžadující časté navazování spojení.



Obrázek 3: Ochrana sítě pomocí jednoho firewallu a bastion host podle [9]

1.5.3 Model sítě s jedním firewallem a demilitarizovanou zónou

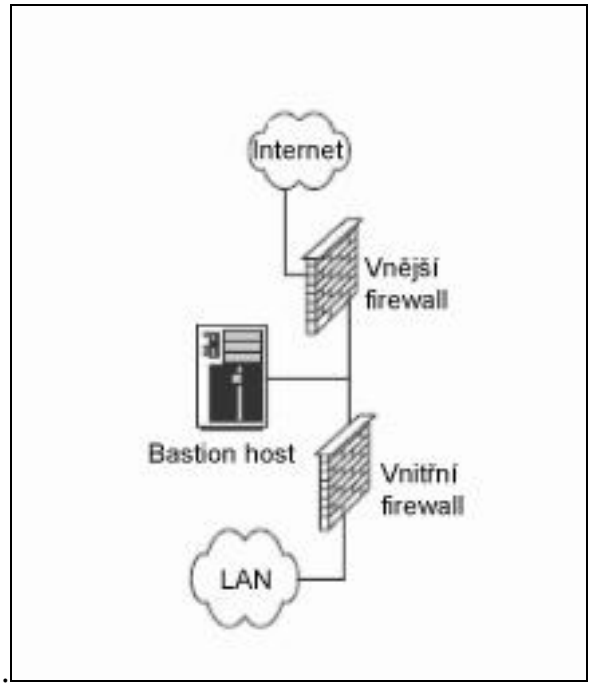
Na obrázku 4 je ukázána základní struktura řešení s demilitarizovanou zónou (DMZ). V této architektuře je bastion host částečně chráněna firewallem. Toto uspořádání umožňuje nastavit bastion host na viz obrázek 2, tak aby propouštěla veškerá odchozí spojení, zatímco firewall může být nakonfigurován tak, aby propustil síťový provoz pouze na portu 80 příchozím spojení do bastion host. To vše za předpokladu, že jde o Web server nebo jiné potřebné spojení z vnější sítě. Je zde umožněno spojení z interní sítě do bastion host, pokud je to nezbytně nutné. V tomto konceptu je potenciálně počítáno s možností aktualizace Web serveru, pokud je to povoleno v pravidlech na firewallu. Ten může propustit data z a do bastion host pro vybrané porty, jejich specifikace záleží na konkrétním nastavení.



Obrázek 4: Ochrana sítě s využitím DMZ podle [9]

1.5.4 Model sítě se dvěma firewally a DMZ

Obrázek 5 představuje situaci obecně použitelné dvojité DMZ konfigurace. V tomto uspořádání může být bastion host chráněna zvenčí a umožňovat spojení do nebo z vnitřní sítě. Datový provoz může být kontrolován ve vnitřní i vnější síti i mimo DMZ. Tato konfigurace je využívána pokud je třeba v síti umístit více než jednu bastion host pro služby a operace, které má organizace poskytovat.

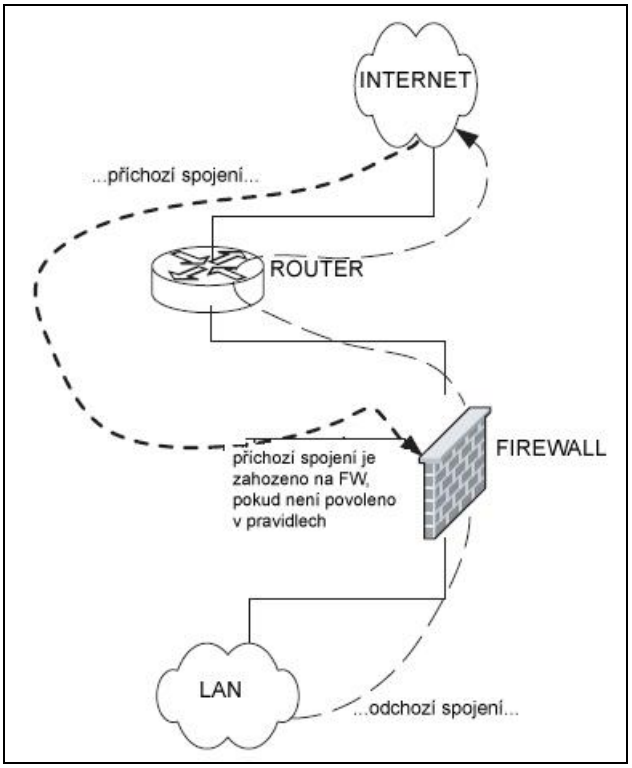


Obrázek 5: Ochrana sítě pomocí dvou firewallů podle[9]

1.6 Datový provoz

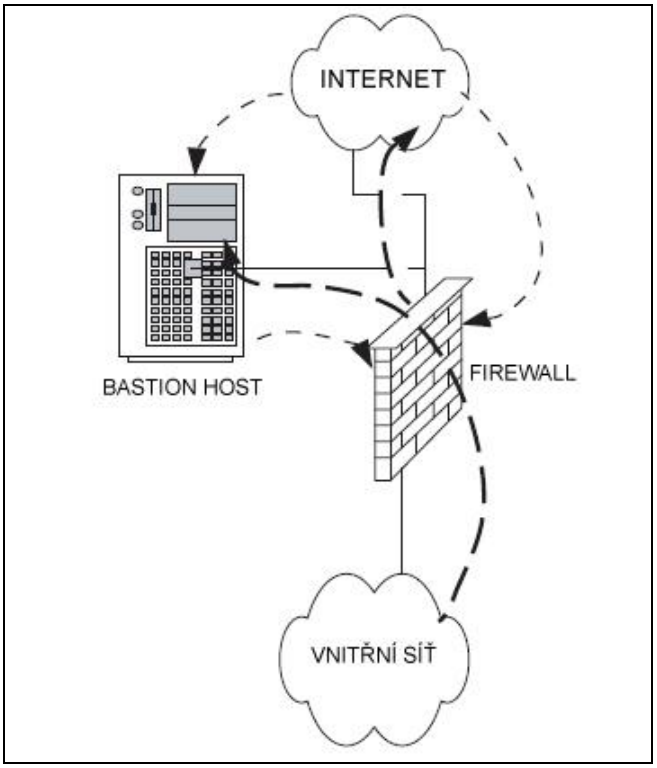
Po předchozím seznámení s možnostmi umístění firewallu v počítačové síti se v této kapitole zaměříme na to, jak v daných modelech probíhá datový provoz.

Na obrázku 6 je znázorněn datový provoz přes základní jednoduchý firewall. Tento druh síťové kontroly může být zajišťován hardwarovým nebo softwarovým firewallem. Datový provoz je v tomto případě neomezený pro odchozí spojení, ale základní konfigurace zahodí veškerá příchozí spojení, která nepocházejí z interní sítě.



Obrázek 6: Datový provoz v síti s jedním firewallem podle [10]

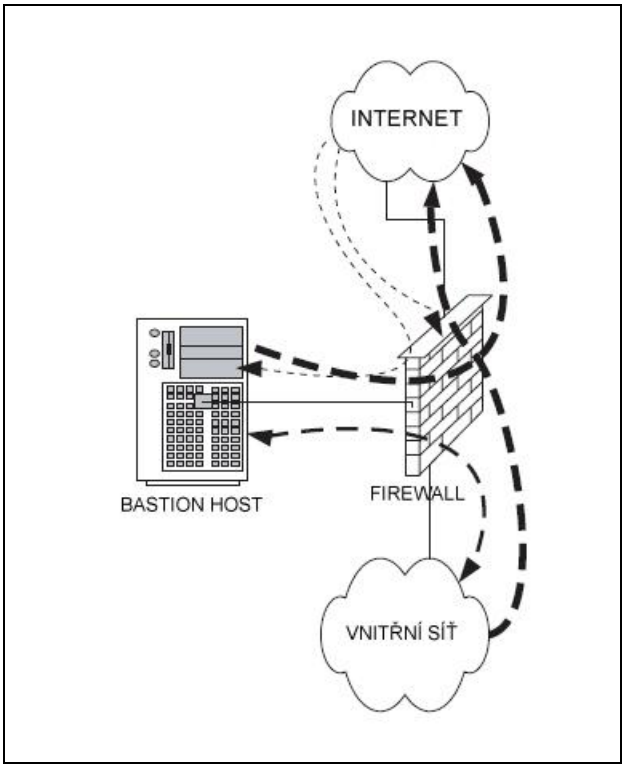
Na obrázku 7 je ukázána situace v síti obsahující bastion host a firewall. Tato koncepce netvoří DMZ, ochrana bastion host je konfigurována individuálně a vyžaduje velkou péči při nastavení. Příchozí spojení z Internetu nebo z bastion host je zahozeno již na firewallu, to poskytuje ochranu vnitřní síti. Odchozí spojení z interní sítě jsou povolena.



Obrázek 7: Datový provoz v síti s jedním firewallem a bastion host podle[10]

Obrázek 8 představuje model, kdy je implementována demilitarizovaná zóna. Zde jde datový provoz přes bastion host a v případě, že je to povoleno tak i přes firewall. Data jsou zahozena, pokud jsou směřována do vnitřní sítě.

Dvousměrný provoz je povolen a specifikován mezi vnitřní sítí a bastion host, odchozí spojení z vnitřní sítě jde přes firewall ven, většinou bez omezení.

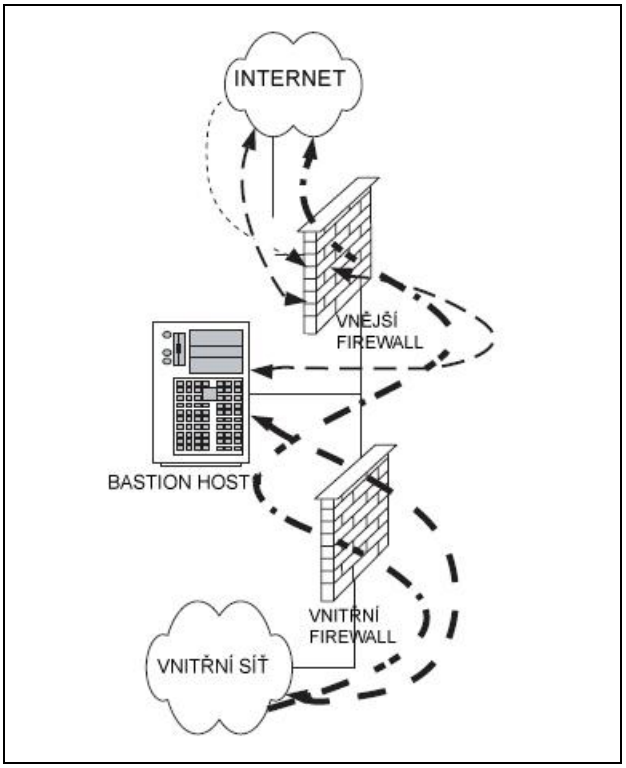


Obrázek 8: Datový provoz v síti s jedním firewallem a DMZ podle [10]

Obrázek 9 obsahuje komplexnější cestu datového provozu a zároveň představuje největší možnosti pro konfiguraci a opatření vzhledem ke službám poskytovaných vně organizace. V tomto případě zde existuje skutečná DMZ, která je samostatná a chráněná od obou sítí, vnější i vnitřní.

Tento typ konfigurace je používán velmi často, když je třeba poskytovat více než jednu službu veřejně, například Web server, DNS a jiné. Datový tok do bastion může být povolen nebo zakázán podle potřeby z vnější i vnitřní sítě. Příchozí provoz do vnitřní sítě může být zahozen na externím firewallu. Odchozí provoz z vnitřní sítě může být povolen nebo omezen pouze na bastion host (DMZ síť) nebo do externí sítě.

Jak je patrné, tento model poskytuje vysokou flexibilitu a funkčnost při ochraně celého systému.



Obrázek 9: Datový provoz v síti s dvěma firewally a DMZ podle [10]

2 Síťová bezpečnost

Pojem síťová bezpečnost nelze zaměňovat s pojmem počítačová bezpečnost. Síťová bezpečnost představuje ochranu počítačových sítí a jejich služeb od nepovolených změn, průniků a destrukce. Síťová infrastruktura je dnes strategická veličina, která spojuje lidi, kontinenty a organizace.

2.1 Bezpečnostní principy

V praxi se používá několik vzájemně provázaných procedur a principů, které umožňují běžný chod organizace, a zároveň zajišťují dodržování pravidel pro ochranu dat. Správci sítí a podnikových systémů mají za úkol zajistit co možná nejlepší přístup k datům a jejich integritu. Jsou však konfrontováni s určitými omezeními. Mezi tato omezení můžeme zařadit rozpočet organizace, fyzické možnosti zařízení, schopnosti uživatelů dodržovat zásady bezpečnosti, apod. Z těchto důvodů organizace přijímají v rámci svých bezpečnostních politik opatření, která napomáhají uchránit jejich data před zneužitím. K základním bezpečnostním principům patří:

2.1.1 Princip (AAA) Autentizace, Autorizace a Audit

Autentizace (authentication) – znamená potvrzení, že uživatel požadující přístup na síťový prvek je platným uživatelem tohoto prvku. Autentizace je dosaženo pomocí představení jeho identity a hesla. **Autorizace** (autorization) - znamená udělení specifického typu služby uživateli na základě jeho autentizace. Autorizace může být konkrétně založena na omezeních, například omezení provádět určité příkazy nebo přechod do privilegovaného režimu. **Účtování** (accounting, auditing) - znamená sledování využívání síťových služeb uživateli. Tyto informace mohou být použity pro správu, plánování, účtování, nebo další účely[9].

2.1.2 Princip (CIA) Důvěrnost, integrita a dostupnost dat

V anglické literatuře např. [6,7] lze tento princip nalézt pod zkratkou CIA (Confidentiality, Integrity and Availability). CIA představuje soubor činností zajišťující ochranu před neoprávněným nahlížením, zničením či modifikací dat a zaručující jejich stálou přístupnost. V několika posledních letech došlo k rozšíření tohoto principu o definování

bezpečnostních rizik a metod řízení rizik tak, aby poskytoval komplexní metodologii ochrany dat.

2.1.3 Princip minimálních oprávnění (least privilege)

Vyjadřuje požadavek, aby všichni uživatelé měli v každém okamžiku pouze minimální množství oprávnění pro přístup k informacím a zdrojům, které stačí právě k tomu, aby mohli provádět činnosti vyplývající z jejich pracovní pozice. Z bezpečnostního hlediska se vždy preferuje přísnější restriktivní politika s možností uvolnění nastavených pravidel.

2.2 Ochrana Informací

Síťová bezpečnost úzce souvisí s ochranou informací. Ochrana informací představuje skutečnost, že pouze autorizovaní lidé a systémy mají přístup k určitým informacím. Experti na ochranu informací mají rozdílný pohled na definici samotné ochrany informací. Mezi základní oblasti však patří:

Důvěrnost/utajení dat - zajišťující, že pouze autorizované subjekty mají přístup k informacím. Zde jsou využívány metody šifrování. Dále autentizace a autorizace, které budou popsány níže.

Integrita dat – zajišťující to, že informace nejsou modifikovány neautorizovanými subjekty či nesprávně modifikovány subjekty autorizovanými. K ověření jsou využívány kontrolní součty a hashovací funkce.

Dostupnost dat - zaručuje, že informace jsou přístupné v momentě, kdy je třeba. Kromě zálohování dat dostupnost dále zahrnuje, že systém zůstane přístupný v případě útoku nebo že důležitá data budou chráněna před smazáním.

Autentizace - proces, který potvrzuje, že uživatelé jsou opravdu ti, za které se vydávají. Dlouhodobě se využívají především hesla k autentizaci uživatelů, ale i další metody jako šifrované tokeny a biometrika.

Autorizace /kontrola přístupu – zajišťuje, že pokud je uživatel jednou autentizován, má výhradně přístup k informacím, ke kterým mu byl udělen přístup od jejich vlastníka. Zajištění může být na úrovni operačního systému za použití systému přístupu k souborům.

Další možností je využití omezení přístupu na úrovni síťových zařízení jako jsou routery a firewally.

Ověření způsobilosti – ověření, že aktivity a transakce v systému nebo na síti mohou být monitorovány a zaznamenávány. Dále je zde zahrnuta možnost rozpoznání neautorizovaného použití systému. Tento proces může mít rozličné formy: logování operačním systémem, logování síťovými zařízeními, logování pomocí IDS.

Princip nepopiratelnosti - *nonrepudiation* - zabraňuje tomu, aby odesílatel nebo příjemce popřeli zprávu. Jedná se o proces, který zaručuje, že osoba, která inicializuje spojení je dostatečně autentifikována a druhá strana nemůže popřít, že byla součástí transakce. Využíváno je zde kryptografie s veřejným klíčem.

2.3 Síťová bezpečnost a Internet

Komunita uživatelů Internetu byla v osmdesátých letech minulého století poměrně malá a sestávala se většinou z odborníků působících na akademické půdě. Hlavním smyslem propojování sítí bylo sdílení informací, a protože skupina uživatelů byla úzce provázaná, nebyl otázce síťové bezpečnosti přikládán velký význam. Technologie jako operační systém UNIX a protokol TCP/IP byly navrhnuty pro toto akademické prostředí a tomu odpovídalo i jejich zabezpečení.

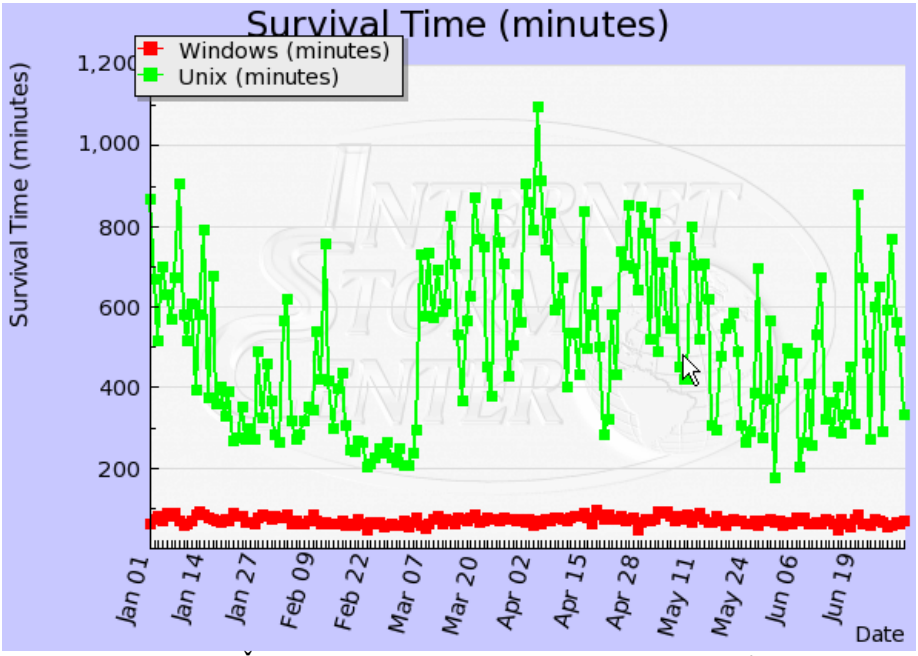
V raných devadesátých letech vzrostl zájem o komerční využití Internetu. Pohled na bezpečnost při využití Internetu v komerční sféře byl však diametrálně odlišný od akademického pojetí. UNIX, TCP/IP a připojení k Internetu se staly předmětem útoků a nebyly schopny uplatnit a zajistit základní principy ochrany informací jako důvěrnost, integrity a dostupnost dat. S růstem komerčního využití Internetu rostl počet připojených společností a byl tak umožněn i vznik obchodních modelů podnikajících přímo na Internetu. Potřeba ochrany dat a síťové bezpečnosti se stala velmi aktuální.

V době, kdy Internet představoval propojení sítí především mezi organizacemi, nebezpečí útoku hrozilo především uvnitř organizace. Tyto interní útoky byly většinou dílem nespokojených zaměstnanců s odpovídajícími právy a mohly mít nemalé následky. Vnější

útoky se vyskytovaly poměrně vzácně vzhledem k omezenému počtu soukromých připojení a nutných znalostí z oblasti informatiky.

S postupem času však nebezpečí externích útoků vzrostlo. V současnosti je k Internetu připojeno na miliony serverů a stanic, které jsou potencionálními cíly pro útočníky. Základna útočníků se s léty rozrostla společně se sdílením informací jak prolomit systém ať už jen pro zábavu či pro zisk.

Můžeme demonstrovat na příkladu ze statistiky, jak moc je Internet „bezpečný“. Časy, kdy bylo možné ponechat v Internetu „nezáplatovaný“ počítač bez dozoru i po několik měsíců, aniž by doznal závažnější újmy, jsou nenávratně pryč. S masivním rozšířením automaticky se propagujících červů je současná životnost implicitních instalací běžných operačních systémů (Windows, Linux) velmi nízká, u některých se pohybuje pouze v desítkách minut, podle [23]. Následující obrázek 10 ukazuje statistiku životnosti operačních systémů v minutách (osa y), přičemž se jedná údaje za první pololetí 2009.



Obrázek 10:Životnost defaultních instalací operačních systémů [23]

2.4 Útoky na počítačové sítě

Přenos dat v síti může být předmětem různých typů útoků. Základem jakékoli obrany musí být i jejich důkladná znalost. Útoky na síť můžeme obecně rozdělit do dvou skupin na útoky strukturované a nestrukturované.

2.4.1 Nestrukturované útoky

Původci nestrukturovaných útoků jsou většinou lidé, kteří mají jen základní vědomosti o programování, systémech obecně. Charakteristickým znakem také je, že nemají příliš trpělivosti při svém počínání. V anglické literatuře se pro tyto hackery používá pojem *script kiddies* [7]. Script kiddies mají sklon pronikat do systémů především proto, aby sklidili obdiv před svou hackerskou komunitou. Využívají přitom hlavně programové prostředky vytvořené zkušenějšími uživateli. Často ani příliš nezkoumají slabá místa systémů. Pokud jejich útok selže, většinou si vyhlédnou další cíl a pokračují ve své činnosti jinde.

Případné nebezpečí spočívá v tom, že tito útočníci využívají hackerské programy bez dostatečných znalostí, a útočí na prostředí, o jehož struktuře často nemají představu. Kombinace těchto faktorů představuje pro podnikovou síť hrozbu ve formě ztráty dat nebo přerušení spojení. Tyto útoky jsou většinou odhalitelné pomocí běžných bezpečnostních nástrojů.

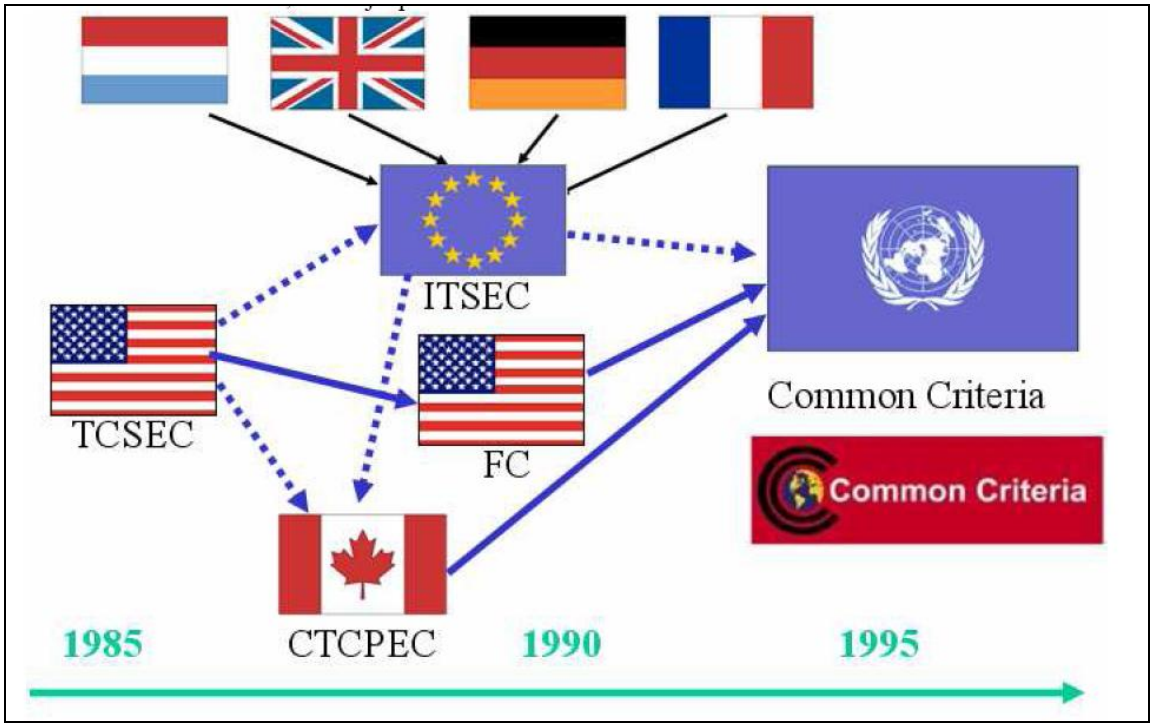
2.4.2 Strukturované útoky

Strukturované útoky jsou daleko větší hrozbou, protože jsou prováděny již hackery se značnými schopnostmi a znalostmi z oblasti informatiky. Pokud již existující nástroj pro prolomení sytému není dost vhodný pro jejich záměr, upraví ho, nebo napíší svůj vlastní skript. Jsou schopni vykonat komplexní proces akcí, kterým objeví slabé místo v systému. Tito hackeři často využívají takzvaných *zero-days exploits* – to znamená, že využijí bezpečnostní díry v systému, který byl právě vydán, nebo na jehož slabé místo ještě nebyla vydána záplata. Motivace těchto útočníků je většinou jiná než pouhé zviditelnění se. Může jít o krádež zdrojového kódu, čísla kreditní karty pro nákupy nebo podvody, pomsta, zničení nebo přerušení spojení. Zabránit těmto útokům lze velmi těžko použitím tradičních zabezpečovacích technik, jako jsou pravidla na firewallech nebo detekování pomocí IDS. Pro tento typ útoků může být použito i jiné metody, například sociální inženýrství.

3 Kritéria hodnocení informační bezpečnosti

V průběhu pouhých čtyřiceti let začala hrát informační technologie důležitou a často rozhodující roli téměř ve všech oblastech organizované společnosti. Uživatelé systémů potřebují věřit, že systémy, které používají, jsou bezpečné. Potřebují mít také měřítka pro porovnání bezpečnostních vlastností produktů či systémů, které chtějí používat. V této oblasti stejně jako v IT dochází k vývoji a změnám standardů informační bezpečnosti.

Za základ pro všechny následující standardy jsou považována americká kritéria Trusted Computer System Evaluation (TSEC), známá pod názvy TSCEC nebo „Orange Book“, vydaná a užívaná pro hodnocení informačních systémů Ministerstva obrany USA. Dále následovaly národní varianty standardů. V Evropě se jimi staly Information Technology Security Criteria (ITSEC) a v Kanadě CTCPEC (Canadian Trusted Computer Product Eval. Criteria). V roce 2000 se pak 6 států dohodlo a ustanovilo jednotný standard ISO/IEC 15408, známý pod názvem Common Criteria. Vývoj kritérií je znázorněn na obrázku 11.



Obrázek 11 Vývoj kritérií hodnocení informační bezpečnosti [17]

3.1 TSEC (Trusted Computer System Evaluation Criteria)

Americká kritéria TSEC jsou široce známým a akceptovaným základem pro hodnocení zabezpečení informačního systémů. Jejich hlavním cílem bylo ošetřit bezpečnost operačního systému, až později vyšly dodatky specifikující i jiné aplikace. V této diplomové práci se o těchto kritériích zmíníme jen velice stručně, hlavní těžiště této práce je zaměřeno na Commnon Criteria a jejich využití v praxi.

3.1.1 Struktura TSEC

TSEC definuje sedm skupin hodnotících kritérií. Tvoří je třídy D, C1, C2, B1, B2, B3 a A1, které jsou sdruženy do čtyř skupin D, C, B a A. Každá třída pokrývá čtyři aspekty hodnocení podle [18]:

- Bezpečnostní politiku
- Účtovatelnost
- Míru záruky
- Dokumentaci

Kritéria odpovídají těmto čtyřem oblastem. Třídy jsou seřazeny podle hierarchie, kde D je nejnižší a A1 nejvyšší třída. Každá třída pokrývá požadavky jak na funkčnost, tak na důvěrnost. Skupiny B a C se pak dále dělí na několik tříd, které dále specifikují požadavky na zařazení do vždy vyšší bezpečnostní skupiny.

3.2 Common Criteria

Jedná se o nejnovější standard pro hodnocení bezpečnosti informačních systémů. V současné době je k dispozici verze 3.1 vydaná v září 2006. Na jejich tvorbě se podílí 11 zemí a dalších 12 zemí Common Criteria (CC) využívá. V září 2004 se připojila i Česká republika a česká verze CC má název ČSN ISO/IEC 15408. V České republice jsou známy také pod pojmem Společná kritéria pro hodnocení bezpečnosti IT. K následujícímu textu bylo využito zdrojů [19, 20, 21].

3.2.1 Struktura Common Criterií

- Úvod a všeobecný model
- Bezpečnostní funkční požadavky
- Požadavky na záruku bezpečnosti

3.2.2 Profily ochrany a cíle bezpečnosti

Společná kritéria definují společnou množinu možných bezpečnostních požadavků rozdělených do dvou skupin: funkční požadavky a požadavky na záruku. Společná kritéria rovněž definují dva druhy dokumentů, které mohou být vytvořeny při použití této společné množiny:

- Profily ochrany (PP, Protection profile) – jsou dokumenty vytvářené uživateli nebo uživatelskými komunitami a identifikují uživatelské požadavky na bezpečnost [19].
- Cíl bezpečnosti (ST, Security target) – jsou dokumenty, typicky vytvářené vývojáři systémů, které identifikují bezpečnostní způsobilost daného produktu. ST může prohlašovat, že realizuje žádný nebo více PP [19].

Následující kapitoly se budou věnovat obecné struktuře profilu ochrany a posléze již konkrétnímu profilu ochrany určenému pro firewally.

3.3 Profil ochrany

Profil ochrany (PP) obsahuje množinu bezpečnostních požadavků vybraných ze společných kriterií. Profil ochrany povoluje nezávislé vyjádření bezpečnostních požadavků pro množinu cílů hodnocení Target of Evaluation (TOE), které budou plně v souladu s množinou bezpečnostních cílů. PP má být opakovaně použitelný a má vymezit požadavky TOE, které jsou známé jako užitečné a efektivní při naplňovaní identifikovaných cílů. PP také obsahuje zdůvodnění bezpečnostních cílů a požadavků.

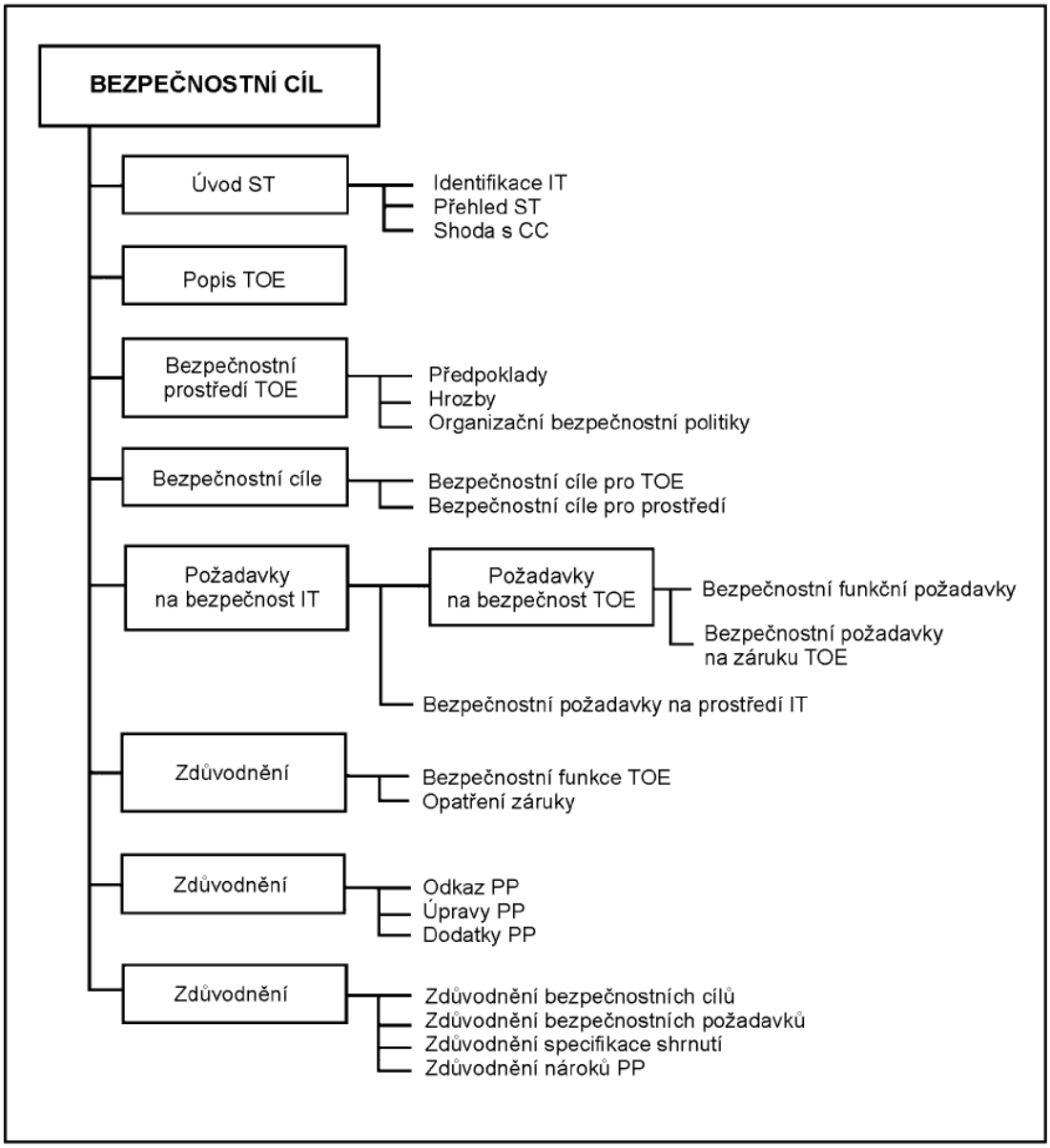
3.3.1 Popis částí Profilu ochrany

Popis TOE

Tato část PP musí popsat TOE tak, aby pomohla porozumět jeho bezpečnostním požadavkům, a musí se zabývat typem produktu a obecnými IT charakteristikami TOE.

Pokud je předmětem hodnocení produkt nebo systém, jehož primární funkcí je bezpečnost, může být tato část profilu ochrany použita k popisu celého systému, jehož bude TOE součástí.

Strukturu jednotlivých částí profilu ochrany ukazuje následující obrázek 12



Obrázek 12: Obecná struktura Profilu ochrany [19]

Bezpečnostní prostředí TOE

Prohlášení o bezpečnostním prostředí TOE musí popisovat bezpečnostní prostředí, ve kterém má být TOE používán. Dále způsob, jakým se očekává, že bude využit. Toto prohlášení musí obsahovat následující informace:

a) **Popis předpokladů** musí popisovat bezpečnostní aspekty prostředí, v kterém bude TOE použit nebo ve kterém je jeho použití zamýšleno.

b) **Popis hrozeb** musí obsahovat všechny hrozby, proti kterým se vyžaduje specifická ochrana v rámci TOE nebo jeho prostředí. Nemusí být uvedeny všechny hrozby, které se mohou vyskytnout v daném prostředí, ale pouze ty, které jsou nutné k bezpečnému provozu TOE.

c) **Popis organizačních bezpečnostních politik** musí určit a případně vysvětlit jakákoli prohlášení nebo pravidla organizační bezpečnostní politiky, s kterými musí být TOE v souladu.

Bezpečnostní cíle

Prohlášení o bezpečnostních cílech musí vymezit bezpečnostní cíle TOE a jeho prostředí. Bezpečnostní cíle by měly čelit všem identifikovaným hrozbám a pokrýt všechny organizační bezpečnostní politiky.

a) **Bezpečnostní cíle pro TOE** musí být jasně uvedeny a vysledovány zpět k aspektům identifikovaných hrozeb, kterým má TOE čelit anebo k organizačním bezpečnostním politikám, které má TOE splňovat.

b) **Bezpečnostní cíle pro prostředí** musí být jasně uvedeny a vysledovány zpět k aspektům identifikovaných hrozeb, kterým TOE není schopno plně čelit anebo k organizačním bezpečnostním politikám nebo předpokladům, které TOE plně nesplňuje.

IT bezpečnostní požadavky

Tato část PP definuje detailně IT bezpečnostní požadavky, které má TOE nebo jeho prostředí splňovat, pokud možno jako funkční komponenty odvozené z druhé části Common Critérií.

4 Profil ochrany pro firewally verze 2.0

Profil ochrany pro firewally je popsán v literatuře [20, 22], z těchto zdrojů jsem čerpal v této kapitole.

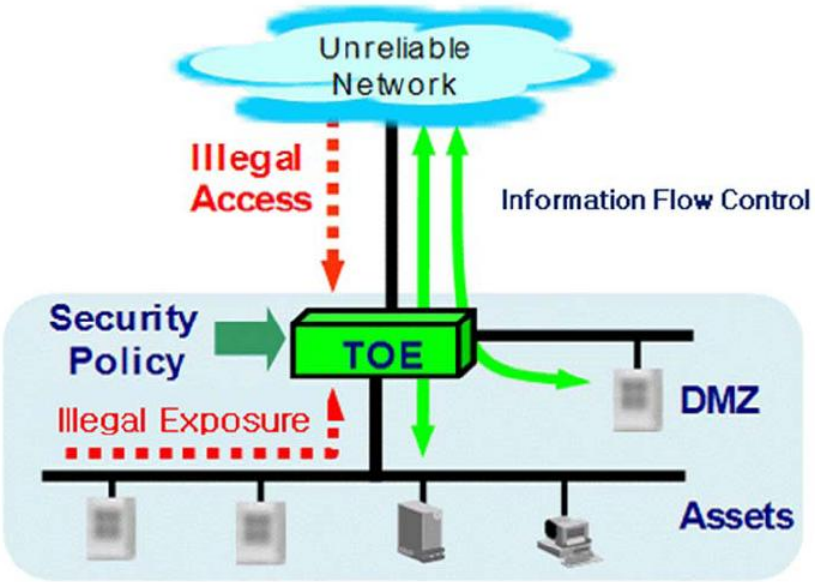
4.1 Popis TOE

Tento profil ochrany definuje bezpečnostní funkční požadavky a zabezpečovací požadavky firewallu. Firewall je zde chápán jako zařízení sloužící k ochraně vnitřních informací a síťové komunikace organizace.

Účelem firewallu je poskytovat kontrolovaný přístup k požadovaným službám v síti. Firewally mohou náležet do různých technických kategorií, například pokud jde o způsob konfigurace nebo řízení přístupu. Dále jsou zde zmiňovány různé architektury firewallů. Tento profil ochrany obsahuje bezpečností požadavky, které jsou běžně využívány bez ohledu na rozdílnou konfiguraci.

4.2 Provozní prostředí TOE

Firewall je umístěn v místě spojení a vykonávání bezpečnostních funkcí externí sítě, jako například Internet, a vnitřní sítě organizace. Veškeré informace mezi vnitřní a vnější sítí musejí projít přes firewall. To znázorňuje obrázek 13.



Obrázek 13:Poloha TOE [22]

4.3 Bezpečností prostředí TOE

Zde jsou vymezeny hrozby, bezpečnostní politiky organizace a předpoklady, které mají být zpracovány TOE a TOE provozním prostředí.

4.3.1 HROZBY

Hrozba Agent

Za útočníka je považována IT entita nebo uživatel, který usiluje o poškození TOE za použití nelegálních metod nebo se pokouší o nelegální přístup k TOE a vnitřním aktivům organizace zvenčí.

Hrozba Address spoofing

Neautorizovaná osoba ve vnější síti se může pokusit obejít politiku pro kontrolu informačního toku podvržením autentizačních údajů (např. podvržením zdrojové adresy) a vydáváním se za legitimního uživatele nebo entitu ve vnitřní síti.

Útočník se může pokusit o přístup do vnitřní sítě pomocí falšování zdrojové IP adresy, která má být považována za interní IP adresu.

Hrozba Continous authentication attempt

Neoprávněná osoba se může opakovaně pokoušet uhodnout autentizační údaje, aby tyto informace použila k zahájení útoku na TOE.

Hrozba Illegal information inflow

Útočník může napadnout interní síť tak, že přes TOE pošle nepřípustnou informaci, což vyústí ve zneužití zdrojů ve vnitřní síti.

Hrozba Illegal information outflow

Při defektu ve fungování TOE může neoprávněný uživatel shromáždit zbytkové informace z předchozích informačních toků nebo vnitřní údaje TOE monitorováním informačního toku TOE.

Hrozba Inpersonation

Neoprávněná osoba se vydává za autorizovaného uživatele.

Hrozba Replay attack

Neoprávněná osoba může použít získané platné identifikační a autentizační údaje pro přístup k funkcím poskytovaným TOE.

Hrozba Stored data damage

Neoprávněná osoba nebo vnější IT entita může být schopna zobrazit, modifikovat anebo smazat s bezpečnostní spojené informace, které byly poslány mezi oprávněným administrátorem a TOE.

4.4 Organizační bezpečnostní politiky

TOE musí být v souladu s následujícími organizačními bezpečnostními politikami.

4.4.1 Předpoklady

Předpoklad Operating System Reinforcement

Nadbytečné služby nebo prostředky musí být odstraněny z operačního systému. Úroveň zabezpečení musí být zvýšena pro lepší ochranu proti zranitelnosti operačního systému. To zajistí spolehlivost a stabilitu systému.

Předpoklad Physical Security

TOE je fyzicky zabezpečené.

Předpoklad Security Maintenance

Když se vnitřní síťové prostředí změní v důsledku změn v konfiguraci sítě, např. zvýšení/snížení hostů nebo zvýšení/snížení služeb apod., musí se změna prostředí okamžitě odrazit v bezpečnostní politice TOE tak, aby úroveň zabezpečení byla zachována stejně jako před touto změnou.

Předpoklad Single Point of Connection

Informace mezi vnitřní a vnější sítí nemohou být přenášeny jinou cestou než skrze TOE.

Předpoklad Trusted Administrator

Oprávněný administrátor TOE nemá žádné zákeřné úmysly. Prošel odborným školením ohledně administrace TOE.

4.5 Bezpečností cíle

Zde jsou popsány cíle TOE a bezpečností cíle prostředí, kde se TOE nachází.

4.5.1 Bezpečnostní cíle TOE

Bezpečnostní cíl Audit

TOE musí zaznamenat a zachovat události spojené s bezpečností s cílem umožnit sledování odpovědnosti s bezpečností souvisejících úkonů, dále poskytuje prostředky k přezkoumání zaznamenaných dat.

Bezpečnostní cíl Data Protection

TOE musí ochránit uložená data v TOE od neautorizovaného použití, modifikace nebo vymazaní.

Bezpečnostní cíl Identification and Authentication

TOE musí jedinečně identifikovat uživatele a autentifikovat identitu uživatele.

Bezpečnostní cíl Information Flow Control

TOE musí kontrolovat tok neautorizovaných informací z a do sítě.

Bezpečnostní cíl Management

TOE musí poskytovat prostředky pro autorizované správce TOE, aby ho mohli administrovat bezpečným způsobem.

4.5.2 Bezpečnostní cíle prostředí

Bezpečnostní cíl Operation System Reinforcement

Nadbytečné služby nebo prostředky musí být z operačního systému odstraněny. Zabezpečení musí být zvýšeno pro lepší ochranu proti zranitelnosti v operačním systému. Tím je zajištěna spolehlivost a stabilitu systému.

Bezpečnostní cíl Physical Security

TOE musí být umístněno ve fyzicky zabezpečeném prostředí a smí být používáno pouze autorizovanými osobami.

Bezpečnostní cíl Security Maintenance

Když se vnitřní síťové prostředí změní v důsledku změn v konfiguraci sítě, např. zvýšení nebo snížení hostů nebo zvýšení nebo snížení služeb apod., musí se změna prostředí okamžitě odrazit v bezpečnostní politice TOE tak, aby úroveň zabezpečení byla zachována stejně jako před touto změnou.

Bezpečnostní cíl Single Point of Connection

Informace mezi vnitřní a vnější sítí nemohou téct jinudy než skrze TOE.

Bezpečnostní cíl Time Stamp

TOE musí přesně evidovat bezpečnostní události pomocí spolehlivého časového razítka poskytovaného operačním prostředním TOE.

Bezpečnostní cíl Trusted Administrator

Oprávněný administrátor TOE nemá žádné zákeřné úmysly. Prošel odborným školením ohledně administrace TOE.

5 Výsledky dotazníkového šetření a řízených rozhovorů

Praktická část této diplomové práce je zaměřena na využívání Common Criterií a výše zmíněného Profilu ochrany pro firewally viz kapitola 4 v praxi. Pomocí dotazníkového šetření a řízených rozhovorů s odpovědnými osobami zjišťuji, jaké je povědomí a využití doporučených norem v českém prostředí. Organizace jsou kromě standardního rozdělení na malé, střední a velké, rozděleny ještě podle svého zaměření na organizace působící ve státní správě, komerční a akademické sféře.

Dotazník, který je součástí přílohy č. 1 této diplomového práce vychází z Common Critérií a z poslední verze Profilu ochrany pro firewally verze 2.0. Protože informace o bezpečnostní politice organizace a firewallech, patří v každé firmě k utajovaným skutečnostem, byla návratnost dotazníků poměrně nízká.

5.1 Cíl průzkumu

Cílem průzkumu založeného na dotazníkovém šetření a osobních řízených rozhovorech je pokus o zmapování situace v současné praxi. V šetření preferuji zejména následující body, které mají souvislost s Commnon Critérii a Profilem ochrany pro firewally verze 2.0:

- Používání bezpečnostních politik v praxi.
- Proškolení odborného personálu.
- Typ organizace.
- Používané zařízení zajišťující bezpečnost sítě.
- Zkušenosti s bezpečnostními incidenty.

5.2 Vzorek respondentů

Získat vzorek respondentů bylo vůbec nejtěžší částí celého průzkumu. Informace o bezpečnostní politice organizace jsou v drtivé většině součástí firemního tajemství. Zde jsem využil především osobních kontaktů a předchozích pracovních zkušeností. Přesto jsem se snažil pokrýt co nejširší okruh organizací napříč Českou republikou, s ohledem na jejich velikost i i náplň činnosti.

5.3 Sběr dat

Byla zvolena metoda kvantitativního výzkumu. Pro sběr dat jsem použil formu dotazníku a dále formu řízeného rozhovoru s pracovníky IT oddělení jednotlivých organizací.

Data z dotazníku umožňují formalizaci a lze je snadněji porovnat. Pro organizace může být snazší vyplnit dotazník především z technických a časových důvodů. Dále garantuje zachování anonymity, což je vzhledem k obsahu průzkumu pro organizace klíčové. V relativně krátkém čase je možné pomocí dotazníků oslovit velký počet respondentů při malých nákladech.

Rizika dotazníkového průzkumu spočívají především v tom, že kladou vysoké nároky na ochotu dotazovaného. Některé otázky může respondent přeskočit nebo na ně neodpovědět.

Forma řízeného rozhovoru s odpovědnými pracovníky umožňuje doplnění a vysvětlení některých otázek s dotazníku a hlubší pochopení souvislostí problematiky bezpečnostní politiky organizace. Poskytuje také prostor pro informace, které dotazník nepostihuje, ale které mohou přispět k závěrům této diplomové práce. Tato metoda je časově náročná, avšak pro analýzu bezpečnostní situace nejvýhodnější.

Dotazník je sestaven z 14 otázek, z nichž 2 jsou volné. Pro distribuci dotazníků bylo využito emailu. Respondentům byl zasílán ve formě editovatelného pdf souboru, který po odeslání zaslal autorovi vyplněná data ve formě xml souboru, což značně zrychlilo zpracování dat a minimalizovalo složitost vyplňování dotazníku pro respondenty. Poslední otázka tohoto dotazníku nabízí možnost zveřejnění či zachování anonymity respondenta.

5.4 Analýza dat a výsledků průzkumu

V průběhu sběru dat bylo náhodným výběrem osloveno 54 organizací. Z oslovených organizací vyplnilo dotazník 21 organizací. Návratnost dotazníků byla tedy 39%. Dva dotazníky byly ke zpracování nepoužitelné, respondenti jej neodeslali pomocí formuláře, ale vložili jako přílohu do emailu, tím došlo ke ztrátě dat a znehodnocení dotazníků. Je nutné uvést, že popis reality byl redukován pouze na organizace, které byly ochotné dotazník vyplnit. Tento průzkum je zaměřen pouze na jeden časový bod. Situace se v organizacích v průběhu času neustále mění. V této práci je zachycen pouze statický obraz

situace ve vzorku českých organizací. Ke sledování vývoje by bylo nutné obdobný průzkum cyklicky opakovat.

Během zpracovávání dotazníků se ukázalo, že pro 60% respondentů je anonymita jejich organizace důležitá. Pro demonstraci uvedu jen několik názvů organizací, které byly ochotny odpovědět a své jméno zveřejnit:

- Ústav teorie informace a automatizace. AV ČR v.v.i.
- Česlog, s. r. o.
- Vodafone, a. s.
- Techsoft, s. r. o
- Všeobecná fakultní nemocnice na Karlově náměstí
- Ministerstvo průmyslu a obchodu ČR
- Úřad pro informace ve vzdělání ČR

Po provedení analýzy byly organizace rozděleny do dvou kategorií po třech skupinách. Prvním hlediskem pro rozdělení do kategorií se stala sféra, ve které organizace působí. Druhým hlediskem pro rozdělení do kategorií je velikost organizace na základě počtu zaměstnanců. Při vyhodnocování dotazníků jsem dospěl k následujícímu rozdělení.

I. Kategorie

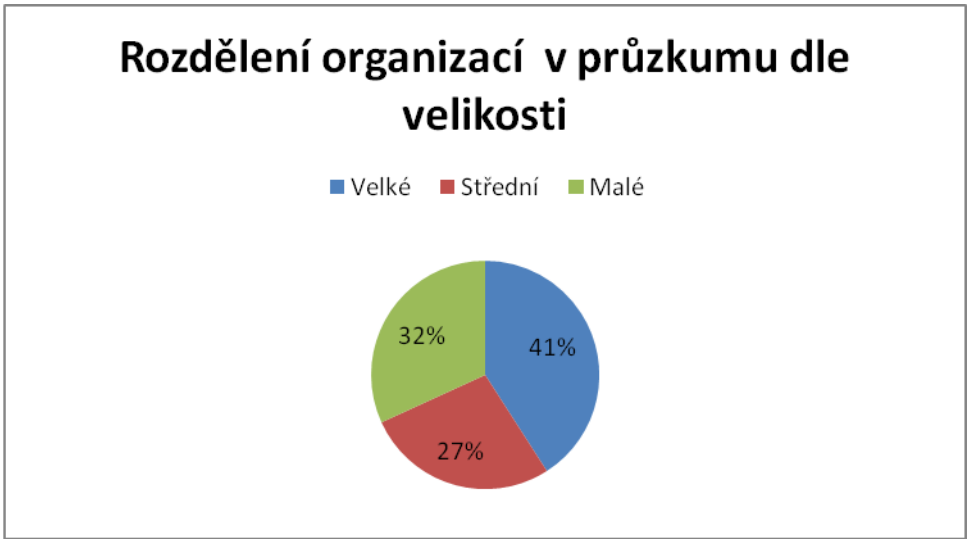
1. Organizace působící v akademické sféře
2. Organizace působící v soukromém sektoru
3. Organizace působící ve veřejné správě.

II. Kategorie

1. Malé organizace do 50 zaměstnanců
2. Střední organizace do 250 zaměstnanců
3. Velké organizace 250 a více zaměstnanců

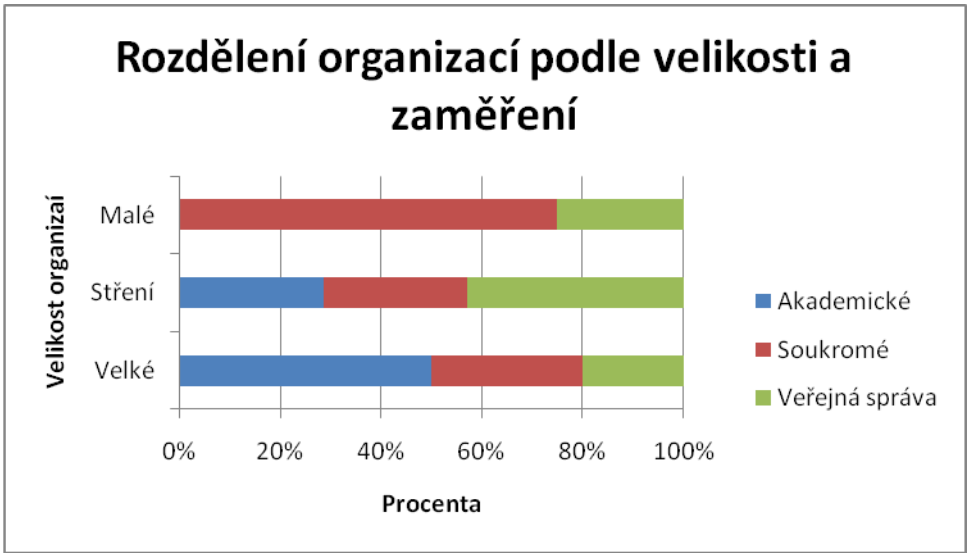
Otázka č. 1

Kolik má Vaše organizace zaměstnanců?



Graf 1: Rozdělení organizací dle velikosti

Graf 1 znázorňuje rozložení organizací do skupin v I. kategorii. Jak je vidět z grafu všechny tři skupiny jsou zastoupeny relativně rovnoměrně s menší převahou velkých organizací.



Graf 2: Rozdělení organizací podle velikosti a zaměření.

Graf 2 kombinuje obě kategorie organizací. Dle očekávání převažují soukromé subjekty v skupině malých organizací, akademické subjekty ve skupině velkých organizací. Středně velké organizace jsou zastoupeny rovnoměrně.

Otázka č. 2

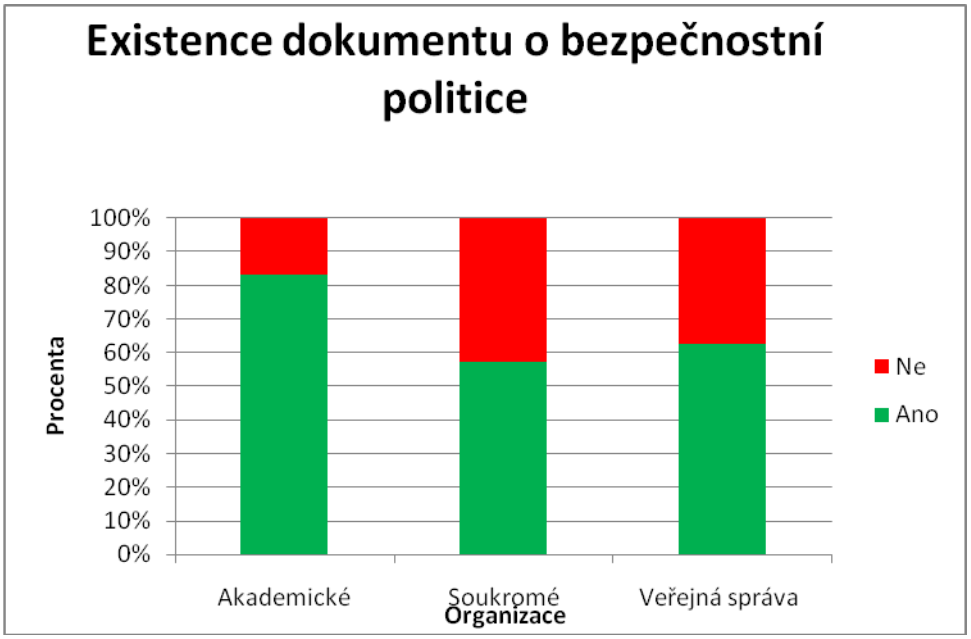
Kolik je v organizaci evidovaných pracovních stanic?

Tabulka 2: Průměrný počet pracovních stanic

Průměrný počet pracovních stanic v organizacích			
	Velké	*Střední*	*Malé*
Akademické	614	175	-
Soukromé	279	76	17
Veřejná správa	160	82	12

Otázka č. 3

Existuje ve Vaší organizaci dokument o bezpečnostní politice?

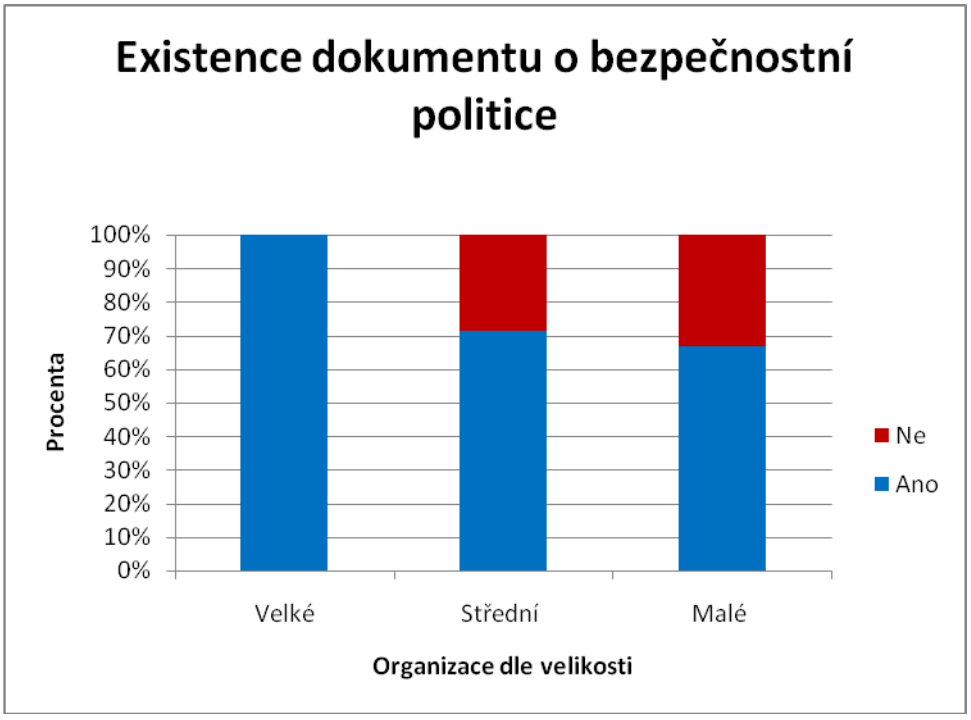


Graf 3: Existence dokumentu o bezpečnostní politice rozdělení dle I. kategorie.

Podle mého šetření (viz graf 3) mají akademické organizace poměrně velké zkušenosti s bezpečnostními incidenty uvnitř jejich počítačových sítí v souvislosti s rozvojem Internetu v akademické sféře, přibližně již od 90 let minulého století. Z tohoto důvodu není existence dokumentu, který popisuje chování uživatelů na počítačové síti, ničím výjimečným. Vzhledem k tomu, že fluktuace osob v těchto typech organizací je poměrně vysoká (studenti, cizí návštěvy, konference atd.), je takový dokument nezbytný.

Ve veřejné správě je situace horší: množství pracovních stanic je menší v porovnání s akademickou sférou, kde má přístup k Internetu téměř každý.

V soukromé sféře je situace nejhorší. Důvodem je často absence personálu kvalifikovaného v oblasti IT anebo dodatečné náklady, které by musely organizace na tvorbu dokumentu popisující bezpečnostní politiku vynaložit.

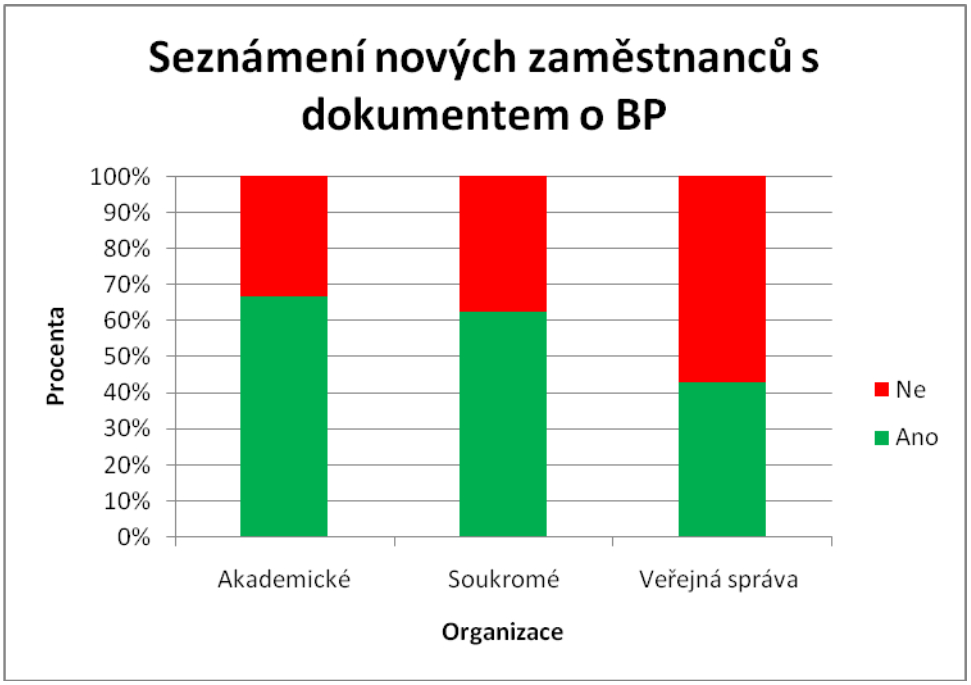


Graf 4: Existence dokumentu o bezpečnostní politice rozdělení dle II. kategorie

Druhé hledisko neukázalo významné rozdíly od prvního, vzhledem k tomu, že v dotazníkovém šetření jsou velké organizace zejména akademické typy organizací a střední organizace jsou z oblasti veřejné správy a částečně soukromých firem. Malé typy organizací jsou pak výhradně soukromé typy firem.

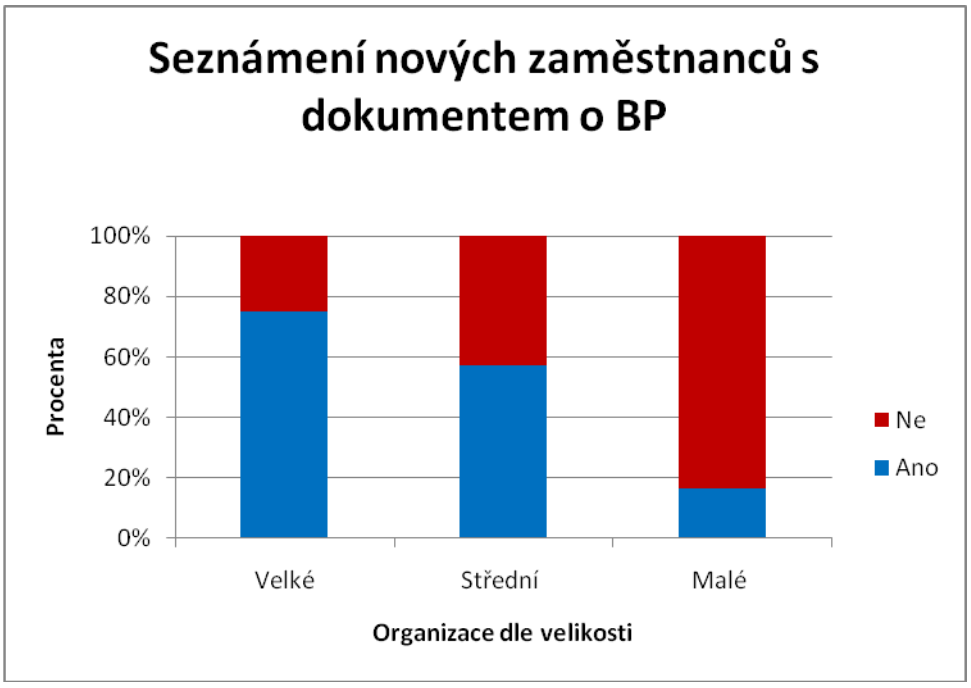
Otázka č. 4

Jsou s tímto dokumentem seznamováni noví zaměstnanci?



Graf 5: Seznámení nových zaměstnanců s dokumentem BP rozdělení dle I. Kategorie

Soukromé a akademické organizace dosáhly rovnocenného výsledku. Dle interview pokud u soukromých organizací existuje dokument o bezpečnostní politice, je velká vůle ze strany vedení a i ze strany odborného IT personálu seznamovat nové zaměstnance s tímto dokumentem. Zřejmě i pro to, že si soukromé organizace uvědomují finanční náklady, které byly spojeny s jeho vytvořením a případnými riziky jeho porušení. Ve veřejné správě je zejména podle řízených rozhovorů situace horší proto, že procesy uvnitř těchto institucí jsou často zmatečné, zatížené dodatečnou byrokracií. Z toho důvodu je výsledek horší než u předchozích dvou skupin organizací.

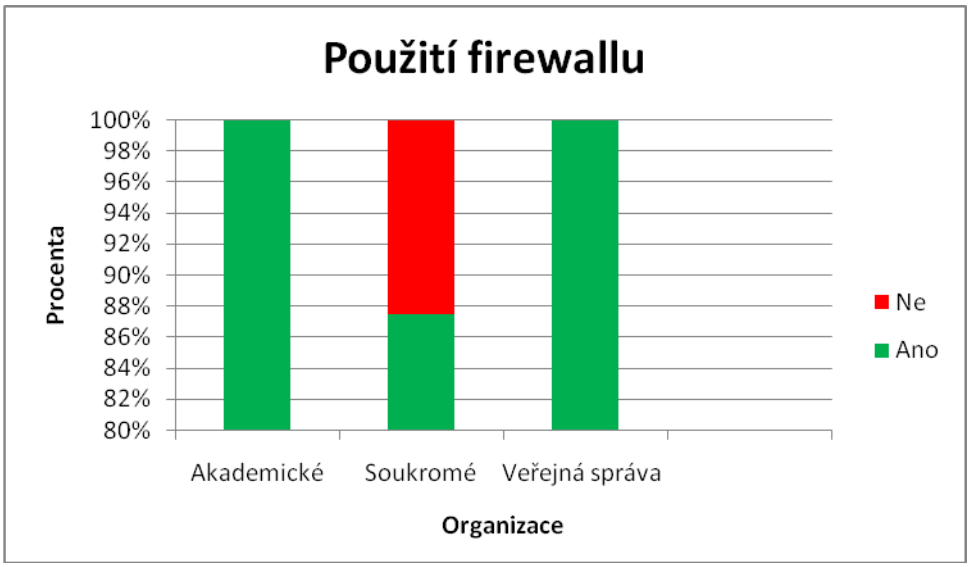


Graf 6: Seznámení nových zaměstnanců s dokumentem BP rozdělení dle II. kategorie

U velkých organizací se opět potvrdilo, že pocházejí zejména z akademické sféry, tudíž výsledek je podobný prvnímu šetření. Ve středních typech organizací se do jedné množiny dostávají organizace veřejné správy a soukromé, proto je výsledek lepší než u malých organizací, kde se jedná o soukromé typy organizací.

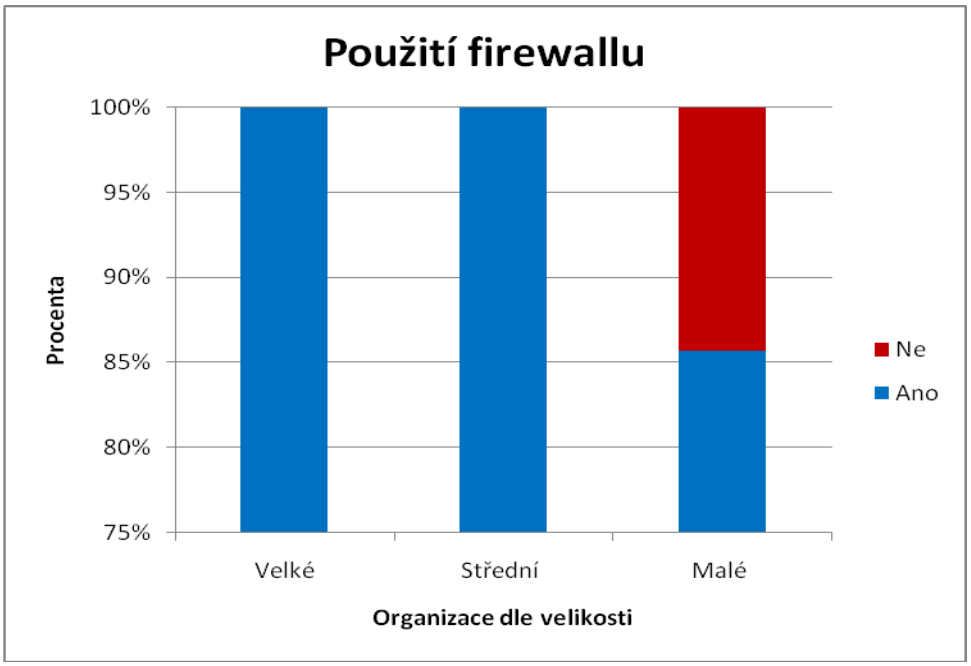
Otázka č. 5

Používá Vaše organizace firewall?



Graf 7: Použití firewallu v organizacích rozdělení dle I. kategorie

Opět se ukazuje, že veřejná správa ani akademické organizace nepodceňují potencionální riziko spojené s používáním informačních a komunikačních technologií. Používají různé typy firewallů, což bude rozebíráno dále. Soukromá sféra má sice nižší použití firewallů, nicméně dosažený výsledek je také poměrně uspokojivý. Musíme si uvědomit, že soukromé organizace, které jsou zároveň malými organizacemi, si často nechtějí firewall pořídit z finančních důvodů.



Graf 8: Použití firewallu v organizacích rozdělení dle II. kategorie

Hodnocení podle druhé hlediska potvrzuje jen výše uvedené závěry, že malé organizace často nechtějí do zařízení typu firewallu investovat finanční prostředky.

Otázka č. 6

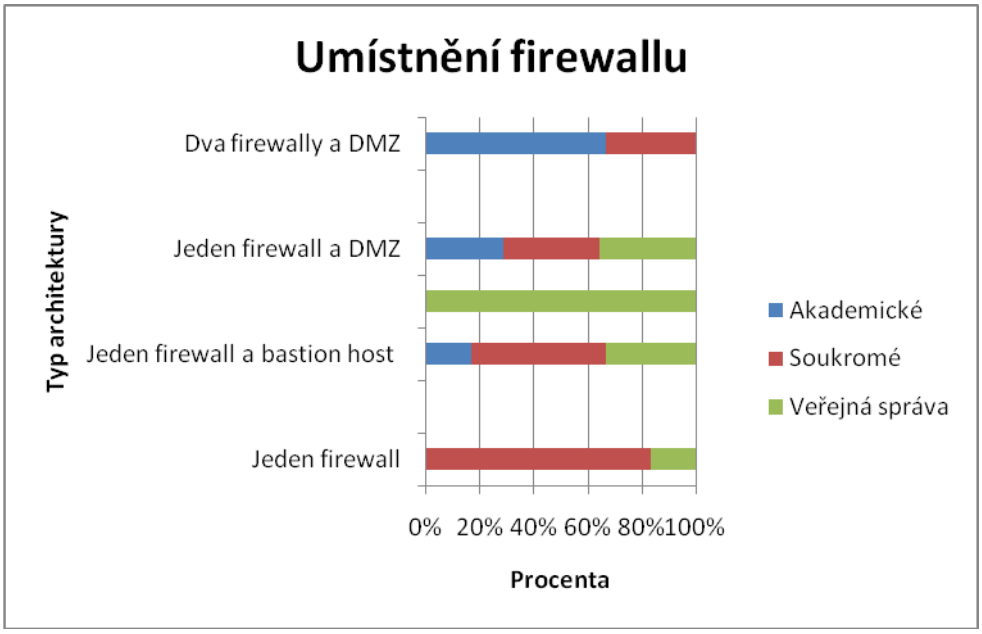
Pokud používáte firewall, kolik firewallů Vaše organizace využívá?

Tabulka 3: Průměrný počet firewallů

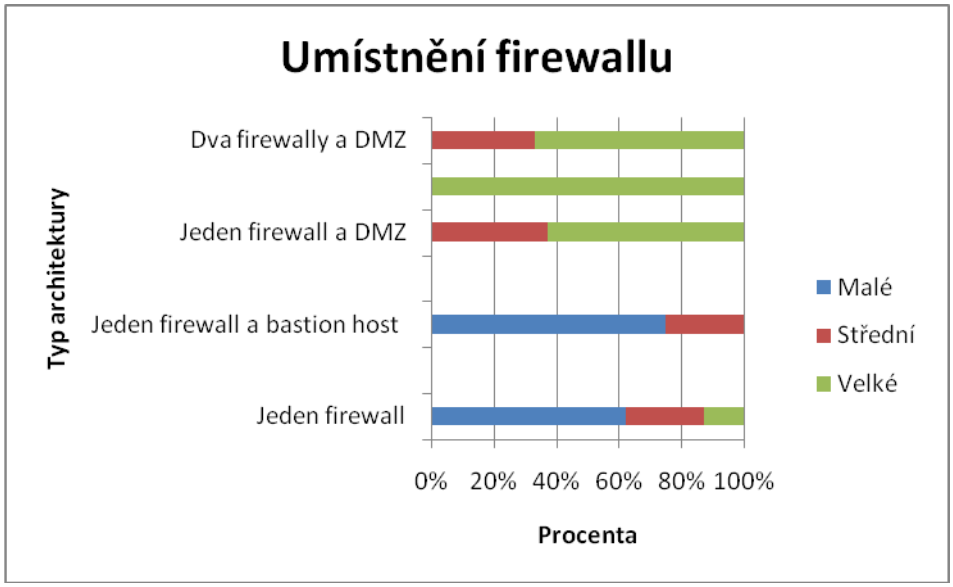
Průměrný počet firewallů v organizacích			
	Velké	*Střední*	*Malé*
Akademické	3	1	-
Soukromé	2	1	1
Veřejná správa	3	2	1

Otázka č. 7

Pokud používáte firewall, kde je firewall umístěn z hlediska architektury sítě?



Graf 9: Umístění firewallu z hlediska architektury sítě rozdělení dle I. kategorie

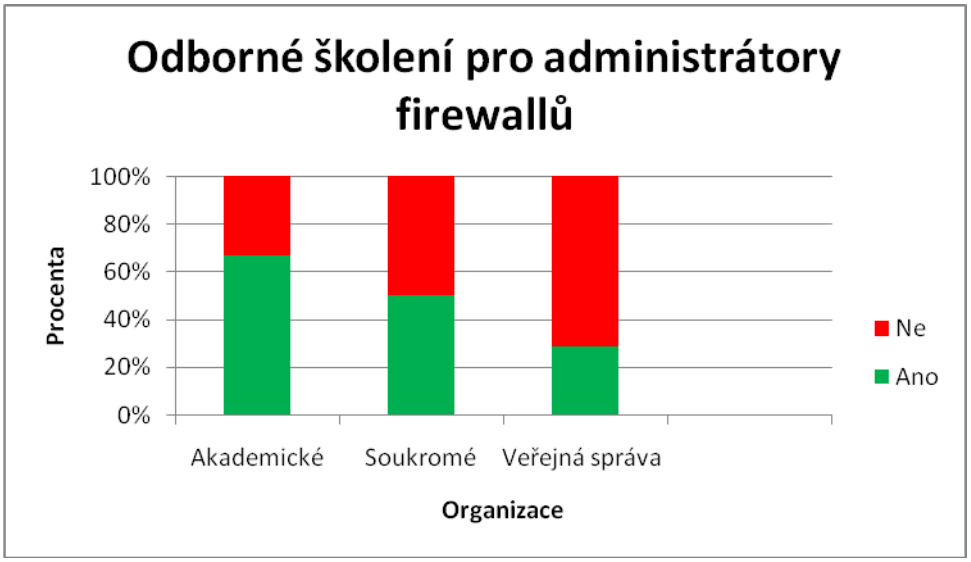


Graf 10: Umístění firewallu v síti z hlediska architektury rozdělení dle II. kategorie

Umístění firewallů v síti je podrobně rozebráno v kapitole 1.5.

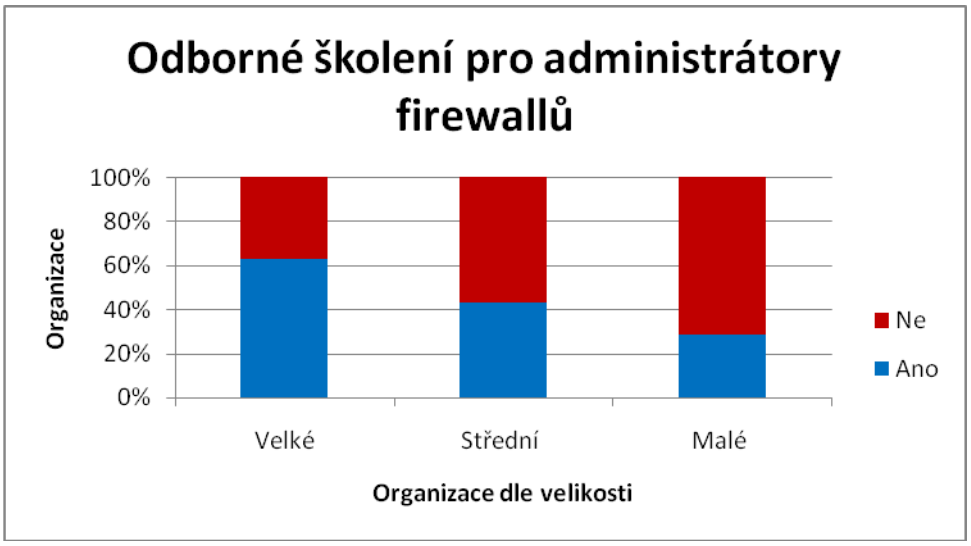
Otázka č. 8

Pokud používáte firewall, prošli administrátoři odborným školením?



Graf 11: Odborné školení administrátorů v organizacích I. kategorie

Opět se ukazuje, že akademické organizace nepodceňují rizika spojená s používáním počítačových sítí, často také pořizují vzhledem k dostatečnému množství finančních prostředků poměrně drahá, výkonná a složitá zařízení, která si vyžadují zaškolení ze strany dodavatele. Soukromé firmy pokud již investují do drahých zařízení jsou většinou ochotny zaplatit i za školení personálu s tím, že vyžadují po zaměstnanci kvalifikační dohodu. Ve veřejné správě je situace špatná zejména z důvodů centrální správy této techniky a z toho plynoucích problémů se zaškolením personálu.

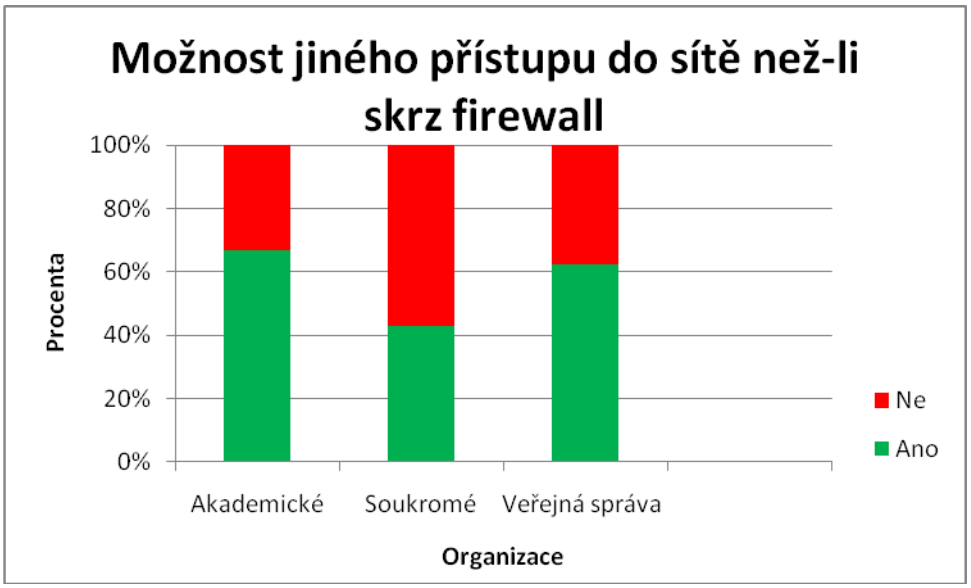


Graf 12: Odborné školení administrátorů v organizacích II. kategorie

U velkých organizací je situace dobrá díky velkému podílu akademických organizací, které byly účastníky šetření, částečně tento výsledek ovlivňují negativním způsobem organizace veřejné správy. U organizací střední velikosti se z výsledků šetření se kombinují veřejnoprávní a soukromé, v tomto případě soukromé organizace vylepšují celkový výsledek. U malých organizací jsou finanční náklady příliš vysoké, aby při zakoupení firewallu ještě navíc investovali dodatečné finance do zaškolení.

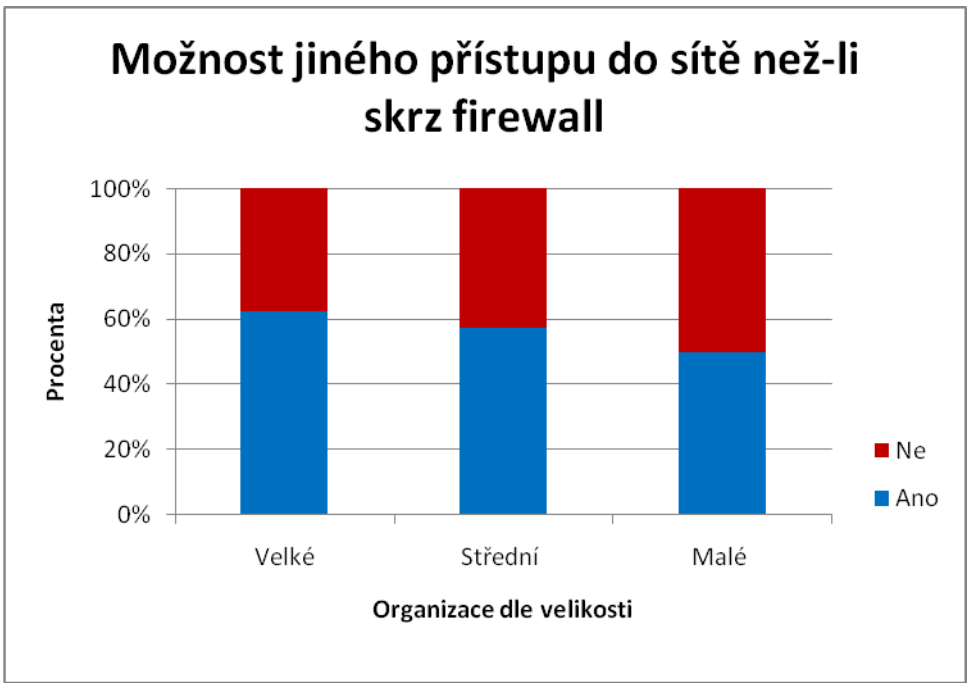
Otázka č. 9

Existuje jiný vnější přístup do sítě než-li skrz firewall?



Graf 13: Možnost jiného přístupu do sítě organizace I. kategorie

Na základě dotazníků a zejména řízených rozhovorů bylo zjištěno, že organizace používají zejména jako alternativní možnost přístupu do sítě organizace technologii typu virtuálních privátních sítí (VPN). Hlavní typy jsou IPsec a SSL VPN připojení. Tento alternativní přístup potencionálně zvyšuje riziko možného útoku, protože VPN zařízení realizující tyto spojení jsou umístěny mimo TOE, což je v rozporu s Profilem ochrany verze pro firewally 2.0. Bohužel, doporučení výrobců, jak umístit VPN zařízení do architektury sítě, jsou velmi často v rozporu s Profilem ochrany pro firewally verze 2.0

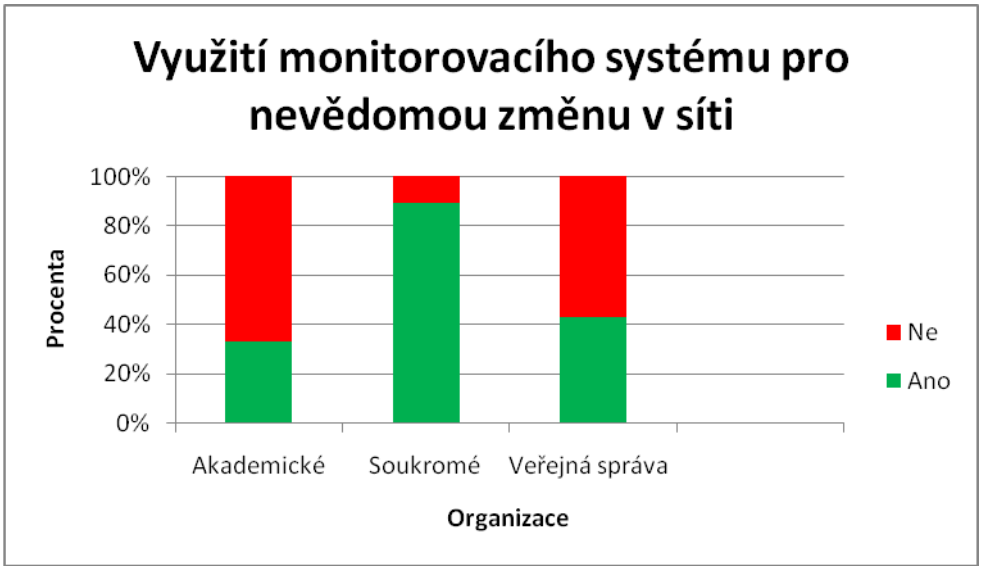


Graf 14: Možnost jiného přístupu do sítě organizace II. kategorie

VPN zařízení jsou ve velké většině drahá a technicky sofistikovaná zařízení, proto se také cena pohybuje v řádech deseti tisíců korun. To odpovídá i zjištěným výsledkům, kdy větší a střední organizace mají dostatek finančních prostředků na jejich pořízení, a tím i jejich zaměstnanci získávají dodatečnou možnost přístupu do organizace zvenčí.

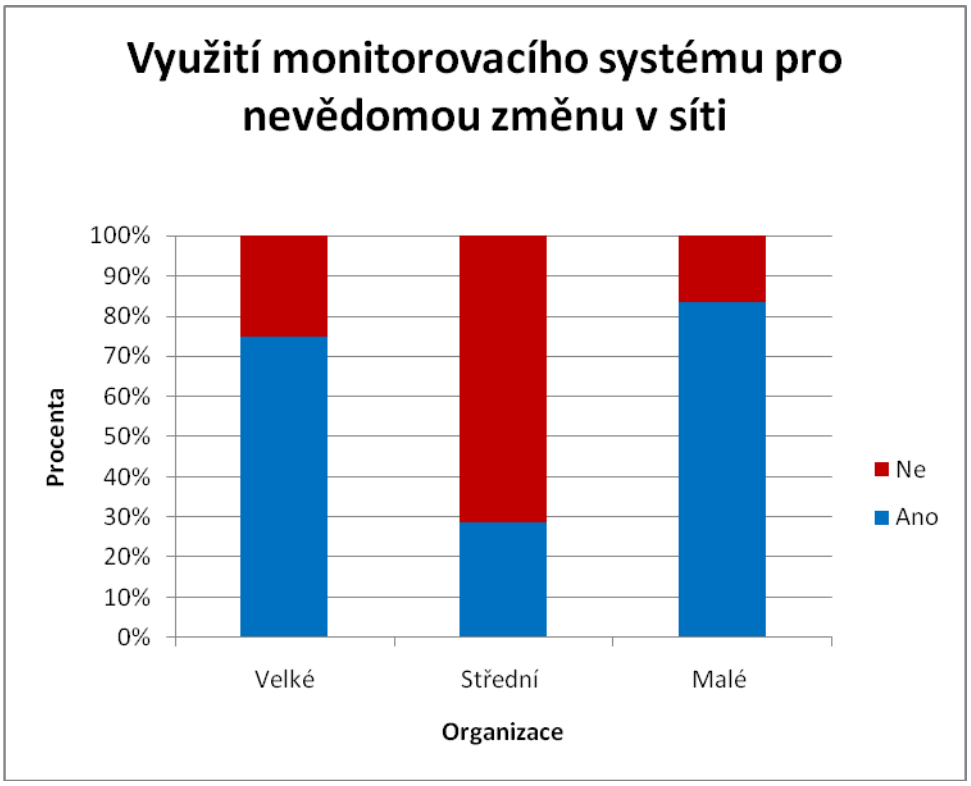
Otázka č. 10

Využíváte monitorovací systém pro nevědomou změnu v konfiguraci sítě?



Graf 15: Monitorovací systém pro nevědomou konfiguraci sítě v organizacích I. kategorie

Z výsledků průzkumu vyplývá, že pořizování výpočetní techniky (PC, notebooky, PDA) v soukromých organizacích se děje většinou jednotně nebo centrálně přes IT oddělení nebo odpovědnou osobu, vzhledem k tomu, že se jedná výhradně o firemní prostředky. Už tento fakt ovlivňuje skutečnost, že uživatelé nemají administrátorské účty na těchto zařízeních, což celkově přispívá k minimalizaci nevědomých změn v počítačové síti. Soukromé firmy kvůli citlivosti dat často využívají systémy pro nevědomou změnu v síti. Těmito změnami se zejména myslí: Nevědomá změna MAC adresy, připojení neznámého zařízení, nevědomá změna IP adresy.

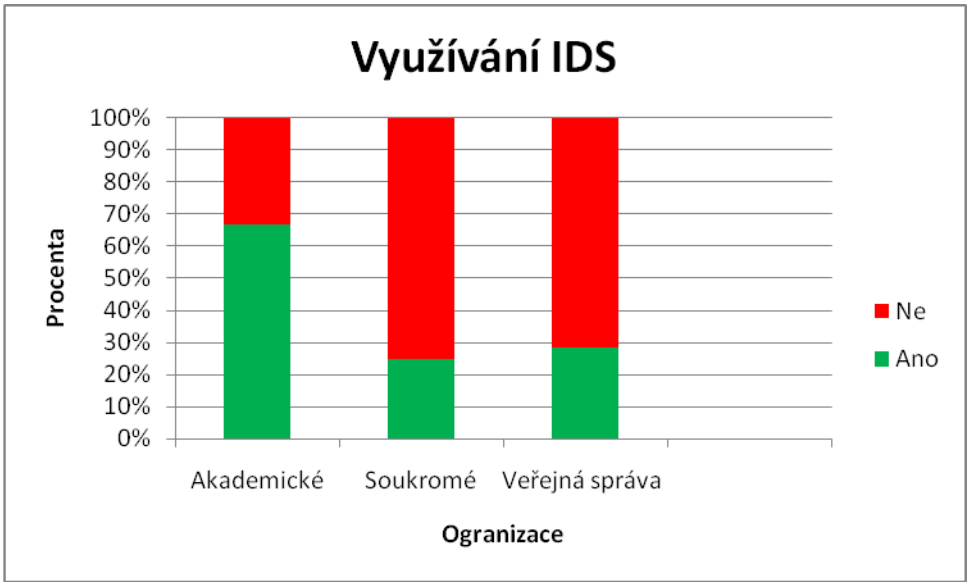


Graf 16: Monitorovací systém pro nevědomou konfiguraci sítě v organizacích II. kategorie

Na základě rozdělení dle hlediska velikosti organizace je patrné ovlivnění výsledků faktem, že velké množství malých organizací bylo zároveň soukromých.

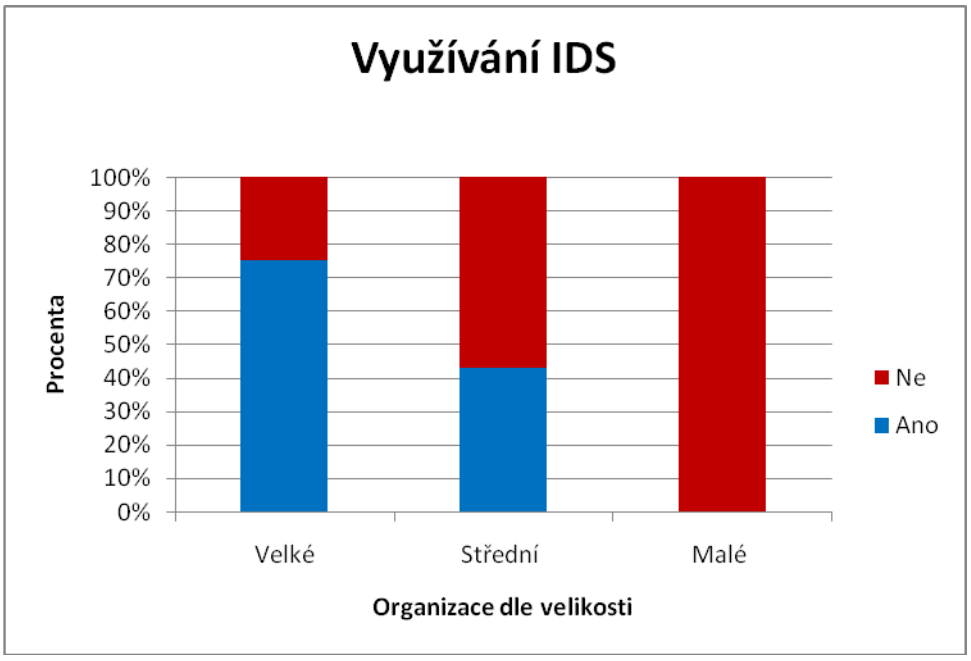
Otázka č. 11

Využíváte Intrusion Detection System?



Graf 17: Využívání IDS organizace I. kategorie

Zjištěná situace je zde podobná jako u otázky číslo 9. Tedy cena zařízení se pohybuje řádově ve statisících. Tyto systémy nejsou v současné době nezbytné pro zabezpečení vnitřní, i když přinášejí vysoké zvýšení bezpečnosti na úrovni samotných dat, která jsou přenášena spojením. Jde o poměrně novou technologii, která se stává stále dostupnější širšímu spektru zájemců. Tato technologie je často součástí TOE. Například akademické organizace velmi často tuto technologii používají při připojení kolejí nebo ubytoven pro zaměstnance. U soukromých organizací se tato technologie používá k blokování komunikačních programů typu: Skype, ICQ apod.

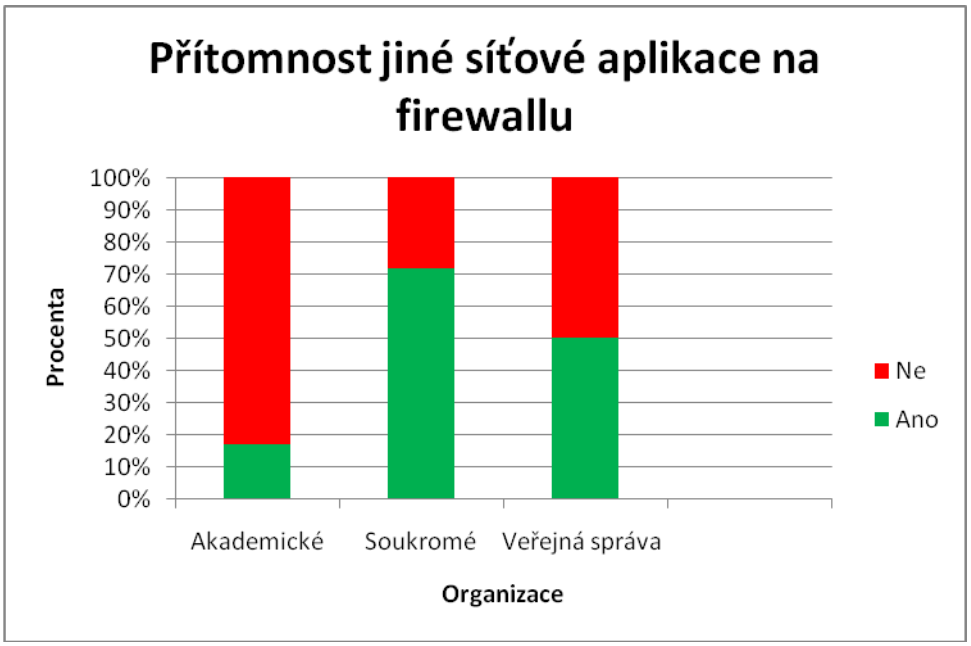


Graf 18: Využívání IDS organizace II. kategorie

Zjištěné výsledky odráží finanční možností jednotlivých typů organizací. Více o technologii IDS viz kapitola 1.2.1.

Otázka č. 12

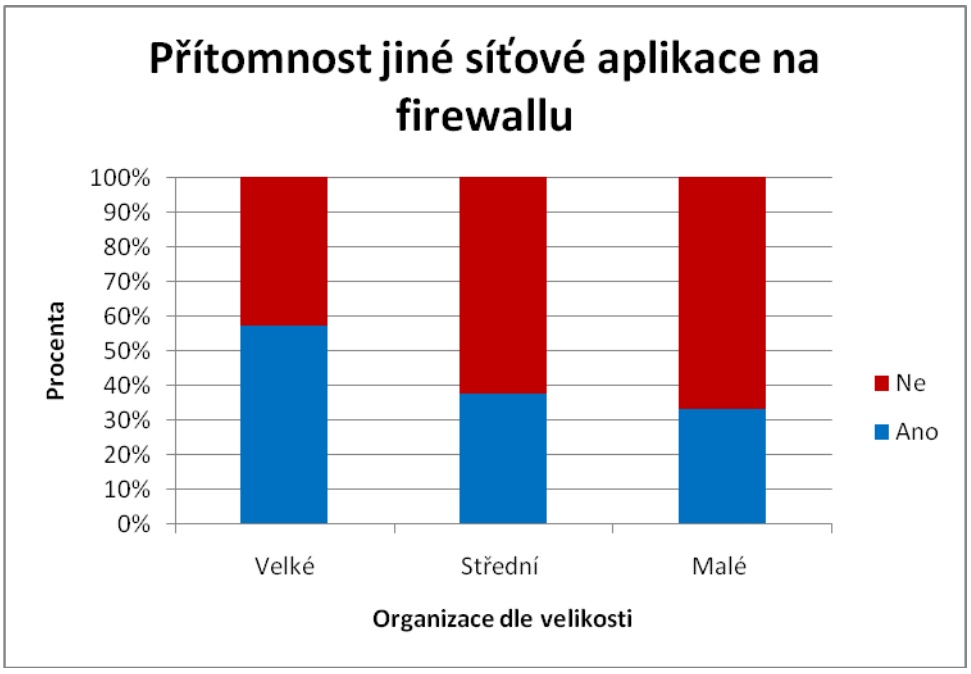
Používáte-li softwarový firewall na Linuxu (IP tables) nebo Windows 2003, Windows 2008 Server, běží na nich ještě jiná síťová aplikace?



Graf 19: Jiná síťová aplikace na firewallu organizace I. kategorie

Pokud používají organizace softwarový typ firewallu, není tak bezpečný jako specializované hardwarové zařízení. Není to však v rozporu s Profilem ochrany pro firewally verze 2.0. Operační systémy trpí skrytými bezpečnostními problémy, které jsou při zjištění periodicky odstraňovány ze strany výrobců. Z bezpečnostního hlediska není vhodné, aby na TOE byla současně provozována i jiná síťová služba, než služba sloužící k zajištění bezpečnosti. Zejména máme na mysli v praxi často souběžný běh TOE a webového serveru, které jsou umístěny fyzicky na jednom stroji. I samotný webový server může trpět skrytými bezpečnostními problémy, které jsou odstraňovány pomocí aktualizací. Toto sloučení služeb je v rozporu s Profilem ochrany pro firewally verze 2.0.

Z výsledků průzkumu vyplývá, že v tomto bodě mají nejhorší výsledek soukromé organizace, které tak zřejmě minimalizují finanční náklady za zabezpečení síťových služeb.

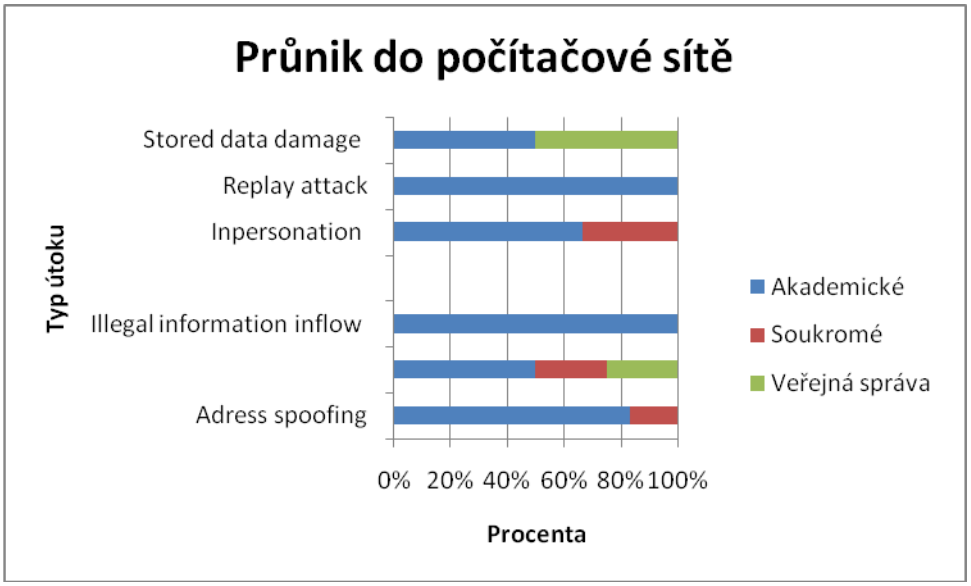


Graf 20: Jiná síťová aplikace organizace II. kategorie

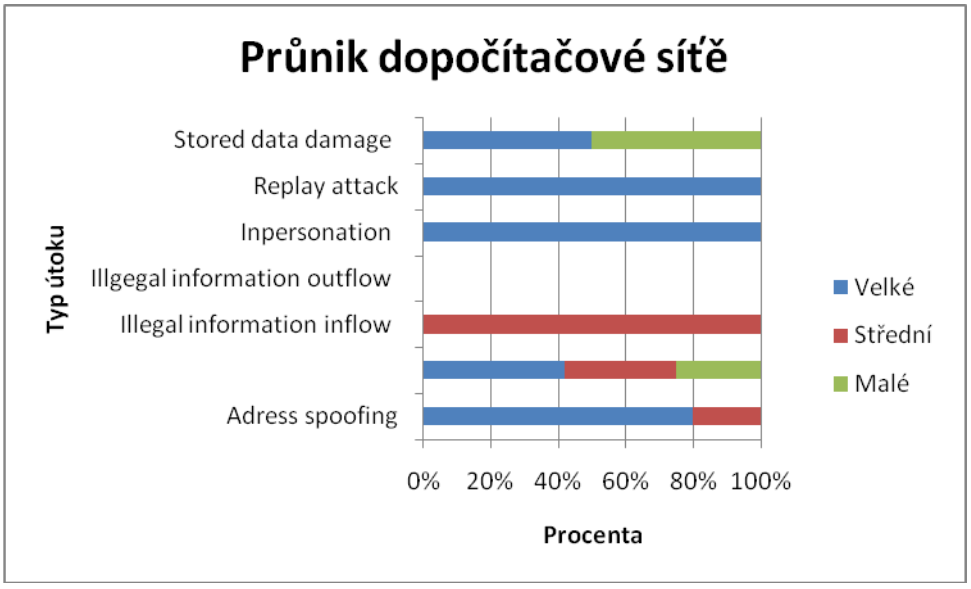
Zjištěné výsledky v druhé kategorii rozdělení odpovídají finančním možnostem organizací.

Otázka č. 13

Zaznamenali jste proniknutí do Vaší sítě, a pokud ano o jaký typ útoku se jednalo?



Graf 21: Průnik do počítačové sítě organizace I. kategorie

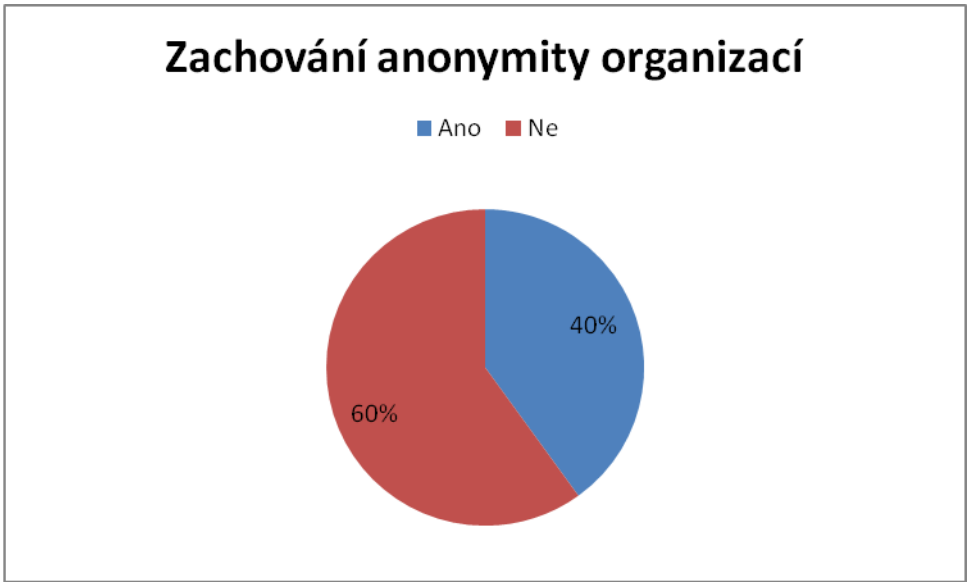


Graf 22: Průnik do počítačové sítě organizace II. kategorie

Vzhledem k tomu, že veškeré organizace v mém šetření zaznamenaly ohrožení jejich počítačové sítě, považuji za vhodné odkázat na typy hrozeb, které byly podrobně popsány viz kapitola 4.3.1

Otázka č. 14

Je možné zveřejnit název Vaší organizace v diplomové práci?



Graf 23: Anonymita organizací v průzkumu

Informace o bezpečnostní politice jsou pro každý subjekt utajované a citlivé údaje, jejichž zneužití může významně ohrozit chod organizace. Proto ochota respondentů sdělovat tyto informace adresně je velice malá, což je vidět i na grafu 23. Bez možnosti zachování anonymity dotázaných organizací by prakticky nebylo možné průzkum uskutečnit.

Shrnutí

Přestože organizace byly vybrány náhodně, jsou dle velikosti rozděleny na početně téměř shodné malé, střední a velké organizace. Ve skupině malých organizací jsou nejčastěji zastoupeny soukromé subjekty, skupinu velkých organizací tvoří především organizace akademické, v třetí skupině jsou zastoupeny organizace všech zaměření.

V současné době (jak ukázal průzkum) organizace nepodceňují existenci dokumentu o bezpečnostní politice. Nejlépe se v tomto směru jeví situace v akademické oblasti. Soukromá a veřejná sféra dosahují velmi podobných výsledků. Z hlediska členění organizací dle II. kategorie je situace obdobná.

V daleko nižším měřítku jsou pak s tímto dokumentem seznamováni noví zaměstnanci organizací. Nejhorší situace dle mého průzkumu je ve veřejné správě a u malých organizací.

Firewally při ochraně vnitřní počítačové sítě využívají všechny oslovené organizace s výjimkou několika malých soukromých subjektů.

Z hlediska architektury umístění firewallu na síti převažuje model s jedním firewallem a DMZ. Tento model poskytuje optimální zabezpečení při přiměřené finanční náročnosti. Méně využívaný je pak model s jedním firewallem a bastion host nebo model s jedním firewallem, který je nasazen především u malých a středních organizací. Model se dvěma firewally a DMZ využívají především velké a akademické organizace.

Profil ochrany pro firewally verze 2.0 vyžaduje, aby administrátoři prošli odborným školením. Situace v praxi však tomuto požadavku často neodpovídá. Je to především proto, že tato školení jsou velmi nákladná. Tato školení si mohou zejména dovolit velké a akademické organizace.

Dalším bezpečnostním požadavkem obsaženým v profilu ochrany pro firewally 2.0 je, aby do vnitřní sítě organizace existoval jediný možný přístup přes firewall. Část organizací však tento požadavek porušuje především tím, že k přístupu do vnitřní sítě využívá technologii typu virtuálních privátních sítí (VPN).

Použití systému pro odhalení nevědomé změny konfigurace v síti a také detekčních systémů IDS a IPS (viz. kapitola 1.2.1) odpovídá v drtivé většině finančním možnostem organizací. Vzhledem k tomu, že tyto technologie představují vynaložení nemalých finančních prostředků, mohou si je dovolit především velké organizace.

Profil ochrany verze 2.0 vylučuje, aby na firewallu současně běžela jiná síťová aplikace. Z výsledku průzkumu vyplývá, že především malé organizace toto porušují. Zřejmě z důvodu úspory finančních prostředků. V praxi se často objevuje souběžný běh firewallu a webového serveru.

Pokus o proniknutí do počítačové sítě zaznamenaly všechny oslovené organizace. Rozdělení dle typu útoku, dle profilu ochrany, je podrobně rozebráno v kapitole 4.3.1

Většina respondentů průzkumu si přála v této diplomové práci nezveřejňovat název své organizace.

6 Návrh zabezpečení – praktický příklad

V této kapitole je navrženo řešení zabezpečení přístupu do počítačové pro soukromou organizaci působící v ČR. Zvolené řešení vychází z poznatků získaných při tvorbě této práce. Při řešení návrhu zabezpečení je využit Profil ochrany pro firewally verze 2.0.

Profil organizace

***Organizace*:** STEP, spol. s r. o.
***Lokalita*:** Praha, Česká republika
***Pozice na trhu*:** Stavební společnost, developer

Stavební společnost STEP, spol. s r.o. byla založena jako jedna z prvních soukromých stavebních společností v roce 1990. Hlavním předmětem činnosti společnosti je provádění stavebních a montážních prací včetně technologických částí v oboru pozemního stavitelství. Společnost STEP působí na našem trhu rovněž jako úspěšný developer. Dále je vlastníkem Sportcentra STEP a hotelu STEP.

Zadání

Organizace potřebuje sjednotit zabezpečení ekonomického úseku, výrobně technického úseku a komplexu vlastního hotelu. Oba úseku jsou umístěny ve společné budově, hotel se nachází v samostatném objektu.

Současný stav

Současná situace (zima 2009) je taková, že oba úseky, tak i samotný hotel, jsou připojeny, přes svůj vlastní router s nedostatečným zabezpečením přímo do Internetu. Toto řešení je nadále nevyhovující.

Požadavky na nové řešení:

- Sjednotit IP rozsahy používaných sítí (použití privátních IP adres).
- Optimalizovat síťovou architekturu, tak aby byl potřeba pouze jeden hraniční router.
- Zvýšit bezpečnost umístěním firewallu mezi hraniční router a vnitřní síť.
- Použít technologii NAT a IDS pro vybrané vnitřní sítě.
- Zajistit bezpečný provozu informačního webového serveru.

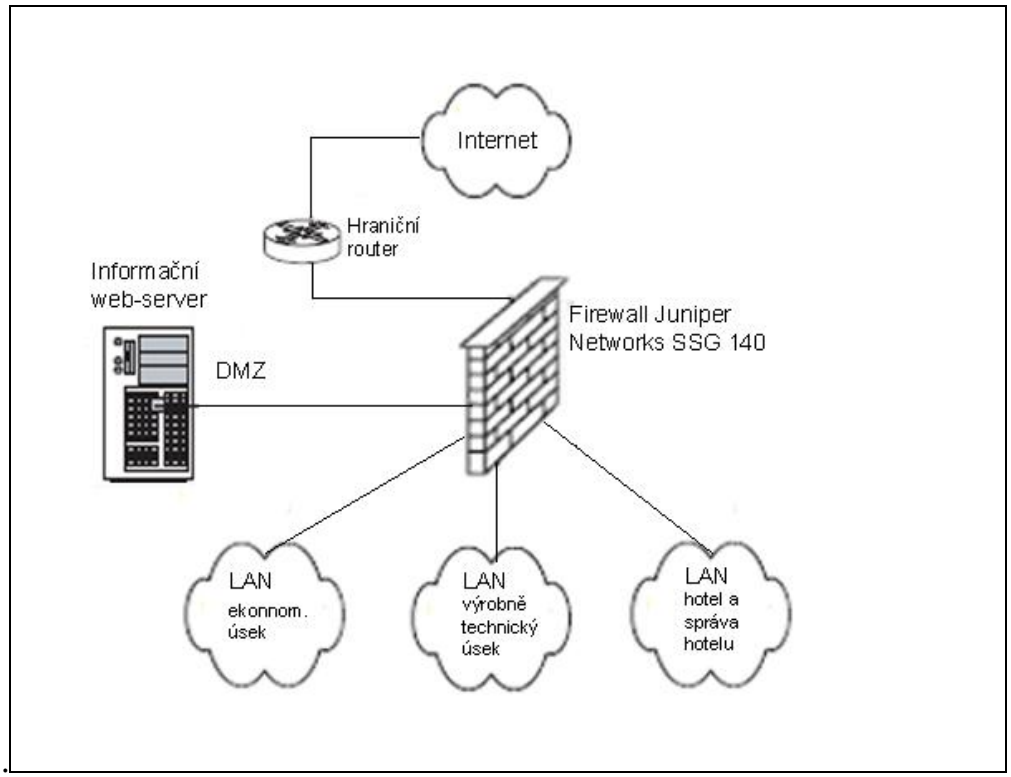
Navrhované řešení

Vzhledem k zadání podle složení sítě, kde se střetávají administrativní složky, návštěvy a ubytování zaměstnanci, je nutné rozdělit vnitřní sítě do několika segmentů:

- Síť pro ekonomický úsek
- Síť pro výrobně-technický úsek a správu hotelu.
- Síť pro hotelové hosty.
- DMZ pro webový server.

Umístění firewallu

Pro umístění firewallu je zvolen model sítě s jedním firewallem a demilitarizovanou zónou, kde demilitarizovaná zóna bude použita pro umístnění webového informačního serveru. Takto umístěný firewall odpovídá umístění TOE v PP pro firewally verze 2.0. Tato architektura je znázorněna na následujícím obrázku 14.



Obrázek 14: Navrhovaný model sítě pro soukromou organizaci

Hardwarové řešení

Jako hardwarové řešení splňující výše uvedené požadavky na provedení byl vybrán firewall od společnosti Juniper Networks. Konkrétně se jedná o model SSG 140. Parametry toho zařízení jsou:

- Maximálně 48 000 současných spojení.
- Maximálně 40 bezpečnostních zón, v našem řešení se využívá 5 bezpečnostních zón (untrust – Internet, DMZ, administrativní síť, síť pro hosty, ubytovací síť).
- Maximálně 1000 pravidel bezpečnostní politiky.
- 8 portů 10/100.
- 2 porty 10/100/1000.
- IDS modul.

Obrázek 15: Firewall Juniper Networks SSG 140 [24]

Organizační bezpečnostní politiky

Operating System Reinforcement

Nadbytečné služby nebo prostředky musí být odstraněny z operačního systém.

Firewall SSG 140 splňuje tento požadavek již svojí povahou. Jedná o sofistikované hardwarové zařízení, které neumožňuje instalace aplikace třetích stran.

Security Maitance

Dojde-li ke změně v konfiguraci sítě, musí se změna prostředí odrazit v bezpečnostní politice zařízení.

K firewallu je dodáván speciální administrační software tzv. Netscreen security manager. (NSM). Tento software se schopen generovat zprávy (reporty) změnách v síti.

Single Point of Connection

Informace mezi vnitřní a vnější sítí nemohou být přenášeny jinou cestou než skrze firewall.

Tento požadavek je zajištěn již samotným umístění firewallu. Dále je v tomto zařízení implementována i funkce VPN koncentrátoru, tedy vzdálená připojení budou procházet přes toto zařízení.

Trusted Administrator

Oprávnění administrátor firewallu prošel odborným školením.

Součástí dodávky firewallu je i odborné proškolení administrátorů ze strany výrobce.

Bezpečnostní cíle

Audit

Firewall musí zaznamenat a zachovat události spojené s bezpečnostním cílem a umožnit přezkoumání zaznamenaných dat.

Tento cíl splňuje dodávaný administrační software Netscreen security manager (NSM), který všechny zaznamenané události uchovává ve formě logu.

Data Protection

Firewall musí ochránit uložená data od neautorizovaného použití, modifikace nebo vymazání.

Firewall SSG 140 autorizuje uživatele s využitím standardu IEEE 802.1X, který je implementován.

Identification and Authentication

Firewall musí jednoznačně identifikovat uživatele a autentifikovat identitu uživatele.

Viz bezpečnostní cíl Data Protection.

Information Flow Control

Firewall musí kontrolovat tok neautorizovaných informací z a do sítě.

Firewall bude kontrolovat veškerou procházející komunikaci, jak autorizovanou, tak neautorizovanou. K tomu je možné využít bezpečnostních pravidel firewallů, ty stanovuji zdrojové i cílové IP adresy a dále zdrojový a cílový port(y), po kterých může komunikace

probíhat. Dále je k monitorování síťového provozu použit vestavěný IDS modul, který filtruje data na aplikační vrstvě, tedy na úrovni samotných dat přenášených pomocí paketů. O veškeré komunikaci je vytvářen provozní log (záznam), který se v pravidelných časových intervalech kopíruje na server, kde je instalován NSM software.

Dále lze pomocí pravidel na firewallu detekovat, sledovat a logovat i takové pokusy o komunikaci, která není povolena. Tyto pravidla se nijak výrazně neodlišují od normálních pravidel, která povolují určité komunikace, až na to, že u nich není nastaven příznak permit (povolit), ale místo toho se použije příznak deny (zakaž).

Management

Firewall musí poskytovat prostředky pro autorizovaného správce zařízení.

Všechny tyto prostředky v sobě obsahuje software Netscreen security manager. (NSM). Tento software je schopen generovat zprávy (reporty) o provozu, zatížení, změnách v síti.

Bezpečnostní cíle prostředí

Physical Security

Firewall musí být umístěn ve fyzicky bezpečném prostředí, a smí být používán pouze autorizovanými osobami.

Toto opatření bezpečnostní politiky musí být provedeno ve spolupráci se samotnou organizace, která musí zajistit odpovídající zabezpečené prostředí pro umístění firewallu.

Firewall Juniper Networks SSG 140 je při správné instalaci a nasazení schopen čelit všem hrozbám uvedeným v Profilu ochrany verze 2.0.

Předpokládaná cena řešení

Samotná cena firewallu se pohybuje v závislosti na kurzu USD mezi 90 000 – 120 000 Kč. Dále je nutné uvažovat podporu pro stahování firmwaru a aktualizací pro IDS na 1 rok, ta se pohybuje mezi 40 000 – 60 000 Kč. A konečně odborné školení, jehož cena je 30 000 Kč.

Celková cena řešení se tedy pohybuje mezi 160 000 až 210 000 Kč.

Předpokládaná doba implementace.

Je odhadována na 3 měsíce (v této době je uvažována i doba potřebná k dodávce zařízení, která podle výrobce činí 3-4 týdny).

Realizace

Vedení společnosti po technické stránce s navrhovaným řešením souhlasilo. Vzhledem k probíhající ekonomické krizi však došlo v období mezi návrhem a realizací zabezpečení vnitřní počítačové sítě ve společnosti STEP k určitým organizačním změnám. Provoz hotelu v poslední době nepřináší požadovaný ekonomický efekt. Proto vedení rozhodlo o jeho pronájmu. V současné době již tedy není provozovatelem hotelu společnost STEP, ale společnost IC HOTELS, a. s. Stavebnictví a development patří k nejpostiženějším oblastem ekonomiky zasažených touto krizí. Protože navrhované řešení by pro společnost znamenalo nyní značné finanční zatížení, bylo rozhodnuto zatím do uvedeného návrhu zabezpečení neinvestovat. Rozhodnutí je ovlivněno i faktem, že hotel je v současné době v pronájmu. Pro zabezpečení ekonomického úseku a výrobně technického úseku bylo zvoleno jiné řešení, softwarový firewall na bázi IP tables.

Závěr

Teoretická část práce ukazuje možnosti jak zabezpečit vnitřní síť organizace a dále podrobněji popisuje technologie s touto problematikou související. Základním zařízením pro ochranu vnitřní počítačové sítě je firewall. V praxi je dnes nejpoužívanější stavový firewall nebo proxy firewall či jejich kombinace. Tato zařízení má možnost získat každá organizace, protože náklady spojené s jejich pořízením jsou velmi variabilní, např. firewall na bázi IP tables je z finančního hlediska velmi levné a poměrně účinné řešení pro menší a střední organizace. Nesmíme ale opomenout nejmodernější technologie, které jsou pro firewally dnes k dispozici. Jsou to detekční systémy (IDS, IPD) také popsané v teoretické části, které detekují škodlivý kód na aplikační úrovni.

Z výsledků mého průzkumu vyplývá, že nejčastěji využívaným modelem, z hlediska umístění firewallů v architektuře počítačové sítě organizace, je model s jedním hraničním firewallem a demilitarizovanou zónou. Toto řešení přináší při přiměřených finančních nákladech velmi dobrou úroveň zabezpečení.

Stále však platí, že pokud jde o komplexní pohled na zabezpečení organizace nejen z hlediska síťového, ale i z hlediska bezpečnosti dat, která jsou pro organizace velmi citlivá, se musíme na informační systém organizace dívat jako na soubor tří prvků: hardware, software a zaměstnanci, kteří s ním pracují. Při zabezpečení jde i o to, aby procesy ve firmě byly jednoznačně určeny a definovány. Například přijímání nového zaměstnance, jeho seznámení s bezpečnostní politikou, vytváření uživatelských účtů. To jsou procesy, které pomocí firewallu nelze ošetřit. Zde hraje důležitou roli lidský faktor.

V této diplomové práce bylo poukázáno na to, že existuje dokument, který definuje minimální množinu bezpečnostních požadavků pro zařízení typu firewall. Přestože nespecifikuje přímo konkrétní typ zařízení a jeho implementaci, je použitelný pro nezávislé hodnocení a porovnávání jednotlivých firewallů. Dále je nutno vyzdvihnout fakt, že hodnocení úrovně bezpečnosti firewallů není spojeno pouze se samotným zařízením a jeho nastavením. Jedná se o celou řadu bezpečnostních cílů, kde je zahrnuta bezpečnostní politika organizace a prostředí, kde se dané zařízení nachází.

V další části této diplomové práce byl proveden průzkum ve vzorku organizací, které působí v České republice. Tento průzkum vychází ze zmíněného Profilu ochrany pro firewally verze 2.0. Potvrdil, že firewally jsou jednou z nejvyužívanějších technologií pro zabezpečení počítačových sítí. Veškeré organizace, které se průzkumu zúčastnily, se již setkaly s nějakou formou pokusu o napadení jejich vnitřní počítačové sítě. V tomto ohledu není rozhodující velikost ani zaměření organizace, přestože s bezpečnostními incidenty mají největší zkušenost především organizace působící v akademické a soukromé sféře. Především větší organizace si uvědomují nutnost existence dokumentu o bezpečnostní politice. Zarážející je však fakt, že i přes existenci takového dokumentu, s ním často nejsou noví zaměstnanci organizací seznamováni.

V průzkumu se nevyskytla žádná organizace, která by splňovala veškeré bezpečnostní cíle určené v Profilu ochrany pro firewally. Zejména se jednalo o nedostatečné odborné proškolení administrátorů firewallů. Dále bylo zjištěno, že do počítačové sítě organizace existuje jiný vnější přístup nežli skrze firewall nebo na firewallu běží ještě jiná síťová služba. Další důvody mohou vyplývat ze samotné podstaty těchto dokumentů. Historicky byla Common Criteria a Profily ochrany vyvíjeny především pro armádní účely, až později došlo k jejich rozšíření mezi odbornou veřejnost. I přes snahu organizací, které se na projektu Common Criterií podílejí, jsou bezpečnostní požadavky navrženy velice restriktivně a často obtížně splnitelné v běžné praxi. Svým způsobem je též zvláštní terminologie užívaná v samotných profilech ochrany. Struktura a obsah těchto dokumentů do značné míry vychází ze samotných Společných kritérií: Profily ochrany obsahují předdefinované funkce a komponenty, nezbytné k dosažení požadovaných bezpečnostních cílů. Je zde snaha o udržení jednotnosti stylu a struktury. Bohužel, výsledný text je někdy vykonstruovaný nebo nejasný. Nicméně tento nedostatek je kompenzován v podobě přínosů opakovaného použití komponent pro ostatní profily ochrany, stejnou interpretací bezpečnostních požadavků pro hodnotitele a možností vzájemného uznávání výsledků hodnocení ostatními národy.

Návrh zabezpečení vnitřní počítačové sítě soukromé organizace byl ze strany organizace po technické stránce akceptován. K jeho realizaci však v této podobě nedošlo vzhledem k omezeným finančním prostředkům a změnám uvnitř fungování organizace. Bylo

realizováno jiné levnější řešení, kde funkci firewallu plní softwarový firewall na bázi IP tables. Tím však nejsou splněna kritéria požadovaná Profilem ochrany verze 2.0.

Přínos své diplomové práce vidím v orientačním zmapování situace zabezpečení počítačových sít ve vzorku českých organizací. Mou práci lze použít pro seznámení se s problematikou referenčních kritérií při nákupu nebo hodnocení bezpečnosti firewallů. Diplomová práce může přispět k dosažení zvýšení úrovně zabezpečení počítačových sítí v jednotlivých organizacích, které se zúčastnily mého průzkumu.

Tato diplomová práce rozšířila mé znalosti, jak po stránce teoretické, tak pro stránce praktické, a představuje základ, na jehož podkladě bych se rád dále touto problematikou v budoucnu zabýval.

Použitá literatura

[1] AVOLIO, Frederick M. , *Firewalls and Internet Security-The Internet Protocol Journal* [online].2007, poslední revize 05.02.2007 [cit. 2009-06-02] Dostupný z WWW: <http://www.cisco.com/web/about/ac123/ac147/ac174/ac200/about_cisco_ipj_archive_article09186a00800c85ae.html>

[2] DOSTÁLEK, Libor, KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. 2. vyd. Praha: Computer Press, 2000. 488 s. ISBN 80-7226-323-4.

[3] DOSTÁLEK, Libor. *Velký průvodce protokoly TCP/IP: Bezpečnost*. 1. vyd. Brno: Computer Press, 2001. 565 s. ISBN 80-7226-513-X.

[4] HONTANÓN, Ramón J. *Linux praktická bezpečnost*. 1. vyd. Praha: Grada Publishing, 2003. 440 s. ISBN 80-247-0652-0.

[5] HÖNIGOVÁ, Alena, MATYÁŠ, Václav ml. *Anglicko-česká terminologie bezpečnosti informačních technologií*. Praha: Computer Press, 1996. 95 s. ISBN 80-85896-44-3.

[6] CHESWICK, William R., BELLOVIN, Steven M., RUBIN, Aviel D. *Firewalls and Internet Security* . 2nd edition. [s.l.] : AT and T Lumeta Corporation , 2003. 397 s. ISBN 0-201-63357-4.

[7] McNAB, Chris . *Network Security Assessment* . 1st edition. [s.l.] : O´Reilly , 2004. 396 s. ISBN 0-596-00611-X.

[8] THOMAS, Thomas M. *Zabezpečení počítačových sítí*. 1. vyd. Brno: Computer Press, 2005. 344 s. ISBN 80-251-0417-6

[9] WOODBERG, Brad, et al. *Configuring Networks NetScreen and SSG Firewalls*. 1st edition. Rockland : Syngress Publishing, 2007. 769 s. ISBN 1-59749-118-7.

[10] ZWICKY, Elizabeth D., COOPER, Simon, CHAPMAN, D. Brent. *Building Internet Firewalls*. 2nd edition. [s.l.] : O´Reilly , 2000. 890 s. ISBN 1-56592-871-7.

[11] *The History of Firewalls* [online]. 2001-2006 [cit. 2009-05-14]. Dostupný z WWW: <http://www.internetfirewall.org/article/internet-firewall-basics/the-history-of-firewalls.html>.

[12] *Přenos dat po síti* [online]. 2008 [cit. 2009-05-23]. Dostupný z WWW: <https://webdev.felk.cvut.cz/courses/Y36PJV/_media/prednasky/s07_net.ppt?id=prednasky%3Aprednaska07&cache=cache>.

[13] *IPv6* [online]. 2008 [cit. 2009-05-23]. Dostupný z WWW: <https://www.ipv6.cz/Vlastnosti_protokolu>.

[14] *UDP* [online]. 2006 [cit. 2009-04-15]. Dostupný z WWW: <http://pc-site.owebu.cz/?page=PRUDPTCP>.

[15] *VPN.muni.cz* [online]. 2007 [cit. 2009-04-11]. Dostupný z WWW: <https://vpn.muni.cz/#cojeto>.

[16] *Počítačové sítě model ISO/OSI* [online]. 2005 [cit. 2009-07-08]. Dostupný z WWW: <http://site.the.cz/index.php?id=4>.

[17] *Hodnocení informační bezpečnosti* [online]. 2006 [cit. 2009-07-06]. Dostupný z WWW: <https://akela.mendelu.cz/~lidak/share/snimky-bis/prednaska5.ppt>.

[18] Department of Defense. *Trusted Computer System Evaluation Criteria*. [s.l.] : [s.n.], 1985. 116 s. Dostupný z WWW: <http://csrc.nist.gov/publications/history/dod85.pdf>.

[19] The Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and General Model*. [s.l.] : [s.n.], 2009. 93 s. Dostupný z WWW: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R3.pdf>.

[20] The Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation : Part 2: Security functional*

components. [s.l.] : [s.n.], 2009. 321 s. Dostupný z WWW: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R3.pdf>.

[21] The Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation : Part 3: Security Assurance components*. [s.l.] : [s.n.], 2009. 232 s. Dostupný z WWW: <http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf>.

[22] SungKyunKwan University. *Firewall Protection Profile V2.0*. [s.l.] : [s.n.], 2008. 68 s. Dostupný z WWW: <http://www.commoncriteriaportal.org/files/ppfiles/FW%20PP-93-EN.pdf>.

[23] SANS. *Survival Time* [online]. 2009 [cit. 2009-06-30]. Dostupný z WWW: <http://isc.sans.org/survivaltime.html>.

[24] Juniper Networks. *SSG 140 Images* [online]. 1999-2009 [cit. 2009-06-06]. Dostupný z WWW: <http://www.juniper.net/us/en/company/press-center/images/image-library/ssg140/>.

Seznam obrázků

Obrázek 1: Firewall jako kontrolní bod mezi veřejnou a privátní sítí podle [10] 15
Obrázek 2: Ochrana vnitřní sítě jedním firewallem podle [9] 21
Obrázek 3: Ochrana sítě pomocí jednoho firewallu a bastion host podle [9] 22
Obrázek 4: Ochrana sítě s využitím DMZ podle [9] 23
Obrázek 5: Ochrana sítě pomocí dvou firewallů podle[9] 24
Obrázek 6: Datový provoz v síti s jedním firewallem podle [10] 25
Obrázek 7: Datový provoz v síti s jedním firewallem a bastion host podle[10] 26
Obrázek 8: Datový provoz v síti s jedním firewallem a DMZ podle [10] 27
Obrázek 9: Datový provoz v síti s dvěma firewally a DMZ podle [10] 28
Obrázek 10:Životnost defaultních instalací operačních systémů [23] 32
Obrázek 11 Vývoj kritérií hodnocení informační bezpečnosti [17] 34
Obrázek 12: Obecná struktura Profilu ochrany [19] 37
Obrázek 13:Poloha TOE [22] 39
Obrázek 14: Navrhovaný model sítě pro soukromou organizaci 67
Obrázek 15: Firewall Juniper Networks SSG 140 [24] 68

Seznam tabulek

Tabulka 1: TCP a UDP porty 12
Tabulka 2: Průměrný počet pracovních stanic 48
Tabulka 3: Průměrný počet firewallů 52

Seznam grafů

Graf 1: Rozdělení organizací dle velikosti 47
Graf 2: Rozdělení organizací podle velikosti a zaměření. 47
Graf 3: Existence dokumentu o bezpečnostní politice rozdělení dle I. kategorie. 48
Graf 4: Existence dokumentu o bezpečnostní politice rozdělení dle II. kategorie 49
Graf 5: Seznámení nových zaměstnanců s dokumentem BP rozdělení dle I. Kategorie 50
Graf 6: Seznámení nových zaměstnanců s dokumentem BP rozdělení dle II. kategorie 51
Graf 7: Použití firewallu v organizacích rozdělení dle I. kategorie 51
Graf 8: Použití firewallu v organizacích rozdělení dle II. kategorie 52
Graf 9: Umístění firewallu z hlediska architektury sítě rozdělení dle I. kategorie 53
Graf 10: Umístění firewallu v sítí z hlediska architektury rozdělení dle II. kategorie 53
Graf 11: Odborné školení administrátorů v organizacích I. kategorie 54
Graf 12: Odborné školení administrátorů v organizacích II. kategorie 55
Graf 13: Možnost jiného přístupu do sítě organizace I. kategorie 55
Graf 14: Možnost jiného přístupu do sítě organizace II. kategorie 56
Graf 15: Monitorovací systém pro nevědomou konfiguraci sítě v organizacích I. kategorie 57
Graf 16: Monitorovací systém pro nevědomou konfiguraci sítě v organizacích II. kategorie 58

Graf 17: Využívání IDS organizace I. kategorie 59
Graf 18: Využívání IDS organizace II. kategorie 60
Graf 19: Jiná síťová aplikace na firewallu organizace I. kategorie 60
Graf 20: Jiná síťová aplikace organizace II. kategorie 61
Graf 21: Průnik do počítačové sítě organizace I. kategorie 62
Graf 22: Průnik do počítačové sítě organizace II. kategorie 62
Graf 23: Anonymita organizací v průzkumu 63

Seznam příloh

Příloha 1 Dotazník

Příloha 1 - Dotazník

Dobrý den,

studuji Fakultu ekonomicko-správní na Univerzitě Pardubice obor Regionální a informační management. V současné době píši diplomovou práci na téma Firewally a síťová bezpečnost. Za tímto účelem si Vás dovoluji poprosit o vyplnění následujícího dotazníku týkajícího se firewallů a bezpečnostní politiky organizace.

Jsem si vědom, že tyto informace jsou pro většinu organizací velmi citlivé, proto prosím zaškrtněte v poslední otázce dotazníku, zda je možné zveřejnit název Vaší organizace v diplomové práci. Prohlašuji, že údaje vámi poskytnuté budou použity pouze pro účely mojí diplomové práce.

Otázky, které neodpovídají profilu Vaší organizace, prosím nevyplňujte. Vyplnění dotazníku by nemělo zabrat více než deset minut Vašeho času.

Dotazník bezpečností politika organizace

1. Kolik má Vaše organizace zaměstnanců?

do 50 **do 250** **250 a více**

2. Kolik je v organizaci evidovaných pracovních stanic?

zadejte počet:

3. Existuje ve Vaší organizaci dokument o bezpečnostní politice?
ANO NE

4. Jsou s tímto dokumentem o bezpečnosti seznamováni noví zaměstnanci?

ANO NE

5. Používá Vaše organizace firewall?

ANO NE

6. Pokud používáte firewall, kolik firewallů Vaše organizace využívá?

zadejte počet:

7. Pokud používáte firewall, kde je firewall umístěn z hlediska architektury sítě?

stručně popište:

8. Pokud používáte firewall, prošli administrátoři firewallů odborným školením?

ANO NE

9. Existuje jiný vnější přístup do sítě než-li skrz firewall (např. VPN apod.)?

ANO NE

10. Využíváte monitorovací systém pro nevědomou změnu v konfiguraci sítě?(např. připojení neznámého PC do sítě apod.)?

ANO NE

11. Využíváte Intrusion Detection System (IDP, IPS apod.)

ANO NE

12. Používáte-li soft.firewall na Linuxu (IP tables) nebo Windows 2003,
Windows 2008 Server, běží na nich ještě jiná síťová služba?

ANO NE