ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačních technologií

DIPLOMOVÁ PRÁCE

Internetová bezpečnost z pohledu uživatele

Vedoucí diplomové práce: RNDr. Dagmar Brechlerová, Ph.D.

autor práce: Jan Bozděch

-- zde bude originál či kopie zadání práce --

Prohlášení

Prohlašuji, že diplomovou práci na téma „Internetová bezpečnost z pohledu uživatele“ jsem vypracoval samostatně. Použitou literaturu a podkladové materiály uvádím v přiloženém seznamu literatury.

V Praze dne 1. dubna 2011 …….

Podpis

Poděkování

Rád bych poděkoval vedoucí diplomové práce RNDr. Dagmar Brechlerové Ph.D za přínosné rady, náměty a inspiraci při jejím samotném psaní. Dále bych rád poděkoval Bc. Renatě Žvejkalové za dodatečné gramatické korektury.

Internetová bezpečnost z pohledu uživatele

Internet security from the perspective of user

Abstrakt

Práce se obsahově zaměřuje především na důkladnou analýzu internetové bezpečnosti a její uplatnění v praktické rovině. Hlavními prvky analýzy je charakteristika a důkladné zmapování způsobů internetové komunikace, se zaměřením na síťově protokoly. Pomocí kritického hodnocení jsou vymezeny možné hrozby a útoky z pohledu síťové bezpečnosti a samotného uživatele. Jsou charakterizovány prvky a metody zabezpečení internetové a síťově komunikace. Cílem je formulovat a vytyčit nebezpečí, která těmto sítím hrozí z vnějšího síťového okolí a také možnosti ochrany před nimi ve formě fyzických či softwarových prostředků a politiky na administrativní úrovni. Hlavním úkolem praktické části je na základě teoretických poznatků a studia odborné literatury navržení komplexního zabezpečení malé podnikové a domácí sítě.

Abstract

The thesis focuses on a thorough analysis of Internet security and its application in practical terms. Main elements of the analysis are the careful characterization and mapping methods of Internet communication, focusing on networking protocols. With a critical assessment are identified potential threats and attacks from the perspective of network security and user. They are characterized by methods of Internet security and network communications. The aim is to formulate and highlight the danger that these networks threaten the external network environment and the possibility protection against them in the form of physical or software resources and policies to administrative level. The main task of the practical part is based on theoretical knowledge and study of literature, designing a complex security small business and home network.

Klíčová slova:

internetová bezpečnost, internet, sociální inženýrství, síťové protokoly, síťové služby, antivir, firewall, internetové hrozby a útoky, ochrana dat

Keywords:

internet security, internet, social engineering, web protocols, web services, antivirus, firewall, network threats and attacks, data protection

Obsah

1 Úvod

Internet, jako informační medium získává stále větší oblibu i praktické uplatnění mezi uživateli komunikačních sítí. Šíře jeho možností jako komunikační, vzdělávací, zábavní i komerční platformy je takřka neomezená. Z tohoto důvodu je dnes internet nejrozšířenějším komunikačním a informačním médiem současnosti.

Internet byl v prvopočátku plánován jako síť pro výměnu informací v rámci vědeckých pracovišť v armádním i civilním sektoru a na universitách. Jeho účelem bylo také v případě válečného konfliktu zamezit svým charakterem úplnému vyřazení komunikace v ozbrojených silách.

Počet připojených počítačů, hlavně z řad soukromých firem i domácností po roce 1993 neuvěřitelným způsobem vzrostl. Dnes již není ve většině zemí vyspělého světa pro nikoho problém připojit se k internetové síti.

V současné informační době se tak na internet přesouvá obrovské množství činností, které před tím vyžadovaly specifické platformy. Na internetu lze komunikovat prostřednictvím mnoha informačních kanálů - jako například pomocí elektronické pošty (e-mail) nebo některého z řady messengerů, které navíc v mnoha případech zvládají i přenos hlasu a obrazu. Je zcela běžné nakupovat přes internetové obchody, provádět bezhotovostní platby a převádět finanční částky mezi subjekty. Na internetu lze vyhledávat informace, zábavu ať již audiovizuální či interaktivní a mnohé jiné věci, které dříve vyžadovaly speciální služby či prostředky.

Všechny tyto nové možnosti přinášejí i značně nová nebezpečí a nové nároky na zabezpečení. Přesun množství obchodních činností a finančních transakcí na síť přilákal také značnou část působnosti organizovaného zločinu. Internet, jako nový druh prostředku zábavy, obchodu i práce, přinesl nový druh kriminální činnosti, respektive vedl k sofistikovanosti těch původních.

To je jeden z hlavních důvodů, proč jsem se rozhodl pro zpracování tématu internetové bezpečnosti a zajištění počítačových sítí. Dnešní uživatel internetové sítě má

již k dispozici značné množství bezpečnostních nástrojů, kterými lze ochránit počítač a svou domácí či firemní síť. Čelí také ovšem stále narůstajícímu počtu útoků zvenčí, na jeho soukromá a citlivá data. Tyto útoky, které bývají prováděny jednotlivci, či organizovanými skupinami, jsou jen těžko stopovatelné. Jejich frekvence a objem narůstá téměř přímo úměrně k nárůstu objemu množství citlivých dat, která se v síti internetu i na uživatelských stanicích nacházejí.

V první části práce je stručně popsána historie vývoje internetové sítě. Nastíněn je její původní smysl a následný vývoj v komerční a veřejné sféře. Na základě dostupné literatury i vlastních zkušeností jsou charakterizovány a vymezeny zásadní mezníky ve vývoji internetu, vysvětleny síťové principy a mechanismy. V další části se již práce zaměřuje na samotnou problematiku bezpečnosti internetu, jsou charakterizovány základní nezbytné prvky potřebné k zabezpečení internetových sítí, nadstandardní kroky i určitá doporoučení pro bezpečnou práci na internetu a ochranu citlivých dat. Součástí je analýza bezpečnosti internetu před útoky zvenčí a zmínění některých zásadních chyb, kterých se uživatelé dopouštějí. Další kapitola se zabývá konkrétními způsoby a metodikou zabezpečení internetových síti a to jak v rámci podniků a obchodních organizací, tak v rámci domácností. Provedena je také specifikace principů fungování firewallů, antivirových a anti-spywarových programů a dalších prvků softwarového zabezpečení.

V závěrečné, teoreticko-praktické části, je snahou a přínosem na konkrétních příkladech hrozeb či útoků proti internetové síti charakterizovat a definovat možnosti obrany. V případě již úspěšného napadení ukázat možnosti řešení nebezpečných či kritických situací. Mnohdy je možné napadenou síť zachránit i s daty, často ovšem, nejsou-li data adekvátně zálohovaná, či jsou-li poškozeny pevné disky, dochází ke ztrátě veškerých dat. V takových případech hrozí v krajním případě navíc i k jejich zneužití jinou stranou. V závěru práce dochází k vyhodnocení zpracování dané problematiky a splnění cílů práce, kterými je definice a charakteristika internetové sítě, její bezpečnosti i bezpečnostních rizik, návrh postupů pro její zabezpečení a případné konkrétní postupy při řešení problémů.

2 Cíl práce a metodika

2.1 Cíl práce

Hlavním cílem práce je praktický návrh zabezpečení počítačové sítě. Konkrétně se jedná o dvě entity - menší firemní síť společnosti, zabývající se kursovým sázením a sázením přes internet a dále malé domácí sítě. Na těchto příkladech práce charakterizuje konkrétní možnosti jejich zabezpečení i možná rizika, která mohou těmto sítím, s ohledem na jejich charakter, hrozit. Úvodem k tomuto praktickému návrhu, bude část praktická, která obsahuje vymezení pojmu internet, dále pak vymezení jeho historie a základních stavebních prvků. Dále deskripce a zhodnocení hrozeb a bezpečnosti v rámci této sítě, tak jak se s nimi může setkat uživatel. V praktické části je názorně ukázán postup a vymezení možnosti řešení bezpečnosti internetové komunikace a problémů s útoky na integritu a bezpečnost sítě. Na příkladu zabezpečení konkrétních sítí jsou navrženy konkrétní příklady zabezpečení a obrany, s následným řešením případných vzniklých komplikací.

2.2 Metodika

Teoretická východiska jsou prezentována na základě dostupné a doporučené literatury a jejího studia. Na tomto základě je charakterizována nejprve historie a principy fungování sítě internet. Dále její jednotlivé součásti, jako například protokoly. Tato část je založena na deskriptivní charakteristice metod fungování internetové sítě, stejně jako další kapitoly teoretických východisek. Dalšími popisovanými skutečnostmi budou rizika, která mohou ohrozit integritu a bezpečnost internetové sítě a to převážně zvenčí, stejně tak jsou na základě nastudované literatury popsány a definovány prostředky jejich zabezpečení. Tyto prostředky budou popisovány jak na základě typologie, tedy jedná-li se o hardwarový či softwarový prostředek, tak také podle vrstvy síťového rozhraní, na které jsou umístěny.

Praktická část a návrhy postupů a řešení vycházejí taktéž z dostupné literatury a zkušeností jak uživatelů, tak správců sítě. Na základě teoretických východisek je deklarován způsob zabezpečení zmíněné firemní sítě. Nejprve dochází k charakteristice konkrétních sítí, jejich funkce a rozsáhlosti. Poté je na základě vyhodnocení potenciálních rizik navržen způsob jejich zabezpečení, tak aby byla zajištěna jak jejich integrita, tak bezpečnost a přitom nebyly kladeny přehnané nároky na finanční výdaje,

jak na pořízení, tak na provoz. Veškeré návrhy vycházejí z charakteru sítě a tedy možné míry ohrožení a míry citlivosti dat.

Na základě komparace obou sítí jsou poté vyvozeny konkrétní závěry.

3 Charakteristika a historie internetu

Tato část se stručně věnuje historii internetu a principům jeho fungování. Snahou je pomocí charakteristiky tohoto fenoménu přiblížit jeho užitečnost a zároveň zranitelnost a zneužitelnost v dnešní moderní informační éře.

3.1 Vývoj internetu.

Historie internetu sahá do 70. let 20. století. Ve Spojených státech během studené války vznikla potřeba nového komunikačního centra. Respektive center. Vojenskou strategií při okupaci či útoku je vždy obsadit či zničit komunikační uzly nepřítele. Ministerstvo obrany USA tak přišlo s myšlenkou vytvoření komunikačních center, která by byla na sobě nezávislá a v případě útoku a po možném zničení některého z nich by ostatní zůstala schopna vzájemné komunikace. Tímto mělo být zamezeno znemožnění komunikace v případě napadení. (CEJPEK, 2005)

Toho mělo být dosaženo vzájemným propojením komunikačních uzlů (serverů a počítačů) fungujících na principu TCP/IP protokolu a nesoucí název ARPANET. Ten byl nejprve provozován na základě propojení 4 uzlů, počítačů. Tyto uzly, rozmístěné různě po světě spolu mohly vzájemně komunikovat nezávisle na všech ostatních, tedy výpadek jednoho či dvou, nevyřadil celou komunikaci, navíc mohly být programovány z jiných uzlů.

Sloužil primárně k přenášení složitých výpočtů mezi vědci a výzkumníky a k provádění těchto výpočtů. Později se počet uzlů rozrostl na 15 uzlů, 37 uzlů a jeho charakter se poměrně nepozorovaně měnil. Výzkumníci daleko více používali tuto síť jako jakousi soukromou poštu a diskusní fóra. Výhoda této sítě totiž byla její decentralizace, na rozdíl od podnikových sítí a sítí institucí na ni bylo možné připojit jakýkoliv počítač, který reflektoval paketový princip přenosu dat. (BARTOŠEK, 1995)

Původním protokolem ARPANETu byl protokol NCP (Network Control Protocol) ovšem s rozvojem technologií byl nahrazen TCP/IP protokolem, který byl propracovanější a byl základem pro síť internet. Jeho princip je popsán níže. V průběhu 70. a 80. let se k síti ARPANET připojovalo stále více uzlů. Bylo to způsobeno

dostupností počítačů pro stále širší sociální skupiny obyvatel. Navíc celému procesu od počátku nahrávala již zmíněná decentralizace sítě a její, i když možná úplně nezamýšlená, „anarchistická“ podstata.

V roce 1987 předala armáda tento projekt také civilním složkám, konkrétně výzkumným laboratořím a univerzitám a vznikla tak síť NSFnet (National Science Foundation net). Připojení pomocí této sítě předznamenalo internetovou podobu do formy, jak jí známe dnes. Umožnilo lepší využití TCP/IP protokolu a v důsledku toho také připojování stále výkonnějších počítačů na sítě se stále rychlejším přenosem dat než tomu bylo u sítě ARPANET. Rozvoj internetu na této platformě poté pokračoval krátký čas periodicky v letech 1986, 1988 a 1990. NSFnet tvoří páteř internetových přenosů ve Spojených státech i dnes, kdy se přidaly v průběhu vývoje ještě instituce NASA, Národní zdravotnický institut a další, jež zapříčinily vznik domén typu *edu., mil., gov., com., org.*

3.1.1 Standard provozu sítí ISO/OSI

Je mezinárodní standard pro provoz komunikace v rámci sítí. Tento model se skládá ze 7 vrstev pracujících na uskutečnění datového přenosu. Přenos zde probíhá formou datových rámců, které ve svém záhlaví nesou adresu cílového uživatele i odesílatele. Těchto sedm vrstev má za úkol vzájemně spolupracovat na přenosu datových rámců tak, aby nižší vrstva usnadňovala práci vyšší síťové vrstvě bez zatěžování daty o způsobu provedení.

Těmito vrstvami jsou (DOSTÁLEK, 2000):

Aplikační vrstva – realizuje aplikačně orientované služby, podporuje různá aplikační rozhraní pro implementaci elektronické pošty, přenosů souborů apod. Její součástí bývají i přímo procesy, které tyto aplikační funkce plní.

Prezentační vrstva – provádí aplikační funkce, které se požadují dostatečně často na to, aby se pro ně vyplatilo najít obecné řešení místo toho, aby každý uživatel hledal jejich řešení sám. Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována.

Relační vrstva - je zodpovědná za synchronizaci a správné řazení paketů v síťovém spojení, za udržení spojení, za zajištění odpovídající bezpečnosti přenášených dat.

Transportní vrstva - zaručuje adresování koncových komunikujících zařízení působících v uzlech sítě a kvalitu přenosu mezi nimi.

Síťová vrstva - je označována jako paketová. Úkolem je určit jednoznačnou adresu či přeložit hardwarovou adresu na síťovou, nalézt směr (optimální cestu) od zdroje k cíli, zajistit a udržet logické spojení mezi dvěma uzly.

Linková vrstva - má za úkol zajistit přenos celých bloků dat (velikosti řádově stovek bajtů), označovaných jako rámce. Řeší se zde i problém soupeření při přístupu k sdílenému přenosovému médiu při žádostí vysílat, tedy nastavení priority pro odeslání.

Fyzická vrstva - zajišťuje přenos na úrovni jednotlivých bitů bez ohledu na jejich význam. Úkolem je předávat tyto bity mezi jednotlivými stanicemi prostřednictvím fyzické přenosové cesty.

V praxi se ovšem v rámci internetu používá ve většině případů protokolů TCP/IP a operace na bázi ISO/OSI probíhají v rámci firemních vnitřních okruhů na některých aplikacích.

3.2 Protokoly síťové komunikace

3.2.1 TCP/IP protokol

Jedná se o soubor protokolů a podprotokolů, na jejichž základě probíhá komunikace a datový přenos mezi stanicemi. Přenos je na počítačích a mezi nimi prováděn na několika vrstvách. Patří sem fyzická a linková vrstva zajištující spojení fyzicky a dále síťová, transportní, relační, prezentační a aplikační vrstva. Protokol TCP/IP se o první dvě zmíněné nezajímá. Přenos poté probíhá formou IP-paketů. Každý paket obsahuje v záhlaví informace o adresátovi, jeho adresu, dále data a také informace o odesílateli. Proto je přenos pomocí TCP spolehlivější než pomocí UDP protokolu, které mohou na počítačích probíhat souběžně. Tedy, protokol UDP, který nepotřebuje

navazovat spojení, pro přenos diagramu, tím zajišťuje menší spolehlivost při doručování. UDP chápe Datagram jako samostatný celek, TCP/IP dokáže rozlišit a brát diagramy i jako součásti většího celku, proto je jejich doručování spolehlivější. Také potřeba TCP navázat před odesláním diagramu spojení s adresátem, a tím ověření jeho dostupnosti, zvyšuje tuto spolehlivost a přesnost adresování. Výhodou protokolu UDP, může ovšem být jeho rychlost, tím že je relace nestavová, tedy neověřuje, je - li adresát připojen či ne, může zasílat diagramy podstatně rychleji. Dále má tento protokol dobré využití ve vnitřních sítích, díky schopnosti doručit diagram více adresátům, nejen konkrétní IP adrese a konkrétní stanici, což bývá využíváno při zasílání například oběžníků.

Problémem tohoto protokolu, a to vcelku zásadním, byl fakt, že při jeho návrhu nebyl brán ohled na bezpečnost, respektive zabezpečení toku dat. Data nejsou chráněna na síťové vrstvě, proto může docházet k jejich ztrátě. Sama o sobě pomocí protokolu nejsou tato data šifrována a to často ani v rámci autentifikace uživatele pomocí šifrovaného hesla.

Proto TCP/IP běží dnes jako soustava přídavných protokolů a podprotokolů, jako je například SSL šifrování, které funguje mezi aplikační a transportní vrstvou a rozšíření protokolu IP pojmenované IPSec, které pracuje přímo na síťové vrstvě a aplikační vrstva tak na jeho běh nemusí brát zřetel.

3.2.2 IP protokol

Tento protokol slouží k přenosu dat mezi jednotlivými stanicemi internetu, tedy i přes mnohé LAN sítě, a to pomoci IP diagramů. Při přenosu se tento datagram vkládá do datové části rámce, se kterým pracuje bezprostředně nižší vrstva - vrstva síťového rozhraní. V hlavičce jsou pak různé řídící informace, potřebné pro doručení datagramu (rámce), jde mj. o fyzickou adresu skutečného odesílatele a bezprostředního příjemce, zatímco v hlavičce IP datagramu jde o IP adresy koncového příjemce a původního odesílatele. Jelikož v datovém rámci mohou být v principu přenášeny i jiné druhy paketů, musí zde být vyjádřeno také to, o jaký konkrétní druh paketu se v daném případě jedná. V každém diagramu jsou podstatné informace jako IHL, což označuje délku hlavičky diagramu (záhlaví), která by měla být vždy násobkem 4, v případě, že

násobkem čtyř není, doplní se obsahem, který nemá na samotný „obsahový smysl“ diagramu žádný vliv.

Dále je to údaj o typu služby, toto ovšem v praxi valný přínos nemělo, účelem mělo být určité nastavení priority pro diagramy, v případě malé šířky pásma. Celková délka poté obsahuje údaj o celkové délce diagramu v bajtech. Dalšími údaji jsou ještě identifikace IP diagramu, kdy je vkládán identifikátor operačním systémem odesilatele a také údaj o celkové životnosti, který slouží pro jednotlivé brány jako pojistka proti obíhání diagramu v síti do nekonečna. Poměrně důležitými kontrolními údaji jsou poté IP adresy odesílatele a adresáta, podle kterých diagram v síti vymezuje svou trasu (DOSTÁLEK, 2000)

3.2.2.1 ICMP protokol

Tento protokol je součástí protokolu IP, slouží k signalizování mimořádných událostí. Jeho účelem je zjistit a signalizovat informace o dostupnosti adresáta. K odpovědi slouží příkaz „ping“ který je na dotaz zaslaný ICMP protokolem nucený odpovědět. Toto slouží k zjišťování nedoručitelnosti datagramu, kdy je tento posléze „zahozen“, zadává podnět ke snížení přenosové rychlosti, je-li adresát nedostupný či špatně dostupný. Případně podává informaci o přesměrování, k čemuž dochází v sítích s více routery, kdy jsou počítače sítě nastaveny na položku „default“ definující jeden ze směrovačů.

3.2.3 UDP protokol

Jedná se o nespojovanou alternativu TCP/IP protokolu, tedy odesílatel zde nenavazuje spojení, odešle svá data do sítě a nestará se, zdali dorazí či se ztratí. Umožňuje ovšem pomocí kontrolního součtu identifikovat případné chyby v přenosu. Bohužel UDP protokol stále neumí odeslat potvrzující informaci o přijetí, tudíž samotný neumožňuje zjistit případnou ztrátu dat. Klade proto větší důraz na aplikace, které se musí samy postarat o potvrzení příjmu datového paketu. Tyto aplikace jsou však jednoduché a nevyžadují trvalé spojení, proto je jejich předností jednoduchost a rychlost.

3.2.4 DNS

Jedná se o tzv. Systém doménových jmen (Domain name server), který byl v rámci IP protokolu utvořen pro jeho zpřehlednění a ucelení, v rámci rozvoje internetu jako celosvětového média. Každému uzlu, či stanici je přidělována konkrétní adresa, a to v číselném formátu. Tento číselný formát se ovšem velmi těžko pamatoval. Zvláště pokud měl uživatel větší množství kontaktů, tedy adres v zmíněném číselném formátu. DNS slouží k překladu těchto číselných adres na adresy jmenné, které jsou na základě práv přidělovány DNS serverem. Tak je každá číselná IP adresa charakterizována také jmennou doménou, což ji pro běžného uživatele činí zapamatovatelnější a podle stanovené domény ji může také lépe charakterizovat. To platí samozřejmě pro uživatele, nikoliv pro síť. Každý uzel má pak svou doménu, které se poté mohou dělit na subdomény. Každá z nich je pak v adrese podle jejich počtu oddělena tečkou. V praxi je zadávání jmenných domén pohodlnější a snažší, ovšem v případě, máme-li podezření či víme, že na stanici DNS nepracuje korektně, je lepší použít IP adresu v číselném formátu. Tyto domény jsou poté shromažďovány na name serverech, které mají možnost reverzního převodu jmenných domén na IP adresy a které přiřazují domény novým uživatelům. (DOSTÁLEK, 2000)

3.2.5 SSL a metody šifrování

SSL Secure Socket Layer - je šifrovací vrstva, která bývá již takřka zpravidla vkládána mezi transportní a aplikační vrstvu, tedy mezi vrstvu používající např. TCP/IP protokol a vrstvu pro poštovního klienta či webový prohlížeč (SMTP, HTTP). SSL vrstva zabezpečuje data právě mezi těmito vrstvami, paket po paketu je šifruje a zasílá je zabezpečené adresátovi.

Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.). Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru. (HALLER, 2006)

Šifrování dat je proces převedení těchto dat z jejich čitelné podoby do nečitelné. K tomu slouží algoritmy, kterými jsou daná data na internetu či některém z disků

šifrována a přístup k nim má jen uživatel, který zná přístupové heslo nebo je držitelem vhodného klíče.

Klíčem je nazýván řetězec znaků, který je použit při matematické operaci zvané šifrování či dešifrování. Zde záleží, jedná-li se o symetrické či asymetrické šifrování. Symetrické šifrování využívá pro šifrování/dešifrování jeden klíč. Podstatnou výhodou symetrických šifer je jejich nízká výpočetní náročnost. Algoritmy pro šifrování s veřejným klíčem jsou často i stotisíc krát pomalejší. Naopak základní nevýhodou symetrického šifrování je distribuce klíče, respektive bezpečného přenosu klíče tak, aby se ho nemohl chopit někdo nepovolaný.

Asymetrická kryptografie má výhodu používání dvou klíčů (soukromého a veřejného). Veřejný klíč je volně šiřitelný a uživatelé mohou s jeho pomocí šifrovat data pro druhou stranu, která pro jejich dešifrování užije svého soukromého klíče. I přes jistou matematickou svázanost obou klíčů je nejdůležitější vlastností praktická nemožnost ze znalosti šifrovacího (veřejného) klíče spočítat dešifrovací (soukromý) a tím se neoprávněně dostat k datům. Strana, která šifruje zprávu, navíc nemusí s příjemci zprávy udržovat žádné tajemství, čímž se eliminuje potřeba výměny klíčů.

Matematicky asymetrická kryptografie postupuje následujícím způsobem:

Šifrování: $c = f(m, e)$

Dešifrování: $m = g(c, d)$

kde m je zpráva, c zašifrovaná zpráva, e šifrovací klíč, d dešifrovací klíč.

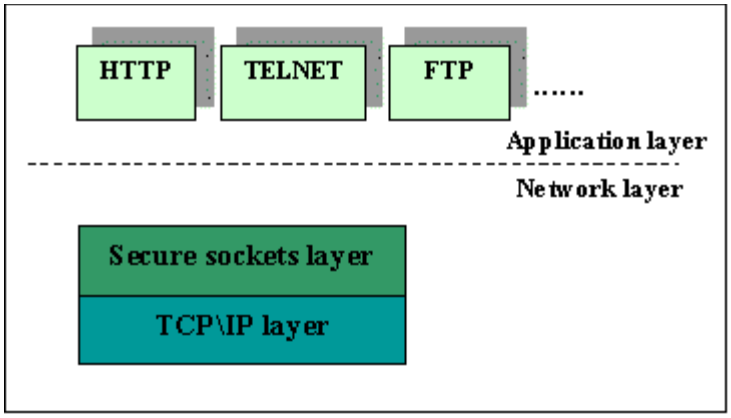
Certifikát, který je přijímán či odmítán při navazování zabezpečeného spojení, je vlastně certifikační autoritou podepsaný veřejný šifrovací klíč. Je to elektronický dokument, který spojuje identitu vlastníka veřejného klíče s jeho veřejným klíčem. Slouží k identifikaci protistrany při navazování spojení a jeho důvěryhodnost je zaručována příslušnou autoritou – třetí stranou tzv. certifikační autoritou (dále CA). CA je důvěryhodná třetí strana, která svým podpisem certifikátu stvrzuje, že klíč patří skutečně danému subjektu, proto je její kvalita a bezpečnostní úroveň pro celý proces velmi důležitá. Pokud dostanu zprávu od uživatele XY a zpráva je podepsána jeho

certifikátem, který vydala CA, tak CA ručí za to, že certifikát byl vydán právě uživatelem XY a nikdo kromě něj nemohl vytvořit příslušný podpis.

Protokol SSL byl původně vyvinut firmou Netscape, poté převzat organizací IETF pod názvem TSL (Transport Security Layer). Tento protokol zabezpečuje šifrování a autorizaci přístupu na úrovni transportní vrstvy modelu OSI. Je implementován výhradně na koncových uzlech sítě. To dovoluje aplikacím na těchto uzlech vyměňovat aplikační pakety šifrované před přenosem po transportní vrstvě. Pro protokol SSL/TSL je charakteristické použití asymetrického šifrování Protokol SSL se dělí na dvě základní vrstvy:

1. HP (Handshake Protocol) je protokol pro výměnu bezpečnostních informací potřebných pro tvorbu šifrovaného transportního spojení. Jsou přenášeny informace ohledně typu symetrického šifrovacího algoritmu, komprimačního algoritmu a data pro výpočet bloku klíčů.

2. RLP (Record Layer Protocol) je nosným protokolem SSL/TSL. Pakety přebírá od aplikační vrstvy, dělí na fragmenty o maximální délce 2^14 B, komprimuje, dopočítává dohodnutým algoritmem kontrolní součet (MAC), zašifruje datovou část fragmentu a přidá 5B záhlaví RLP.



Obrázek 1 - Pozice protokolu SSL v TPC/IP modelu zdroj: http://www.svetsiti.cz, 20.2.2011

Ustavení SSL spojení probíhá následovně:

1. Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
2. Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
3. Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
4. Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude šifrovat následná komunikace. Ten zašifruje veřejným klíčem serveru a pošle mu ho.
5. Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
6. Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
7. Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
8. Aplikace od teď dál komunikují přes šifrované spojení. Například POST požadavek na server se do této doby neodešle.

3.3 IPSec

IPSec je rozšíření IP protokolu, které poskytuje bezpečnost pro IP protokol a protokoly vyšších vrstev. Nejdříve se vyvinul pro nový standard IPv6 a následně byl zpětně implementován na IPv4. IPSec architektura je popsaná v RFC2401 - Security Architecture for the Internet Protocol. Několik následujících odstavců poskytuje krátký úvod do IPSec technologie. V IPv4 bylo užití IPSec uživatelsky volitelné, v novějších IP nové generace verze 6 je použití povinné.

IPSec užívá dva rozdílné protokoly-hlavičky (AH a ESP), aby zajistil ověřování identity, neporušenost a důvěryhodnost komunikace. Může chránit buď celý IP datagram, nebo pouze protokoly vyšší vrstvy. Příslušné módy se nazývají tunelový mód a transportní mód. V tunelovém módu je IP datagram plně zapouzdřený do nového IP datagramu, který používá IPSec protokol. V transportním módu je pouze užitečná část

IP datagramu zpracovaná IPSec protokolem tím způsobem, že se vkládá IPSec hlavička mezi IP hlavičku a hlavičku protokolu vyšší vrstvy.

Pro ochranu důvěryhodnosti IP datagramů IPSec protokoly užívají standardní symetrické šifrovací algoritmy. IPSec standard požaduje zavedení NULL a DES. Dnes jsou však obvykle užívané silnější algoritmy jako 3DES, AES a Blowfish.

Pro ochranu proti útokům typu DoS (Denial of Service), což je útok využívající chyb v programech či hardware, které jsou často uveřejňovány na stránkách výrobce či bezpečnostních konferencích a fórech. IPSec protokoly užívají tzv. okno. Každému paketu je přiřazeno sekvenční číslo a je přijatý, pouze jestliže číslo paketu je v rámci daného okna nebo novější. Starší pakety jsou okamžitě zrušeny. Toto chrání proti útokům založeným na opakování paketů, kdy útočník zaznamená původní pakety a přehraje je později v naději prolomení obrany. Obzvláště toto ocení majitelé internetového bankovnictví, kdy šifrování zamezí opakování datagramu s přidanou hodnotou pro výši částky.

Pro správnou funkci IPSec je nutné zajistit vzájemnou výměnu klíčů mezi komunikujícími stranami. Toto lze provést buď ručně, nebo pomocí protokolu IKE (Internet Key Exchange) pro dynamickou správu klíčů. (STALLINGS, 2003) (PEŠA, 1999)

IPSec jako takový je ovšem už od začátku svého vývoje poměrně chybový a jeho implementaci podpořilo spíše konsenzuální rozhodování v rámci firmy, než samotná spolehlivost.

3.3.1 HTTP protokol

Jedná se o protokol, který běží na protokolu TCP/IP, jeho předchůdcem před rokem 1990 byl Gopher. Hypertext transfer protokol, jak z ní název zkratky HTTP, je protokol, který je primárně určený k vyhledávání v síti internet/intranet.

Komunikace protokolu HTTP probíhá na úrovni klient/server a to oboustranně. Klient protokolem odešle dotaz na server pomocí identifikátoru (URI) a server požadavek zpracuje, vyřízne jeho název a pomocí zjištěné IP adresy ji přes DNS databázi převede jako informaci pro uživatele, čímž zpravidla dochází k zobrazení

požadované webové stránky. Starší verze HTTP navazovaly spojení zvlášť pro každý dotaz, napoprvé se zobrazilo jen jádro stránky s dalšími odkazy a při každém dalším dotazu bylo třeba navázat spojení nové. Novější verze již počítají s navázáním spojení přes TCP jednou pro více relací.

Protokol je bohužel omezen pouze na relaci klient - server, neumožňuje zasílání asynchronních událostí ze serveru klientovi. Zásadním problémem HTTP protokolu je ovšem jeho nemožnost zabezpečení formou autentifikace či šifrování. To poté musí být řešeno protokolem HTTPs, které běží na modulu SSL/TLS a klient je nucen mít certifikát, tedy veřejný šifrovací klíč, který užívá ke své autorizaci. Navíc jeho schopnost projít firewally ho činí terčem pro nosiče útočných programů, virů a podobně.

3.3.2 Poštovní protokol SMTP

Protokol SMTP definuje přenos zpráv elektronické pošty prostřednictvím přenosu sedmi bitových ASCII znaků formátovaných do řádků s oddělovači vytvořeným transportním spojením TCP. Znaky jsou přenášeny v bytech s přidanou nulou zarovnanou zleva. Opět se jedná o relaci klient/server, která je navazována na portu 25. Komunikace probíhá tak, že klient MUA (Mail User Agent) předá zprávu prvnímu MTA (Mail Transfer Agent) zabezpečujícímu poštovní provoz v doméně odesílatele a ten ji pošle dále na příslušný MTA, spravující poštu v doméně adresáta zprávy.

Problémem tohoto protokolu může být množství jeho omezení, nejzásadnější je nutnost dostupnosti klienta (adresáta). Pokud ten dostupný není, protokol celou relaci vyhodnotí jako chybu a pokouší se o opakované doručení. Doručení koncovému adresátovi zajišťují jiné protokoly a to nejčastěji POP3 (Post Office Protocol, verze 3), nebo IMAP (Internet Message Access Protocol), které slouží pro získávání pošty ze samotného poštovního serveru.

Přenos dat přes SMTP, je stejně jako u HTTP primárně nezabezpečený, je možné protokol odposlouchávat a neumožňuje navíc ověření identity odesílatele, což umožňuje zasílání závadných či nebezpečných dat z adres na první pohled důvěryhodných, pokud uživatel nevyužije možnost prozkoumání cesty přes poštovní servery. Proto je i zde vhodné používat alespoň SSL šifrování. (DOSTÁLEK, 2000)

3.3.3 POP3 protokol a IMAP

Jak již bylo uvedeno, slouží pro stahování poštovních zpráv z poštovních serverů. Jeho užití bylo nevhodnější v dobách navazovaného (např. vytáčeného) připojení. Šlo stáhnout poštu ze serveru a poté ji již v klidu číst v offline režimu uloženou na disku. Problémem je zde ovšem horší možnost správy a třídění stahované pošty, protokol stáhl veškerou adresovanou poštu i s případným spamem a zároveň duplikoval obsah serveru. Dalším protokolem pro stahování a práci se samotnou poštou je IMAP4. Ten na rozdíl od POP3 pracuje s poštou přímo na serveru, jako by byla uložena na lokálním disku, to omezuje majitele navazovaného připojení, ovšem umožňuje lepší práci s poštou a její třídění, aniž by ji bylo nutné i se spamem stahovat na disk. Nedochází také k nežádoucím duplikacím.

3.3.4 FTP protokol

Tento protokol slouží k přenosu souborů v počítačových sítích na bázi TCP/IP. Je využíván buďto správci serverů, kteří pracují přímo v serverovém operačním systému anebo běžnými uživateli k přenosu a sdílení souborů.

FTP a jeho uživatelské rozhraní předává vrstvě interpretu příkazů žádost ve formě požadavku, který je definován normou FTP a vyplývá ze samotného operačního systému. Protokol FTP umožní v hostitelském počítači vyhledávat soubory a kopírovat soubory na hostitelský počítač nebo z něj. K hostitelskému počítači se je většinou nutno přihlásit pomocí jména a hesla - je nutno mít na tomto počítači zřízen účet. Existují však i servery, které umožňují přihlášení i anonymnímu uživateli, který poté však nemusí mít přístup ke všem souborům na tomto serveru. Tyto anonymní FTP servery slouží právě široké veřejnosti ke sdílení vlastních či firemních dat. Značná část souborových manažerů typu Total Commander má ve svém systému zabudováno FTP rozhraní sloužící k přenosu dat v rámci lokální vnitřní sítě, či k jejich ukládání na internetové FTP servery pro lepší dostupnost, či úsporu místa na lokálním pevném disku.

4 Vymezení a analýza bezpečnosti internetu

Internet jako komunikační a informační médium, obzvláště na přelomu tisíciletí, zaznamenal obrovský růst a rozvoj. Rozšířil se takřka do celého světa a ve vyspělých zemích má téměř každá rodina možnost připojení se k této síti. Pozitivní trend s sebou ale nese značná rizika a nové hrozby. Internet byl terčem mnoha útoků již od samého počátku, ovšem s přesunutím velkého počtu sociálních i komerčních činností na jeho platformu se stal terčem ještě mnohem lákavějším.

Možnost internetu provádět platební a jiné finanční operace v řádu vteřin, maximálně dní, láká mnohé k přesunu trestné činnosti právě na tuto platformu. Zdání naprosté anonymity a mnohdy nemožnosti naprosto spolehlivé autentifikace otevírá lidem, kteří se šířením internetových hrozeb, útoků či poplašných situací zabývají zcela nové pole působnosti. Přesun na internet zaznamenalo dokonce i odvětví organizovaného zločinu či terorismu, který zavedl nový termín kyberterorismus.

Podle analýzy nárůstu internetového zločinu a kvality zabezpečení sítí, je tento druh zločinu na vzestupu a hlavně se stává sofistikovanějším.

Na základě získaných informací (KRČMÁŘ, 2010) je zřejmé, že podnikové sítě nejsou dostatečně chráněné před internetovými červy. Domácí uživatelé častěji čelí potenciálně nežádoucím programům a internetovým podvodům. Za druhé pololetí roku 2010 například výrazně stoupl počet odchycených „nigerijských podvodů“ (odesílatel slibuje podíl na penězích uložených v bance, pro jejich získání je ale nutné zaslat určitou částku na odesílatelem specifikovaný účet). Vzrostl také počet falešných antivirových aplikací, které slibují ochranu počítače zdarma, ale místo toho do počítače nainstalují škodlivý software. Pokračuje také šíření útoků pomocí předem sestavených sad nástrojů, které umožňují spuštění internetového útoku a úspěšné napadení cizího počítače i lidem bez technických znalostí. Například sada nástrojů Eleonore cílí (KRATOCHVÍL, 2010) na zranitelná místa několika webových prohlížečů a zároveň se snaží najít slabé místo i v aplikacích, které se vyskytují na většině osobních počítačů. Tyto sady nástrojů pro internetové útočníky mají formu komerčního softwaru a jejich tvůrci své produkty pravidelně aktualizují a zdokonalují tak, aby se co nejlépe dokázaly vyhnout odhalení ze strany bezpečnostních aplikací. (Microsoft, 2010)

V této kapitole je tak na základě dostupných zdrojů provedena analýza bezpečnosti internetu. Nejprve jsou vymezeny hrozby, které se týkají jednotlivých vrstev sítě, následně jsou popsány detailněji hrozby programů typu virů, červů, spyware, keylogger a dalších. Na závěr je provedeno vyhodnocení jejich závažnosti.

První ohroženou vrstvou je vrstva síťového rozhraní. Jak bylo uvedeno výše, jedná se o fyzické provedení sítě, pomocí kabelů, konektorů, modemů síťových adaptérů aj. Na nich rozlišujeme několik typů sítí, nejznámější jsou dvě, a to LAN a WAN. Nejvýznamnější hrozby na této vrstvě jsou přerušení spojení/komunikace, rušení komunikace, odposlech sítě či modifikace, tedy úprava přenášených dat.

4.1 Odposlech sítě

Samotné útoky dělíme na aktivní a pasivní. Účelem pasivního typu útoku je získávání a shromažďování informací o našem počítači a naší síti. Jejím prostředkem je právě odposlech sítě anglicky Spoofing či Wiretapping. Útočník se snaží získat co nejvíce informací o obsahu našeho počítače, o tom co na síti děláme, v jaké frekvenci a jakým způsobem. Tato metoda se dá přirovnat k odposlechu telefonu či monitoringu pošty, koneckonců v elektronické podobě pošty to tak opravdu funguje. Útočník shromažďující data tak o nás může zjistit mnoho věcí, které mu pomohou poznat náš charakter a charakter práce na síti, přístupu k bezpečnosti a případně lépe připravit následný aktivní útok.

Pro takovýto odposlech je třeba získat přístup ke kabeláži popř. k nezabezpečené síti (velmi zranitelné v tomto bývají nezabezpečené Wi-fi sítě či přenosy Bluetooth) a poté již není problém pomocí speciálních programů provádět tento monitoring. Může tak sledovat všechny datové packety v síti, která bývá často nešifrovaná. Pro postiženého běžného uživatele je tento hardwarový typ odposlechu takřka nezjistitelný, protože nedochází k aktivnímu poškozování počítače, dat či síťového příslušenství. Nejzranitelnější jsou po získání přístupu k síťové vrstvě právě výše zmíněné protokoly (HTTP,SMTP,POP3) které nemají vlastní zašifrovaný způsob přenosu a je třeba využití šifrovacích modulů SSL či některého z algoritmů. (BISHOP, 2002)

4.1.1 Odposlech hesel a modifikace přenášených dat

Autentizace uživatele je častým cílem jak pasivních, tak aktivních útoků. K jeho zjištění se využívá různých metod a postupů od naprosto elementárních lidských až po sofistikované programové.

Nejlehčím způsobem je odkoukání hesla. Nedává-li si uživatel pozor při psaní hesla, píše-li si ho i s popiskem, který ho konkrétně přiřazuje ke službě například na papírek u monitoru, do peněženky či mobilu, může se lehko stát, že ho útočník nechtěně nebo cíleně objeví takřka bez práce.

Další metodou je útok hrubou silou. Útočník se snaží většinou automaticky vygenerovat všechna možná hesla a uhodnout tak správné. Proniknutím do záznamů logovacích souborů se tato cesta značně ulehčuje, heslo musí být někde fyzicky uloženo a útočníkovi se může podařit jej získat právě z tohoto umístění. Pokud by heslo bylo uloženo v nezakódované podobě, útočník by tak mohl s vynaložením minimálního úsilí získat požadovaný přístup. Většinou jsou však tyto hesla uložena v zašifrovaném tvaru. Pro jejich rozšifrování může útočník opět použít metodu útoku hrubou silou, kdy se bude pokoušet generovat náhodná hesla, nebo na základě informací o dané osobě bude zkoušet „jednoduchá“ slova. Uživatelé často používají jednoduchá slova, či jména blízkých nebo často používaných věcí, převážně z důvodu zapamatovatelnosti. Pokud takto ovšem činí a útočník má například z předchozího odposlechu sítě informace o jejich osobě, může být pro něj odhalení hesla poměrně snadnou záležitostí.

Často bývají k získání hesla použity programy monitorující stisknuté klávesy na klávesnici. Tyto keyloggery se dělí na dvě skupiny, starší jsou softwarového charakteru a můžete se jimi infikovat podobně jako spyware. Jejich účelem je usídlení se v operačním systému a zaznamenávání a odesílání zpráv na vzdálené stanice. Primárně mají monitorovat stisknuté klávesy i ty funkční, ovšem některé dokáží zaznamenávat i pohyb a kliknutí kurzoru myši. To samozřejmě umožňuje zachycení hesel, PIN kódů, síťové komunikace (Skype, ICQ) navštívené webové stránky a mnoho dalších funkcí. Dalšími modernějšími typy jsou hardwarové keyloggery, které reagují na vývoj softwaru proti škodlivému obsahu sítě. Jedná se například o prodloužení kabelu, které se zapojí mezi počítač a klávesnici, není odhalitelné pomocí softwaru a ani běžný

uživatel, pokud neví co a kde hledat, má mizivou šanci toto zařízení objevit. Jeho výhodou je, že není závislé na volbě operačního systému, což mu dále umožňuje zachytit znaky ihned po zapnutí počítače, tedy i hesla do biosu a jiných systémů. Takovýto program se může dostat do počítače různými způsoby, často si jej nainstaluje nevědomky sám uživatel např. prostřednictvím trojského koně. Vděčnými stránkami, ze kterých se šíří, jsou různé stránky s popiskem Adult, warez stránky, či hazardní stránky a další podobné, které pro zobrazení dalšího obsahu vyžadují stažení a instalaci dalšího souboru či pluginu, který bývá zpravidla infikován. Na Internetu je k dispozici celá řada takovýchto programů, asi mezi nejznámější patří Homekey Logger, který je freeware. Mezi další patří např. Stealth Keylogger, Spytech SpyAgent, SpyMyPC PRO, Ardamax Keylogger atd. Tyto programy mohou být zneužity s poměrně nepříjemnými finančními následky pro koncového uživatele. Hardwarové keyloggery již vyžadují fyzický přístup k počítači, použití je tedy vyšší při útocích s bohatým očekávaným výsledkem, jako u bank a jiných finančních institucí. Je pravdou, že pro zvědavého nadšence či málo zkušeného hackera nemají tyto programy valné ceny. Zkušení útočníci si kódují vlastní programy, či již zmíněné upravují pro svou potřebu. Jejich dostupnost formou freeware ovšem může vést ke škodám z neopatrnosti, které mohou mít daleko větší následky, než útok zkušeného hackera, který za sebou zametá stopy a nepoškozuje, co nemusí.

Dalším rizikovým faktorem je ukládání hesel přímo v prohlížeči. Málo zkušený uživatel nabude dojmu, že jeho heslo je v bezpečí, ovšem mnoho prohlížečů má již dnes službu zobrazení hesel pro případ, že je uživatel zapomene. Při neopatrném umožnění i krátkodobého přístupu cizích osob k počítači, může být uživatel následně velmi nemile překvapen.

Další složitější ale vcelku účinnou a oblíbenou metodou je i odposlech pomocí tzv. ARP cache poisoning, tedy otrávení cache protokolu ARP. Dá se považovat i za útok modifikací přenášených dat. Jeho principem je získání MAC adresy oběti a využití k prohlížení dat na jeho počítači. Mezi IP adresou a MAC adresou není žádná spojitost (matematická) tudíž je nelze zjišťovat potřebným výpočtem. ARP tedy vyšle ARP požadavek, který k adresování místo IP adresy používá MAC adresu.

Útok spočívá v tom, že oběti je zaslán paket, ve kterém je mu řečeno, že brána má MAC adresu stejnou jako útočník. Dále je zaslán paket bráně, že oběť má MAC adresu stejnou jako útočník. Tím se docílí, že počítače pro vzájemnou komunikaci budou dosazovat MAC adresu útočníka a switch pošle data útočníkovi, kterého má za původní oběť. Útočník si data prohlédne a odešle je, ovšem teď již se správnou MAC adresou. Oběť tak svá data dostane. Tento způsob je velmi těžko zjistitelný, je k němu ovšem potřeba, aby záznam s přidělenou MAC adresou byl uložen na počítači potenciální oběti a také aby neuplynula doba, kdy je toto uchováno v ARP cache, což lze zajistit zasíláním ping s falešnou adresou v nějakém pravidelném intervalu. (HALLER, 2006)

Při modifikaci přenášených dat se povětšinou pasivní forma odposlechu linky mění na aktivní útok. Princip u modifikace, která ovšem probíhá na vyšších vrstvách častěji, je podobný jako u odposlechových analyzátorů. Zvláště oblíbené jsou v tomto právě sítě Ethernetu. Rozdíl mezi pasivním odposlechem a aktivní infiltrací je v tom, že pasivní útočník pouze sbírá data o vás, vaší činnosti na síti a jiné pro něj zajímavé informace, ovšem nijak je dál neupravuje. Aktivní útočník monitoruje poštu a data, navíc je ovšem zasílá dál mnohdy pozměněná tak, aby mu pokud možno pomohla při další infiltraci. Doufá přitom, že ani odesílatel ani adresát, pokud je pouze prostředníkem, si ničeho nevšimne.

4.2 Chybná autentizace

Jedná se vlastně o úmyslné zmatení adresáta při provádění autentizace. Účelem takovýchto útoků je přesvědčit autentizační mechanismus, že jsem někdo jiný, nejlépe ten, kdo má přístup a práva. Tím se útočníkovi otevírá šance zjistit informace, ke kterým nemá přístup, a možnost získávat a odesílat data, která by odesílat nemohl z důvodu nevlastnění práv. Používá se k tomu z části již zmíněný odposlech hesla, popřípadě přesvědčení brány o vlastnictví požadované adresy ať již IP, či lépe MAC adresy, která obsahuje i číselný kód modemu, tedy konkrétního fyzického prvku dané sítě.

Spoofing se ovšem používá často i úmyslně v rámci vlastní sítě a to k servisním účelům, kdy pomocí tohoto odposlechu sítě zjišťují správce či systém, je-li někdo připojený či se zapomněl odhlásit od počítače a tím nutí systém udržovat v paměti jeho

nastavení a pravomoci naprosto zbytečně, čímž se u rozlehlých sítí může odčerpávat kapacita. (BISHOP, 2002) (STALLINGS, 2003)

4.3 Nedostupnost služby a zpoždění služby

Zde se jedná o primárně poškozující typ útoku. Při úspěchu nedojde k prolomení systému, útočník nezíská přístup k důvěrným datům, ovšem může způsobit výrazné ekonomické škody. Odkládání služby je časté u odesílání elektronické pošty, kdy je útočník schopen neustále oddalovat odeslání a opakovat ho znovu a znovu, či pozdrží obdržení potvrzení autorizace, což při obchodní korespondenci či vyřizování objednávek může být velice nepříjemné.

Nedostupnost služby se zpravidla způsobuje zasíláním dotazu, na který není systém schopný odpovědět a neví si s ním rady, což způsobí jeho nedostupnost – pád. Dalším a velmi oblíbeným způsobem útoku je zahlcování systému dotazy a požadavky v takové míře, že jeho zpracovací kapacita není schopna takový objem zvládnout a tím dojde k pádu systému a jeho nedostupnosti. Takovýto útok poté může způsobit vážné finanční škody zvláště v sítích komerčních institucí, navíc, ačkoliv jejich principem není prolomení systému, mohou indikovat snahu o vyzkoušení systému a jeho bezpečnosti pro případnou infiltraci. Často ovšem také problémy se zdržováním či nedostupností služeb systému souvisí spíše se špatně nastaveným prostředím síťových služeb a zabezpečením, či lidskou chybou, než s cíleným útokem. (BISHOP, 2002)

4.4 Chyby v programech

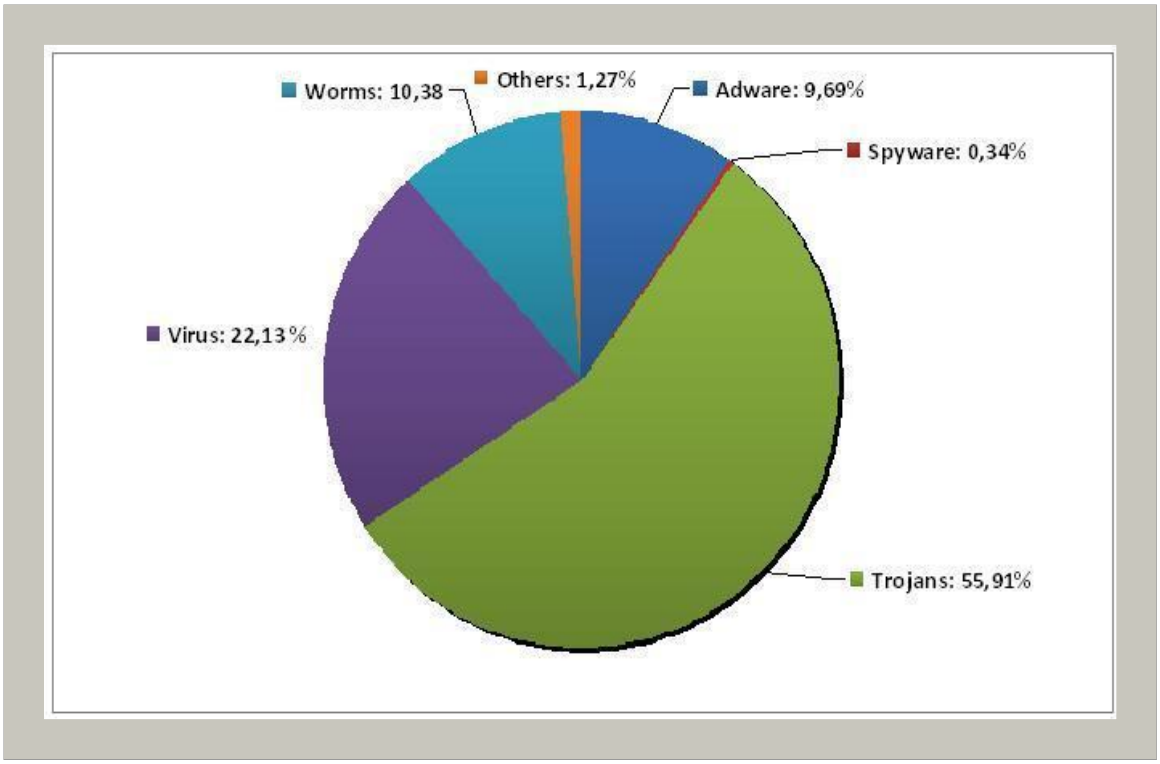
Jedná se o programy distribuované k operačnímu systému a dalším programům užívaným na počítačích, které vyžadují přístup k internetu kvůli aktualizacím, patchům a podobně. Internetové programy a aplety či pluginy zmíníme dále.

Útok formou využití chyb v programech, patří v současné době k nejčastějším pro svoji relativní jednoduchost. Skoro každý program obsahuje nějaké chyby a ty navíc bývají často zveřejněny na oficiálních stránkách distributora, či výrobce programu, či operačního systému, nebo i na veřejných fórech určených například k poradenství v těchto věcech.

Odtud bohužel mohou útočníci tyto informace bez omezení čerpat a pomocí odposlechu sítě i zjistit, je-li na cílové stanici program nainstalován, popř. v jaké aktualizované verzi. Poté na základě seznamu chyb mohou podniknout skrze tyto programy útok proti cílovému počítači.

4.5 Sociální inženýrství, phishing a jeho nástroje.

Sociální inženýrství pracuje na podobném principu jako spoofing, ovšem primárně na „vrstvě lidského faktoru“. Cílem tohoto útoku je oklamat konkrétního člověka, uživatele a přimět ho dobrovolně vykonat věci, které by každý bezpečnostní systém hlásil jako pokus o infiltraci. V dnešní době je množství antivirových programů, firewallů, šifrovacích algoritmů a programů pro sociální inženýrství lákavým cílem, protože lidský faktor je podstatně náchylnější k ovlivnění a špatnému rozhodnutí na základě získaných informací, než softwarové vybavení.



Obrázek 2 - Nejrozšířenější hrozby za rok 2010 Zdroj: www.JustIt.cz 8.1.2011

Jednou z technik sociotechniky je využívání lidských emocí. Nejvíce využívanými emocemi jsou strach, zvědavost, touha a soucit, které patří do skupiny takzvaných univerzálních emocí. Univerzální emoce jsou emoce, které čas od času

prožívá každý člověk. Pod vlivem emocí často jednáme zkratovitě. Emoce přebijí racionální stránku našeho myšlení a donutí nás jednat impulzivně.

Z uvedeného lze jasně vyvodit, že obětí sociálního inženýrství jsou převážně běžní uživatelé internetu, u kterých se předpokládá menší míra „bezpečnostní i počítačové“ gramotnosti a proto mají vyšší náchylnost na ovlivnění podvodnou výzvou. Nejčastěji se jedná o e-mailové výzvy, velmi často vydávající se za bankovní dům, kdy je požadováno z důvodu lepší ochrany, či nutnosti opravení chyby, zaslání přihlašovacích údajů k internetovému bankovnictví, číslo účtu, či PIN k platební kartě. Podnikové sítě trpí naopak většinou útoky červů a virů, které ovšem do systému velmi často dostane lidský faktor v podobě nezodpovědného zaměstnance.

4.5.1 Viry

Počítačové viry jsou soubory, které jsou schopné samostatně se šířit. Tedy přesněji pomocí hostitele, kterým je spustitelný soubor či knihovna. Spouštěcím mechanismem je spuštění napadeného souboru, tím se souběžně spustí i prováděcí kód viru a ten má tak možnost napáchat škody, ke kterým byl vytvořen. Dokud je tedy soubor, i když nakažený, nespuštěn, není aktivní ani virus.

Možnými nebezpečími jsou:

- Snížení výkonu programů – je to způsobeno aktivitou viru při jeho spuštění a následné činnosti. Nejvíce v tomto ohledu ovšem hrozí tzv. červi, kteří svým duplikováním v systému mohou způsobit až jeho kolaps.
- Snížení výkonu počítače – je většinou způsobeno infikováním napadených programů běžících na pozadí, či usazením se v paměti počítače u rezidentních virů.
- Vynášení důvěrných informací – toto způsobují viry, jež dokáží vyhledávat podle zadaného klíče citlivé informace a vynášet je cizímu uživateli, či backdoor viry, které útočníkovi umožní přístup na váš počítač.
- Poruchy programu nebo systému – často způsobeno chybou v prováděcím kódu viru, čímž ten odmítne dále pracovat, a pokud s ním běží i původní proces, může i ten být vypnut.

- Jiné nepříjemnosti – jako například zpomalení internetu, jeho sítě či prohlížeče, chyby na disku, neustálé stahování neznámých prvků z internetu a jejich instalace (Downloader). U vytáčeného připojení díky dialerům zase hrozí značný nárůst plateb za telefonní linku a další.

4.5.2 Červy

Tento škodlivý software pracuje na podobném principu jako virus, s tím rozdílem, že na rozdíl od viru nepotřebuje hostitele, tedy přenašeč v podobě nějakého souboru. V síti rozmísťuje kopie sebe sama na připojené počítače a tím se šíří. Respektive je součástí datových paketů a od již infikovaných stanic se šíří dál, a to jak náhodně, tak cíleně dle nastaveného klíče, přičemž využívá detekce bezpečnostních chyb v operačním systému, které poté infikuje a následně se v systému množí. Právě z toho vyvstávají největší komplikace, kdy jsou neustále napadány nové a nové části systému a to vede buďto k výraznému zpomalení, nebo naprostému zhroucení systému.

Techniky možného šíření jsou zpravidla dvě: Dvojitá přípona (např. PCX.EXE) - Windows zpravidla zobrazí pouze první, takže si uživatel myslí, že se jedná o obrázek (.PCX), nikoliv spustitelný soubor (.EXE) a HTML scripty, které zajišťují automatické spuštění přílohy.

4.5.3 Trojské koně

Principem takovéhoto koně je provádění systémem nedokumentovatelných činností. Většinou se jedná o destruktivní či špionážní akce v systému napadeného počítače. Často se vydává za užitečnou utilitu ke známým programům či k ulehčení nebo zefektivnění práce systému. Po svém spuštění ovšem nepozorovaně provádí přesný opak.

Backdoory – jsou moderní verze Trojských koní, které mají za účel získat útočníkovu kontrolu nad napadeným počítačem. Backdoor se ukryje tak, aby minimalizoval možnou detekci, a tím vytvoří zadní vrátka, nastaví svoje spuštění v závislosti na každém startu počítače a monitoringem sítě zjišťuje pokusy o vzdálené napojení. Najde-li takový pokus, umožní útočníkovi připojení a tím často i ovládání

souborových adresářů, soukromých dat a podobně. Z tohoto důvodu jsou backdoory logicky považovány za velmi nebezpečné a škodlivé. (STŘIHAVKA, 2001)

4.5.4 *Spyware, adware*

Spyware je špionážní program, který shromažďuje informace o uživatelích. Můžou to být např. údaje o navštěvovaných webových serverech, nainstalovaných aplikacích na počítači apod. Spyware se snaží o získání hesel k účtům, k různým aplikacím. Takto získaná data odesílá na definované adresy. Často bývá ukryt na stránkách s pochybným obsahem, či je součástí volně stažitelných paradoxně antispywarových programů, jejichž instalací a spuštěním testu, si počítač spíše infikujete, než vyčistíte. (STŘIHAVKA, 2001)

Adware bývá i součástí instalací programů, zejména freewarových a bez souhlasu s jeho instalací není možné nainstalovat daný program. Často bývá jako tzv. přídavný program podmínkou pro bezplatné užití programu. Velká část tohoto softwaru nebývá nijak zvlášť nebezpečná, slouží spíše k reklamním účelům, kdy stahuje z internetu bannery a reklamu a zobrazuje jí uživateli. Rozhodně ale může obtěžovat, či zpomalit činnost systému nebo internetové linky.

4.6 Nebezpečné programy v rámci internetu

Samotný internet a jeho prohlížeče, obsahují mnoho programů, které jsou založeny na skriptech, tyto programy jsou instalovány, alespoň jejich jádro i na počítač uživatele a jsou potenciálním nebezpečím pro jeho operační systém.

4.6.1 *Programy v JavaScript*

Jedná se o skript, který má za úkol zautomatizování některých činností a je pevnou součástí HTTP kódu, čímž se spolu s ním stahuje. V určitý čas při určité činnosti se spustí a je potenciálně nebezpečný z hlediska infekcí viru či červa. Na internetu je ovšem již standardem a tudíž patří k relativně bezpečným, navíc je složité se mu dnes na internetu vyhnout. Tyto programy jsou součástí webové stránky, útočník tak často může využít podobných skriptů k útokům proti uživatelově identitě. Je to nešvarem HTML5, tedy rozšíření HTML4 o nové, hlavně interaktivní prvky, jako je

právě množství skriptů či frameworků. Původně byl Javascript koncipován tak, že vůbec neumožňoval přístup na systém souborů. Postupně se však začaly objevovat bezpečnostní mezery v implementaci Javascriptu v Internet Exploreru. Bylo např. zjištěno, že pomocí určitých příkazů lze vysledovat oblíbené položky (bookmarks) uživatele, nebo že je možno prostřednictvím Javascriptu dokonce přivést prohlížeč k nestabilitě a pádu. Útočník však nejdříve musí svou potencionální oběť nalákat na svou stránku. Těmito stránky byly převážně warezové stránky, nabízející různé možnosti stáhnutí filmů, her a programů zdarma, stránky s označením Adult a podobné. Ovšem díky rozšíření metody Cross-Site Scriptingu zkráceně XSS. Tento způsob využívá děr v zabezpečení stránky. Uživatelská data zaslaná například přes URL jsou ukládána v rámci různých fór a guestbooků, často neošetřená a tím dostupná útoku. Pokud útočník tato data nějakým způsobem získá, může naprogramovat skript, který umístí do html kódu stránky. Návštěvník při příští návštěvě stránky fóra a přečtením příspěvku nějakého uživatele předá například svá cookies, a tím i možné přístupové heslo útočníkovi.

Java Aplety

Tyto aplety jsou již často nedílnou součástí internetových stránek a lze je spouštět z jakéhokoliv počítače, respektive operačního systému, pokud má překladač tohoto jazyka – součást volně šiřitelného Java pluginu. Pokud je uživatel na stránce, která obsahuje Java aplety, počítač ho stáhne. Jeho výhodou i rizikem je skutečnost, že se jedná o plnohodnotný program, na rozdíl od skriptu, a tudíž může provádět na vašem počítači různé souborové operace. V případě napadení virem, protože může z podstaty sloužit jako hostitelský soubor, se tak může na vašem počítači provádět i vykonávací kód viru. (STŘIHAVKA, 2001)

4.6.2 Prvky ActiveX

ActiveX je ve své podstatě framework aplikace. Tedy je jakousi softwarovou strukturou používanou k vývoji jiných komplexnějších aplikací. ActiveX má využití v řadě Windows aplikací zejména v těch přímo od Microsoftu. Ovšem asi nejznámější použití této platformy jsou tzv. ActiveX Controls, což jsou malé stavební bloky, které mohou vytvářet aplikace pracující přes internet pomocí webového prohlížeče. Slouží

v podstatě k vytváření interaktivních a multimediálních moderních prvků na webové stránce. ActiveX vytvořila přímo firma Microsoft, a vytvořila ho tak, aby byl kompatibilní pouze s webovým prohlížečem Internet Explorer a dalšími prvky právě od společnosti Microsoft. Dnes je ovšem možné ho využít i v jiných prohlížečích, ovšem je často třeba nainstalovat vhodný plugin. Problém je ovšem v tom, že dokáže přidávat i prvky z počítače, které lze spouštět, například spravování pošty, čímž se vaše pošta může objevit nečekaně tam, kde nechcete. Právě pro tuto vlastnost, kdy může ovládat některé souborové prvky ve vašem systému, je velmi zneužitelná. Navíc právě interaktivní a multimediální obsah, který umožňují přidávat, je často obsahem útočných stránek pochybného obsahu, které ovšem mají zpravidla vysokou návštěvnost.

4.7 Vyhodnocení bezpečnosti internetu podle hrozeb

Z výše uvedeného vymezení internetu a hrozeb, kterým mohou být sítě vystaveny, může uživatel dojít k přesvědčení, že internet je sítí velmi nebezpečnou, a že již samotné připojení znamená ohrožení a zkázu jeho dat či celé stanice.

Také převedení komerce a finančních operací na síť, vytvořilo z internetu ještě lákavější cíl i pro organizovaný zločin. Na síti se vyskytuje velké množství škodlivého softwaru, který hledá mezery v zabezpečení síťového rozhraní, či v programech v rámci operačního systému. Stále více je využíván znovuobjevený trend sociálního inženýrství, které s ohledem na zdokonalování obranných prostředků chytře útočí na slabý článek každé sítě průměrně informačně zdatného uživatele.

Odborníci provádějící analýzu bezpečnosti a hrozeb na internetu, právě tuto metodu sociálního inženýrství označili za největší hrozbu současnosti. Stále více se zaměřuje na internetové bankovnictví a zjišťování potřebných identifikačních a autorizačních údajů pomocí podvodných oznámení či poplašných zpráv (hoax).

Skutečností ale je, že pokud uživatel přistupuje zodpovědně k zabezpečení sítě, používá antivir (nejlépe placené verze), firewall a alespoň základní šifrování, může být v bezpečí i na internetové síti. Totéž platí i pro uchovávání citlivých informací, pokud uživatel rozumně ukládá tyto informace a navštěvuje pouze důvěryhodné stránky, měl

by být na internetu v bezpečí. To, co je totiž největší bezpečnostní hrozbou internetové sítě, je lhostejnost či nezodpovědnost jejích uživatelů.

V následující praktické části se bezpečnostními prvky a prvky ochrany spolu s příkladem zabezpečení a řešení problémů budeme věnovat podrobněji a konkrétněji.

5 Metody zabezpečení internetové komunikace

V této kapitole se práce věnuje konkrétním metodám zabezpečení internetové sítě a její komunikace. Je specifikován princip antivirových programů, Firewallů, některých šifrovacích algoritmů a prostředků detekce narušení sítě a další bezpečnostní prvky.

Tyto bezpečnostní mechanismy dělíme na:

- **softwarové** bezpečnostní mechanismy (mnohdy označované jako logické bezpečnostní mechanismy) princip řízení přístupu v daném operačním systému, kryptografie – symetrická (s tajným klíčem), asymetrická (s veřejným a privátním klíčem), standardy pro návrh, kódování, testování, údržbu programů, ochranné nástroje v operačních systémech, např. ochrana paměti, ochrana souborů řízením přístupu, obecná ochrana objektů, tj. přístupové matice, přístupové seznamy, hesla, autentizace přístupu k terminálu, mechanismy určené pro autentizaci zpráv.
- **hardwarové** bezpečnostní mechanismy (mnohdy označované jako technické bezpečnostní mechanismy) šifrovače a autentizační a identifikační karty.
- **administrativní** bezpečnostní mechanismy (výběr důvěryhodných osob, hesla, právní normy, zákony, vyhlášky, předpisy).

Nejprve je ovšem potřeba zmínit prvky administrativní ochrany. Tou je samotný přístup uživatele sítě či organizace, která sítě provozuje a spravuje. Každá organizace, která má vnitřní komunikační síť a navíc je připojena k internetu potřebuje nastavit nejprve pravidla pro jeho užívání a bezpečnost v rámci personální politiky. Nejprve je třeba rozhodnout, zdali povolíme přístup k internetu všem zaměstnancům, kteří vykonávají svou pracovní náplň na počítačích, či omezíme-li jejich práva pouze na intranet a přístup k internetu bude mít pouze management a správci sítě. Možnosti nastavení pravidel jsou například tyto:

Promiskuitní, tedy nejméně omezující. Je postavena na odpovědnosti a uvědomění jednotlivých uživatelů. Spoléhá se na to, že uživatelé budou vykonávat pouze takové činnosti, které jsou jim povoleny. Jejich oprávnění však nejsou technickými prostředky omezeny.

Liberální dávající uživatelům volnost ve vybraných oblastech mimo výslovně zakázaných činností. Při dodržování těchto zákazů se však již nespoléhá pouze na uvědomění uživatelů, ale vynucuje si je technickými omezeními. Je bezpečnější než promiskuitní politika, ale náročnější na provozní náklady. Probíhá například filtrace internetových adres a stránek a zaměstnanec se tak dostane pouze na některé, které potřebuje ke své práci nebo je u nich vysoká pravděpodobnost, že neohrozí integritu a bezpečnost sítě. Navíc bývá omezeno či přímo zakázáno stahování dat z internetu.

Opatrná zakazuje dělat vše, co není výslovně povoleno. Tato politika již volí opačný přístup k uživatelům. Vychází z toho, že vše je zakázáno a jednotlivým uživatelům na základě jejich pracovních činností a postavení přiděluje oprávnění. Toto je uplatňováno převážně v podnicích ekonomického charakteru či v bankovních domech, kde zaměstnanci pracují s důvěrnými daty klientů a jakákoliv infekce sítě, by mohla mít katastrofální následky nejen pro firmu ale i pro její klienty.

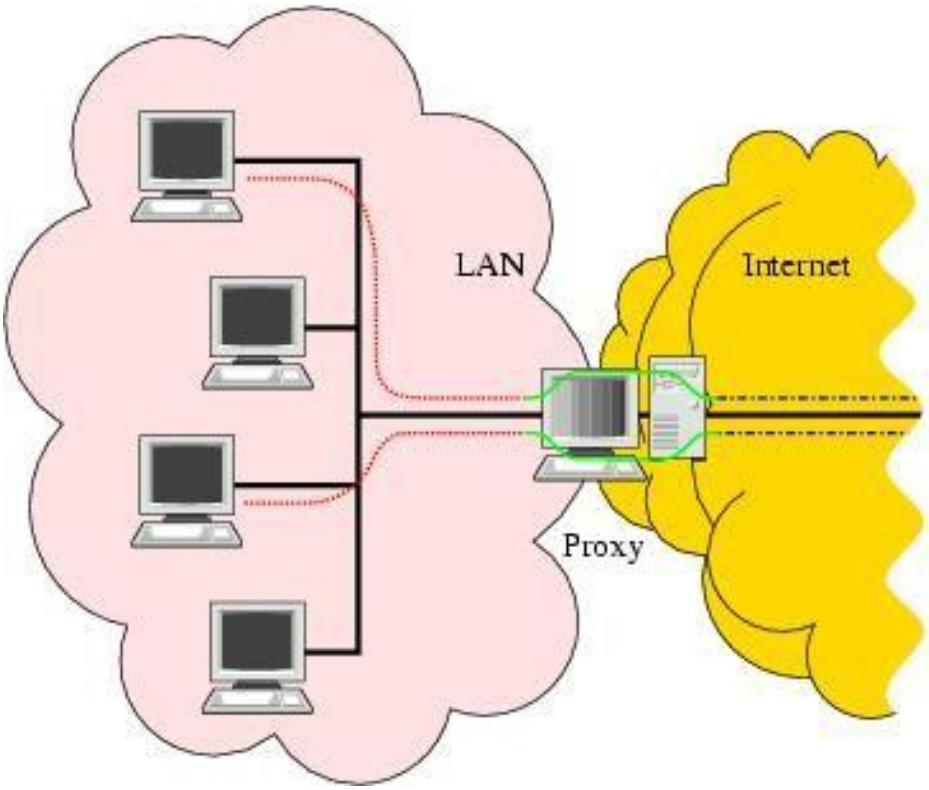
Paranoidní zakazující dělat vše, tedy i to, co by mohlo být povoleno. Je nejbezpečnější, v konečném důsledku však může vést k izolaci systému, snížení výkonnosti uživatelů, kteří jsou příliš omezováni. (HANÁČEK, a další, 1997)

5.1 Softwarové prvky zabezpečení

Základními obrannými mechanismy jsou překladače IP adres, které se umisťují za vnější sít s veřejnými adresami a před vnitřní síť například podniků, kde jsou již privátní IP adresy jednotlivých uzlů či stanic. NAT (Network Address Translation) je tedy takovou první vstupní ochranou vnitřní sítě před útoky zvenčí. Výrazně útočníkovi ztěžuje mapování typologie sítě a počet provozovaných systému ve vnitřní síti, navíc překladem IP adres pomáhá řešit možný problém s jejich nedostatkem.

5.1.1 Proxy

Proxy pracuje na aplikační úrovni. V dnešní době je velmi rozšířený u LAN sítí. Pracuje ambivalentně na jedné straně jako server a na druhé také jako klient. Jako server přijímá požadavky na zobrazení webového obsahu z webového serveru a posílá je právě na požadovaný server, kde se mu dostane odpovědi. Poté již požadovaný obsah převede do prohlížeče. Při dalších požadavcích navíc Proxy zkontroluje svůj cache, do kterého již jednou zobrazované stránky či obsah ukládá a místo odeslání požadavku na webový server odešle svou lokální kopii, což zpravidla urychlí zobrazení daného obsahu. Proxy server je schopen monitorovat internetovou komunikaci a případně odhalit přítomnost virů, navíc díky odeslání vlastní IP adresy na webový server, místo adresy klienta, umožňuje jistou anonymitu surfování, což je mnohdy zneužitelné útočníky, ovšem tato anonymita není stoprocentní, protože některé Proxy servery přidávají identifikátor klienta do požadavku. Proxy navíc může být jak softwarového, tak hardwarového charakteru. Velká část poskytovatelů internetu ovšem pro urychlení linky od připojení pomocí Proxy ustoupila.



Obrázek 3 - Zapojení Proxy mezi internet a LAN 1 Zdroj: http://www.netspojeni.cz., 28.2. 2011

5.1.2 Detekce narušení IDS

Systém IDS je pasivní soubor nástrojů, který slouží k detekci narušení systému a vnitřní sítě. Respektive slouží k monitorování a detekování událostí v síti internetu, které by mohly být potenciálním narušením bezpečnosti či integrity sítě. Jak bylo zmíněno, jedná se o pasivní prvek obrany, který není schopen zabránit pokusům o průnik do sítě. Jediná jeho vlastnost je tak signalizační, kdy na takovýto pokus upozorní. Sám o sobě by tedy kromě alarmování nebyl moc platný, proto je doplněn prevenčním systémem IPS a firewallem, které se tak vzájemně doplňují.

IDS má tři kategorie, patří sem uzlově orientovaná kategorie detekce narušení HIDS a síťově orientovaná NIDS, jako třetí kategorie je ještě hybridní verze obou zmíněných. HIDS vyžaduje konkrétní software umístěny na tomto systému, poté je schopen monitorovat události o jednotlivých uzlových bodech jako jsou logovací události apod., které zaznamenává a porovnává s událostmi, které má uloženy ve své znalostní databázi.

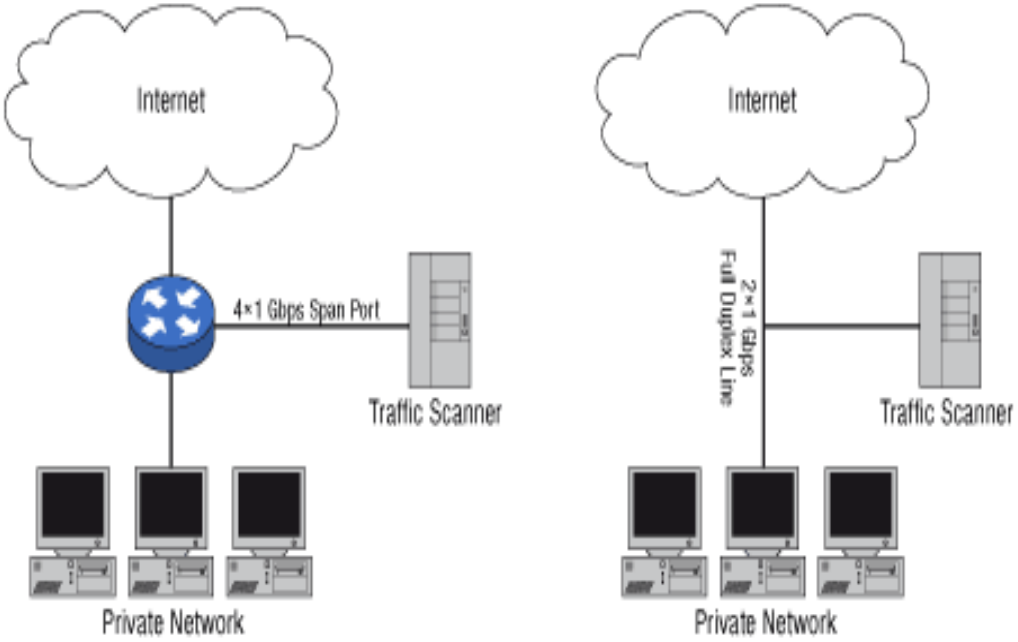
NIDS se povětšinou zařazuje sériově do datového toku - přijímá a analyzuje datové pakety. Z této analýzy pak usuzuje napadení, jak již bylo řečeno, ne vždy se ovšem jedná o skutečnou hrozbu, detekční systém varuje před všemi událostmi, které dle jeho úsudku mohou být ohrožením. Přijímá tyto pakety ve zvláštním segmentu sítě, kde pomocí větvení či zrcadlení sítě přesně rekonstruuje tok dat a hledá v něm vzory nežádoucího chování sítě, které zaznamenává a provádí reporting sporných událostí. Tuto službu nabízejí i některé routery s vyšším výkonem.

Hybridní systémy poté kombinují monitory uzlových bodů a datového toku. (ENDORF C., 2005)

5.1.3 Detekční a preventivní systém IPS

Jedná se o produkt, který se vyvinul na IDS, respektive na platformě jeho NIDS verze, kdy se již nezapojuje sériově do datového toku, ale má také za úkol analyzovat datový tok. Pomocí statistické analýzy vyhodnocuje hrozbu a navíc je schopen tato data modifikovat, čímž je schopen aktivně bránit případnému narušení. Je tedy vyšší verzí detekce s možností aktivní obrany.

ISD a IPS je poměrně důležitým bezpečnostním prvkem a to pro lokální sítě menších kanceláří a podniků ale i velkých organizací. Jako „první linie“ zabezpečení ve spolupráci s firewallem by měla být dnes již standardem při zakládání a zabezpečování podnikové sítě.



Obrázek 4 - Umístění IDS sondy v síti 1 Zdroj: http://www.cesnet.cz, 28.2.2011

5.1.4 Filtrace

Je metoda aktivní kontroly procházejících paketů a jejich vyhodnocování, na jehož základě dochází k propuštění či blokování konkrétních paketů. Filtr ovšem v zásadě nemění obsah paketů, pouze rozhoduje který propustí a který zahodí.

Filtrace probíhá na několika úrovních:

Na linkové vrstvě – kde se zpravidla provádí na přepínačích či na některých typech firewallů.

Filtrace protokolů IP a TCP – opět ji lze provádět pomocí některých firewallů či na směrovači sítě.

Filtrace aplikačních protokolů – zde se ovšem často nejedná o čistou filtraci, protože Proxy na aplikační vrstvě i brána často pakety změní. Opět jen některé firewally provedou čisté odfiltrování.

Cílem filtrace je vytvořit nepropustný filtr, který by chránil síť před útoky zvenčí a zároveň umožnil volný přístup zaměstnanců či uživatelů sítě na internet. Co se linkové vrstvy týče, je relativně bezpečná, nejvíce úspěšných útoků a infiltrací probíhá na aplikační vrstvě a jejích protokolech.

Docílit pomocí filtrace stavu, aby klienti vnitřní sítě mohli na servery v Internetu a klienti z Internetu nemohli na servery v intranetu, lze snadno pro protokoly TELNET, HTTP, HTTPS, POP, klienty a několik dalších. Problematický je však provoz protokolů FTP, SMTP a všech aplikačních protokolů využívajících UDP (tj. zejména DNS). Problém FTP se řeší pomocí tzv. pasivního FTP či secure FTP. Problémy se SMTP a DNS se řeší tak, že se povolí pouze komunikace mezi jedním konkrétním počítačem v Internetu a intranetem. Problémy s protokolem UDP (tj. zejména DNS) se řeší tzv. aktivními filtry, tj. filtry, které umožňují odesílat datagramy z vnitřní sítě do Internetu, ale odpověď je možné odeslat pouze v určitém krátkém časovém intervalu. Nevyžádané odpovědi se zahazují.

5.1.5 Filtrace na IP protokolu a TCP.

Filtrace na IP protokolu probíhá na směrovači (routeru), jejím principem je rozhodnout, které počítače (IP adresy) spolu mohou komunikovat. Filtrem lze omezit komunikaci tak, aby spolu mohly přes router komunikovat jen počítače o zadaných IP adresách. Kromě jednotlivých IP adres je ve filtrech možné zadávat i adresy sítí, podsítí či supersítí. Při tvorbě filtru jsou teoreticky možné dvě varianty. Buď se vše implicitně povolí a dopisují se pravidla specifikující, které počítače kam nesmí. Nebo se naopak vše implicitně zakáže a pouze vybraným se něco povoluje. Z bezpečnostních důvodů se většinou dává přednost druhé variantě (považuje se obecně za bezpečnější). Bezpečnostní riziko při propojení dvou sítí přes Internet s filtrací na úrovni IP adres spočívá v tom, že někdo v Internetu, kdo se nachází mezi oběma sítěmi, se nelegálně může prohlásit za IP adresu, která patří protější síti.

U protokolu TCP se zabezpečení provádí pomocí proxy. Proxy může být generická nebo transparentní. Z transparentní proxy nemusí vést klient žádný dialog. Transparentní proxy získá IP adresu a port originálního serveru z IP datagramu, který obdržela její serverová část od klienta. Pochopitelně, že transparentní proxy může mít volitelně tabulku, kde je uvedeno od koho může kam akceptovat spojení. Dále může mít tabulku uvádějící transformaci IP adres či portů mezi tím, co obdrží od klienta a IP-adresou či portem na který bude skutečně její klientská část navazovat spojení. Generická proxy, je proxy, která je obecně konfigurovatelná správcem sítě. Existuje na bázi serverové a klientské. Serverová je spuštěna a očekává zasílání požadavků a klientská je nastavena na jeden konkrétní server. Pokud bychom chtěli klientům umožnit přístup na větší množství serverů, je potřeba pro každý nastavit klientskou generickou Proxy zvlášť.

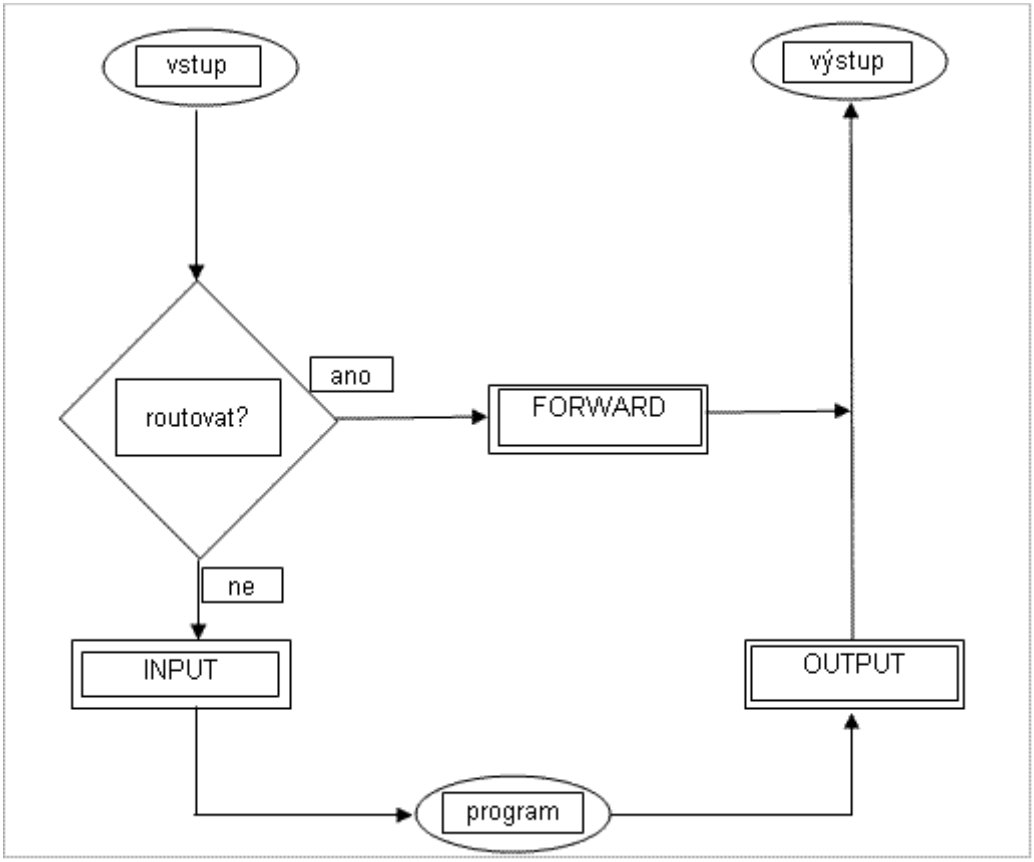
Aplikační brána (proxy firewall, proxy server, aplikační proxy) je ochrana na aplikační vrstvě. Dochází k úplnému oddělení sítí. Spojení probíhá tak, že klient pošle proxy severu požadavek na otevření spojení s nějakou službou v jiné síti a aplikační brána toto spojení otevře. Všechna data jdou vždy přes proxy server, který rozhodne, zda je propustí nebo zahodí. Proxy server tak 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. Při předávání může být definována sada pravidel, co je možné a co není možné předávat. Může se podobně jako při filtraci na routerech povolovat komunikace skrze proxy jen některým počítačům. (DOSTÁLEK, 2001)

5.1.6 Firewall

Firewall je systém tvořený jedním i více počítači, tak, aby bezpečně oddělil vnitřní síť od vnější sítě internetu a zároveň umožnil uživatelům bezpečný přístup na internetovou síť, mají-li k tomu práva.

Firewall spolupracuje se svými vhodnými doplňky IDS a IPS a tvoří tak jeden celek v monitoringu a zabránění útoku z vnější sítě. Využívá všech dostupných nástrojů, jako filtrování, Proxy či Bránu (Gateway). Ukládá informace o provozu na síti do logů, ve kterých lze najít nejen jednotlivé konkrétní akce ale vytvářet i sumarizované reporty.

Dřívější pasivní verze firewallů kladly značný důraz na lidský faktor, kdy správce sítě musel ručně tyto reporty procházet a zvláště u rozsáhlých sítí s velkým provozem často docházelo ke zjištění problému se značným zpožděním.



Obrázek 5 - Schéma Firewallu zdroj: http://cs.wikibooks.org/wiki, 5.3.2011

Aktivní firewally kromě zápisu logů mají ještě nastavitelné volitelné funkce ve formě poplachů, kdy provedou přesně specifikovanou činnost, jako je například zaslání varovného e-mailu, SMS zprávy na předem určený kontakt.Dojde k ukončení postiženého proxy či filtru pokud na něm došlo k události vyhodnocené jako nebezpečí. Dále zapsání IP adresy potenciálního útočníka na tzv. blacklist. Dokonce provede i ukončení celého systému. Nadstavbovými požadavky na firewally je i potřeba ochrany sítě na linkové, nejen aplikační vrstvě.

Firewally mají rozhraní vždy označená jako vnější a vnitřní, mnohdy jde o označení pro formu z důvodu konfigurace. Občas ale firewally kontrolují pakety, přicházejí-li na rozhraní jim určené. Jakákoliv událost vybočující z tohoto standardu je pak hlášena jako potenciální nebezpečí. Základem každého firewallu je buď proxy nebo

filtrace. Vzhledem k tomu, že pojem firewall není úplně přesně vymezený, respektive necharakterizuje konkrétně „co přesně je“, může se jednat o aplikaci, počítač či filtr, ať již umístěný v aplikační vrstvě, tak na vrstvě linkové. Pracuje buďto jako filtr nebo jako cílový bod v rámci TPC resp. UDP protokolu. Jako cílový bod pracuje převážně v případě protokolu HTTP. (DOSTÁLEK, 2001) (KOŠŤÁL, a další, 1997)

Firewally dělíme na:

Paketové filtry - jsou často implementovány na routerech. Vyznačují se vysokou rychlostí, avšak nízkou úrovní zabezpečení, protože kontrolují pouze zdrojovou a cílovou adresu a port. Neumožňují logování událostí a nejsou ani schopné upozornit administrátora na podezřelé aktivity.

Aplikační brány - jsou podstatně bezpečnější než paketové filtry, ale na druhou stranu jsou pomalejší a omezují uživatele na úzce vymezený okruh služeb (běžně 3 až 7), které jsou podporovány. Pro každou další službu je zpravidla nutné napsat nový tzv. proxy, neboli aplikaci, která se postaví mezi chráněnou a nedůvěryhodnou síť a kontroluje všechny pakety pro danou službu. Navíc, protože proxy pracují v aplikační vrstvě OSI modelu, nijak nechrání před případným útokem samotný počítač, na kterém běží.

SMLI Gateways - v sobě zahrnují to nejlepší z obou předchozích skupin: rychlost paketových filtrů a zároveň zabezpečení na stejné (nebo lepší) úrovni, jako aplikační brány. Vzhledem k tomu, že kontrolu provádějí na nejnižší možné softwarové úrovni (před síťovou vrstvou OSI modelu), chrání dokonale nejen vnitřní síť, ale i samy sebe.

Firewally dnes mají velké množství funkcí, jejich provozovatelé na ně kladou velký důraz, obzvláště když jejich provozní náklady nebývají malé. Firewall dokáže například optimalizaci připojení a řešení problému s IP adresami. Ohledně prvého se jedná o ukládání dat do cache (Proxy) a jejich opětovné načítání z brány firewallu, což je rychlejší a umožňuje to vlastnit i pomalejší linku. U řešení nedostatku IP adres, lze opět využít Firewall, za kterým poté mohou být libovolné IP adresy nezávislé na poskytovateli připojení.

Firewally mají ovšem i své nedostatky, patří mezi ně to, že:

- Firewall chrání pouze proti útokům z vnější sítě, nikoliv proti vnitřním útokům.
- Nechrání před útoky vedenými přes data např. prostřednictvím pošty, www atd., (např. viry v zašifrovaném souboru), pokud není samozřejmě doplněn antivirovým programem.
- Nezabrání odposlechu, modifikacím, nebo zničení dat při přenosu po síti.

Pokud uživatel vytvoří alternativní cestu pro připojení do vnější sítě, vyřadí tak firewall z provozu. Nemusí to být přímo fyzické připojení pomocí telefonní linky (např. modemem), či bezdrátové připojení, stačí vytvořit šifrovaný spoj – „tunel“.

5.1.6.1 Osobní Firewall

Osobní Firewall je aplikace, která se instaluje přímo do operačního systému uživatele a monitoruje jeho síťovou činnost.

Firewall se usadí na nejnižší vrstvě operačního systému (mezi síťovou a protokolární vrstvu) a zkoumá všechen síťový provoz. Jak na Internetu, tak také po místní síti LAN. Porovnává je poté s informacemi, které má uloženy nejprve v obecné formě od výrobce a poté i v konkrétní formě, které se naučí od uživatele. Jestliže nějaká aplikace chce s někým navázat kontakt, firewall to oznámí (zobrazí název aplikace, kam volá, po jakém portu a protokolu) a dá na výběr akci. Uživatel pak může povolit nebo zakázat, popřípadě nadefinovat pravidlo, aby tuto volbu provedl příště firewall automaticky. Firewall také zkoumá všechny pakety, které přicházejí z Internetu. Navíc zabraňuje útočníkům získat kontrolu nad počítačem tím, že ošetřuje některé známé chyby v programech. Firewall není schopen prohlížet obsah paketů na vyšších vrstvách. Mnoho moderních útoků probíhá na aplikační vrstvě. Firewall jim tedy nemůže zabránit. V takových případech je potřeba nasadit jiný typ ochrany, jako je IDS nebo IPS. (KOŠŤÁL, a další, 1997) (DOSTÁLEK, 2001)

Na trhu je v současné době velké množství takových aplikací a jsou dostupné i ve volně stahovatelných verzích či Trial verzích, ty bohužel ale často neobsahují všechny funkce. Proto by měl uživatel, který zabezpečuje svůj operační systém, raději investovat

do placené verze. Obstojnými Firewally jsou již navíc vybavené i mnohé antivirové programy, které je nabízejí jako své rozšíření.

5.2 Antivirové programy

Antivirové programy kontrolující příchozí soubory, ať již elektronickou poštou, stažené webovým prohlížečem, či některým z download managerů, pracují na několika principech a kromě aktualizace systémového zabezpečení by měly patřit k základnímu bezpečnostnímu prvku koncového uživatele.

5.2.1 Scanning

Antivirový program využívá vlastní databázi známých virů. Testuje prohledávané soubory na výskyt určité posloupnosti bytů, která identifikuje vir z databáze. Jedná se o nejstarší a stále pravděpodobně nejrozšířenější způsob detekce napadení virem. Tato metoda umožňuje nalezení pouze těch virů, které jsou již zaneseny v databázi známých virů. Databáze musí být proto pravidelně aktualizována, aby bylo skenování skutečně účinné. S ohledem na stále se zvětšující počet virů a dalšího škodlivého softwaru, však tato metoda klade značný důraz na velikost virové databáze a proto není přílišnou perspektivou do budoucna, protože s nárůstem velikosti databáze se zpomaluje rychlost detekce.

5.2.2 Heuristická analýza

Antivirový program se nespoléhá na databázi známých virů, ale analyzuje kód souboru a jeho význam. Hledá v něm postupy, které jsou typické pro viry a které se v normálních programech nevyskytují. Pokud je jich příliš mnoho, prohlásí soubor za zavirovaný. Výhodou této metody je možnost nalezení virů, které ještě nebyly analyzovány a zaneseny do databáze virů. I zde je využíván scanner, ovšem složitější a mnohdy rychlejší, jeho nevýhodou je ovšem riziko častých planých poplachů. Novinkou je přidání i tzv. emulátoru kódu, který v bezpečném prostředí simuluje činnost souboru a tím ověřuje jeho bezinfekčnost.

5.2.3 Kontrola integrity dat

Antivirový program sleduje změny v systému souborů. Využívá toho, že uložením viru do některého souboru dojde ke změně souboru, kterou je možné detekovat. Pokud dojde ke změně textového souboru, pravděpodobně se nejedná o následek činnosti viru, ale pokud dojde ke změně v některém programu nebo systémovém souboru, je možné, že příčinou je napadení virem.

Antivirový program si nejprve při prvním spuštění vytvoří databázi souborů na disku. Při dalších spuštěních srovnává aktuální stav souborů s příslušnými položkami ve své databázi a zjišťuje, zda se od posledního průchodu nezměnily. Výhodou kontroly integrity je možnost nalezení dosud neznámého viru.

5.2.4 Rezidentní ochrana

V systému je neustále spuštěn proces, který kontroluje prováděné operace. Může jít o některý z výše zmíněných nástrojů. Mohou být sledovány podezřelé operace se soubory a systémovými oblastmi disku. Například při pokusu o zápis do boot sektoru je operace přerušena a uživatel dotázán, zda zápis povolí. Dále jsou při rezidentním sledování obvykle kontrolovány spouštěné programy na přítomnost viru. Když chce uživatel spustit některý program, antivirový program nejprve zkontroluje, zda neobsahuje virus. Většina antivirových programů kombinuje více z uvedených způsobů a nechává na uživateli nastavení té kombinace, která mu vyhovuje. Rezidentní sledování je obvykle neustále spuštěno na pozadí a v pravidelných intervalech podle nastavení uživatele se provádí kompletní kontrola souborů na pevných discích. Jistou nevýhodou může být mírné zpomalení systému, ovšem tato neustálá kontrola veškeré nevýhody rozhodně převažuje ve prospěch rezidentního štítu. (STŘIHAVKA, 2001)

5.2.5 Karanténa

Jedná se o bezpečné úložiště souborů, které jsou infikované a antivir je nedokáže vyléčit nebo je nelze smazat a také o podezřelé soubory, u kterých není jasné, zda jde o infekci či nikoliv. Toto úložiště je lokalizováno na části disku a soubory jsou tam ukládány tak, aby je nebylo možné spustit, a to ani nechtěně. (STŘIHAVKA, 2001)

6 Postupy při řešení konkrétních problémů: Zabezpečení podnikové sítě vs. Domácí sítě. Řešení možných komplikací.

V této kapitole jsou prakticky demonstrovány způsoby zabezpečení na příkladech podnikové a domácí sítě. Jsou definovány prvky, které zabezpečí linkovou i aplikační vrstvu, a to u podnikové sítě. U domácí sítě se práce zabývá spíše zabezpečením z pohledu koncového uživatele, tedy hlavně softwarovému na aplikační vrstvě. S ohledem na téma práce, které má být z pohledu uživatele, jsou charakterizována i případná řešení vzniklých komplikací v domácí síti. V podnikové síti uživatel, není-li také správcem, nemá moc možností do zabezpečení sítě a její administrace zasahovat.

Podnikovou sítí bude menší vnitřní síť firmy, zabývající se kurzovým sázením s licencí i pro internetové sázky. Podnik vlastní svou placenou doménu www.sazejonline.cz a má také vlastní datový server. Počítačů k zapojení je celkem 8. 6 z nich je umístěno na přepážkách, jeden v kanceláři provozního vedoucího pobočky a jeden plní právě roli serveru.

Jedná se o síť LAN a k propojení počítačů používá kabeláž UTP, která je velmi odolná proti rušení, postačí kategorie 5e (DOSTÁLEK, 2000) pro přenos maximálně 100Mbit/s a také koncovky RJ45 pro zapojení do síťové karty a switche. Každý počítač je vybaven ethernetovou síťovou kartou.

Server je napojen pomocí bezdrátového přístupového bodu k webovému serveru poskytovatele a k tomuto má ještě další dvě rozhraní. Jedno nastavené jako důvěryhodné pro připojení stanic pracovníků na přepážkách a počítače vedoucího, druhé nedůvěryhodné, kam se připojují klienti z internetu za účelem internetového kurzového sázení. Server má nainstalovaný firewall, který chrání před útoky zvenčí, na linkové vrstvě jsou také prvky IDS monitorování akcí směrem z internetu a také IPS přímo v datovém toku, s možností modifikace potenciálně útočných datagramů.

Zabezpečení bezdrátového přístupového bodu je provedeno systémem WPA2 s nastaveným vlastním přístupovým klíčem, který lze uložit například na flash disk, a dále pomocí protokolu IPSec ze serveru brány na směrovač poskytovatele připojení.

Serverový počítač obsahuje dva segmenty pro provádění potřebných služeb. První segment plní také úlohu brány do systému, je na něm nainstalován běžně užívaný Microsoft Windows Server a pracují na něm firewall, DNS pro přidělování jmenných domén stanicím a tvoří také datový, respektive souborový server se sdílením tiskáren.

Druhým segmentem je poštovní server s nainstalovanou linuxovou distribucí Debian provádějící poštovní služby a také webové služby přes Apache.

6.1 Analýza a vyhodnocení rizik bezpečnosti.

Plánování bezpečnostních opatření by mělo začít rizikovou analýzou. V procesu rizikové analýzy se vymezují rizika a jejich možné důsledky. Nejprve se vymezí všechna možná rizika, která by mohla ohrozit počítačovou síť nebo informační systém. Ve druhém kroku se navrhnou možná protiopatření včetně jejich ceny. Riziková analýza vede k plánu návrhu bezpečnostních opatření, který vymezuje odpovědnosti za realizaci určitých kroků směřujících ke zvýšení bezpečnosti. S ohledem na druh podnikání sázkové kanceláře, budou požadavky na zabezpečení a tudíž i náklady na vyšší úrovni. Citlivost dat, která mohou proudit a být ukládána na vnitřní síti, je vcelku vysoká.

Hlavní kroky rizikové analýzy jsou tyto:

- vymezení hodnot prvků systému
- stanovení zranitelnosti hodnot systému
- odhad pravděpodobnosti zneužití zranitelných míst
- výčet odhadu ročních ztrát
- výčet použitelných bezpečnostních opatření a jejich ceny
- plán ročních úspor dosažených v důsledku zavedených bezpečnostních opatření

Vymezíme-li hodnotu stanic a serveru, s ohledem na jejich nízký počet v rámci provozovny, nedostaneme se k příliš vysokým hodnotám. Co se zranitelných hodnot systému týče, zde, protože kancelář provozuje sázkovou činnost a to i po internetu, bude pracovat s velmi citlivými daty klientů a bude mít ve svých aplikacích prostředky pro disponování s prostředky finančními i autentifikačními.

Tato skutečnost si vyžádá zvýšení nákladů i požadavků na zabezpečení sítě. Opět s ohledem na citlivost dat, je zde i větší pravděpodobnost snahy o průnik do systému, ať již pro odposlouchávání a snahu o poznání typologie sítě, tak před možnými útoky červy či zahlcením systému a zapříčiněným nedostupnosti služeb pro klienty. To samozřejmě v případě úspěchu povede k finančním ztrátám a možné hrozbě soudních žalob klientů, protože i oni by v takovém případě mohli pociťovat ztrátu.

6.1.1 Politika zabezpečení sítě a logické schéma

Jako zabezpečení sítě byl vybrán na síťové vrstvě detekční systém IDS a IPS spolu s firewallem, který odděluje vnitřní síť od vnější sítě internetu. Filtrování je na linkové vrstvě zajištěno routerem, respektive switchem, který je v něm zabudován. Zmíněný router provádí filtrování na úrovní protokolů, zde IP a TCP na kterých běží tato síť. Ukrytí vnitřní sítě a jejích adres nám poskytne proxy, který díky cache urychlí načítání stránek již zobrazených.

S ohledem na charakter podnikání a citlivost dat je vnitřní datový tok sloužící zaměstnancům ke komunikaci se serverem i vzájemně oddělen od vnější sítě internetu. Výhodou je rychlejší datový přenos na této úrovni a zajištění větší míry bezpečnosti před odposlechem jak sítě, tak hesel a dalšími útoky zvenčí. Na firewallu běží software na bázi proxy, tvořící tzv. aplikační bránu přes kterou přicházejí veškeré požadavky na webový a poštovní server. Brána si generované požadavky „přivlastní“ a zasílá je na server jako své. Vygenerovanou odpověď poté obdrží ona a nikoliv přímo stanice či uživatel, z jehož IP adresy byl odeslán. To umožní správci sítě monitorovat a případně blokovat datový tok z vnější sítě internet.

Pro propuštění sítě je ponecháno na vedení a poté na správci sítě, jaké nastaví zabezpečení pro datový tok, tedy jestli určí implicitní zákaz, čímž zakáže veškeré

služby sítě a povolí jen ty, které jsou nutné pro provoz (co se webových služeb týče, jde pro tento druh podnikové sítě o vhodnější nastavení) nebo ponechá implicitní povolení, kdy naopak povolí veškeré služby vnější sítě a zakáže pouze ty potenciálně rizikové. Druhá možnost dává zaměstnancům větší možnosti i svobody užívání sítě, ovšem zvyšuje rizika infiltrace či útoku zvenčí.

Zapojení firewallu je možné přes metodu demilitarizované zóny. Přenos packetů tedy probíhá tak, že z PC je odeslán požadavek na internetový server. Požadavek jde přes směrovače do proxy brány, kde se vyhodnotí a jménem brány odešle příslušnému serveru. Ten jej po obdržení zpracuje a zpět odešle požadovanou informaci. Ta dojde zpět na proxy bránu, zkontroluje se, a buďto je zahozen nebo poslán dále na cílovou stanici, odkud požadavek vyšel. Jeho nevýhodou je sice vyšší cena s ohledem na zapojení dvou směrovačů mezi webserver a proxy bránu a poté mezi proxy bránu a stanice ve vnitřní síti, ovšem stupeň bezpečnosti je zde nejvyšší, což s ohledem na možnou výraznou citlivost dat v sázkové kanceláři oceníme.

6.2 Síťové služby

6.2.1 DNS

Na serveru běží reverzní překladač IP adres na jmenné domény. DNS v rámci Microsoft Serveru 2003 má velkou část služeb implementovanou již v základním režimu po spuštění operačního systému, ovšem je možné nastavit potřebné parametry ručně pomocí příkazu netstart. Zde pak je možné pomocí příkazového řádku nastavit parametry pro spouštění služeb v rámci lokálních procesů, zakázat jejich automatické spuštění (třeba omylem uživatelem) či nastavit jejich spuštění ručně.

S ohledem na vlastnictví placené domény sázkovou kanceláří, se DNS server při převodu IP adres na jmennou doménu obrací na místní jmenný server DNS. Zde se postupuje hierarchicky a to shora dolů, kdy kořenový adresář nejvyšší domény předává informaci níže podle potřeby a ve chvíli kdy on či některý z kořenových serverů nižších doménových řádů narazí na údaje relevantní odesílateli, odešle odpověď a ukončí tak požadavek.

Řešení požadavku vzneseného DNS na DNS server je možné dvěma způsoby a to rekurzivně a nerekurzivně.

Rekurzivní řešení dotazu - server převezme vyřizování dotazu, sám místo tazatele prochází strom doménových jmen a až najde odpověď, pošle ji tazateli. Rekurzivní přístup sice server více zatěžuje, ale jelikož jím projde odpověď, může být uložena do vyrovnávací paměti a poskytnuta při příštím stejném dotazu ihned z paměti. Takto se obvykle chovají lokální jmenné servery.

Nerekurzivní řešení dotazu - server se dotazem dále nezabývá, tazateli pouze poskytne adresy dalších serverů, na něž se má obrátit pro další informace. Takto se obvykle chovají servery nejvyšší úrovně a obecně vyšších úrovní doménové hierarchie, neboť rekurzivní řešení dotazu by kapacitně nezvládly. Setkají se s ním obvykle majitelé domén nižšího řádu.

Pro DNS je využíváno jak protokolu UDP, tak TCP. UDP je zpravidla využíván pro dotazy s menším objemem přenesených dat, jako je reverzní překlad IP adres. DNS využijeme i pro poštovní služby v rámci druhého segmentu serveru. DNS služby v rámci vnitřní sítě jsou provozovány DNS instalovaným na serveru s bránou a firewallem. Tím je oddělen od sítě internet, což mu umožňuje libovolné přidělování jmenných adres v rámci vnitřní sítě a to nezávisle na poskytovateli internetu či placené domény. Ta je jediná viditelná zvenčí spolu s firewallem. Konfiguraci forwardingu pro adresování dotazů, buďto na vnitřní DNS server či na jmenný server poskytovatele, nastaví dle potřeby administrátor. Vnitřní jmenný server bude v seznamu nastaven jako hlavní, server poskytovatele jako vedlejší.

Zabezpečení samotné DNS provedeme pomocí systému DNSSec. Ten přináší pro DNS metodu ověřování pomoci digitálního podpisu. Problémem DNS v tomto ohledu je skutečnost, že je strukturován do zón, tudíž klíče generované DNSSec jsou platné pouze pro zónu nikoliv pro celou doménu. DNSSec využívá asymetrický způsob šifrování, ovšem nevyužívá certifikátů, pouze veřejné klíče ukládá do vět KEY typu. Toto je však pouze zdánlivé, protože věta KEY je certifikována, v případě DNS resp. DNSSec podepsána správcem hierarchicky nadřízené domény. Doména www.sazejonline.cz, respektive správce, podepíše KEY pro celou zónu a v případě subdomény musí provést

delegaci pravomocí na konkrétní subdoménu, aby byla přístupná z internetu. K tomu je užita věta typu NS, která definuje pravomoci jednotlivých domén v rámci DNS. Na pravé straně musí být jméno domény, které je přidělena číselná IP adresa větou typu A. Nejprve je uvedena autoritativní doména a následně subdomény. Pravá strana nesmí obsahovat ukazatel na CNAME pomocí věty NS. CNAME je takzvaný alias jednotlivých stanic. V případě použití DNSSec je třeba k větě NS při delegaci pravomocí na subdoménu připojit i větu KEY veřejného klíče zóny, správce zónu elektronicky podepíše (de facto certifikuje) a podpis uloží do věty typu SIG, tedy Signature. Více v: (DOSTÁLEK, 2001) I zde je tedy princip založen na veřejném a privátním klíči, kdy jeden bez druhého nebude schopen ověření.

E-mailová komunikace je prováděna poštovním serverem nainstalovaným na druhém segmentu s Linuxovým operačním systémem. Každý zaměstnanec má přidělenu emailovou adresu, která se skládá z jeho jména a příjmení pro jeho jedinečnou identifikaci (v případě shody dvou jmen rozlišeno přidáním číselného znaku). Jméno je odděleno tečkou a po znaku @ následuje doména. Místní poštovní server zajišťuje rozesílání pošty v rámci místní domény, poštu v rámci internetu zajišťuje nadřazený poštovní server komunikující s místním pomocí protokolu SMTP. Po správnou funkci je ještě třeba v DNS nastavit záznam MX u poskytovatele poštovních služeb pro naši doménu, aby bylo zajištěno správné adresování/směrování. V případě nedostupnosti poštovního serveru na aplikačním linuxovém prostředí bude příchozí pošta ukládána na záložním serveru u poskytovatele poštovní služby, k čemuž provedeme ještě jeden záznam MX. Tedy nastavíme vlastní poštovní server jako hlavní, pomocí MX mu udělíme vyšší prioritu a server záložní označíme vyšším číslem, čímž mu udělíme nižší prioritu.

6.3 Webové služby a nastavení

Na aplikačním serveru, tedy segmentu s linux prostředím bude webové služby poskytovat aplikační server Apache. Na starosti bude mít, jak služby intranetu pro zaměstnance, tak připojení k vnějšímu internetu. Webové služby jsou prováděny na protokolu TCP/IP a samotným aplikačním protokolem bude nejpoužívanější HTTP respektive HTTPs protokol.

6.3.1 Sdílení souborů a tiskáren

Souborové složky zaměstnancům, šifrované pomocí EFS jsou umístěny na prvním segmentu, tedy serveru brány. EFS je šifrovací mechanismus, který zabezpečuje souborové složky na stanicích či datových serverech, jeho výhodou je schopnost obnovy pro případ ztráty klíčů. Agent obnovení navíc lze umístit na čipovou kartu a není nutné mít ho uložen na disku počítače administrátora. Souborové složky jsou pro každého zaměstnance omezeny na určitou velikost, která zaručí možnost ukládání menších souborů potřebných k práci, avšak zamezí ukládání nevhodného obsahu z internetu či přenosných médií. Přístup do složky má pouze zaměstnanec, jemuž je určena a jemuž je přístupná na základě zalogování po procesu autentifikace a také administrátorovi pro případ potřeby. Na serveru je i tisková fronta pro pracovníky přepážky, vedoucí má u stanice síťovou tiskárnu, vlastní a přepíná ji v nastavení pro tisk.

Jméno	Typ	Data
(Default)	REG_SZ	(hodnota není nastavena)
EfsConfiguration	REG_DWORD	0x00000001 (1)

Nastavení registru

Systémový klíč: [HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindows NTCurrentVersionEFS]
Jméno hodnoty: EfsConfiguration
Typ dat: REG_DWORD (DWORD hodnota)
Hodnota dat: (0 = vypnout EFS, 1 = zapnout EFS)

Obrázek 6 - Ukázka nastavení EFS šifrování

6.3.2 Směrování v rámci sítě

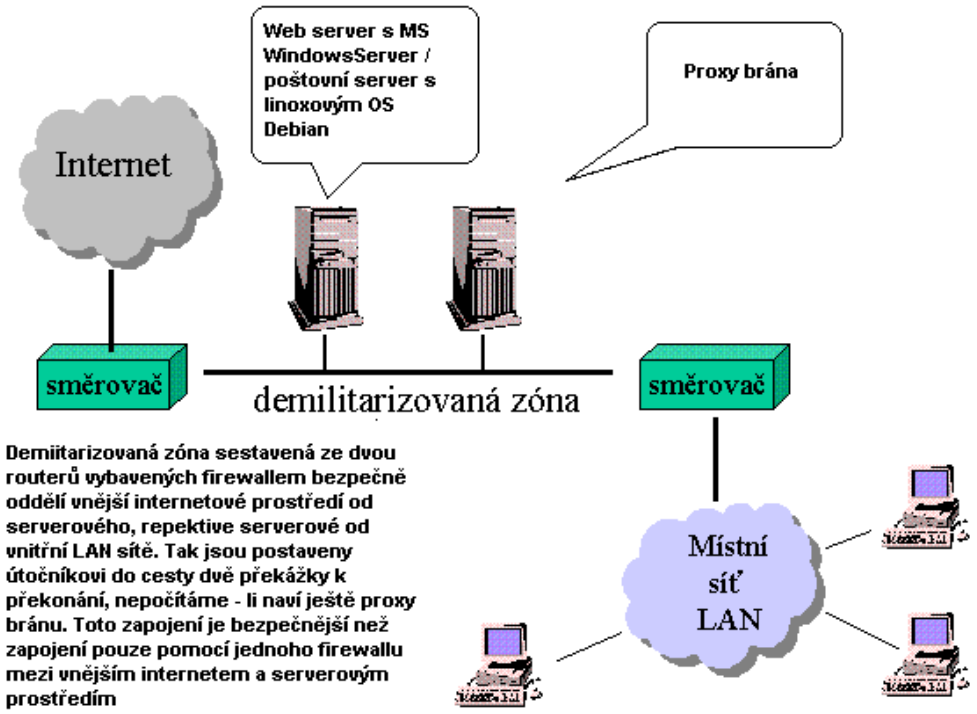
Směrování v rámci vnitřní sítě i internetu provádí local server na prvním segmentu s umístěným firewallem. Zde končí veškeré vstupy a jsou poté dále směrovány dle vyhodnocení požadavku a rizika. K pomoci jsou již dva zmíněné routery tvořící demilitarizovanou zónu. Stanice se tohoto směrování aktivně neúčastní a to ani stanice vedoucího, mají pouze nastavenu implicitní adresu pro jejich segment.

6.4 Nastavení komunikačních pravidel administrativně i softwarově.

Pravidla pro komunikaci v síti jsou nastavena restriktivně, s ohledem na povahu činnosti. Co není vysloveně povoleno, je zakázáno. Zaměstnanci mají zamezeno stahování z internetu a připojování k některým serverům. Stahování je povoleno pouze ze zabezpečených serverů a FTP serverů. Proto je pro každý z povolených serverů zřízená generická proxy. Zakázáno je spouštění jakékoliv aplikace v došlé poště, rozesílání hromadných zpráv, které se netýkají pracovní činnosti.

Nastavení webového prohlížeče je prováděno administrátorem a přístup do jeho nastavení je pouze z jeho účtu, tedy z profilu administrátora. Zaměstnanci nemají možnost cokoliv na nastavení prohlížeče měnit. Toto je z důvodu nastavení bezpečnosti a eliminaci uživatelské chyby při neoprávněném a neopatrném zásahu do nastavení zabezpečení. Webovým prohlížečem je Mozzila Firefox, z důvodu jeho lepší zabezpečenosti oproti Internet Exploreru od společnosti Microsoft. Pro potřeby práce v rámci Microsoft distribucí a rozhraní je nainstalován plugin se zobrazovacím jádrem IE. Právo stahovat pluginy má opět pouze administrátor sítě.

V nastavení firewall pro komunikaci jsou utvořeny dvě skupiny. Zaměstnanci s pravidly nastavenými pro vnitřní síť a klienti, pro které jsou nastavena pravidla pro přístup z vnější sítě internet. Klienti nemají možnost komunikace přímo se stanicí vnitřní sítě, tedy zaměstnancem, tato komunikace probíhá pouze přes dvojici routerů a firewall. (Viz obrázek: Zapojení pomocí demilitarizované zóny.)

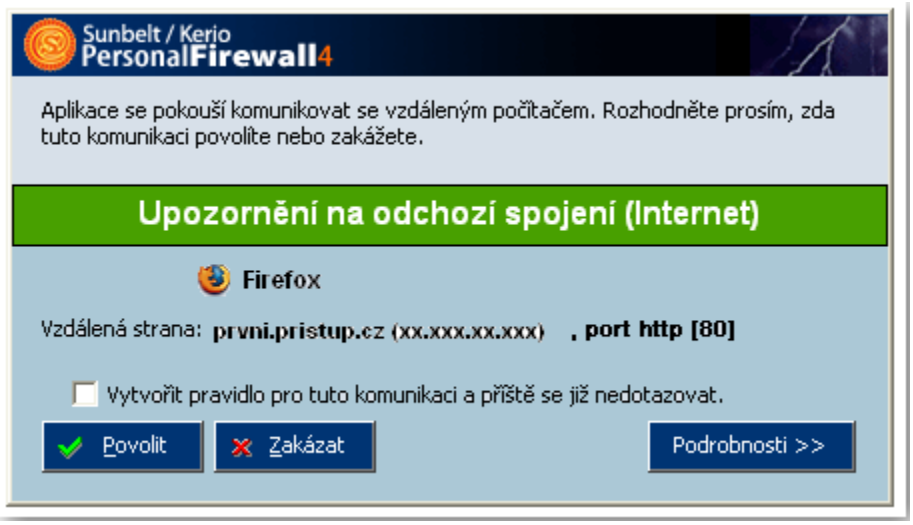


Obrázek 7 - Zapojení pomocí demilitarizované zóny Zdroj:http://www.earchiv.cz/a98/a812k205.php, 2.3.2011

Nejprve je nainstalován a nastaven vhodný firewall. Zde je to firewall Sunbelt Kerio Winroute. Ta proběhne standardně přes instalačního průvodce, kde po odsouhlasení licenčních podmínek administrátor zvolí jednu z možností v tomto případě Advanced (Rozšířená instalace), kdy se firewall po objevení neznámé aplikace dotáže administrátora na druh akce, která má být vykonána a zda má pro ni vytvořit pravidlo, čímž administrátor nastaví specifická pravidla pro chování firewallu. Po odblokování firewallu operačním systémem prohledá Kerio veškerá připojení na stanicích a otevře dialogové okno, zda nalezené připojení na internet je připojením k důvěryhodné síti. Nastavena je volba NE, jedná-li se o připojení do vnějšího internetového prostředí.

Následuje tvorba pravidel pro síťovou komunikaci. V Sunbelt Kerio FW je možnost nastavit automaticky pravidla pro síťovou komunikaci, administrátor ovšem volí spíše vlastní nastavení, tedy pravidla pro libovolnou jinou aplikaci a ta lze nastavit na hodnoty povolit/zakázat/ptát se, podle nichž bude dále firewall pracovat. Administrátor podle pravidel komunikace na síti prosazovaných společností nastaví většinu aplikací na - zakázat. Jedná se o aplikace typu Bittorrent, download managerů a

dalších podobných programů pro práci se soubory a jejich stahování. Podle rozsahu portů některých zemí je možné zablokovat i komunikaci se zemí, kde je vysoký podíl útočných stránek. Jsou-li tyto porty známy, lze je firewallem odblokovat a tím se vyhnout částečně spamu ze známých portů.



Obrázek 8 - Dialogové okno upozornění FW Sunbelt Kerio

Obrázek výše ukazuje dialogové okno, které Kerio zobrazí při prvním pokusu o připojení prohlížeček internetu. V tomto případě jde o prohlížeč Mozilla Firefox. Zaškrtnutím volby Vytvořit pravidlo pro tuto komunikace etc. a povolením následně je umožněn prohlížeči přístup na internet, pro jistotu je ovšem zakázáno zpětné navazování komunikace z internetu směrem k prohlížeči, může se jednat o potenciální útok.

Pro emailové klienty, v této firmě jde o klienta Thunderbird je nutné nastavení resp. povolení odpovídajících portů. POP3 a SMTP pracují defaultně na portech 110 respektive 25. Pro použití zabezpečeného připojení jsou povoleny dále porty 995 (POP3S) a 465 pro (SSL SMTP) protokol.

6.4.1 Filtrování HTTP

Přístup k vnějším webovým stránkám není přímo znemožněn, zaměstnanci mají možnost navštěvovat zpravodajské servery i některé důvěryhodné portály, pro tyto účely je ovšem nastaveno filtrování. Vhodné je filtrování pomocí konkrétních slov a termínů, které obsahují potenciálně útočné stránky. Důležité je také nastavení částečného zakázání některých prvků webových stránek, jako jsou javascripty a jiné scripty, ActiveX a podobné interaktivní aplikace. Ovšem připojení přes zabezpečené HTTPS či FTPS nelze pomocí Kerio firewallu sledovat, to je možné pouze u nezabezpečeného připojení. Tyto zabezpečené komunikace je možné pouze blokovat zamezením přístupu na konkrétní servery komunikačními pravidly.

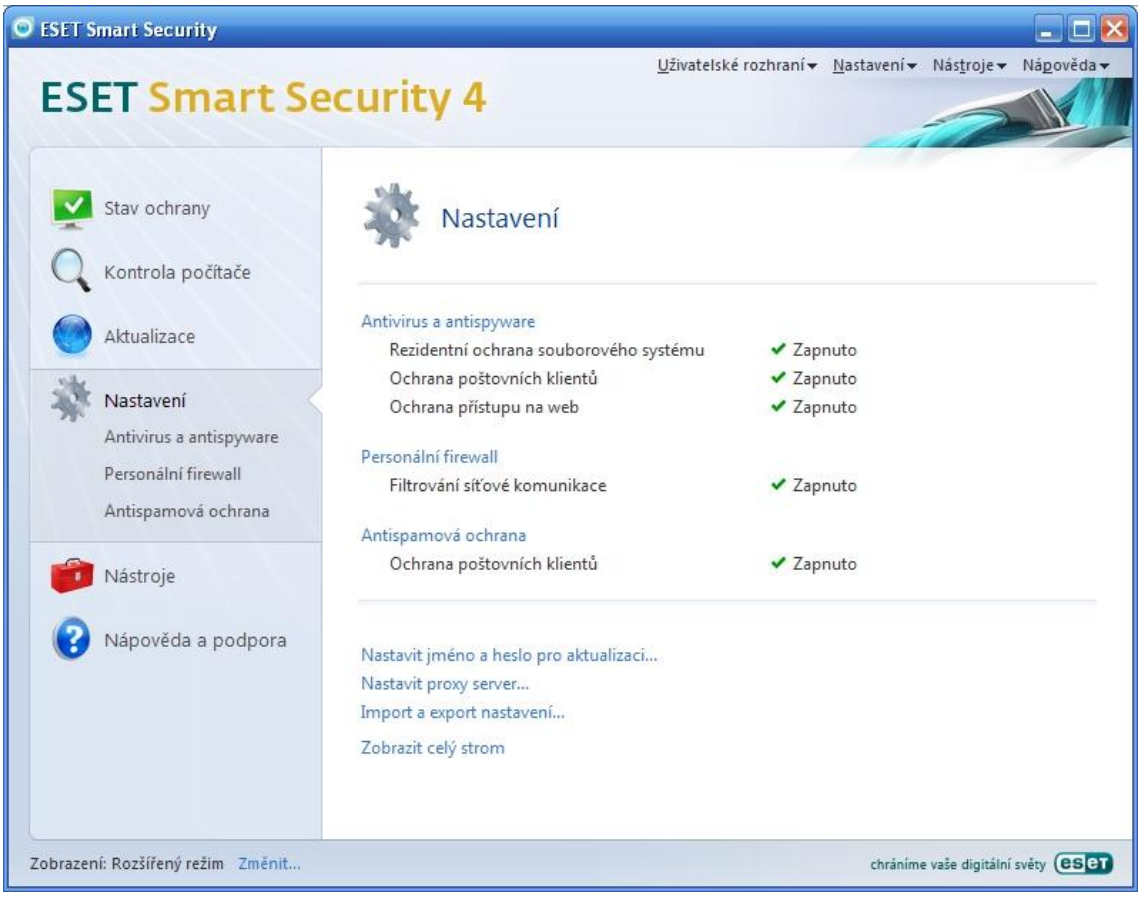
Pro případné filtrování URL můžeme nastavit v Kerio tyto možnosti:

Pro stránky s povoleným přístupem lze nastavit tyto doplňkové kontroly / omezení:

- Filtrovat z HTML kódu Java applety (filtrování všech elementů),
- Filtrovat z HTML kódu objekty ActiveX (filtrování všech elementů),
- Filtrovat z HTML kódu tagy Script (filtrování všech elementů),
- Filtrovat z HTML kódu automatické otevírání nových oken (tzv. pop-up blocker),
- Filtrovat položky Referer z jiných domén (často se používají pro sledování, odkud návštěvník na stránku přišel),
- Zamezit přístup na stránky obsahující zakázaná slova v HTML kódu
- Neprovádět antivirovou kontrolu (může zrychlit přístup na důvěryhodné stránky, obecně se však doporučuje antivirovou kontrolu provádět).
- Zakázat - uživatel bude přesměrován na stránku firewallu s informací o zakázaném přístupu.
- Zahodit – uživateli se stránka bude jevit jako nedostupná

6.4.2 Ochrana stanic

K ochraně jednotlivých stanic je použit antivirový software, v našem případě ESET Smart Security, který nabízí všechny dostupné prvky ochrany včetně rezidentního štítu. Nastavení je opět prováděno administrátorem a uživatelům vnitřní sítě je zamezeno přistupovat do jeho nastavení.



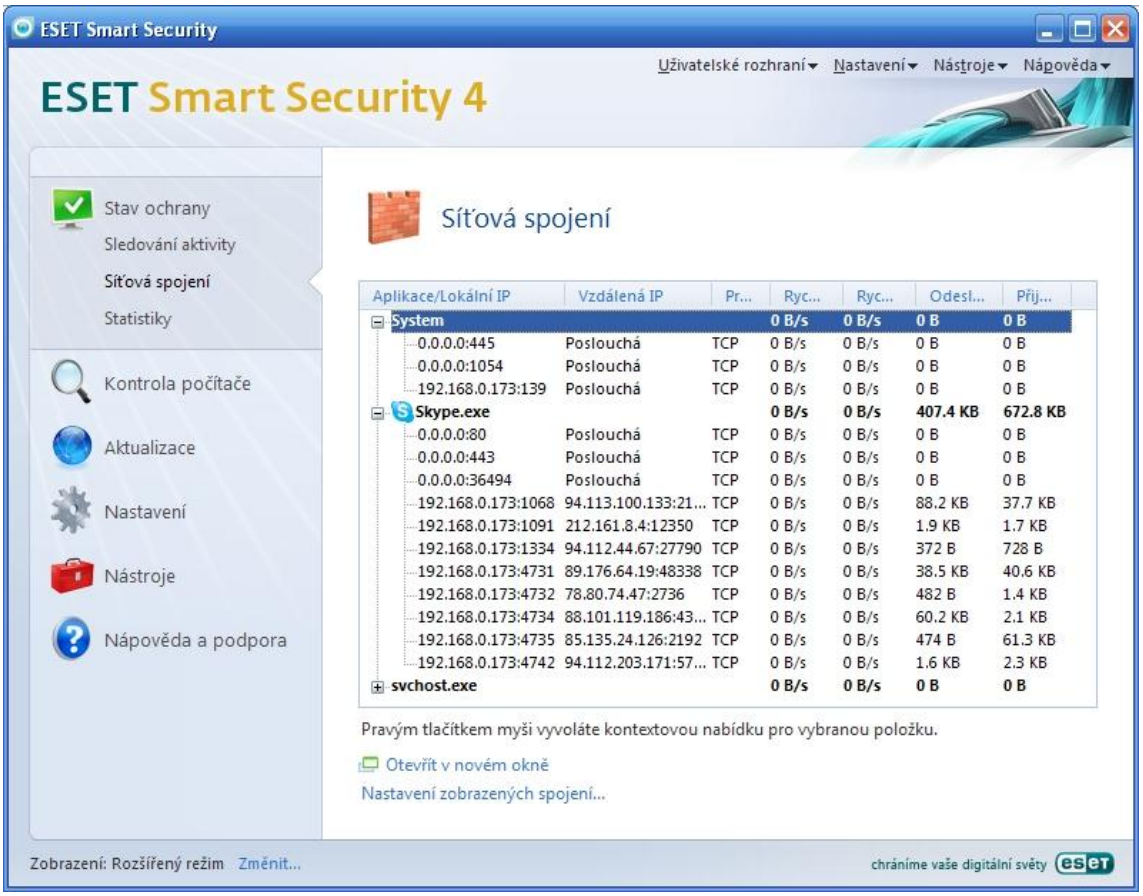
Obrázek 9 - Přehled nastavení ESET Smart Security

Uvedené dialogové okno zobrazuje stav ochrany stanic pomocí ESET Smart Security. Je patrné, že všechny dostupné funkce jsou zapnuté a stanice je tak v režimu maximálního zabezpečení v rámci možností programu. Je zapnuta rezidentní ochrana, která v reálném čase monitoruje možné nestandardní události, ochrana poštovních klientů (Thundebird) a také osobní firewall pro konkrétní stanici. V rámci klientů pošty je nastavena i antispamová ochrana. V možnostech nastavení firewallu je poté vybrán administrátorský režim, který bude pracovat na základě pravidel určených

administrátorem a v případě události nedefinované či neopatřené pravidly bude tato automaticky zamítnuta.

Dále je možné v nastavení IDS určit pravidla pro detekci známých útoků, povolit služby jako je sdílení tiskáren či komunikaci v rámci neznámé zóny či kontrolu packetů. Je možné nastavení detekce změny aplikací, kdy firewall povolí změnu důvěryhodných (podepsaných) aplikací. Ve volbě Zobrazení spojení je možné nastavit překlad IP adres na názvy stanic či porty na kterých počítač naslouchá a jiné.

Na obrázku níže je poté zobrazena funkce monitorování síťové aktivity, kde jsou znázorněny jednotlivé aplikace či programy, které komunikují s vnější sítí a také jsou vypsány IP adresy, které se pokouší o komunikaci se stanicí a dále porty na kterých stanice naslouchá. Tato spojení lze poté jednotlivě či hromadně zablokovat či si o nich zobrazit podrobnosti, stejně tak je možné blokování jednotlivých portů.



Obrázek 10 - Monitor síťové komunikace v ESET Smart Security

Je použit i osobní firewall, pro zvýšení ochrany a detekce potenciálních nechtěných protokolů a aplikacích. Firewall Commodo Internet security, který se v testech umístil velmi dobře, navíc nám ušetří náklady, jedná se o bezplatnou verzi. Proti případným spyware je nainstalován scanner Ad-aware, který nabízí i ochranu v reálném čase a sleduje případné změny registrů, které nahlásí a nepovolí bez našeho souhlasu.

Níže uvedený obrázek znázorňuje okno rozhraní Ochrany v reálném čase, kde v prvé kolonce jsou zobrazeny běžící procesy, v prostřední jsou události, kdy dochází k pokusu o změnu či přístup k registrům operačního systému a v poslední kolonce je seznam zablokovaných IP adres, které se pokoušely o komunikaci se stanicí a jimž nebyla tato komunikace povolena či jsou na černé listině výrobce software. Všechny tři možnosti je možné zapnout ve volbách nastavení.

Obrázek 11 - Ad-Aware přehled ochrany v reálném čase

Aktualizace těchto prostředků je prováděna podle naplánování administrátorem, nejlépe v době po či před pracovní dobou.

6.5 Používání software a hardware vnitřními uživateli/zaměstnanci

V rámci podniku a jím nastavených pravidel bezpečnosti, která jsou zde restriktivní, je vhodné definovat pravidla pro užívání programového i hardwarového vybavení pracoviště. Každý zaměstnanec by měl být pečlivě proškolen, s jakým zařízením přijde do styku a s jakým bude pracovat. Jednotlivým zaměstnancům firmy jsou nastavena pravidla pro přístup k jednotlivým počítačům, připojování periférií, zásah do konfigurace OS či software a mnohé další. Díky restriktivní politice a citlivosti dat, se kterými sázková kancelář pracuje, mají výše zmíněné vesměs zakázáno. To platí i o softwaru. Zaměstnanci mají omezenou kapacitu na jím vyhrazeném diskovém prostoru na nezbytné minimum. Nesmějí stahovat žádné soubory z internetu ani instalovat z přenosných médií. Je vhodná pravidelná kontrola síťové komunikace, pro odhalení případného nedodržování.

6.6 Pohled samotných uživatelů

Centrem bezpečnosti v operačním systému Windows XP je Centrum zabezpečení. Zde můžeme nastavit možnosti internetu, automatické aktualizace, nastavení firewallu. Dále hlídá i použití antivirového programu a varuje nás před zastaralostí virových definic, popřípadě nepřítomností antiviru. Kromě všech těchto základních programů je vhodné použít i specializovaný program pro odhalování spyware, adekvátní je v tomto ohledu již zmíněný Ad-Aware, který nabízí i rezidentní ochranu, solidním nástrojem je i program Malwarebites, který prohlíží systémové i souborové složky a vyhledává malware či některé viry infekce v root adresářích. Kromě nastavení automatických aktualizací počítače, je tedy nutné vždy používat minimálně následující trojici programů: firewall, antivirový program a program pro odhalování spyware. Mnohé z antivirů samy na potřebu aktualizace upozorní, někdy je nepřístupný server a aktualizace neproběhne v potřebné relaci. Výše zmíněné ovšem neznamená, že na počítači musí být nainstalován pouze jeden program od každého z prvků ochrany. Některé programy integrují funkci firewallu a antiviru a zrovna tak lze použít současně i více programů odhalujících spyware. Toto řešení lze považovat za vhodnější, neboť žádný program není 100% spolehlivý, proto lze tímto zdvojením zvýšit bezpečnost počítače. Zatímco u detektorů spyware lze použít více programů současně, firewall bude

pouze jeden. Mnohé antiviry s vestavěnými firewall či více firewallů se v operačním systému špatně snáší a nezřídkakdy dochází ke kolizím, což ohrožuje celkovou bezpečnost systému, paradoxně tedy vícenásobné zabezpečení může systém ohrozit.

6.7 Domácí síť a její zabezpečení.

Jak bylo napsáno v úvodu kapitoly, práce se zabývá také problematikou zabezpečení menší domácí sítě, která se logicky od podnikové liší. Počet počítačů, které je třeba propojit, je 3. Dva jsou pracovní stolní PC a jeden je notebook. K propojení opět použijeme UTP kabel typu 5e s konektory RJ45. Stolní PC budou propojeny přes router se zabudovaným switch a možností připojení počítače přes Wi-fi. Společný počítač v obývacím pokoji bude spojen s routerem, do kterého je zapojen modem poskytovatele připojení. Router respektive bezdrátový přístupový bod kombinovaný s routerem má 4 LAN rozhraní. Do budoucna se nepočítá s nákupem stolního PC, maximálně dalšího notebooku, proto je počet LAN rozhraní routeru dostatečný. K přístupovému bodu je přes kabeláž připojen druhý stolní počítač v pokoji dětí. Notebook, který používá celá rodina, je poté připojen bezdrátově naklonováním MAC adresy a zabezpečen pomocí WPA2 s privátním klíčem, uloženým na médiu flash.

I zde je třeba zhodnotit potenciální rizika a podle toho investovat do zabezpečení. Výhodou domácí sítě je fakt, že většinou neoperuje s příliš citlivými daty, a pokud ano jsou to data dotyčných uživatelů, proto nároky na bezpečnost nejsou nijak velké. Výjimkou je případ, kdy je na některé ze stanic uloženo například podnikové hospodářství a dokumentace k podnikání jednoho z členů rodiny, zde se potom vyplatí investovat do bezpečnosti více.

Značná část modemů i routerů již má zabudován alespoň základní firewall. Proto může uživatel zvýšit bezpečnost pomocí šifrování. Jako administrátor může pomocí EFS zašifrovat souborové složky, pro lepší ochranu může použít i některý multifunkční balík jako třeba PGP. Samozřejmostí by měl být antivirový program a firewall. Operační systémy jsou jím již dnes vybaveny, ovšem jejich úroveň není tak komplexní, zvláště u produktů Microsoft, lépe je na tom Linux či Unix.

Firewallů i antivirů je na výběr celá řada a je poté na uživateli, jaké si nastaví zabezpečení. Je vhodné pohlídat si kompatibilitu firewallu i antiviru, aby v jejich provozu při rezidentní ochraně nedocházelo ke kolizím. Vždy je lepší použít placené verze, které zajišťují zákaznický servis a bezproblémový přístup k aktualizacím. Ty je potřeba provádět zodpovědně a co nejčastěji. Je možné i provádět vlastní nastavení, pokud se na to uživatel cítí.

Nastavení zón firewallu slouží pro vylepšení vlastností ochrany.

Jak již bylo uvedeno výše, DNS stejně jako firewall pracuje se zónami.

Pravidla a zóny jsou základním stavebním kamenem firewallu a bez nich je téměř k ničemu. Pro běžného uživatele stačí ponechat nastavení v automatickém režimu, ovšem pro administrátora či zkušenějšího uživatele znamená možnost ovlivnění nastavení šanci firewall v mnohém vylepšit. Nastavení pravidel a zón není možné ve všech režimech filtrování - v automatickém režimu nemá význam a není přístupné.

Zóna, jak již bylo zmíněno, je v podstatě pseudosíť (domácí, pracovní, veřejná WiFi třeba na autobusových linkách či nemocnicích), do které je počítač připojen. U zóny (sítě) ještě rozlišujeme, zda ji pokládáme za důvěryhodnou, nebo ne. Důvěryhodná síť bude logicky domácí síť. Veřejná WiFi oproti tomu rozhodně důvěryhodná být nemůže, protože je možné se do ní přihlásit prakticky bez problému a při vhodném softwaru je možné i zachytávat segmenty datového toku či odposlouchávat porty apod.

Pravidlo ve firewallu představuje způsob jeho chování ve vztahu k nějaké konkrétní aplikaci (třeba k internetovému prohlížeči nebo messengeru či download manageru), ke konkrétnímu komunikačnímu protokolu, nebo k součástem operačního systému. Většina antivirů či firewallů proto nabízí právě rozšíření možnosti nastavení s více možnostmi. Toto je vhodné spíše pro podnikové administrátory, ovšem běžný uživatel, pokud si dá záležet, může výrazně zvýšit zabezpečení své domácí sítě, samozřejmě také může mnoho věcí pokazit.

Dále je vhodné nastavit zabezpečení prohlížeče, nastavit filtrování pomocí SSL/SSL 3.0 a zároveň i TLS. K volnému používání existuje i program CCleaner a jemu podobné, který čistí a opravuje registry, promazává cookies i cache prohlížeče.

Z pohledu uživatele je tedy zabezpečení domácí sítě vcelku jednoduchou záležitostí, alespoň na dostačující úroveň. Dále je vhodné nastavit pravidla používání sítě, stahování souborů a přístupu ke stránkám, i zde je možné zavést je podobně jako v podnicích restriktivně či liberálně. Bezpečnost každé sítě je totiž tak slabá, jaký je její nejslabší článek. U většiny sítí to bývá právě uživatel.

6.8 Rizika podnikové i domácí sítě

Kromě běžných výše zmíněných útoků, infekcí a infiltrací hrozí síti ještě další nebezpečí a tím je ztráta dat. Ta nemusí být vždy způsobena nějakým úspěšným útokem na síť.

6.8.1 Hardwarová příčina ztráty dat

Nejnebezpečnější formou je porucha pevných disků. Při poruše jiných součástí počítače může dojít k pádu systému či nefunkčnosti počítače, ovšem data zpravidla zůstanou zachována. V případě poruchy pevného disku už tomu tak zpravidla nebývá. Zálohování dat je tak pro každý systém prioritou. K problémům a ztrátě dat může dojít kdykoliv, při přehřátí procesoru či grafického adaptéru, kdy nejlépe v průběhu práce dojde ke zhroucení systému a ztrátě neuložených dat. Při bouřkách může dojít k poškození zdroje napájení počítače či spálení základní desky a opět ztrátě neuložených dat. K ochraně proti těmto nežádoucím jevům je vhodné použít systém přepěťové ochrany, v těchto domácích podmínkách se nejčastěji využívají bezpečnostní zásuvky. Zárukou kvality a zkušeností jsou v tomto segmentu výrobky firmy APS.

Toto vše tedy je také třeba v rámci péče o bezpečnost řešit.

6.8.2 *Softwarová příčina ztráty dat*

Mezi softwarové příčiny ztráty dat je potřeba zařadit i útoky viz kapitola 4. Jde přitom o úmyslné poškození či zničení dat, či shození systému. Ke ztrátě dat však může dojít i neúmyslně, sem můžeme zařadit různé chyby v software, které se mohou např. projevit pouze v určitých situacích, nebo kombinacích s konkrétním hardwarem. Softwarové příčiny jsou poměrně časté – např. při použití OS Windows, který má často problémy s kompatibilitou s opensource programy, či programy konkurenčních firem. V rámci domácích síti je to ovšem velmi často chyba uživatele, který zanáší systém mnoha programy, které poté odinstaluje, ovšem záznamy v registrech a knihovny zůstávají, což může způsobovat kolizi aplikací. Proto je vhodné užívat pouze potřebné programy, v opačném případě provádět pravidelně čištění a opravu registrů, defragmentaci disku a občas i kontrolu povrchu pevného disku.

Zálohování dat je také velmi důležitou součástí. Při práci je důležité často ukládat a v určitých intervalech překopírovat uložená data například na DVD disk či jiná vhodná archivační média. Operační systémy nabízejí také mechanismy pro usnadnění zálohy dat. Je vhodné je využít s ohledem na správný výběr podstatných dat. Zálohování 500GB harddisku na DVD nosiče není asi nejlepší metodou. V podobných situacích se může dobře osvědčit přenositelný disk s několika GB kapacitou nebo právě vhodný a uvážlivý výběr zálohovaných dat.

6.9 Ekonomická stránka zabezpečení

Důležitou roli při zabezpečování sítě hraje i náročnost ekonomických investic při jejím zakládání, ale také při provozu. Zakládáme-li firemní síť, pořizujeme nejprve stanice. Pro naší malou kancelář byl počet stanic stanoven na 8. Na přepážkách je umístěno 6 stanic, které se pohybují cenově v relaci mezi 5-10 tisíci korun u kancelářských typů. Pro nás bude nejspíše vhodná střední cesta 8 tisíc korun za jednu stanici. Taktéž monitory doporučuji ve střední třídě, kdy je dobré zvolit již prověřeného výrobce, což může zajistit delší životnost a lepší zákaznický servis. Zde se budeme pohybovat v relaci kolem 2500-3500 korun za jeden monitor. S ohledem na skutečnost, že jedna ze stanic bude zároveň serverem, můžeme ušetřit na tomto. Shrnuto na stanice i s periferiemi vynaloží kancelář 85-95 tisíc korun.

Další položkou bude firewall. Naše výdaje budou vyšší, z důvodu rozhodnutí zapojit firewallovou ochranu metodou demilitarizované zóny, tedy za pomoci dvou routerů. Cena jednoho se bude pohybovat ve vyšší třídě, tedy kolem 20 tis. korun, s tím že druhý, skrytý za proxy můžeme vybrat levnější verzi cca kolem 12-15 tis. korun. Výhodou těchto firewallů, je solidní uživatelské rozhraní, velké množství zabezpečovacích funkcí, jak filtrování, tak detekce (IDS, IPS) potencionálních útoků.

Náklady na softwarové vybavení budou řešeny nejlépe multilicencí, která umožní využití OS, antivirů či personálních firewallů, pro jednotlivé stanice i v širší míře. Zde se může souhrnná cena vyšplhat také k několika desítkám tisíc korun. Operační systém, se bude pohybovat v relaci 5-6 tisíc korun, Serverový OS Microsoft také kolem 6 tisíc korun, Linuxový OS pro aplikační server může být v relaci do tisíce korun za placenou distribuci. Licence Eset Smart Security (Antivir i s firewallem) se dá sehnat v relaci kolem 1500 korun, ovšem je třeba každý rok či v jiném rozmezí dle distribuce obnovovat licenci, pro dostupnost aktualizací. Vyšplháme se tedy k částce kolem 13 tisíc korun, k tomu je třeba připočíst i kancelářské balíky a speciální aplikace pro práci s kurzovým sázením, které nám patrně cílovou cenu zvednou o přibližně 10 tisíc korun. Pořizovací cena se tak může vyšplhat i s dalším softwarem do výše cca 120-130 tisíc korun. K tomu je třeba připočíst i náklady na provoz a připojení, v případě outsourcingu administrování sítě i náklady pro externího dodavatele služeb.

Data, která ovšem v této firmě budou proudit do sítě z venku a poté i v rámci vnitřní sítě, jsou s ohledem na druh podnikání velmi citlivá. Jejich zneužití, či únik chybou zabezpečení sítě, či chybou uživatelů vnitřní sítě a pracovníků s databázemi, může mít velmi vážné následky pro podnikání a také v trestně právní rovině. Proto je doporučeno na implementaci síťové bezpečnosti nešetřit náklady.

Co se týče domácí sítě, zde náklady s nákupem stanic nejspíše odpadnou, respektive již byly využity a potřeba sítě přišla až vlastnictvím zmíněného množství stanic. Nákladem bude tedy hlavně poskytované připojení, které se pohybuje v relaci okolo 500-1000 korun ve velmi slušné přenosové rychlosti. Rozhodli jsme se zabezpečit síť pomocí firewallu vestavěného v routeru, který má navíc funkci přístupového bodu pro připojení pomocí Wi-fi. Zde půjde o relaci v rozmezí 500-900 korun. Antivirový

program s osobním firewallem opět kolem 1000 korun plus výdaje za obnovení licence. V konečném součtu náklady nepřesáhnou, nepočítáme-li cenu stanic, 5-6 tisíc korun.

7 Závěr

Rozvoj internetové a intranetové sítě přinesl světu nové obrovské možnosti. Vytvořením platforem pro setkávání, studium, zábavu, obchod a výměnu informací se otevřely uživatelům zcela nové obzory. Anarchistická, i když do značné míry zdánlivá, podstata internetu, která se utvořila, umožňuje takřka každému uživateli svobodný prostor pro seberealizaci i úspěch.

Tato podstata sebou ovšem nese i mnoho nebezpečí a negativních prvků.

Cílem této práce bylo charakterizovat a vymezit pojem internetu, zmínit jeho krátkou historii a vývoj. Na základě nastudované dostupné literatury bylo účelem popsat stavební kameny a prvky této sítě, jejich principy a rizika. Dále určit potenciální hrozby takové sítě a také popsat způsoby její ochrany. Hlavním cílem praktické části bylo na konkrétním příkladu tyto principy demonstrovat. Tyto cíle byly prezentovány s co nejvyšší mírou srozumitelnosti i pro ne příliš informačně zdatné uživatele. Byly nastíněny principy zabezpečení sítě, se kterou se může uživatel jako zaměstnanec setkat. Z tohoto důvodu bylo také provedeno stručné definování malé domácí sítě, z důvodu alespoň částečného srovnání.

Nebyla opomenuta ani možná nebezpečí, konkrétně ztráty dat, která mohou vyplynout z běžné činnosti, nikoliv jen z útoku a která kladou také značné nároky na bezpečnost, pravidla provozu a užívání stanic a také náklady na zabezpečení a softwarovou vybavenost.

Zabezpečení internetové sítě je záležitost poměrně náročná a často také relativně drahá. Je třeba klást důraz na její správnou architekturu. Přesně definovat priority, jako je zabránění úniku hesel, zabezpečení dat zaslaných jinými uživateli a obsahující části nebo celé autentifikační a autorizační údaje. Kvalitní a dobře umístěný firewall je nezbytností. Má-li jako sázková kancelář či jakákoliv další společnost přístup k citlivým datům a zabývá-li se komerční činností, je vždy riziko pokusu o prolomení obrany a zneužití těchto dat poměrně vysoké, je tudíž zodpovědností a prvořadou snahou, tato data ochránit, proto jsou považovány výše uvedené návrhy zabezpečení jako minimální a rozhodně se nedoporučuje na jejich implementaci šetřit, ať již nezajištěním

dostatečných prostředků hardwarových či softwarových. Dále je prioritou vhodné proškolení uživatelů, jak pro práci s aplikacemi, tak v rámci bezpečnostní politiky firmy, protože největším nebezpečím pro vnitřní síť, při dodržení uvedených zabezpečení, je samotný uživatel.

Uvedené cíle se v rámci rozsahu práce podařilo uspokojivě splnit. Pro bližší a důkladnější architekturu nejen internetového zabezpečení by byla vhodná konkrétní pracovní zkušenost na pozici bezpečnosti v IT se zaměřením na počítačové sítě.

8 Seznam použitých zdrojů

BISHOP, M. 2002. *Computer Security: Art and Science.* Boston : Addison Wesley, 2002. 0-201-44099-7.

CEJPEK, J. 2005. *Informace, komunikace a myšlení.* Praha : Karolinum, 2005. 80-246-1037-X.

DOSTÁLEK, L. 2000. *Velký průvodce TCP/IP a DNS.* Praha : Computer Press, 2000. 80-7226-3234.

DOSTÁLEK, L. 2001. *Velký průvodce TCP/IP: Bezpečost.* Praha : Computer Press, 2001. 80-7226-513-X.

ENDORF C., MELLANDER J., SCHULTZ E. 2005. *Detekce a prevence počítačového útoku.* Praha : Grada Publishing, 2005. 80-247-1035-8.

STALLINGS, W. 2003. *Network Security Essentials.* místo neznámé : Prentice Hall, 2003. ISBN 0-130-35128-8.

STŘIHAVKA, M. 2001. *Vaše bezpečnost a anonymita na internetu.* Praha : Computer Press, 2001. 80-7226-586-5.

KRATOCHVÍL, P. 2010. Eleonore Exploits Toolkit . *Chip.* [Online] 8. Srpen 2010. http://www.chip.cz/novinky/bezpecnost/2010/08/eleonore-exploits-toolkit.

KRČMÁŘ, PETR. 2010. Největší hrozby internetu? Trojské koně, phishing a sociální sítě. *ROOT.CZ.* [Online] 17. Únor 2010. http://www.root.cz/clanky/nejvetsi-hrozby-internetu-trojske-kone-phishing-a-socialni-site/.

HALLER, M. 2006. Odposloucháváme data na přepínaném Ethernetu 2. *LUPA.* [Online] Červen 2006. http://www.lupa.cz/clanky/odposlouchavame-data-na-prepinanem-ethernetu-2/.

Microsoft. 2010. Internetový zločin je stále vynalézavější. *Microsoft.* [Online] Microsoft, 22. Duben 2010. http://www.microsoft.com/cze/presspass/msg/20100429_news1.mspx.

BARTOŠEK, M. 1995. Krátce z historie Internetu. Brno *: Zpravodaj ÚVT MU : bulletin pro zájemce o výpočetní techniku na Masarykově univerzitě*, 1995. 1212-0901

HANÁČEK, P. a STAUDEK, J. 1997. Bezpečnost informačních systémů. Praha : *LANcom : Časopis pro počítačové sítě a počítačovou komunikaci,* 1997. 1210-2997.

KOŠŤÁL, D a STAUDEK, J. 1997. Firewally, bezpečnostní oddělovací uzly. Praha : *LANcom : Časopis pro počítačové sítě a počítačovou komunikaci*, 1997. 1210-2997.

PEŠA, R. 1999. Počítačové viry. *Zpravodaj ÚVT MU.* Brno : autor neznámý, 1999. 1212-0901.

9 Terminologický slovník

AH - Authentification Header – typ hlavičky, který slouží především k ověření totožnosti odesilatele datagramu a správnosti jeho obsahu v protokolu IPSec

ARP – Adress Resolution Protocol

BIOS - Basic Input-output System - základní program, který je uložen většinou v paměti ROM, a obsahuje instrukce pro zavedení operačního systému. BIOS zajišťuje ovládání základních komponent a periferií počítače

DNS – Domain Name System - převádí číselné IP adresy do jmenné formy a zpět na číselnou

DNSSec – Domain Name System Security Extensions - bezpečnostní rozšíření DNS, umožňuje ověření původu dat

EFS – Encrypting File System – šifrovací mechanismus pro zabezpečení dat

ESP - Encapsulating Security Payload – typ hlavičky, která slouží v IPSec protokolu k zašifrování přenášeného datagramu

FTP – File Transfer protocol - slouží k přenosu souborů mezi počítači v rámci počítačové sítě

HP – Handshake protocol – protokol SSL, kterým jsou přenášeny informace ohledně typu symetrického šifrovacího algoritmu, komprimačního algoritmu a data pro výpočet bloku klíčů.

HTTP – Hypertext Transport Protocol - internetový protokol pro hypertextové dokumenty v HTML formátu

HTTPS - Hypertext Transfer Protocol Secure - umožňuje zabezpečit spojení mezi prohlížečem a webovým serverem

IDS - Intrusion Detection System - systém pro detekci možného průniku do sítě, dělí se na HIDS (host based) a NIDS (network)

IPS - Intrusion Prevention System - systém prevence, jehož účelem je monitorovat, identifikovat a pokusit se zabránit možnému průniku do počítačového systému a dále o tom vypracovat záznam/log

IMAP - Internet Message Application Protocol - protokol sloužící pro vzdálený přístup ke schránce elektronické pošty

IP – Internet Protocol - protokol jenž je součástí TCP/IP protokolu a na němž probíhá většina relací internetu

IPSec - IP security - rozšíření IP protokolu o bezpečnostní prvek umožňující autentizaci a šifrování každého diagramu

MX - součást DNS, určující mailové servery a nastavující jejich prioritu)

NCP - Network Control Protocol – Protokoly NCP slouží k ustavení a konfiguraci různých parametrů síťového protokolu pro protokoly IP

NS – položka DNS, delegující pravomoci na jednotlivé domény a subdomény v rámci zóny

PGP – Pretty Good Privacy - je balík programů, který umožňuje šifrovat a dešifrovat zprávy, digitálně je podepisovat, ověřovat identitu odesílatele a spravovat klíče.

POP3 - Post Office Protocol version 3 - protokol sloužící ke stahování elektronické pošty z poštovního serveru ke klientovi

RLP - Record Layer Protocol - nosný protokol SSL/TSL

SIG - typ záznamu kde je uložen podepsaný veřejný klíč v rámci DNSSec

SMTP – Simple Mail Transfer Protocol internetový protokol k přenosu elektronické pošty

TCP – Transmision Control Protocol sada protokolů pro komunikaci v rámci počítačových sítí

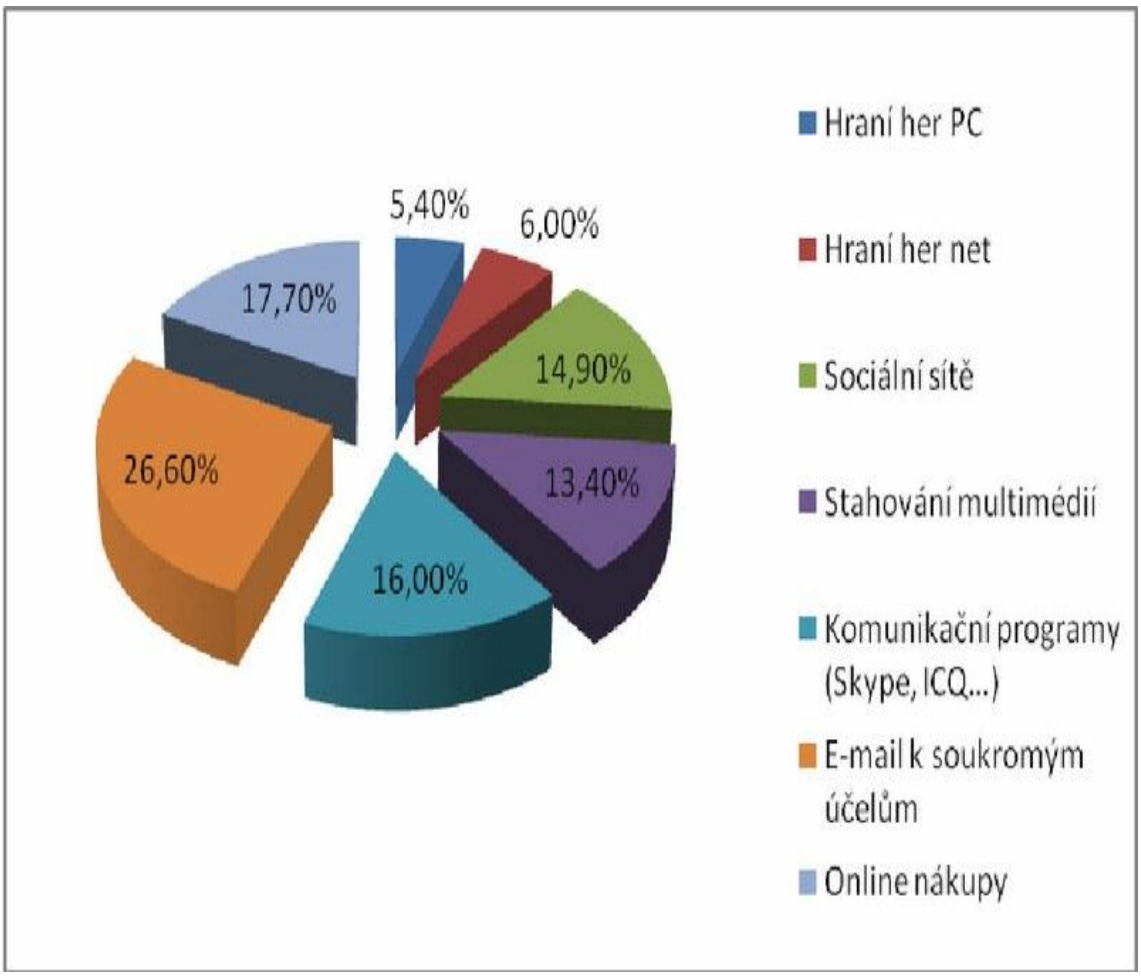
UDP – User Datagram Protocol - protokol pro komunikaci v rámci poč. sítí

10 Seznam Obrázků

11 Seznam příloh

Příloha 1 : Monitoring Aktivity zaměstnanců na síti

Možné využití spoofingu. Firmy monitorují síťovou činnost svých zaměstnanců. Problém, který dnes víří rozporuplné diskuse o jeho legálnosti, či etické nezávadnosti.



Monitoring aktivity zaměstnanců na síti

Obzvláště ukazatel užívání sociálních sítí, s ohledem na jejich prokázanou nedůvěryhodnost až nebezpečnost, dává zaměstnavatelům do značné míry za pravdu.

Příloha 2: Tabulka typů a počet bezpečnostních incidentů hlášených uživateli na pracoviště CIRT za období 2008-2010.

Typ incidentu	2008	2009	2010	Celkem
Phishing	65	220	206	491
Virus	0	121	178	299
Malware	53	96	42	191
Spam	47	28	101	176
Trojan	66	6	26	98
Botnet	0	3	46	49
Probe	0	3	14	17
Portscan	10	4	1	15
Other	1	5	8	14
DoS	1	5	2	8
Crack	1	0	4	5
Copyright	0	0	1	1
Celkem	244	491	629	1634

Zdroj:CESNET.CZ : Výroční zpráva 2010

Pracoviště CIRT je modelové pracoviště zastřešené společností CESNET, které má za úkol sloužit jako místo poslední záchrany při bezpečnostních problémech uživatelů internetu. Čísla v tabulce udávají počet hlášených incidentů uživateli za uvedené období.

Příloha 3: Ukázka wordlistu pro prolamování hesel (okruh myslivost)

lasice hranostaj
Mustela erminea
lasice kolčava
Mustela nivalis
tchoř tmavý
Mustela putorius
tchoř světlý
Mustela eversmanni
kuna lesní
Mustela martes
kuna skalní
Mustela foina
jezevec lesní
Meles meles
vydra říční
Lutra lutra
norek americký
Lutreola vison
mýval severní
Procyon lotor
medvěd hnědý
Ursus arctos
vlk euroasijský
Canis lupus
liška obecná
Vulpes vulpes
psík mývalovitý
Nyctereutes procyonoides
kočka divoká
Felis silvestris
rys ostrovid
Lynx lynx
veverka obecná
Sciurus vulgaris
ondatra pižmová
Ondatra zibethicus
bobr evropský
Castor fiber
zajíc polní
Lepus europaeus
králík divoký
Oryctolagus cuniculus
prase divoké
Sus scrofa
los evropský
Alces alces
jelenec viržinský
Odocoileus virginianus
daněk skvrnitý
Dama dama
jelen evropský
Cervus elaphus
sika japonský
Cervus nippon nippon
sika Dybowského
Cervus nippon dybowskii
srnec obecný
Capreolus capreolus
kamzík horský
Rupicapra rupicapra
koza bezoárová
Capra aegagrus
muflon
Ovis musimon
potápka roháč
Podiceps cristatus
kormorán velký
Phalacrocorax carbo
volavka popelavá
Ardea cinerea
labuť velká
Cygnus olor
husa velká
Anser anser
husa běločelá
Anser albifrons
husa malá
Anser erythropus
husa polní
Anser fabalis
berneška tmavá
Branta bernicla
kachna divoká
Anas platyrhynchos
kopřivka obecná
Anas strepera
čírka modrá
Anas querquedul
čírka obecná
Anas crecca
hnízdák euroasijský
Anas penelope
ostralka štíhlá
Anas acuta
lžičák pestrý
Anas clypeata
zrzohlávka rudozobá
Netta rufina
polák velký
Aythya ferina
polák chocholačka
Aythya fuligula
hohol severní
Bucephala clangula
luňák červený
Milvus milvus
luňák hnědý
Milvus migrans
orel mořský
Haliaeetus albicilla
včelojed lesní
Pernis apivorus
krahujec obecný
Accipiter nisus
jestřáb lesní
Accipiter gentilis
káně lesní
Buteo buteo
káně rousná
Buteo lagopus
orel skalní
Aquila chrysaetos
orel královský
Aquila heliaca
orel křiklavý
Aquila pomarina
moták lužní
Circus pygargus
moták pilich
Circus cyaneus
moták pochop
Circus aeruginosus
raroh velký
Falco cherrug
sokol stěhovavý
Falco peregrinus
ostříž lesní
Falco subbuteo
dřemlík tundrový
Falco columbarius
poštolka obecná
Falco tinnunculus
orlovec říční
Pandion haliaetus
tetřev hlušec
Tetrao urogallus
tetřívek obecný
Tetrao tetrix
jeřábek lesní
Tetrastes bonasia
koroptev polní
Perdix perdix
orebice horská
Alectoris graeca
křepelka polní
Coturnix coturnix
bažant obecný
Phasianus colchicus
bažant královský
Syrmaticus reevesii
krocan divoký
Meleagris gallopavo
perlička obecná
Numida meleagris
lyska černá
Fulica atra
drop velký
Otis tarda
sluka lesní
Scolopax rusticola
bekasina otavní
Gallinago gallinago
racek chechtavý
Larus ridibund