Bezpečnostní rizika v prostředí internetu

Security risks on the internet

Bc. Robert Zemko

Diplomová práce
2011

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

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

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Robert ZEMKO**
Osobní číslo:	**A09692**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Bezpečnostní rizika v prostředí internetu**

Zásady pro vypracování:

1. **Pro vlastní potřebu zpracujte rešerši literatury a pramenů, které se vztahují k tématu diplomové práce.**
2. **V úvodu diplomové práce v rámci východiskové hypotézy specifikujte zkoumaný problém, vymezte a analyzujte bezpečnostní hrozby v kyberprostoru.**
3. **Specifikujte vlastnosti subsystémů ochrany, definujte výhody, nevýhody a rizika vznikající jejich používáním.**
4. **Analyzujte bezpečnostní problémy současného systému.**
5. **Proveďte kyberforenzní analýzu digitálních dat v případě relevantního útoku.**
6. **Navrhněte systém bezpečnostních opatření a postupů ke zlepšení stávajícího systému ochrany.**
7. **Proveďte vyhodnocení a ověření návrhu, včetně možností jeho využití v praxi.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **BAYUK, Jennifer. Cyberforensics : Understanding information security investigations. 1st edition. New York : Springer, 2010. 167 s. ISBN 978-1-60761-771-6.**
2. **MITRA, Ananda. Digital Security : Cyber Terror and Cyber Security. 1st edition. New York : Chelsea House, 2010. 120 s. ISBN 978-0-8160-6791-6.**
3. **STAMP, Mark. Digital Security : Cyber Terror and Cyber Security. 1st edition. New Jersey : Wiley & Sons, 2005. 416 s. ISBN 0471738484.**
4. **LAYTON, P. Timothy. Information Security: Design, Implementation, Measurement, and Compliance. 1st edition. New York : Auerbach, 222 s. ISBN: 0849312701.**
5. **JIROVSKÝ Václav, Kybernetická kriminalita : nejen o hackingu, crackingu, virech a trojských koních bez tajemství, První vydaní, Praha: Grada, 2007, 288 s, ISBN 978-80-247-1561-2.**

Vedoucí diplomové práce: **PhDr. Mgr. Stanislav Zelinka**
Ústav bezpečnostního inženýrství

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

Termín odevzdání diplomové práce: **27. května 2011**

Ve Zlíně dne 25. února 2011

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

ABSTRAKT

Cieľom diplomovej práce je určenie bezpečnostných rizík v prostredí kyberpriestoru, metódy ochrany jednotlivých subsystémov a analýza bezpečnostného systému v spoločnosti, kyberforenzná analýza vedúca k odhaleniu potencionálneho útočníka, bezpečnostné opatrenia k zlepšeniu systému v spoločnosti, overenie a vyhodnotenie návrhu v praxi.

Kľúčová slová: Bezpečnosť, ochrana, kyberpriestor, sieť, analýza, prepínač, smerovač, firewall

ABSTRACT

Goal of this thesis is to identify security risks in the environment of cyberspace, methods of individual subsystems and analysis of security system in organization, cyberforensics analysis leading to detection of a potential attacker, security precautions to improve the system in a company, verify and evaluate the proposal in practice.

Keywords: Security, protection, cyberspace, network, analyze, switch, router, firewall

Poďakovanie:

Rád by som poďakoval PhDr. Mgr. Stanislavovi Zelinkovi, za jeho odborné rady pri spracovaní diplomovej práce a mojej rodine za poskytnutú podporu pri písaní.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

Každý z nás používa informačné systémy. Počítače sa stali neoddeliteľnou súčasťou každodenného života. Komunikačne siete sa rozšírili do mnohých spoločností a domácností. Či už interné komunikačné siete, alebo externé siete ako internet, pre každého z nás je dôležitá neustála komunikácia. Tak ako aj s výhodami komunikácie, prišli aj nevýhody a tak sa začali objavovať bezpečnostné hrozby a potencionálne riziká. Najcennejšou hodnotou pre spoločnosti a domácnosti je ochrana dát a utajenie informácií pred nepovolanými osobami. Dcérske pobočky potrebujú komunikovať s materskou spoločnosťou, užívatelia vymieňajú dáta. Z roka na rok, rastie množstvo novo pripojených užívateľov do sietí a rovnako aj útoky. Atraktivita útokov rastie, pretože moderná spoločnosť sa snaží takmer všetko pretransformovať do elektronickej podoby. Citlivé dáta môžu tak byť zneužité tretími osobami, napríklad rodné čísla, čísla kreditných kariet. A preto spoločnosti musia reagovať na aktuálne hrozby bezpečnostými opatreniami, ktoré implementujú do stávajúceho systému. Takýmito opatreniami minimalizuje riziká hroziace pre spoločnosť. Sto percentná ochrana neexistuje, ale musia sa eliminovať riziká na čo najmenšiu úroveň.

Diplomová práca sa zaoberá bezpečnostnými rizikami v prostredí siete internetu. V teoretickej rovine je práca rozdelená na dve kapitoly. V nich sú vysvetlené jednotlivé hrozby a riziká v kyberpriestore, ktoré reálne hrozia užívateľom. Na druhej strane existujú jednotlivé riešenia, ktoré slúžia k minimalizovaniu hrozieb a rizík. V praktickej časti práce sa analyzoval bezpečnostný systém spoločnosti a tak sa našli potencionálne riziká, ktoré by sa neskôr môhli prejaviť. V prípade relevantného útoku, existuje kyberforenzná analýza, pomocou ktorej sa skúmajú jednotlivé spojitosti, vedúce k dopadnutiu potencionálneho útočníka. Systém bezpečnostných opatrení, metód a postupov zaistí dôkladnu ochranu proti jednotlivým hrozbám. Posudzovanie každého systému je individuálne. Samozrejme po implementácii nového systému bezpečnostných opatrení sa overoval návrh a testovala funkčnosť bezpečnosti v spoločnosti.

I. TEORETICKÁ ČASŤ

1 BEZPEČNOSTNÉ HROZBY V KYBERPRIESTORE.

V súčasnej dobe pojem bezpečnosť, zohráva dôležitú úlohu. Čoraz viac užívateľov sa denno - denne stretáva s hrozbami, ktoré na nich pôsobia. Mechanizmy zabezpečenia, útokov, hrozieb, rizík. Čo sa skrýva za útrobami virtuálneho sveta? Dá sa týmto hrozbám predchádzať? Aké riziká plynú z hrozieb? Aká škoda vznikne pre jednotlivca, spoločnosť? Každí z nás sa už stretol s nejakým bezpečnostným problémom, či už vírus, trójan, spam, atď. Mnoho ľudí bezpečnosť podceňujú. Dáta sú najcennejším artiklom, v digitálnom svete. Kybernetická kriminalita má svoje opodstatnenie v kyberpriestore. Štúdium kybernality zakladá nový interdisciplinárny odbor zabývajúci sa nelegálnymi a škodlivými aktivitami v počítačovom priestore, ktoré sú založené na zneužití počítačovej technológie. V tejto kapitole sa dočítate o histórii kyberpriesotoru, vzniku sietí, pojmy ako sú kybernetická kriminalita, prečo je tak dôležitá bezpečnosť, špecifikovanie bezpečnostných hrozieb. [1]

1.1 História kyberpriestoru

V roku 1968 vznikla prvá sieť ARPANET (Advanced Research Projects Agency Network), bola predchodcom internetu. Princíp fungovania tejto siete bola na báze prepínania paketov. V roku 1990 túto sieť premenovali na internet. V dobe vzniku protokolu TCP/IP, nikto nepredpokladal, že sa mäsovo rozšíri internet. A tak na bezpečnostné charakteristiky sietí a protokolov sa nekládol taký dôraz. Vývin technológií bol rýchli a tak v tej dobe sa nekládli také bezpečnostné požiadavky, ako dnes. Slabiny technológii sa stali hlavným cieľom nelegálnych aktivít. [2]Termín „kyberpriestor“ prvý krát použil spisovateľ William Ford Gibson v roku 1984 vo svojej knihe Neuromancer, kde ho definoval takto:

Konsensuálna halucinácia každý deň, okúsená miliardami oprávnených deťí, ktoré sa učia základy matematiky. Grafická reprezentácia dát, abstrahovaných z bánk všetkých počítačov ľudského systému. Neodmysliteľná komplexnosť. Línie svetiel zoradené v priestore mysli, zhluky a súhviezdia dát. Ide o počítačový trojrozmerný svet analogický s internetom, v ktorom sa užívatelia pohybujú pomocou virtuálnej reality.

1.2 Kyberpriestor

Kyberpriestor, ako taký spája realitu s virtuálnym svetom. Všetky aktivity sa uskutočnujú prostredníctvom počítačových a telekomunikačných sietí a počítačových systémov. Realitu zohráva v tomto prípade len človek, ktorý určuje príkazy. Medziľudské aktivity pomaly vymieňajú informačne systémy. V 21. storočí kyberpriestor, je vytvorený z globálnej infraštruktúry sietí, ktoré sú závislé medzi sebou. Pri najmenšom výpadku infraštruktúr, škody spôsobia veľký rozsah škôd. Pri zlyhaní napr. letiskovej infraštruktúry ide o životy, lebo všetko je závislé na kyberpriestore.. Zo sociálneho hľadiska, každý z nás môže individuálne ovplyvňovať, vymieňať názory, zdieľať informácie, poskytovať sociálnu podporu, obchodníci môžu robiť obchody, prevody peňazí, vytvárať videá, pesničky, hrať počítačové hry cez internet, zapájať sa do politických diskusií a používať taktiež globálnu sieť.

Pre lepšie pochopenie tohto termínu si uvedieme príklad. Pri odosielaní mailu, našim kamarátom s celého sveta komunikujeme cez siete. Pri čítaní mailu, pracujeme zase s počítačom, alebo prenosným zariadením ako PDA. Komunikácia je tzv. cez dráty, ktoré sú pospájané po celom svete. Takže komunikácia sa uskutočňuje v kyberpriestore.

1.2.1 Kyberkriminalita

Tak ako vznikol kyberpriestor, tak vznikla aj kyberkriminalita. V reálnom svete sa páchajú trestné činnosti, tak aj vo virtuálnom svete. S nástupom technológií vznikol aj priestor pre páchanie trestných činností a obohacovaní sa. Prvým problémom v dnešnej spoločnosti je to, že na zabezpečenie sietí, informačných systémov, nebol v začiatkoch tak kladený dôraz. Ďalším problémom, je postih osôb páchaných trestnú činnosť v kyberpriestore. Riziko je takmer nulové, kdežto pri ozbrojenom prepadnutí, hrozí riziko úmrtia . V reálnom svete, tak aj v kyberpriestore existuje zanechanie stôp a páchateľ sa dá vypátrať. Čím skôr sa začne s vyšetrovaním, tým existuje väčšia šanca dostať dotyčného páchateľa. Takisto vidím problém v dnešnej justícii, kde páchatelia nie sú dostatočne potrestaní a tak nemajú odstrašujúce príklady. Nie veľmi veľa prichytených ľudí pyká za svoje hriechy, tak ako by mali. Preukazovanie viny, je totiž veľmi ťažké a prácne. Spoločnosť sa musí naučiť posudzovať tieto hriechy inak.

Kyberkriminalitou rozumieme takú činnosť, ktorou je porušovaný zákon a je v rozpore s ním. Cieľom tohto druhu kriminality, je hardware, software, siete, dáta, atď. Táto kriminalita je páchaná prostredníctvom počítačov, softwaru a sietí za účelom dosiahnuť motív (škodu, zisk, dáta, atď.)

Útočník pracuje v globálnom prostredí, odkiaľ sa môže napojiť kdekoľvek na svete, kde je sieť. Najväčšou hrozbou je zmena identity, pod ktorou útočník vystupuje. Ak získa náš účet, tak bude vystupovať ako my. Alebo, môže kvôli maskovaniu využiť viacero počítačov aby zmenil svoju identitu, a vystopovanie bolo takmer nemožné. Útočník je vždy napred. Snaží sa nájsť bezpečnostné slabiny a využiť ich. Útočníci bývajú nadpriemerne inteligentní.

S hrozbami sa stretávame každý deň. Za riziko v hrozbách vidím odcudzenie dát. Nikto z nás by nechcel, aby fotky zo spoločnej dovolenky, sa dostali niekomu cudziemu do rúk. To je ešte tá lepšia varianta. Tou horšou variantou dneska vidím odcudzenie personálnych údajov z firemného prostredia. Rodné číslo, informácie o tom kde sa človek narodil, kedy, kde býva, čísla kreditných kariet. Chápanie bezpečnosti sa nesmie brať na ľahkú váhu. Nie len fyzické osoby sú terčom útokov. Právnické osoby držiace svoje know-how a technológie, sú lákadlom. Podľa stupňov utajenia, by sa mali k bezpečnosti tak aj správať. Terčom bývajú informácie aj o armáde a výzbroji štátov.

1.2.2 Kybervojna

Časopis The Economist, opisuje kybervojnu, ako novú generáciu vojny.[3] Novodobý pojem, ktorý je odvodený od kyberkriminality. Sú do nej zapojený jednotlivci, organizácie, štáty.

Kybervojna sa skladá z viacero druhov hrozieb: Špionáž, sabotáž, vyradenie súpera. Hlavnou motiváciou dnes je armáda, korporácie, civilné prostredie (Internetoví poskytovatelia, z infraštruktúra). Pekným príkladom je spoločnosť WikiLeaks, ktorá uverejňovala tajné skutočnosti, ktoré sa stali. Vládam po celom svete sa to nepáčilo, tak začali konať. Odstavili web stránku, ktorá poskytovala utajované informácie. WikiLeaks priaznivcom sa to nepáčilo, tak začali bojovať s vládou, pre uchovanie tejto stránky. Vlády dali príkaz na zmrazenie účtov pre túto spoločnosť, aby nemohla fungovať. Toto nemohlo ostať bez odplaty, tak hackeri na celom svete sa spojili a začali napádať organizácie, ktoré mohli za odstávku. Visa spoločnosť, Maestro, Paypal, Diners. Využívajú silu spoločného

útoku a zhadzujú servery. Snažia sa bojovať proti vláde. Ďalším pekným príkladom bol útok v Severnej Kórei. Boli napadnuté industriálne počítače, ktoré mali na starosť jadrový program. Tak isto aj Irán, Rusko a Gruzínsko, atď. Každopádne sa kybervojna stala novým fenoménom vojny medzi štátmi.

1.2.3 Kyberterorizmus

Nedávne počítačové útoky, mnohé z nich sa klasifikovali ako nová odroda terorizmu. Sú na vzostupe a každá krajina by sa mala chrániť sama, so všetkými možnými prostriedkami. Ako spoločnosť, máme dostatok operačnej a legálnej praxe k naplneniu techník bojového terorizmu, sme pripravený s ním bojovať. Ale čo kyberpriestor? Sme dostatočne pripravení bojovať s kyberpriestorom? Tento druh terorizmu je sofistikovaný, pretože využíva zložité operácie.

Existuje však mnoho nepresných interpretácií a pojmov kyberterorizmu. Kyberterorismus je premyslený, politicky motivovaný útok proti informáciám, počítačových systémov, počítačových programov a dát, ktoré vedú k násiliu čiastkových národných skupín alebo tajných agentov.[1]

Skupiny využívajú rôzne sofistikované metódy komunikácie, aby sa dohodli kedy má dôjsť k útoku. Napríklad kódovanie textu do obrázku. Existujú programy, ktoré zašifrujú text do obrázka. Čiže to znamená, že dokážeme zakódovať akýkoľvek text do obrázku s tým, že vtedy sa stane útok. A ak by sa náhodou dostal tento obrázok niekomu do rúk, tak tam nič neuvidí, pretože sa mu ukáže obrázok. Bez špeciálnych postupov, techník a softwaru, ide veľmi ťažko odhaliť túto metódu. Profesionálnejšie programy slúžia k zakódovaniu máp a súradníc. Typickou obeťou kyberterorizmu sa stal Izrael, Irán, Severná Kórea, USA, Rusko, atď.

1.2.4 Kyberšikana

Je čoraz populárnejšia. Vyskytuje sa hlavne na sociálnych sieťach, ako je Facebook, Twitter, atď. Postihuje hlavne deti, ktoré chodia do škôl. Nový fenomén sa dostáva do popredia spoločnosti. Cieľom je nahnať strach, zistiť čo najviac informácii o danej osobe a postupne tieto informácie sa snažiť zneužiť. Nie len deti, ale takisto aj zamestnávatelia sa snažia zisťovať informácie o aktivitách svojich zamestnancov a prostredníctvom monitorovania to aj zneužívať na pracovisku. Rada z takýchto prípadov spadá do

kriminálnych činov. Najčastejšie sa realizuje pomocou fotiek, nahráviek na elektronické zariadenie, najčastejšie pomocou mobilného telefónu, alebo digitálneho fotoaparátu. Tieto materiály sa snažia vystaviť na Internete. Na dotknuté osoby to má neblahý dopad. Spôsobenie psychickej traumy, psychické zrútenie a iné. Nikto by to nemal podceňovať a v prípade podozrenia nahlásiť to na políciu.

1.3 Osoby v kyberpriestore

Jedným z dôležitých faktov je ten, že treba rozoznávať osoby, ktoré participujú v kyberpriestore. Sú to užívatelia, ktorý sú identifikovaní pomocou IP adresy, alebo pomocou podľa užívateľského mena. Každý uživateľ, či už patrí do verejnej IP adresy, alebo neverejnej adresy, komunikuje s ostatnými užívateľmi, a tí sa pohybujú v kyberpriestore.

Ľudia, ktorí pracujú v kyberpriestore, delíme na viacero typov:

- Basic users (obyčajní užívatelia)
- Hackeri
- Phreakeri
- Crackeri
- Bezpečnostní špecialisti

Práve **obyčajní používatelia** sa stávaju častým terčom útokov. Môžu svojou nevedomosťou napáchať viac škody, ako úžitku. Preto rada znie: „Ak používatelia niečo nevedia, treba sa opýtať IT špecialistu, alebo osobu zaoberajúcou sa bezpečnosťou IT“. Práve tieto osoby poradia, ako zabezpečiť správne počítač, alebo server, prepínač, smerovač, atď. Preto treba porozmýšľať pred tým, ako začneme niečo nastavovať.

Hackeri patria k najlepšie zdatným používateľom. Netreba si predstavovať ľudí, ktorí majú omastené vlasy a okuliare. Taký je obraz médií, ktoré vytvorili vlastný obraz o nich. Sú to vysoko inteligentní ľudia, ktorí majú vlastné pravidlá a zásady. Zväčša žijú v komunitách a sú uzavretí.

Pojem hacker, vznikol zhruba v pädesiatych rokoch minulého storočia v komunite rádioamatérov, označoval sa ním šikovný a nadšený jedinec, schopný hľadať nové zapojenia a metódy k zlepšeniu svojho vysielača. Slovo hacking bolo prevzaté z anglo-

amerického výrazu, označovala sa ním nenútená prechádzka, bez nejakého zrejmého cieľa. Potom sa podarilo tomuto výrazu udomácniť na americkej univerzite MIT (Massachusetts institute of technology) v Bostone. Hack označovalo, riešenie problémov hravo a rýchlo. Študenti slengovo používali toto slovo, pre spáchanie nejakej neprístojnosti v MIT. [1]

V šesťdesiatych rokoch skupinka technologických nadšencov vedená Johnom Draperom, využívala nedokonalosť v telefonnej siete. Uskutočňovali nespoplatnené hovory. Základom mechanizmu bol tón o kmitočtu 2600Hz, ktorým sa riadilo prepínanie diaľkových hovorov. Dokázal to pomocou píšťalky. [1]

Definícia hackera charakterizuje schopnosť do detailu pochopiť detaily programovateľných systémov a hľadať metódy ako ich vylepšiť. S nadšením programujú, vytvárajú si vlastné skripty, dokážu spracovať dokonale technologické postupy. Dosiahnuté znalosti získali samoštúdiom. Sú zdatní v bezpečnostných otázkach. Ale majú aj negatívne stránky.

Existujú aj dobrí hackeri, ktorí po zistení chýb kontaktujú administrátora, aktívne s ním spolupracujú na odstránení nedostatkov až do konca. Pracujú ako strážcovia kyberpriestoru. Používajú aj špecifické písmo pre nich.

Zlí hackeri, patria k aktívnym hrozbám v kyberpriestore. Často označovaní ako Black hackers (čierny hackeri). Zaoberajú sa podobnou činnosťou ako dobrí hackeri, ale s tým rozdieľom, že poškodia systém, alebo napáchajú škody. Snažia sa získať výhody pre seba, alebo predať informácie odberateľom. Napríklad pre korporácie, ktoré chcú získať citlivé dáta, tak zväčša najmú tento typ hackerov. Najhoršia kombinácia je tá, ktorá spojuje teroristov a hackerov dohromady. Nie je nič horšie, ako poskytovať informácie pre teroristické skupiny. Závisia na tomto životy. Treba to tvrdo postihovať a nastaviť súdy tak, aby mohli konať v skrátených konaniach a boli títo ľudia tvrdo potrestaní.

Neutrálni hackeri, sú na rozmedzí dobrých a zlých hackerov. Nevedia sa rozhodnúť pre ktorú skupinu budú pracovať. Problém je v úlohách, ktoré plnia, a ich morálne zásady, kam sú schopní zájsť.

Najznámejším hackerom bol Kevin David Mitnick. Svojimi prienikmi spôsobil škodu v hodnote 300 miliónov dolárov. Okolo Mitnicka sa vytvorila legenda, ktorá rozprávala o tom, že sa nabúral do databáz úradu FBI a takisto si upravoval záznam o sebe. Podarilo sa mu dostať do počítača Pentagonu a nebol ďaleko od toho, aby spustil jaderné zbrane. Bol opakovane zatknutý za drobné krádeže, narušovanie slobody. Prepustený bol pod

podmienkou, že na tri roky sa nedotkne počítača. V súčasnosti, je uznávaným odborníkom a má svoju firmu Mitnick Security Consulting. Nesmie sa zabudnúť na osoby, ako je Richard Stallman, zakladateľ GNU/GPL licencie.

Crackeri sa zameriavajú na prelamovanie ochrany. Zväčša sa snažia prelomiť software, za účelom získať ho bez nutnosti kúpy. Napríklad program na generovanie sériových čísiel, alebo odblokovanie skúšobných verzií. Takisto prelamujú ochranu Wifi, ochranu WEP, WPA, WPA2 či už TKIP,AES. Crackeri na rozdiel od hackerov, vytvárajú straty. Niekto si povie, že crackeri nám uľahčujú život, keď dávajú k dispozícii svoje know-how. Sériové generátory umožnia registrovať hry, programy, atď. bez nutnosti registrácie. Pre tvorcov softwaru vznikajú obrovské straty. Spoločnosť sa musí naučiť správať tak, že bude podporovať výrobcov a kupovať ich produkty. Crackeri majú potešenie z deštrukcie ochrany. Je evidentné, že polícia, nemá dostatok informácií o týchto komunitách.

Phreakeri je označovaná skupina hackerov, ktorá sa zameriava na telefóny a telefonné ústredne. Uskotočnovali dlhé hodiny hovorov, z telefonných búdiek a využívali telekomunikačné siete zdarma. Phreakeri uskutočnovali častokrát diskusie, kde bolo zapojených niekoľko desiatok užívateľov. V súčasnosti sa zameriavajú na GSM siete a na odposluch siete a vyžívanie GSM kanálov k volaniu. Dokážu preberať kontrolu nad mobilnými telefónmi. Dávať si treba obzvlášť na situácie, keď volajú z neznámeho čísla. Človek sa snaží zavolať späť, ale automaticky to je audiotext, alebo služba ktorá je spoplatnená vysokou sumou.

1.4 Nástroje útočníkov

Najdôležitejší element pri útokoch. Následujúci zoznam nie je úplný, z dôvodu pribúdania stále nových nástrojov. Uvedené budú najpoužívanejšie a najrozšírenejšie. Existujú tri typy nástrojov:

- **Hardwarové nástroje** - patria k nim techniky hľadania bezpečnostných dier v čipových kartách. Pekný príklad je telefonný automat, alebo telekomunikačná karta E1, T1.
- **Softwarové nástroje -** patria k najpoužívanejším. Boli, sú a budú vyvíjané zdatnými programátormi. Uvedený zoznam používaných nástrojov je uvedený

nižšie v kapitole bezpečnostné hrozby 2.6. Označované tiež ako hackerské nástroje.

- **Sociálne inžinierstvo** - patrí k sofistikovaným útokom , kde už bežné metódy ako sú hardwarové a softwarové nástroje nefungujú. Práve tento typ útokov sa stáva najvyhľadávanejším, pretože ešte stále sa nájdu ľudia, ktorí uveria a spravia to, čo útočníci chcú. Tento typ bude uvedený neskôr v podkapitole.

1.5 Úvod do bezpečnostných hrozieb v kyberpriestore

Patria sem všetky hrozby ktoré spadajú do kyberpriestoru. Aktívne, alebo pasívne ohrozujú klientov v kyberpriestore. Rozlišujú sa aj podľa možnej miery infikovanosti. Musí sa rozlišovať, pre aký operačný systém je hrozba vytvorená a akú zraniteľnosť má operačný systém a aké riziko plynie z toho. Náklady na opravu škôd po hrozbách dosahujú milióny dolárov ročne. Pre lepšiu analýzu bezpečnostných hrozieb, sú uvedené operačné systémy, ktoré deň čo deň obsluhujú potreby užívateľov. Z pohľadu najväčších škôd tam patria sieťové operačné systémy, ktoré obsluhujú nespočetné množstvo užívateľov a pri ich výpadku by bola ochromená infraštruktúra. **Pri sieťových operačných systémoch denno denne, hrozí riziko**. Aj pri automobiloch je toto pravidlo. Najkradnutejším vozidlom je Škoda, Volkswagen, atď. A to len preto, lebo je najväčší dopyt po nich, ľudia potrebujú náhradné diely, zlodeji sa vyznajú v nich, pretože sa stali najpoužívanejšími. Takisto aj v operačných systémoch. V následujúcich kapitolách, budú uvedené bezpečnostné hrozby.

1.5.1 Operačné systémy využívané v kyberpriestore

Operačné systémy delíme na:

Užívateľské operačné systémy:

Windows: patrí tam MS-DOS, Windows 3.11, Windows 95, Windows 98, Windows 98 SE, Windows ME, Windows 2000, Windows XP, Windows Vista, Windows 7, ďalším prírastkom bude Windows 8. Tvorcom týchto operačných systémov je gigant Microsoft. Všetky operačné systémy sú komerčné, tzv. poskytované za peniaze.

Linux: patrí tam Ubuntu, Kubuntu, Gentoo, Slax, atď. Je pod licenciou GNU/GPL, hlavná vďaka patrí Richardovi Stallmanovi. Tento druh systému sa stal populárnym preto, lebo nie je komerčný, tzv. za úplatu. Nie je tak rozšíreným OS, ako je Windows. Avšak, pozitívum

na ňom je, že nie je tak vyhľadávaným terčom útočníkov. Ďalšou výhodou, je to, že tento typ OS, sa dá postaviť na mieru. Nevýhodou je, že je ťažší pre užívateľov migrujúcich z OS Windows na Linux. Ale v dnešnej dobe, prispôsobujú Linux užívateľom, snažia sa aby užívatelia nemali s ním problémy.

Iné: Patria do nich Chrome OS od spoločnosti Google, mobilné OS typu Symbian, Windows Mobile, Android - jadro Linuxu.

Uživateľské skupiny, sú najpoužívanejšími a najpočetnejšími operačnými systémami na svete. Z hľadiska bezpečnosti, medzi najzraniteľnejšie systémy patrí skupina Windows, pretože sú najpoužívanejšími a útočníci sa primárne zameriavajú na ich slabiny. Linuxové typy nepatria k tým najvyhľadávanejším, pretože nemajú také zastúpenie ako v predchádzajúcom prípade. A typy, ako sú mobilné OS, sa stali najnovším typom útokov, ktoré napádajú útočníci, pretože mobil obsahuje nespočetné množstvo osobných údajov ako sú kontakty, mobile banking, atď. Mobily sa synchronizujú s počítačmi a tam vzniká riziko migrácie škodlivého softwaru. Pomaly, ale iste sa z nich stávajú vreckové počítače obsahujúce technológie ako Wifi, Bluetooth, Infra, mobilný internet a tieto technológie prinašajú aj nevýhody. Všetko, čo sa pripája do kyberpriestoru nesie svoje riziká.

Sieťové operačné systémy:

Sieťový operačný systém je software, ktorý kontroluje sieť a jej správy (napríklad pakety), prevádzku a požiadavky, viacero užívateľov má prístup ku sieťovým zdrojom, ako dáta, atď., a poskytuje služby pre administratívné funkcie, vrátane bezpečnosti.

Sieťové operačné systémy nám poskytujú následovné funkcie:

- Súborové a tlačové zdieľanie.
- Správa administrácie užívateľov.
- Uživateľská administrácia.
- Vykonávanie auditov.
- Systémový management.
- Clusterové schopnosti.
- Bezpečnosť.

- Zálohovanie.
- Vzdialenú správu.
- Vysoká dostupnosť.
- Základná podpora pre hardwarové porty.
- Inštalované komponenty:
- Klientská funkcionalita.
- Serverová funkcionalita.

Inštalované komponenty nám predstavujú súčasný prístup viacerých používateľov, ktoré im poskytujú rôzne služby (programy typu server). Môžu byť inštalované na samostatnom počítači (dedikovanom) – napr. Novell Netware, atď., alebo spolu s klientskými programami (za takýmto počítačom môže pracovať uživateľ) – napr. Windows NT / 2000, UNIX, Solaris, a iné.

Klientské programy sú tie, ktoré využivajú služby serverov. U "lepších" sieťových operačných systémov, je prístup užívateľov k súčasne zdieľaným prostriedkom riadený prístupovými právami a zabezpečený (napríklad menom a heslom používateľov) a na základe autentizácie sú pridelené prístupové práva.

Na rozdiel napr. od WINDOWS 95/98/ME, kde je prístup uživateľov z iných počitačov riadený spoločne, autentizačný = prihlasovací proces k samostatnému počítaču sa dá ľahko obísť, iba v spolupráci s Novell alebo WIN – NT serverom sa dá urobiť individuálne zdieľanie, ak je niekto prihlásený k takémuto serveru, WIN 9x to zistí a umožní mu pridať prístupové práva, každému individuálne ku každému zdieľanému prostriedku. Pri práci už od uživateľa nežiada heslo.

Typy serverov:

Súborový server – súborové služby, na centrálnom disku sú uložené zdieľané súbory.

Databázový server – na server sú uložené databázy i s riadiacim programom schopným komunikovať s klientom napr. pomocou jazyka SQL (structured query language).

Tlačový server – zabezpečuje tlačové služby na zdielaných tlačiarňach.

Aplikačný server – zabezpečuje chod aplikácií (podoba s terminal serverom).

HTTP server – poskytujúci WWW stránky, najčastejšie Apache.

Mail server – poštový server:

SMTP – (Simple Mail Transfer Protocol) – slúži na odosielanie pošty a jej presun medzi servermi.

POP3 – (Post Office Protocol) – slúži na príjem pošty.

IMAP – Na rozdiel od protokolu POP3 je optimalizovaný pre prácu v pripojenom režime, keď správy zostávajú uložené na serveri a priebežne sa sťahujú, keď je to potrebné.

Terminal server – je možné pracovať v režime terminálu.

WAP server – poskytuje WAP stránky (internet pre mobilné telefóny)

Bootp server – (Bootstrap Protocol) v sieti TCP/IP oznámi stanici so sieťovou kartou jeho adresu a ďalšie jeho informácie.

DHCP server – (Dynamic Host Configuration Protocol) podobne ako v predošlom, ale poskytuje adresu dynamicky. To znamená prvú voľnú.

DNS server – (Domain Name Servicess) v sieti TCP/IP poskytuje meno počítača s danou číselnou internetovou adresou.

FTPD server – (File Transfer Protocol Daemon) poskytuje služby FTP, čiže prenos súborov medzi vzdialenými počítačmi).

NATD server – (Network Address Protocol Daemon) prekladá IP adresy medzi počítačovými sieťami

PROXY server – je to vlastne pamäť CACHE na prechodné uloženie, už uložené webstránky na serveri sa pohotovo "zobrazia"

Tento zoznam patrí medzi najzákladnejší, samozrejme existuje viacero typov serverov. Tieto servery môžu byť na jednom fyzickom počítači (serveri), alebo môžu byť v sieti aj viaceré.

Server typu Unix/Linux(SCO UNIX, Free BSD, Debian)

Je viacúlohový, viacužívateľský operačný systém pre sieťové prostredie a aplikácie, pracuje v textovom režime, avšak môžeme pracovať aj v grafickej nadstavbe x-window

(KDE, Flux, Gnome). Nemusí byť súčasťou inštalacie. Jedna z najväčších výhod je, že umožnuje hardwarovým počítačom vykonávať náročne úlohy na strane servera. Azda jeho najväčšou výhodou je hardwarová náročnosť a nemá také systémove nároky, ako napríklad u Windows NT, 2000,atď.

Bezpečnosť považuje veľa odborníkov za najdôležitejšiu súčasť v počítačovom svete. Nikto sa dobrovoľne nevzdá svojich dát. Avšak s pomocou Unixu, môžeme toto riziko eliminovať.

Patrí medzi najkvalitnejšie bezpečnostné operačné sieťové systémy. Každému súboru je pridelený vlastník toho súboru, ktorý môže nastaviť prístupové práva iným klientom siete.

Root je najmocnejší užívateľ systému, ktorý má najvyššie práva a može robiť čokoľvek. Mazanie užívateľov, pridávanie, konfigurácia celého systému, riadi server, administruje.

Unix je nasadený v komerčnej sfére a nie je zadarmo. Netreba si to mýliť s **Linuxom**, ktorý má úplnú inú licenčnú politiku (GNU/ GPL) a je voľne šíriteľný dobrovoľnými firmami a programátormi, ktorý ho chcú zlepšovať. Vyžaduje zdatných užívateľov, pretože má textový režim (jednoduchšie a rýchlejšie), vyžaduje znalosť príkazov.

Nevyžaduje antivírusovú ochranu, resp. vyžaduje len takú, aby dokázal ochrániť klientov a siete. Jeden z desiatich Unix serverov, je nakazený počítačovým vírusom. Kdež to u Windows serverov je to naopak.

Obľubu si získal v poslednom čase Linux, ktorý je takmer totožný s jeho bratom Unixom. Rozdielna je adresárová štruktúra a to minimálne, a príkazy ktoré sú takmer podobné Unixu.

Jeho výhodou je voľná šíriteľnosť. Používa ho aj NASA v Spojených štátoch amerických. V dnešnej dobe je rozšírený v oblasti webových serverov, kde dominuje svetovému trhu kvôli jeho cene. Prieskum ukázal, že v tomto smere je špička. Umožňuje aj komunikáciu s prostredím Windows pomocou servera SAMBA a dokáže v samostatnom okne simulovať aj prostredie Windows.

Server typu Novell

Vyvinutý americkou firmou Novell, ako riadiaci systém pre lokálne počítačové siete, viacúlohový, viac-užívateľský. Beží na súborovom serveri (môže ich byť viac). Umožňuje

ostatným počítačom zapojeným v sieti, využívať serverové diskové priestory (uložené súbory) i v zdieľanom móde – súčasné využitie viacerými užívateľmi a ďaľšími službami, napríklad tlač na sieťových tlačiarňach, výmena správ medzi uživateľmi, atď. Pre komunikáciu v sieti používa prenosový protokol IPX/SPX. Je to systém typu klient-server. Na riadiacom počítači beží program server (nemožno súčasne používať iné aplikácie) – jedná sa o vyhradený (DETICATED) server, na strane pracovnej stanice program klient

pre určitý operačný systém používaný pracovnou stanicou, ktorý umožňuje spoluprácu s riadiacim počítačom.

Pracovná stanica je vlastne samostatný počítač (PC). Nie je to len terminál, úloha je spracovaná pracovnou stanicou, jej procesorom a operačnou pamäťou. Možnosť spracovať určitú úlohu závisí od výkonu pracovnej stanice (nie len od serverového počítača).

Pomerná väčšina sa už stretla s Novelom, na vysokých školách a vo firmách, poskytuje študentom vlastné diskové kvóty, vlastné prihlasovacie meno a heslo, lepší prístup k súborom. Aktuálna verzia je Novell Netware 6.

V lokálnej počítačovej sieti sú dva typy staníc:

riadiace počítače (servery):

- OS Novell Netware

pracovné stanice (workstations):

- MSDOS
- WINDOWS
- UNIX, …
- MAC OS Apple
- OS-2 – so sieťovou podporou

Bezpečnosť v sieti sa zabezpečuje:

- Atribútmi súborov a adresárov
- Prístupovými právami užívateľa a skupiny užívateľov k adresárom a súborom(poprípade ďalším zdrojom siete.)
- Prístupové práva k objektom

Server typu Windows

Verzie:

- WINDOWS NT server verzia 3
- WINDOWS NT klient verzia 3- oproti verzii server len mierne obmedzené serverové funkcie.
- WINDOWS NT server verzia 4
- WINDOWS NT klient verzia 4- oproti verzii 3 rozlišuje veľké a malé znaky
- (case sensitive).
- WINDOWS NT 4 terminal server – operačného systému typu host (terminal server) na základe patentu firmy Citrix, klient-terminál má grafické rozhranie.
- WINDOWS 2000 – 32 a 64 bitové operačné systémy typu klient-server.
- WINDOWS 2000 professional – ako klient.
- WINDOWS 2000 advanced server – pokročilé nastavenie servera, má viac možností.
- WINDOWS 2003 – zlepšená verzia Windowsu 2000, marketingový ťah.
- WINDOWS 2008 – doteraz najaktuálnejší sieťový operačný systém z rady Windows. Rozšírená podpora virtualizácie, úložiska atď. Menšie rozdiely nájdeme medzi produktovými riešeniami, ako menšie podnikové riešenie a podnikové riešenie – tzv. Licenčná politika.

Prihlasovanie užívateľov na konzole sa deje prihlasovacím oknom po stlačení klávesovej skratky CTRL-ALT-DEL. Na cudzích počítačoch po nainštalovaní príslušného klienta sa buď pri spustení systému objaví prihlasovacie okno, alebo sa k serveru dostaneme cez okolité počítače.

Pri inštalácii systému vznikne užívateľ s menom **administrátor**, ktorý sa stáva správcom systému s maximálnymi právami (heslo je treba veľmi dôkladne chrániť pred zneužitím). Ten potom vytvára ďalších užívateľov a prideľuje im prístupové práva k zdieľaným prostriedkom servera, inštaluje software, ruší užívateľov a podobne.

Prístup k vzdialenému zdieľanému prostriedku je možný cez meno tohto prostriedku v sieti, ktoré je vo forme: \\meno_počítača_v_lan\

Adresáre na diskoch si môže užívateľ dokonca aj **namapovať,** čo znamená, že im priradí voľné písmeno disku podľa konvencií. Napríklad: \\meno_počítača_v_lan\c-disk\ namapujeme ako disk Z:\

Bezpečnosť sa zabezpečuje pomocou:

- Aktualizácií
- Monitorovania
- Prístupovými právami

Server typu Solaris

Solaris, označovaný ako SunOS, je operačný systém Unixového typu, vyvinutý spoločnosťou Sun Microsystems pôvodne pre počítače používajúcu architektúru SPARC (založenú na architektúre procesorov RISC).

Využitie prevážne ako výkonné pracovné stanice pre grafické aplikácie (CAD/CAM) a neskoršie aj ako servery. Po dlhšiu dobu existencie existuje implementácia Solarisu pre architektúru x86, čerstvo so Solarisom 10 pribudla architektúra x86-64, kdežto pre platformu Itanium nebola uvoľnená. Ešte existuje aj pre architektúru PowerPC a uvažuje sa aj o ďalších architektúrach, napríklad ARM.

SunOS je založené na BSD vetve Unixu, pri vývoji verzie 5 ale došlo k prechodu na Systém V. Táto verzia bola distribuovaná ako Solaris 2.0. SunOS 5.10 je predávaný ako Solaris 10. Názov SunOS je názov pre operačný systém, Solaris je nič iné, ako SunOS s grafickým prostredím ONC+ a sieťovými službami a aplikáciami.

Solaris sa vyznačuje robustnosťou a stabilitou, dobre zvláda SMP konfigurácie s veľkým množstvom procesorov(desiatky až stovky).Ponúka virtualizáciu systému a prišiel s novým typom súborového systému ZFS.

Ako prvým grafickým prostredím pre Solaris je OpenWindows, v Solarisu 2.6 ho nasledoval CDE (Common Desktop Environment). V Solarisu 10 je prostredie Java Desktop System, založené na GNOME (je aj v Linuxe).

Zdrojové kódy Solarisu sú distribuované pod licenciou ako CDDL (Common Development and Distribution License, schválená Open Source Initiative ako Open source software). Projekt OpenSolaris bol zahájený 14. júna 2005, ďalšia verzia bude vyvíjaná pod touto licenciou a aj kódom. Výhodná je najmä pre študentov, ľudí ktorí si ju vyskúšať.

1.6 Bezpečnostné hrozby v kyberpriestore

Vychádzajú z rizík, ktoré existujú v kyberpriestore. Hrozba využíva riziko, ktoré existuje. Aktívum sú v tomto prípade cenné dáta. Bezpečnostné hrozby sú rafinovanejšie každým rokom. Dole je uvedený list najčastejších hrozieb, ktoré sú používané.

Trojské kone

Najnebezpečnejšie, najobľúbenejšie a najpoužívanejšie nástroje hackerov. Tieto trójske kone vznikli pomenovaním od Trójskeho koňa v grécku. Použili ho ako dar, koňa si zobrali ako dar, lenže nevedeli, že kôň bude naplnený vojakmi. A tak cez noc vojaci povyskakovali a dobyli mesto Tróju. V počítačovej terminológii označujeme program, ktorý vykoná záškodnícku činnosť. Do spustiteľného súboru, či už .exe, .bat, atď. je vložený škodlivý kód. Po spustení súboru, sa nainštaluje bez toho, aby sme niečo vedeli, že sa nainštalovalo. Trójske kone sa používajú na monitorovanie, získavanie dát, hesiel, aby o tom užívateľ nevedel.

Vírusy

Majú deštruktívny charakter. Tak isto, ako existujú biologické vírusy a tie majú za úlohu škodiť a napádať, tak isto existujú aj pre počítače. Základným princípom vírusu, je šírenie, potom napádanie infikovaného počítača. Spomaľujú počítače, kradnú systémové prostriedky, poškodzujú súbory a tak z dôležitých súborov sa stávajú prakticky bezcenné dáta. Odporučenie je zálohovať všetky dôležité dáta. Najznámejším vírusom bol ILoveYou. Niektoré šikovnejšie vírusy, dokážu uniknúť antivírusom, dokážu byť maskované a zvládajú mutovanie.

Červy

Patria medzi najdeštruktívnejšie spomedzi hrozieb. Červy majú za úlohu, napadnúť čo najviac súborov a poškodiť ich. Patria do podtriedy vírusov. Na rozdiel od počítačových vírusov, červ nepotrebuje na svoje šírenie hostiteľský program. Šíria sa bleskovou rýchlosťou. Obsahujú podprogramy, ktoré zabezpečujú jeho kopírovanie a ďalšie šírenie. Môžu dosiahnuť rekordný objem dát. Existujú dva typy červov. Sieťové a emailové.

Spam

Spam je nevyžiadaná a hromadne rozosielaná správa prakticky rovnakého obsahu. Ide o zneužívanie elektronickej komunikácie, najmä e-mailu. Zväčša je používaný ako reklama, hoci za krátku históriu elektronickej komunikácie bol spam použitý aj z iných dôvodov. Existuje veľa rôznych médií, ktoré sú spamermi zneužívané. Môže to byť napríklad spomínaný e-mail, instantné zasielanie správ (napríklad ICQ), skupiny Usenet, krátke textové správy.

DoS (Denial of Service)

Netreba si to mýliť s DOS od spoločnosti Microsoft. Hlavnou úlohou je postupné vyradenie služby z prevádzky. Napríklad služby bežiace na serveroch. Apache, MySql,atď.

Funguje tak, že v čo najkratšom intervale sa posiela čo najviac dotazov na cieľ, až dovtedy, kým sa nevyradí služba. Pri tisíc osobách, robiacich to iste, je to skoro isté, že to vyradia.

Sniffery

Slúžia pre odpočúvanie sieťovej komunikácie. Dôležitým parametrom pre odpočúvanie, je umiestnenie sniffera v sieti. S pomocou snifferu, dokážeme odchytiť komunikáciu na sieti. Napríklad, prihlasujeme sa do nezabezpečeného webu. Obyčajné http://. Tak uvidíme meno a heslo, ktoré sa zadalo, do prihlasovacieho formulára. Funguje tak, že sieťová karta sa aktivuje do promiskuitného módu, tzn., že odchytáva všetky pakety na vstupe.

Skenery

Hlavnou náplňou skenerov, je kontrolovať, či počítač má otvorený port. Na každom porte beží služba. Napríklad port číslo 80 je http. Skenery poskytujú informácie o danom počítači. Je to analýza, prostredníctvom ktorej sa dozvieme o počítači, aké porty sú otvorené, aký operačný systém tam je. Táto analýza sa dá **využiť ako audit, stávajúcich bezpečnostných opatrení súčasného systému.**

Backdoors

Ich princíp spočíva v tom, že využíva bezpečnostné diery. Útočníci si vytvoria zadné vrátka, tzn. program, ktorý bude slúžiť na vzdialenú kontrolu nad počítačom. Pri bežnom používaní počítača, užívateľ nezistí čo robí útoční s jeho počítačom.

Rootkity

Pochádza so slova root, v linuxových operačných systémoch to znamená, najvyšší užívateľ, z pohľadu hierarchie. Je niečím takým, akým je vo Windowse administrátor. Podobné ako backdoors. Rootkity sú vytvorené tak, aby ostali v utajení.

Debuggery

Crackeri ich využívajú na analýzu programov. Napríklad .exe súbory nedokážeme upraviť kódovo, tzv. že prepíšeme kód. Využíva sa assemblorovský zápis programu, na najnižšej úrovni. Najznámejším analyzátorom kódu je OllyDebbuger. Crackeri ich využívajú na crackovanie programov, hier, získanie sériových čísel, zistenie programu ako sa chová.

Phishing

Patrí k nástrojom sociálneho inžinierstva. Sociálne preto, lebo pracuje s ľuďmi a snaha je nachytať na ľudskej nevedomosti alebo naivite. Phishing znamená rybárčenie, v počítačovej terminológii je to označenie pre nachytanie ľudí do pasce. Ide o to, že útočník správnou interpretáciou si získa dôveru užívateľa. Útočník získa prihlasovacie meno, heslo a údaje a tak môže disponovať s údajmi. Netreba sa dať zlákať na emaily typu, dobrý deň,

sme administrátori zo seznam.cz a z dôvodu údržby systému potrebujem, aby ste vyplnili prihlasovacie údaje a obratom ich zaslali. Stránka bude vyzerať totožne so zoznamom, len s tým rozdielom, že je falošná. Pozor na podvodníkov! Rada znie, kontrolovať stránky, či sú šifrované ak odosielame heslo. Keď ideme do internet bankingu, tak musí byť adresa banky. Nie IP adresa, alebo nejaká iná stránka.

Dešifrovanie hesiel

Posledným nástrojom je dešifrovač hesiel. Používa techník, ako **slovníkový útok, alebo metóda hrubou silou.** Slovníkový útok spočíva v tom, že existuje textový súbor (slovník) s menom a heslom a ten súbor používa pri kombináciach mien a hesiel. Napríklad peter peter. Metóda hrubou silou spočíva v testovaní kombinácii znakov, čísel. Métoda hrubou silou je najnáročnejšou metódou na výpočetný výkon. Tu platí pravidlo pri tvorbe hesiel. Čím ťažšie heslo, tým viac času treba na jeho prelomenie. Najlepšie heslo tvorí kombinácia znakov, čísel, malých a velký písmen. Najhoršími heslami sú krátke a známe heslá.

Cross-site scripting (XSS)

Je metóda narušenia WWW stránok využitím bezpečnostných chýb v skriptoch (predovšetkým neošetrené vstupy). Útočník vďaka týmto chybám v zabezpečení webové aplikácie dokáže do stránok podstrčiť svoj vlastný javascriptový kód, čo môže využiť buď k poškodeniu vzhľadu stránky, jej znefunkčneniu alebo dokonca k získavaniu citlivých údajov návštevníkov stránok.

2 ŠPECIFIKÁCIA SUBSYSTÉMOV OCHRANY

Definovanie ochrany v kyberpriestore nie je jednoduché. Vo všeobecnosti, bezpečnosť je široko abstraktná. V kyberpriestore chápeme bezpečnosť, ako ochranu voči prístupu k informáciám neautorizovanými osobami a zámernými útokmi. Bezpečnosť sa chápe tiež ako, schopnosť systému ochrániť informácie a systémové zdroje k dosiahnutiu dôvernosti a integrity. Systémové zdroje obsahujú procesory, disky a programy.

Počítačová bezpečnosť je často spojovaná s troma oblasťami, ktoré sú označované ako "DIA":

Dôveryhodnosť - Zaistenie informácií, že nebudú zneužité neautorizovanými osobami.

Integrita - Zaistenie informácií, že nebudú pozmenené neautorizovanými osobami.

Autentifikácia - Zaistenie, že užívatelia sú osobami, za ktoré sa vydávajú.[4]

2.1 Bezpečnosť siete

Bezpečnosť sietí sa považuje za jednu najdôležitejšiu súčasť v oblasti bezpečnosti. Sieť je tvorená dvomi, alebo viacerými zariadeniami, či už počítač, sieťové zariadenie, prepínač, smerovač, firewall, atď., a poskytujú výmenu dát medzi sebou. Postupne v ďalších kapitolách je rozpísane, prečo je tak dôležité mať sieť, aké sieťové topológie je vhodné použiť, prostredie siete, zabezpečenie siete, najviac záleží od infraštruktúry siete, ako je navrhnutá, aké prvky obsahuje. Nesmie sa zabúdať na nastavenie siete, toto je veľmi dôležitý faktor.

Základná terminológia: [5]

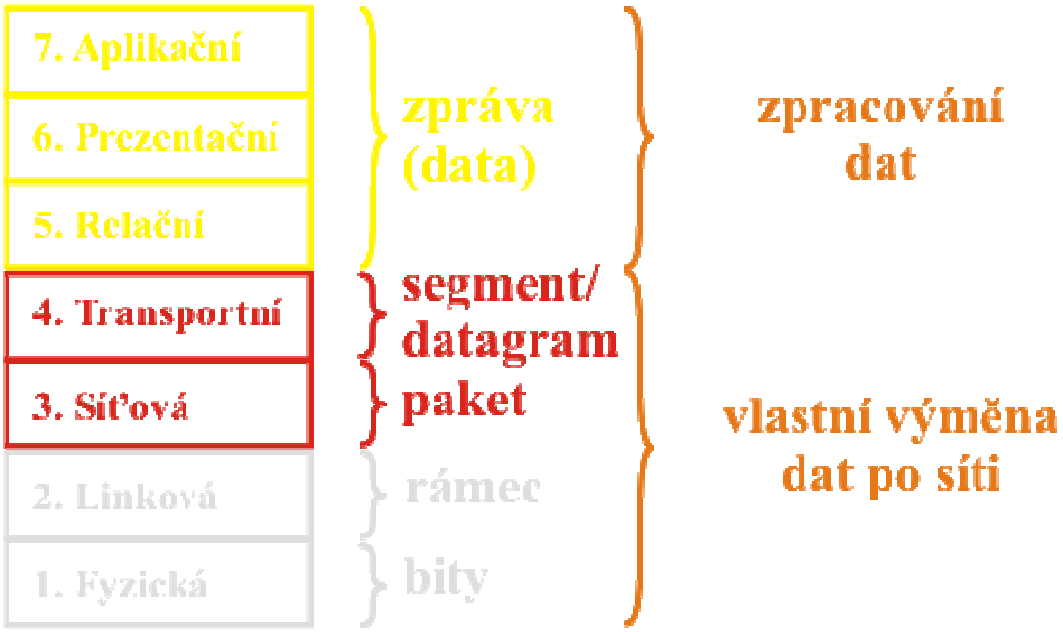
- **internet** - Je akákoľvek sústava vzájomne prepojených sietí, internetov je veľké množstvo, internet má vlastníka, napríklad korporácia.
- **Internet** - Meno jednej konkrétnej sústavy vzájomne prepojených sietí.
- **intranet** - Tvorí príslušnú časť siete organizácie, slúžiacu pre samostatnú organizáciu, poskytuje aplikácie a služby vo vnútri organizácie.
- **extranet** - Tvorí príslušnú časť organizácie, slúžiaci pre poskytovanie aplikácií a služieb externým organizáciám a užívateľom.

- **DMZ -** Demilitarizovaná zóna je sieť medzi vnútornou a verejnou sieťou, Internetom. Hlavnou úlohou DMZ, je vyčleniť adresy, alebo rozsah IP adries tak, aby boli viditeľné z verejnej siete a služby sa tak oddelili od vnútornej siete. DMZ sa nastavuje pomocou schopného smerovača, alebo firewallu, záleží od toho, čo zákazník očakáva. Zjednodušene DMZ, je ďalšou vyčlenenou sieťou, je možné tak izolovať zariadenia.

Rozdelenie sietí podľa veľkosti:[5]

- **PAN** - personal area network (personálna sieť).
- **LAN** - local area network (lokálna sieť).
- **CAN** - campus area network (kampusová sieť).
- **MAN**- metropolitan area network (metropolitná sieť).
- **WAN**- wide area network (širokorozsiahla sieť).
- **GAN**- global area network (globálna sieť).
- **VLAN** - virtual LAN (virtuálna sieť).
- **WLAN** - wireless LAN (bezdrátová sieť).
- **VPN** - virtual private network (súkromná virtuálna sieť).

Pre lepšie chápanie bezpečnosti, ako siete fungujú, je veľmi dôležitý OSI model (Open Systems Interconnection Reference). Model sa skladá z jednotlivých vrstiev, je ich sedem a ich súčasťou je návrh štruktúry komunikačných a sieťových protokolov.



Obr. 1 OSI Model[5]

2.1.1 Normy počítačových sietí

Hlavnou inštitúciou zaoberajúcou sa tvorbou noriem v počítačových sieťach, je IEEE (Institute of Electrical and Electronics Engineers) organizácia. Táto inštitúcia bolo založená na začiatku osemdesiatych rokov, označovaná ako IEEE 802, štandard pre počítačové siete. Postupne si vytvoril tento inštitút pracovné skupiny ako napr. 802.3, 802.11,atď.

Druhy noriem IEEE:[5]

- **802.1** - Otázka adresácie, komunikácia medzi sieťami a správa siete.
- **802.2** - Pod vrstva LLC linkovej vrstvy, logické riadenie spoja.
- **802.3** - **Lokálna počítačová sieť s prístupovou metódou CSMA/CD, metóda kolízie. Túto normu využíva sieť typu ethernet. Je najpoužívanejším typom na komunikáciu.** Technológiou priniesla firma Xerox a Intel.
- **802.4** - Lokálna počítačová sieť s prístupovou metódou Token Bus.
- **802.5** - Lokálna počítačová sieť s prístupovou metódou Token Ring. S touto technológiou prišla firma IBM.
- **802.6 -** Metropolitné siete MAN.
- **802.7** - Siete s prenosom v preloženom pásme

- **802.8 -** Siete na báze optickej infraštruktúry.
- **802.9 -** Siete integrujúci hlasový a dátový prenos.
- **802.10 - Bezpečnosť a zabezpečenie sietí**
- **802.11 - Bezdrôtové siete, 2.4Ghz, 5Ghz**
- **802.15 -** Bluetooth siete, bezdrátové pripojenie dvoch zariadení
- **802.16** - Bezdrátová sieť WiMax pracujúca na frekvenciách 2.3GHz, 2.5GHz, 3.2GHz.

2.1.2 Topológia sietí

V dnešnej dobe, mnoho ľudí podceňuje topológie sietí, netreba sa však ponáhľať pri výstavbe infraštruktúry. Správne zvolená topológia má vplyv na bezpečnosť siete. Je mnoho aspektov, ktoré majú vplyv na topológiu siete. Sú nimi rozsah siete, finančný objem prostriedkov na stavbu infraštruktúry, hardwarové umiestnenie prvkov, použitá technológia.

Treba zobrať do úvahy rozsah siete, financie, náklady, správu, fyzické umiestnenie a nakoniec použitý hardware. Administrátor má zásluhu pri návrhu akú topológiu správne zvoliť. Je to prvý krok, pri výstavbe siete. Ak sa urobila chyba pri návrhu topológie a zistíme to, až keď je sieť postavená, budeme mať ďalšie nadbytočné náklady na modifikáciu.

Topológie sa rozlišujú na:

Hviezdicová topológia:

Obr. 2 Hviezdicová topológia

Označuje prepojenie počítačov do tvaru pripomínajúcu hviezdu. Ide o najpoužívanejšiu metódu prepojovania medzi počítačmi do centrálneho prvku. Počítače sú prepojené pomocou káblu (UTP,FTP,STP) k aktívnemu prvku hubu, prepínača, smerovača. Neodporúča sa používať staré prvky ako HUB, pretože ten požiadavky rozosiela všetkým počítačom v sieti a zbytočne zahlcuje sieť. Prepínač a smerovač vie, na ktorý počítač poslať požiadavku. [5]

Výhody:

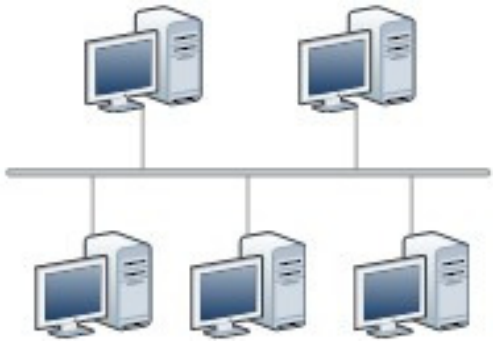
- Najpoužívanejší typ topológie.
- Jednoduchá administrácia, nastavovanie, zapájanie, modifikácia.
- Poruchy sa dajú rýchlo riešiť.
- V prípade výpadku počítača, alebo kábla nezlyhá celá sieť, pretože pre jedno zariadenie je určený jeden kábel.

Nevýhody:

- Ak zlyhá centrálny prvok, zlyhá celá sieť.
- Potreba veľké množstvo káblov u väčších sietí.

Zbernicová topológia:

Spojenie počítačov je riešené prenosovým médiom (zbernica), ku ktorej sú pripojené všetky koncové počítače. Problém vzniká vtedy, ak chcú dvaja klienti na sieti vysielať v rovnaký okamžik, vtedy vzniká riziko kolízie. Táto situácia sa nám stáva veľmi často, tak preto museli vymyslieť systém, ktorý tieto kolízie eliminuje. Preto v tomto type topológie sa používa metóda náhodného prístupu. [5]



Obr. 3 Zbernicová topológia

Výhody:

- Vhodná pre malé siete, ktoré nevyžadujú veľké prenosové rýchlosti.
- Nevyžaduje toľko káblov, ako pri hviezdicovej topológii.
- Ušetrenie nákladov pri výstavbe tejto topológie.
- Vhodná pre malé siete, ktoré nevyžadujú veľké prenosové rýchlosti.

Nevýhody:

- Neobsahuje aktívne prvky.
- Náročná na údržbu, pri vzniku havárie.

Kruhová topológia:

Obr. 4 Kruhová topológia

Najčastejšie označovaná. Schémou je kruh. Táto metóda je pomalá a neefektívna. Aby fungovala sieť, kruh musí byť v poriadku, musí fungovať. Dáta sa pohybujú v kruhu od odosielateľa postupne cez všetkých, až k príjemcovi. [5]

Výhody:

- Vyvážený výkon pri veľkom počte užívateľov.
- Rovnaký prístup pre všetky počítače.
- Použité množstvo média je menej, ako pri hviezdicovej topológii.

Nevýhody:

- Dáta musia ísť skrz každý počítač medzi odosielateľom a príjemcom, čo znižuje priepustnosť siete.
- Zlyhanie jedného počítača má dopad na funkčnosť sieťe.
- Modifikácia siete má za následok prerušenie siete .

Stromová topológia:

Obr. 5 Stromová topológia

Táto topológia vychádza zo stromu, ktorý je rozvetvený. Na pozícii uzlov v strome sa nachádza hub alebo switch. Ak dôjde k výpadku koreňa, sieť sa rozpadne na niekoľko menších sietí. Výpadok prepojovacieho uzlu spôsobí výpadok časti siete.[5]

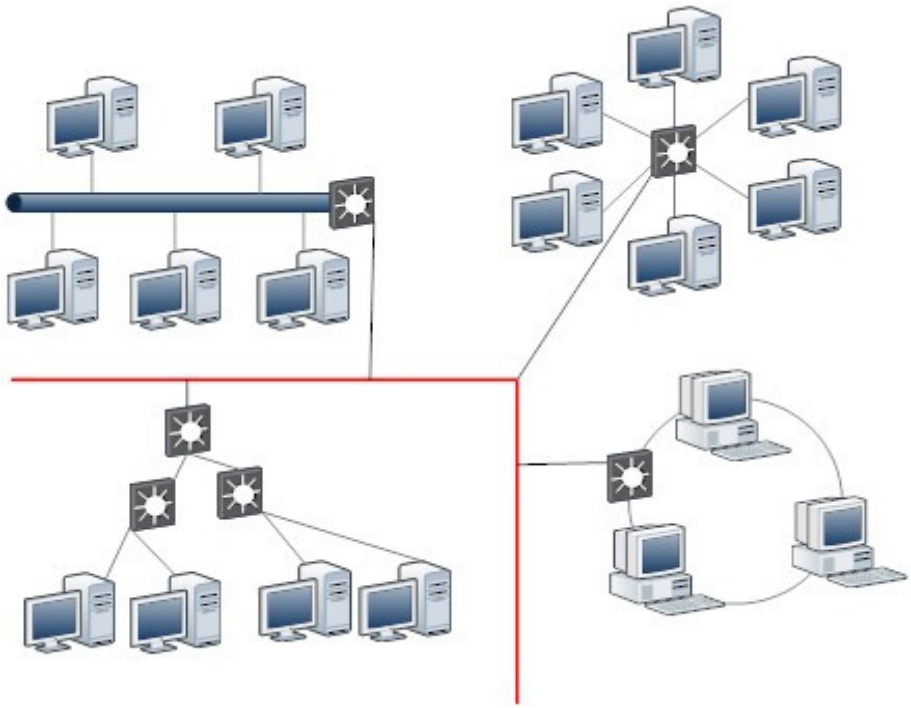
Výhody:

- Široké spektrum možností.
- Pri výpadku prepojovacieho uzla, nevypadne celá sieť, ale len tá, ktorá sa odpojí.
- Náklady na káble sú menšie ako u hviezdicovej topológie.

Nevýhody:

- Komplexnosť siete, pri väčšej infraštruktúre je neprehladná schéma zapojenia.
- Náročnosť na údržbu a znalosť.

Chrbticová topológia



Obr. 6 Chrbticová topológia

Chrbticové topológia sa používa ako nosný systém s vysokou rýchlosťou prenosu, najčastejšie pomocou optického pripojenia. Prepája najčastejšie WAN, MAN, CAN, LAN dohromady.[5]

Výhody:

- Široké spektrum možností.
- Rýchlosť dátovej komunikácie.
- Tento druh topológie používa aj Internet.

Nevýhody:

- Zraniteľnosť, škody nemalého rozsahu.
- Drahá technológia, zariadenia a kabeláž.

2.1.3 Monitorovanie bezpečnosti siete

Pri výmene dát v kyberpriestore, vznikajú určité riziká. Tie riziká treba riešiť a nejako sa ich snažiť eliminovať. Na kontrolu prevádzky siete sa používa metóda monitorovania. V sieti je potrebné zabezpečiť plynulý chod bez narušenia. Namerané hodnoty v sieti slúži pre dôkladnú analýzu a porovnávanie údajov. V sieti treba optimalizovať dátové toky tak, aby bola zaistená čo najväčšia priepustnosť. Netreba dopustiť, aby došlo k bezpečnostnému incidentu. Treba stále monitorovať a sledovať bezpečnostnú situáciu okolo. Monitoring znamená široké spektrum možností a podôb, ktoré je možné uplatniť. Ďalšou variantou je logovanie. Logovanie je sledovanie udalostí, najčastejšie na smerovačoch, serveroch, atď., za cieľom zistiť neštandardné správanie systému, poprípade vedú k odhaleniu útokov.

Monitorovací systém možno postaviť, ako:

- **Vlastný systém -** je možné postaviť na vlastných znalostiach, vytvorenie skriptov, ktoré budú slúžiť na monitorovanie. Výhoda je tá, že človek bude mať kompletný prehľad o tom ako monitoring prebieha a riešenie bude odpovedať požiadavkám. Nevýhoda je znalosť programovacieho jazyka, kompletné znalosti o sieťových protokoloch
- **Bezplatné produkty -** ich hlavnou výhodou je, že sú bezplatné. Nevýhodou je, že musíme investovať svoj čas a svoje znalosti a pomaly zlepšovať tieto systémy. Ako príklad, bezplatného monitorovacieho softwaru je Nagios, atď.
- **Komerčné produkty -** majú komplexnú ponuku možností. Inštalácia prebieha formou pár klikov a monitorovanie je rozbehnuté za pár minút. Nutné je vedieť adresy zariadení, ktoré sa pôjdu monitorovať. Komerčný systém, je napríklad What's Up, alebo NetFlow.

2.1.4 Rádius Server pre WiFi

Rádius bol vyvinutý spoločnosťou Livingston Enterprises, Inc., v roku 1991 ako prístupový server k autentifikácii a správe účtov a neskôr prešiel do IETF spoločnosti, ako štandard.

V skratke Rádius (Remote Authentication Dial In User Service), je vziadelená autentifikácia v užívateľskej službe, je to sieťový protokol, ktorý poskytuje centrálnu autentifikáciu, autorizáciu a správu účtov pre počítače pripájajúce sa a využívajúce sieťovú službu. [6]

Je často používaný internetovými poskytovateľmi a spoločnosťami, kde je kladený dôraz na **zabezpečenie**. Používajú ho k správe pripojenia k **Internetu**, alebo **vnútorných sietí**, **bezdrôtových sietí, a integrovaných e-mailových služieb.**

Rádius je klient/server protokol, ktorý funguje na aplikačnej vrstve, používajúci UDP k transportu dát. Rádius klienti komunikujú so serverom, server zväčša býva na Linuxe alebo Windows serveroch.

Zabezpečuje tieto dôležité funkcie:

- Autentizácia užívateľov, alebo zariadení pred poskytnutím ich prístupu do siete.
- Autorizácia tých užívateľov, alebo zariadení k určitým sieťovým službám, ktoré sa budú používať.

Postup autentizácie:

- Klient požiada, o prihlásenie do siete WiFi access point, alebo smerovač s WiFi.
- WiFi access point, alebo smerovač s WiFi odošle dotaz na overenie identity.
- Klient odošle svoju identitu.
- WiFi access point, alebo smerovač s WiFi prepošle prijatú identitu od klienta na server Rádius, cez nekontrolovaný kanál.
- Rádius pošle klientovi požiadavku, cez prístupový bod na špecifikáciu autentifikačnej metódy, ktorá bude použitá, napríklad PEAP, CHAP, atď.
- Klient odpovie Rádiusu odoslaním svojich autentizačených údajov, napríklad certifikátom, alebo menom a heslom.
- V prípade úspešnej autentizácie odošle Radius šifrovaný autentizačný kľúč, alebo certifikát WiFi access pointu, alebo smerovaču s WiFi.
- WiFi access point, alebo smerovač s WiFi pošle vygenerovaný certifikát, alebo kľúče ku klientovi.

2.1.5 VPN zabezpečenie siete

Virtuálna privátna sieť je počítačová sieť, ktorá používa verejnú infraštruktúru ako je Internet k poskytovaniu vzdialených kancelárií, alebo individuálnym užívateľom s cieľom

zabezpečiť prístup k sieti organizácie, alebo domova. Je primárne určená na zabezpečenie siete, s cieľom šifrovať dáta. Princíp spočíva v zabaľovaní dát počas výmeny, používajú kryptografickú metódu medzi dvoma, alebo viacerými sieťovými zariadeniami, ktoré nie sú v rovnakej súkromnej sieti. Zariadenia ako firewall, smerovač s podporou VPN musí podporovať VPN funkciu. Najčastejšie prepojenie vo VPN používajú pobočky firiem medzi sebou, keď potrebujú pracovať tak, ako keby boli v rovnakej sieti. **Bezpečnosť** tohto druhu siete je riešené pomocou IPSec protokolu, ktorý šifruje komunikáciu v sieti.

2.1.6 Rozdelenie sietí na jednotlivé VLANY z hľadiska bezpečnosti

Z hľadiska bezpečnosti je vhodné si sieť rozdeliť na niekoľko VLANOV. VLAN znamená virtuálna sieť, je to skupina počítačov, sieťových zariadení, atď., ktoré komunikujú na spoločnej broadcastovej doméne bez ohľadu na ich fyzickú konektivitu. Konfigurácia prebieha softwarovo, na prepínačoch. Ak sa rozčlenia VLANY jednotlivo a pridáme do nich sieťové zariadenia, tak oddelíme z hľadiska bezpečnosti iné zariadenia. Umožňuje vytvoriť skupiny a do nich zariadenia, ktoré budú spolu komunikovať.

Základné pravidlá v bezpečnosti:

- Dobre porozumieť návrhu siete a VLANs.
- Sieťové zariadenia sa zapájajú na zvlášť prepínače.
- Komunikácia medzi VLANs je zabezpečená pomocou firewallov, smerovačov a prepínačov.
- Použiť šifrované heslo pre prístup na prepínač.
- Pri použití trunkov by sa mali definovať len potrebné VLANs
- Koncové zariadenia patria do módu access

Najpoužívanejšie prepínače sú od spoločnosti Cisco. Existuje na nich príkaz Port Security. Tento príkaz umožňuje nastaviť na portoch filtráciu podľa MAC adries. Ak sa stane, že do portu príde iná MAC adresa, paket sa zahodí a port sa vypne na dobu neurčitý. Takto zabránime potencionálnym útočníkom, pripojiť sa na prepínač. Tento bezpečnostný krok, slúži na ochranu, proti útoku na MAC adresy.

2.2 IDS systémy

Systémy na detekciu útokov. Najčastejšie sú riešené pomocou, softwaru. Hardwarové riešenia existujú, avšak sú drahé. Výhoda u hardwarových je tá, že je akcelerovaný IDS systém, pomocou ASIC/FCPGA.

Princíp spočíva v tom, že zabezpečuje detekciu neobvyklej situácii. Systémy fungujú v promiskuitnom režime(odpočúvací mód). Systém ak vyhodnotí snahu o napadnutie, tak zruší sieťovú reláciu. Spočívajú v nastavení firewallov, prepínačov, smerovačov. Pomocou ACL (access control list) sa nastavuje bezpečnostná politika. Nevýhoda je, že prvý pokus o útok prebehne, po zaregistrovaní pokusu, automaticky systém funguje. Takže sa musí chvíľu čakať. Známym open-source systémom je Snort. Ponúkajú ho zadarmo a pri trochu šikovnosti, to zvládne väčšina.[7]

2.3 IPS systémy

Preventívne systémy napadnutia. Na rozdiel od IDS funguje tak, že zadrží útok hneď v počiatku. Nie je nutné konfigurovať prepínače, firewally, smerovače, atď. Rozdiel medzi IDS a IPS je v cene. Niekoľko výrobcov ponúka riešenia na zabezpečenie siete. Jedným zo známych výrobcov je Cisco, IBM, HP, atď. **Existujú dva typy riešení:**

- **In-Line IPS**
- **Out-Of-Band**

V prvom type riešenia IPS je umiestnené medzi vonkajšou a vnútornou sieťou, ktorú chceme chrániť. Vykonáva sa celková analýza z celkových paketov prejdených cez IPS. Prípadne ak nastanú problémy, tak zakáže sieťovú reláciu.

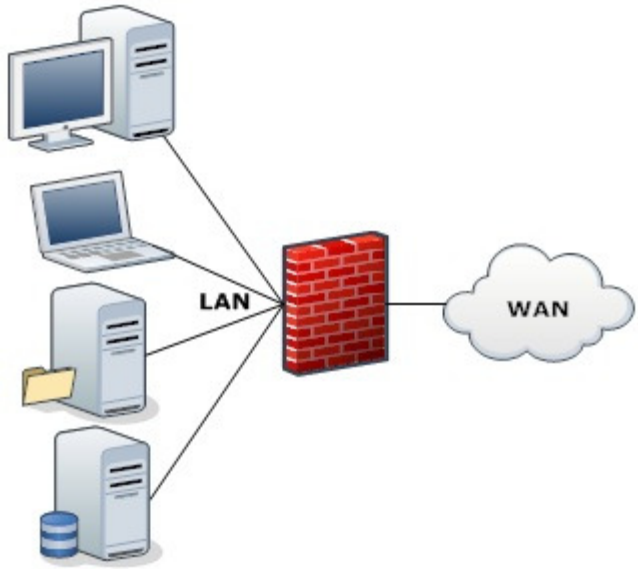
Druhý typ riešenia je na báze sledovania celkovej prevádzky prechádzajúcej z, až do vnútornej siete bez toho, aby bolo fyzicky prepojený. IPS napodobní spojenie, ktoré má na starosti to, že konkrétny počítač sa neinfikuje.[7]

2.4 Firewally

V preklade je to ohnivý múr. Firewall je zariadenie, alebo set zariadení navrhnutých tak, aby dovoľovali, alebo zakazovali sieťové spojenia vychádzajúcich z pravidiel a boli

pravidelne používané na ochranu sietí proti neautorizovanému prístupu. Buď existuje hardwarový, alebo softwarový. [7]

Mnoho personálnych operačných systémov obsahuje softwarovo založené firewally vedúce k ochrane hrozieb z kyberpriestoru. Mnoho smerovačov, ktoré prepúšťajú dáta medzi sieťami obsahujú firewally a dokážu základné smerovacie funkcie.



Obr. 7 Firewall

Firewally rozdeľujeme:

- **Prvá generácia: Paketové filtre**

  Paketová filtrácia firewallov pracuje hlavne v prvých troch vrstvách OSI modelu, čo znamená, že väčšina práce sa koná medzi fyzickou a sieťovou vrstvou, s troškou práce aj v transportnej vrstve s cieľom zistiť zdrojové a cieľové čísla portov.

  Ak paket pochádza od odosielateľa a je zapnutá filtrácia vo firewallu, zariadenie porovná záznamy, ktoré sú nakonfigurované vo firewallu a podľa toho paket pustí alebo zahodí. Napríklad, ak existuje na firewallu pravidlo na zablokovanie služby telnet, tak pri snahe pripojiť sa cez telnet, firewall zablokuje pripojenie. [7]

- **Druhá generácia: Firewally na aplikačnej vrstve v OSI modelu**

  Aplikačný firewall je oveľa viac bezpečný a spoľahlivý v porovnaní s paketovými firewallmi, pretože pracujú na všetkých siedmych vrstvách OSI modelu od aplikačnej dole až po fyzickú vrstvu.

Dobrým príkladom aplikačných firewallov je Kerio Personal Firewall. Aplikačné firewally môžu filtrovať vyššie vrstvy protokolov ako FTP, Telnet, DNS, DHCP, HTTP, TCP, UDP a TFTP. Napríklad, ak spoločnosť chce blokovať všetky informácie súvisiace k pojmu "terorista", potom filtrácia podľa obsahu môže byť blokovaná na firewallu k patričnému slovu. [7]

Vo Windowsoch je používaný buď integrovaný firewall, alebo nejaký softwarový doinštalovaný, dobrým príkladom je Kerio Personal Firewall. Nastavuje sa zväčša pomocou grafického rozhrania. Sú tam prichádzajúce a odchádzajúce spojenia, ktoré sa nastavajú. Záleží len na bezpečnostnej politike spoločnosti. V Linuxe je postup o trošku rozdielny, pretože skoro všetko sa nastavuje cez príkazový riadok. Existuje samozrejme aj grafické nastavenie firewallu v Linuxe. Ale nie je doporučené takto nastavovať firewall v Linuxe, pretože existuje určité bezpečnostné riziko.

2.5 Bezpečnostná politika

Je z jednou často opomínaných častí vo firmách, školách, atď. Je dôležitou súčasťou každého bezpečnostného systému. Obsahuje súhrn bezpečnostných požiadaviek na úrovni fyzickej, personálnej, administratívnej, počítačovej a komunikačnej bezpečnosti. Bezpečnostná politika musí byť ako dokument schválený vedením spoločnosti ako záväzná vnútropodniková smernica. Bezpečnostná politika je chápaná ako základný písomný dokument organizácie, obsahujúci predstavu vedenia o riešení bezpečnosti a základné požiadavky na jednotlivé bezpečnostné oblasti celého IS. Bezpečnostná politika ponúka odpovedať na niekoľko základných otázok: [8]

- **Čo chceme chrániť**
- **Prečo to chceme chrániť**
- **Ako to chceme chrániť**
- **Čo budeme robiť, keď dôjde k zlyhaniu systému**

Bezpečnostná politika IT by mala byť vypracovaná vo forme bezpečnostného projektu na komplexnú ochranu informačných systémov, v ktorom budú definované jednotlivé hrozby, ktoré sú relevantné pre aktíva IS a následne by mali byť popísané metódy na ich ochranu (protiopatrenia). Ide o metódy technickej, mechanickej, organizačnej a režimovej ochrany.

V závere bezpečnostného projektu by mali byť definované hrozby, ktoré boli pokryté, a ktoré neboli pokryté z určitých dôvodov. Pri tvorbe bezpečnostného projektu, najmä pri určovaní protiopatrení by mala byť zvažovaná aj nákladovosť na jednotlivé prvky ochrany. Bezpečnostný projekt na komplexnú ochranu IS obsahuje: [8]

- **Bezpečnostný zámer**
- **Analýzu kvalitatívneho zabezpečenia**
- **Analýza rizík**
- **Hodnotenie rizík vo vzťahu k existujúcim opatreniam,**
- **Návrh nových alebo doplňujúcich protiopatrení**
- **Plán implementácie nových alebo doplňujúcich ochranných opatrení**
- **Bezpečnostné smernice**
- **Havarijný plán a plán obnovy IS**

2.6 Antivírusy

Antivírusový software je používaný k prevencii, detekcii a slúži aj k odstráneniu škodlivého softwaru, obsahujúci počítačové vírusy, počítačové červy, trójany, spyware (špionážny software), rootkity. Antivírusy tvoria dôležitú súčasť súčasť dnešnej počítačovej bezpečnosti v kyberpriestore. Nie je to sto percentná ochrana, ale minimalizujú sa riziká tým a tým pádom aj dopad na aktíva. Netreba zabúdať, že antivírus treba aktualizovať. Bez aktualizácie to nemá zmysel, pretože je nutné mať databázu vírusov aktualizovanú. Pretože potom idú percentá účinnosti ochrany dole.

História antivírusov vznikla zhruba v roku 1988. Pri vzniku prvých vírusov, sa objavil aj antivírus. Prvé antivírusy boli jednoduché, jednoúčelové. Hovorí sa, že tvorcovia vírusov, sú aj zároveň tvorcovia antivírusov a bolo to kvôli peniazom.

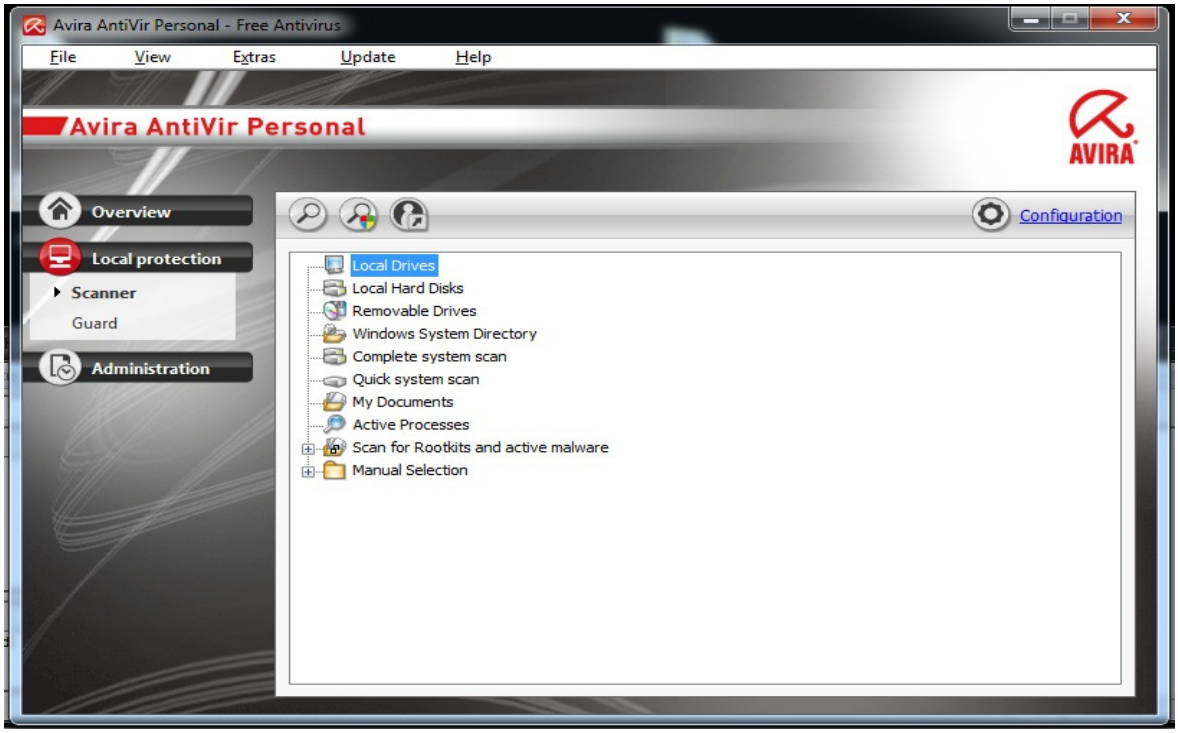
Antivírusy rozdeľujeme na typy:

- **klient**
- **server**

Antivírusy typu klient používame na koncových zariadeniach pre užívateľov.

Antivírus sa skladá z týchto častí:

- **On-access scanner -** Nepretržite kontroluje dáta, s ktorými užívateľ pracuje. Funguje na princípe rezidentného štíta.
- **On-demand -** Užívateľ má možnosť urobiť antivírusový test vo vybranej oblasti. Znamená to, že sa spraví test na požiadavku užívateľa.
- **Quarantine -** Je to karanténa pre detekované vírusy. Jej funkciou je uchovávanie vírusov v bezpečí.
- **Update -** Je databáza aktuálnych vírusov. Je povinnosťou každého užívateľa, mať tento zoznam aktualizovaný.
- **Pluginy** - Obsahujú rôzne moduly pre antivírus. Napríklad moduly kancelárskeho balíka Office, OpenOffice, atď. Kontrolujú dokumenty, či nie sú napadnuté. Dôležitá súčasť je modul pre poštu. Pri príjmaní e-mailov, sa overuje či neobsahujú škodlivý software.
- **Scheduler -** Je plánovač, cez ktorý si užívateľ navolí, kedy bude chcieť skenovať dáta. Naplánovaná akcia, kedy sa spustí kontrola.
- **Integrita dát** - zabezpečuje celistvosť, neporušenosť dát.



Obr. 8 Antivírusový program Avira

Hore v obrázku číslo osem, je uvedený príklad antivírusu. Názorná ukážka antivírusu pre užívateľov. Na obrázku je znázornený skener, kde sa bude skenovať, rýchly sken. V najvyššej lište sú zobrazené položky súbor, zobraziť, extra, aktualizácia a pomoc.

Až 65 % domácich používateľov internetu a antivírusových programov si neaktualizuje svoj softvér a vystavuje sa tak obrovskému nebezpečenstvu internetových útokov. Vyplýva to z prieskumu, ktorý pre spoločnosť ESET realizovala v prieskumná agentúra Harris Interactive® na americkom trhu. Pritom tento spôsob reaktívnej ochrany sa výraznou mierou podieľa na schopnosti antivírusového systému chrániť dáta.[9]

Podľa bezpečnostných špecialistov, neexistuje účinná ochrana proti zero-day (nulový útok). To znamená, že útoky sú realizovateľné za pomoci bezpečnostných slabín software. Alebo, vydané záplaty, šikovní ľudia si nájdu slabiny a zneužijú ich.[9]

Niekoľko antivírusových programov: Avast, Avira, AVG, ESET Nod32, Kaspersky, Norton Antivirus, atď.

2.7 Sandbox

V počítačovej bezpečnosti, sandbox je ochranný mechanizmus pre separátne bežiace programy. Je často používaný k spúšťaniu netestovaného kódu, alebo nedôveryhodných programov z neoveriteľných tretích strán a nedôveryhodných užívateľov. [7]

Sandbox, je pomerne novým bezpečnostným nástrojom pre bezpečnosť. Poskytuje pevne kontrolovateľnú sadu zdrojov pre hostiteľské programy k ich behu, ako je disk a pamäť. Sieťový prístup, má schopnosť kontrolovať hostiteľský systém alebo čítať zo vstupov zariadení, ktoré bývajú zvyčajne zamietnuté alebo ťažko nedostupné. V tomto zmysle, sandbox je špecifickým príkladom virtualizácie.

Niekoľko príkladov sandboxu:

Apletové programy, ktoré sú spustené na virtuálnom stroji, alebo interpretátor skriptovacieho jazyku robí sandboxovanie. Aplety sa nachádzajú najčastejšie vo webových prehliadačoch, ktoré používajú mechanizmus k bezpečnému spusteniu nedôveryhodného kódu vo web stránkach. Tri najpoužívanejšie apletové implementácie sú. Adobe Flash, Java aplety a Silverlight.

Virtuálne stroje emulujú kompletne hostiteľský počítač, na ktorom je tradičný operačný systém. Má možnosť bootovať a bežať na aktuálnom hardwaru. Hostiteľský operačný systém je sandboxovaný v tom zmysle, že nebeží natívne na hostiteľovi a má možnosť prístupu k hostiteľským zdrojom len cez emulátor.

Sandboxovanie na natívnych hostoch: Výskumníci v oblasti bezpečnosti spoliehajú na tieto technológie k analýze škodlivého softwaru, ako je malware, spyware, atď., na zistenie toho, ako sa chová škodlivý software. Vytvorením prostredia, ktoré napodobňuje cieľové počítače, výskumníci môžu zistiť, ako škodlivý software infikuje a napáda cieľových hostiteľov.

V operačnom systéme Linux, existuje bezpečný mód (seccomp), je to sandbox, ktorý je vstavaný do Linuxového jadra. Ak je aktivovaný seccomp, dovolený je iba zápis (w), čítanie (r), opustenie (q) a systémové volania. [7]

Na internete existuje veľké množstvo programov poskytujúcich sandbox, či už ako freeware, shareware, alebo inú licenciu podporujú. Jednoduchým príkladom, poslúži softwarový nástroj VMWARE, ktorý slúži na virtualizáciu operačných systémov.

Samozrejme existujú aj bezpočetné množstvá programov, ktoré umožňujú virtualizovať len programy.

2.8 Kryptografia a steganografia

Od samého začiatku civilizácie existovali spôsoby, ako skrývať, ochrániť a šifrovať informácie. Pre laikov dosť často opomínané slová. Avšak po príchode IT sektora, internetu, technológii majú čoraz väčší význam. Spektrum využitia je veľké. Šifrovanie hesiel, šifrovanie komunikačných kanálov, šifrovanie dát, elektronický podpis, ukrytie informácií do obrázkov. V ďalších kapitolách, budú vysvetlené pojmy.

2.8.1 Kryptografia v oblasti bezpečnosti

Kryptografia, alebo šifrovanie je náuka o metódach utajovania zmyslu správ, prevodom do podoby, ktorá je čitateľná, len so špeciálnou znalosťou. Slovo kryptografia, pochádza z gréckeho pôvodu. Kryptós je skrytý a gráphein znamená písať. Niekedy je tento pojem obecne používaný pre vedu, týkajúcej sa šiframi. Ďalší dôležitý pojem je kryptoanalýza. Zaoberá sa dešifrovaním správ.

Kryptografia sa snaží spravidla pozmeniť správu použitím matematických operácií tak, aby bola nečitateľná pre nikoho, kto neovláda postup jej dešifrovania. Správa sa posiela verejnými komunikačnými kanálmi. Predpokladá sa, že nikto okrem adresáta, nebude schopný dešifrovať správu. Preto sa neustále vyvíjajú zložitejšie kryptografické techniky a metódy, ktoré zašifrujú správu oveľa zložitejším spôsobom. Existujú totiž aj metódy, ako sa dostať k zašifrovanej správe. Tieto metódy dešifrovania vyvíja tajná služba, armáda, špionáž. Je možné dešifrovať dáta hrubou silou, záleží však na výkonnostných parametroch počítačov. Kvalitná šifra spočíva v tom, keď doba rozšifrovania je dlhšia ako doba, po ktorú musí byť správa utajená.

Šifrovanie sa rozdeľuje na:

- **Symetrické**

  „Symetrické šifrovanie je postup, ktorým jednoznačne zašifrujeme správu S (Správa) pomocou kľúča K s (väčšinou) pevne danou dĺžkou na zašifrovaný text T, pričom zo zašifrovaného textu T dostaneme pôvodnú správu S len za podmienky,

že poznáme pri šifrovaní použitý kľúč. Symetrické šifrovanie sa skladá z dvoch častí, zašifrovanie (Encryption) a dešifrovanie (Decryption), pričom platí:

E(S, K) = T

D(T, K) = S

pričom E a D je u väčšiny algoritmov rovnaká funkcia (teda používame rovnaký postup na šifrovanie aj dešifrovanie). Príkladom symetrického šifrovania je DES (Data Encryption Standard). "[7]

- **Nesymetrické**

„Problém so symetrickým šifrovaním je v prenose kľúča. Kľúč K sa totiž musí preniesť cez nejaké médium. To bola v minulosti jedna z najväčších priorít medzinárodnej špionáže. Už vôbec nebolo možné kľúč preniesť cez elektronický kanál, ktorý je veľmi ľahko odpočúvateľný. Fyzický prenos je na druhej strane veľmi pomalý. Asymetrické šifrovanie tento problém rieši veľmi efektívne. Asymetrické šifrovanie je séria postupov, pri ktorých jednoznačne premeníme text T1 na text T2 pomocou kľúča Kn (n=1,2). Skladá sa z dvoch častí. Prvá časť (šifrovanie - encryption) premení text M na text T pričom použije kľúč K1 (väčšinou označovaný ako verejný kľúč - public key). Druhá časť (dešifrovanie - decryption) premení text T na text M, pričom sa použije kľúč K2 (väčšinou označovaný ako súkromný kľúč - private key). V zásade platí, že z K1 sa žiadnym matematickým postupom nedá získať K2. Súkromný kľúč K2 je kľúč, ktorý vlastní len človek, ktorému je správa určená. K1 je verejný kľúč, ktorý môže vlastniť ktokoľvek (daná osoba ho teda môže poskytovať na stiahnutie na internete). Text M zašifrovaný pomocou kľúča K1 sa teda dá dešifrovať len za pomoci kľúča K2, ktorý má len človek, ktorému je správa určená (z toho vyplýva, že text T na text M nemôže dešifrovať ani ten, kto ho zašifroval, pretože nemá súkromný kľúč K2, potrebný na túto operáciu). [7] Na odvodenie sa použije tento vzťah:

E(M, K1) = T

D(T, K2) = M

K2 != F(K1)

2.8.2 Šifrovanie dát

Šifrovanie dát sa pomaly, ale iste dostáva aj k bežným užívateľom. Nie je to už devíza veľkých korporácií. Výpočtová technika z dôvodu neustáleho pokroku, sa zlepšuje. Neustále je kladený dôraz na objem dát, informácie. Prišli USB disky, nový trend SSD diskov, ktoré ženú ľudí k neustálemu zamýšľaniu nad problémami, kde uchovávať dáta. Narastajúca kapacita a množstvo úložných zariadení, zvyšuje riziko ukladania citlivých dát. Súkromné fotografie, projektové dokumentácie, údaje o elektronickom bankovníctve, financie firmy v elektronickej podobe a iné.

Šifrovanie dát takto poskytuje riešenie na tento problém. Táto metóda poskytuje zamedzenie prístupu neautorizovaným osobám k osobným dátam. Potencionálny páchateľ tak stratí šancu odcudziť dáta, pokiaľ nerozšifruje algoritmus. Jedná sa o proces, keď z čitateľného média pomocou šifrovacieho algoritmusu vytvoríme, zašifrované dáta. Dešifrujú sa späť vložením autentizačného prvku. Buď heslo, tvár, atď. Možnosti šifrovania existuje mnoho. Od freewarových programov, cez platené programy až po hardwarové zariadenia. K zdarma dostupným programom patrí napríklad DiskCryptor, TrueCrypt.

Metódy šifrovania dát sa rozdeľujú:

- **Súborové šifrovanie** - Spočíva v použití zvoleného kľúča, alebo hesla k zašifrovaniu súborov. Šifrovať sa dajú pevné disky, USB disky, atď.
- **Diskové šifrovanie** - Šifruje sa celý disk ako celok. Software poskytuje šifrovanie celého disku, vrátane oddielu MBR. Užívateľ má o starosť menej, pretože šifruje sa celý disk. Nevýhodou tohto zabezpečenia je rapídne spomalenie počítača**.**[7]

2.8.3 Autentizácia a autorizácia

Je to proces, prípadne overenie identity, najčastejšie používaná v oblasti počítačov, sietí. Každý užívateľ má určité prístupové práva. Najčastejšie funguje autentizácia zadaním hesla, USB kľúčom, alebo pomocou biometrie, najčastejšie býva odtlačok prstu, rozpoznávanie tváre. **Autentizácia spočíva v overení predpokladanej identity užívateľa**. Autentifikácia =Autentizácia. Napríklad Rádius server, umožňuje autentifikovať sa do WiFi siete pomocou certifikátov. Samotná autentizácia môže prebehnúť niekoľkými spôsobmi:

- **Niečo vie** - táto autentizačná metóda je najpoužívanejšia a je najčastejšia založená na znalosti užívateľského mena a hesla. Autentizácia zvyčajne prebieha tak, že používateľ je systémom vyzvaný na zadanie svojho hesla.
- **Niečo má** - tento typ autentizácie býva založený na vlastníctvo nejakého predmetu (USB token, smart card, kalkulátor). Autentizácia zvyčajne prebieha tak, že používateľ je systémom vyzvaný k používaniu predmetu.
- **Niečo je** - tento typ autentizácie je založený na overenie biometrických charakteristík (odtlačok prsta, snímka dúhovky). Autentizácia zvyčajne prebieha tak, že používateľ je systémom vyzvaný, aby priložil napríklad prst k snímaču.

Pre zvýšenie bezpečnosti, sa často vyššie uvedené metódy autentizácie kombinujú. V takom prípade sa hovorí o viacfaktorovej autentizácii, pretože na preukázanie identity je nutné použiť viac faktorov. Najpoužívanejšou metódou je metóda niečo vie.

Pri výbere vhodnej autentizačnej metódy sa použijú tieto otázky:

- **Bezpečnosť -** aké ťažké je danú autentizačnú metódu prelomiť?
- **Náklady na obstaranie -** koľko stojí zavedenie danej autentizačný metódy, nákup HW, SW a inštalácia a konfigurácia na strane poskytovateľa tejto služby?
- **Náklady na nasadenie -** aké sú počiatočné náklady na sprevádzkovanie technológie.
- **Náklady na prevádzku -** koľko stojí poskytovateľa tejto služby správa a podpora danej autentizačnej metódy?
- **Náročnosť** - ako ľahko dokáže používateľ danú autentizačnú metódu sám sprevádzkovať a začať používať?
- **Použiteľnosť** - ako ľahké je používanie danej autentizačnej metódy pre užívateľa? Koľko krokov musí užívateľ urobiť a koľko času mu to zaberie?
- **Mobilita -** do akej miery je zvolená autentizačná metóda nezávislá na HW a SW vybavení? Môže sa užívateľ autentizovať odkiaľkoľvek?
- **Budúcnosť -** aká bude perspektíva do budúcnosti a na ako dlho postačí postavený systém?

Typy autentizačných prostriedkov:

- **Hardwarový token -** Tento typ autentizácie je založený na vlastníctvo nejakého predmetu. Najčastejšie USB kľúč s šifrovacím zariadením. Cena tohto USB kľúča vyjde od 50euro a vyššie. Výhodou tohto zariadenia je, že pri útoku hrubou silou nezlyhá.
- **Softwarový token -** SW token, má podobu aplikácie, ktorá sa musí nainštalovať na hostiteľské zariadenie. Je teda spravidla uložený, na rovnakom zariadení, z ktorého prebieha autentizácia. Úroveň bezpečnosti, ktorú je SW token schopný poskytnúť je tak priamo závislá na bezpečnosti hostiteľského systému, ktorým môže byť ako počítač, notebook, tablet, atď. Aby mohol užívateľ začať token používať, musí zadať správne heslo. Ak by používateľ niekoľkokrát po sebe zadal chybné heslo, tak sa šifrovacie kľúče zničia.
- **Certifikát -** Predpokladom je, že USB tokene je uložený užívateľský certifikát a privátny kľúč, potom sa jedná o tzv. HW token. Ak by bol certifikát a súkromný kľúč uložený priamo na počítači, z ktorého sa autentizácia vykonáva, jednalo by sa o tzv. SW token. Ten však nie je možné považovať za bezpečný, pretože môže byť ľahko skopírovaný.
- **Mobilný telefón -** Vôbec za najväčšiu výhodu mobilných zariadení možno považovať skutočnosť, že väčšina ľudí už ich vlastní a nemusia si tak žiadny autentizačný predmet zhotovovať. Pre autentizáciu potom stačí iba zavolať z telefónu na číslo, na ktorom je poskytovaná služba. Ďalšou možnosťou je vybaviť mobilný telefón patričným softvérom a využívať ho ako autentizačný kalkulátor a synchrónny alebo asynchrónny generátor jednorazových hesiel. Rovnako tak môže byť mobilný telefón použije na príjem OTP zaslaných formou SMS.
- **Grid karta -** Ide o papierovú alebo plastovú kartu, na ktorej sú uvedené jednorazové heslá.
- **OTP -** (One Time Password) môžu použiť len raz, takže prípadná kompromitácie hesla v okamihu jeho zadávaní nepredstavuje riziko. OTP môže byť zariadením generované v podstate neustále v pravidelných krátkych intervaloch (tzv.

synchrónny mód) alebo je OTP generované až po zadaní serverom poskytnutých dát (tzv. asynchrónny mód).

- **PIN -** Aby bolo možné niektoré autentizačné zariadenie použiť, je nutné zadať PIN (Personal Identification Number). Ako už táto skratka napovedá, zvyčajne sa jedná skutočne len o číslo, majúci zvyčajne 4 až 8 cifier. Nové tokeny umožňujú zadať aj písmená a špeciálne znaky. Avšak to nič nemení na tom, že tento PIN alebo skôr heslo pre prístup k predmetu užívateľ príliš často nemenia a tak môže byť pre útočníka pomerne ľahké ho odpozorovať a potom autentifikačný predmet oprávnenému užívateľovi ukradnúť alebo si ho jednoducho len na malú chvíľu požičať. Pre úplnosť treba dodať, že drvivá väčšina autentizačných SMS sa posiela nešifrovane, takže tu existuje určité riziko, že sa k nim dostane minimálne mobilný operátor.

Po autentifikácii nasleduje **autorizácia**. Spočíva v nastavení prístupových práv zdrojov, ktoré sú spájané s bezpečnosťou informácií a počítačovou bezpečnosťou vo všeobecnosti ku kontrole prístupu. **Autorizácia je definovanie prístupovej politiky**. V priebehu procesu, systém používa kontrolu prístupových pravidiel v počítačovom systéme. Systém sa potom rozhodne podľa nastaveného filtra, či užívateľov autentizuje, tzn. prístup povolí, alebo prístup zamietne. Dobrým príkladom poslúži, prihlasovanie sa do domény, alebo na zaheslovaný disk, atď.

2.8.4 Steganografia v oblasti bezpečnosti

Súvisí s kryptografiou, jej úlohou je nie šifrovať správy, ale ukrývať ich. Steganografia je veda, ktorá sa zaoberá skrývaním správ. Odosielateľ a príjmateľ jedine vedia o skrytej správe. Slovo steganosgraphein pochádza z gréckeho pôvodu slov steganos - schovaný a graphein - písanie. Od samého počiatku je využívaná k ukrývaniu správ či už vo vojnách, alebo v civilnom sektore. Skrývanie správ bolo veľmi veľa krát nutné k prežitiu. [7]

V kyberpriestore je ideálnym médiom na ukrývanie obrázky, audio súbory atď. Najčastejším médiom sú obrázky. Napríklad obrázok vo formáte BMP s rozlíšením 1280 x 800 sa pohybuje okolo 3,5 MB. Obrázok je matica čísel, kde každý bod predstavuje nejaké číslo. Farebný obrázok sa skladá z RGB filtru. RGB je trojica farieb (R) červená, (G)

zelená, (B) modrá. Odtiene sú riešené pomocou hodnôt v rozmedzí od 0 až do 255. Takže pre každú farbu je možnosť zakódovať až do 8 bitov. Súčasne sa tieto farby líšia v bitovom zápise iba posledným, najmenej dôležitým bitom, ktorý sa nazýva Least Significant Bit (LSB). V dobre vybraných prípadoch je teda možné zameniť farbu bodu za veľmi podobnú farbu tak, aby sa to vo výslednom obrázku neprejavilo výraznými zmenami. Vytvára sa tak priestor na uloženie dodatočnej informácie ľubovoľného charakteru. Informácia je zapísaná v binárnom tvare, a to tak, že do každého LSB bitu každého bajtu obrázka sa zapíše 1 bit stegosprávy. Teoreticky je teda možné zapísať do obrázka BMP, stegosprávu s kapacitou jednej osminy pôvodného BMP obrázku. V prípade spomínaného obrázka je to až 437 KB. To je slušná kapacita pre celú knihu alebo pre viacero obrázkov vo formáte JPG. [7]

Ďalším médiom je zvuk (audio). Pri tomto druhu ukrývaní správy sa využíva nedokonalosť ľudského ucha. Ľudské ucho pracuje na frekvencii od 18Hz pre najcitlivejšie ucho, štandard je od 22Hz, až po 22KHz. Používa sa technika skrývania do posledného signifikatného bitu (LSB), tak ako je aj u obrázkov. Množstvo dát, ktoré je potrebné skryť závisí od vzorkovacej frekvencie a počtom kanálov zvuku. Príliš veľká hustota správy spôsobuje šum. Tak treba dávať pozor. [7]

V oblasti bezpečnosti to možno použiť, ako nástroj na ukrývanie správ. Účel je poslať správu niekomu, tak aby ju nevideli ostatní, s cieľom aby to videla len cieľová osoba. Ak je osoba vo vysokom postavení vo firme, tak sa odporúča použiť tento druh ochrany z cieľom minimalizovať riziká.

2.9 Fyzické zabezpečenie

Nie len bezpečnosť v kyberpriestore, zohráva hlavnú úlohu. V oblasti bezpečnosti existuje viacero úskalí. Jedným z nich je fyzické zabezpečenie priestorov, predmetov, atď. Potencionálny útočník (zamestnanec firmy, alebo cudzia osoba), môže obísť radu bezpečnostných opatrení. Pozor si treba dávať na odcudzenie dát, médií, ľudí ktorí sa snažia odpozerať heslá. Fyzický prístup do dôležitých miest, kde sa nachádza vybudovaná infraštruktúra. Pri výpadku infraštruktúry by nastal kolaps. Stačilo by, keby útočník pocvakal káble vedúce k smerovačom, serverom a dôležitým prvkom v sieti.

Ochrana proti odcudzeniu dát existuje. Záleží však na samotnom užívateľovi, aby čo najviac eliminoval riziká na čo najmenšiu úroveň. Napríklad ochrana môže byť, mať nastavené heslo na užívateľskom konte. Ak sa nepracuje s počítačom, je dôležité byť odhlásený. Zabezpečiť počítač proti odcudzeniu. Riešenie je namontovať bezpečnostné zámky. Efektívna možnosť zabezpečenia, je šifrovať dáta. Oddeliť citlivé dáta, od bežných dát.

Ochrana proti infraštruktúre má viacero možností. Jednou z nich je nasadenie kamerového systému, tie modernejšie využívajú IP kamery, kde sa dá nahrávať obraz na média, alebo odosielať po sieti. Potom sa dá využiť EZS systém, ktorý umožňuje monitorovanie priestoru, pomocou detektorov, či už PIR, ultrazvukových, atď. Dôležitou súčasťou modernej zabezpečovacej techniky je prístupový systém, často označovaný ako Access systém. Poskytuje detailné informácie o tom, kto, kde, kedy bol. Tento systém je hlavne nevyhnutnosťou pri ochrane serverovní, dátových centier. Najlepšou možnosťou je skombinovať tieto systémy dohromady, aby sme eliminovali riziko čo najnižšie. Vychádzame však z reálnych možností, ktoré sú k dispozícii. Ignorovanie týchto bezpečnostných opatrení, môže mať fatálny následok pri podcenení.

II. PRAKTICKÁ ČASŤ

3 ANALÝZA BEZPEČNOSTÉHO SYSTÉMU V SPOLOČNOSTI

Analýza bezpečnosti tvorí dôležitú súčasť bezpečnostnej politiky. Analýza, je metódou na rozkladanie a rozbor jednotlivých vlastností. V tomto prípade je snaha definovať, čo najviac vlastností systému, napr.: počítače, sieť, šifrovanie, poukázať na bezpečnostné problémy, prípadne navrhnúť bezpečnostné opatrenia na odstránenie nedostatkov.

Po konzultáciách so spoločnosťou, sa zadefinovali požiadavky, čo potrebovali. Z hľadiska bezpečnostných dôvodov a opatrení, sa nebude konkretizovať názov spoločnosti a detailné informácie. Po dôkladnej analýze a implementácii riešení, sa chystá spoločnosť spraviť ďalší bezpečnostný audit. Pretože plánuje sa vyhnúť nepríjemnostiam, ktoré by mohli neskôr nastať. Je to Sarbanes-Oxley-Act. Pochádza z USA, v roku 2002 ako odpoveď na bezpečnostné audity zabezpečujúce spoľahlivosť podľa štandardu. Je určený predovšetkým pre IT prostredie, hlavnou úlohou je prekontrolovať správnosť elektronických záznamov.[10]

Zadefinovali sa tieto požiadavky:

- Analýza siete, zabezpečenie siete
- Analýza WiFi siete, zabezpečenie WiFi siete
- Analýza bezpečnosti serverov, zabezpečenie serverov
- Analýza bezpečnosti softwaru

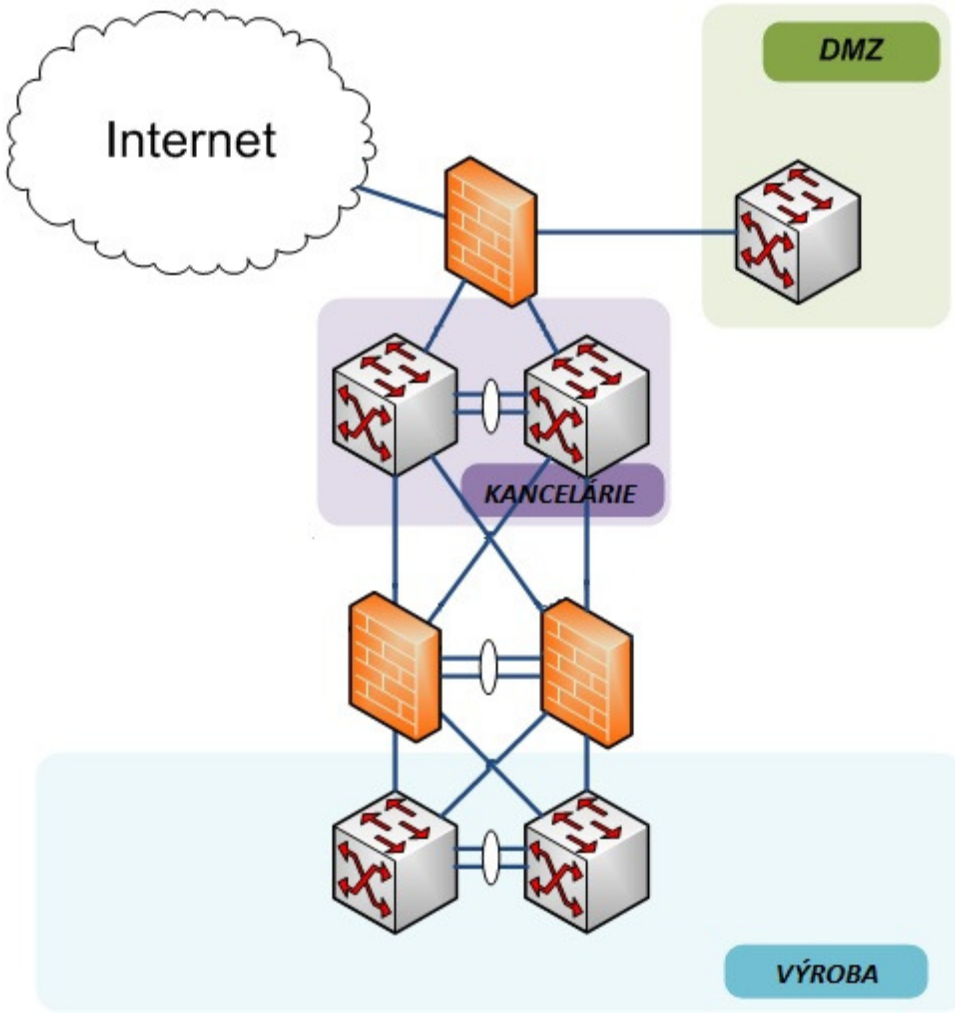
3.1 Analýza siete

Analýza siete pozostáva z určenia topológie, sieťových prvkov, kontroly nastavenia prepínačov, smerovačov a firewallov.

Sieť spoločnosti je pripojená na sieť ISP optickým pripojením, rýchlosťou 20Mbit/s. S optického optopanelu od ISP, to vedie do smerovača od spoločnosti CISCO. Z Cisco smerovača, je prepoj riešený pomocou core prepínačov, edgových prepínačov a medzi nimi sú firewally od spoločnosti Juniper. Sieť pozostáva s MDF racku a IDF rackov. MDF (main distribution frame) rack, je hlavným rackom, odkiaľ sa napájajú ďalšie IDF (intermediate distribution frame) racky. Prepojenia medzi nimi je riešené na báze optiky. Z jednotlivých IDF rackov sa potom napájajú jednotlivé počítače z kancelárium.

Sieť obsahuje Cisco menežovateľné prepínače, ktoré sa dajú konfigurovať ku konkrétnym požiadavkám zákazníka. Zásadným problémom pri skúmaní bolo, že menežovateľné prepínače boli zle nastavené. V kapitole 5.1 bezpečnostných opatrení sa dostaneme k tomu, čo sa konfigurovalo. V podstate ide o to, aby boli prepínače správne nakonfigurované do akých virtuálnych, nesmie sa zabúdať na šifrovanie hesiel, keď sa prihlasuje vzdialene cez službu Telnet, SSH. Nesmie sa opomenúť na nastavenie portov na prepínačoch, aby im náležali koncové zariadenia s MAC adresou. Pri nesprávnej konfigurácii, by sa útočník mohol pripojiť na port a oddiaľ by mohol spraviť útok.

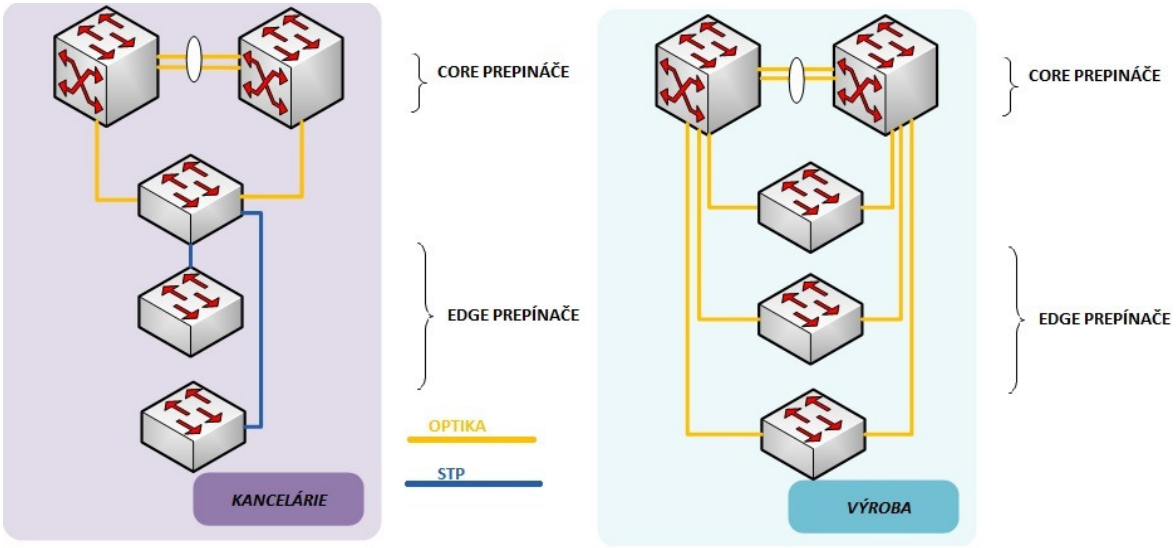
Sieť je rozdelená na viacero zón. Internet, zóna DMZ, kancelárska a výrobná sieť.



Obr. 9 Schéma zapojenia siete v společnosti

V podstate pri tejto analýze išlo o správnu konfiguráciu menežovateľných prvkov, tak aby súčasnou konfiguráciou nebola ohrozená bezpečnosť. Tento obrázok popisuje MDF rack.

Ďalej je to prepojené s core prepínačov, na jednotlivé IDF racky optikou, kde sa nachádzajú menožovateľné Cisco prepínače. Prepojenie z kancelárskych IDF je riešené tak, že od core prepínačov je to prepojené na jeden edge prepínač a ďalšie edge prepínače sú prepojené STP káblom. Vo výrobnej sieti, všetky prepoje medzi sebou sú riešené pomocou optiky. Doporučenie, ktoré som zabezpečil, bolo pridať redundantné spoje medzi sebou, z dôvodu spoľahlivosti média a sieťových prvkov. Vo výrobe je zakázaný internet.

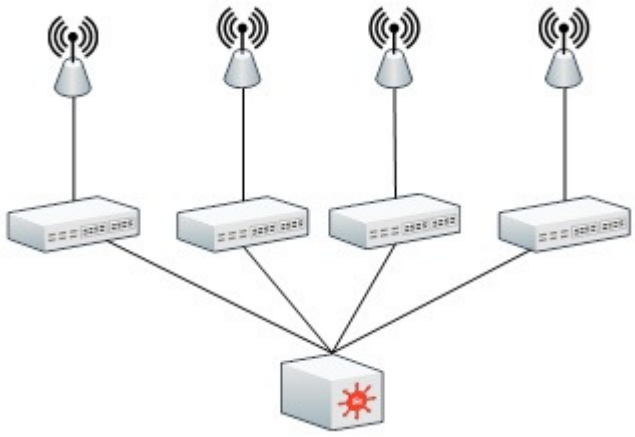


Obr. 10 Schéma zapojenia prepínačov

Požiadavkou spoločnosti bola: Správna konfigurácia menožovateľných prvkov a doladenie bezpečnosti z hľadiska siete, plus implementácia sofwaru na monitorovanie.

3.2 Analýza WiFi siete

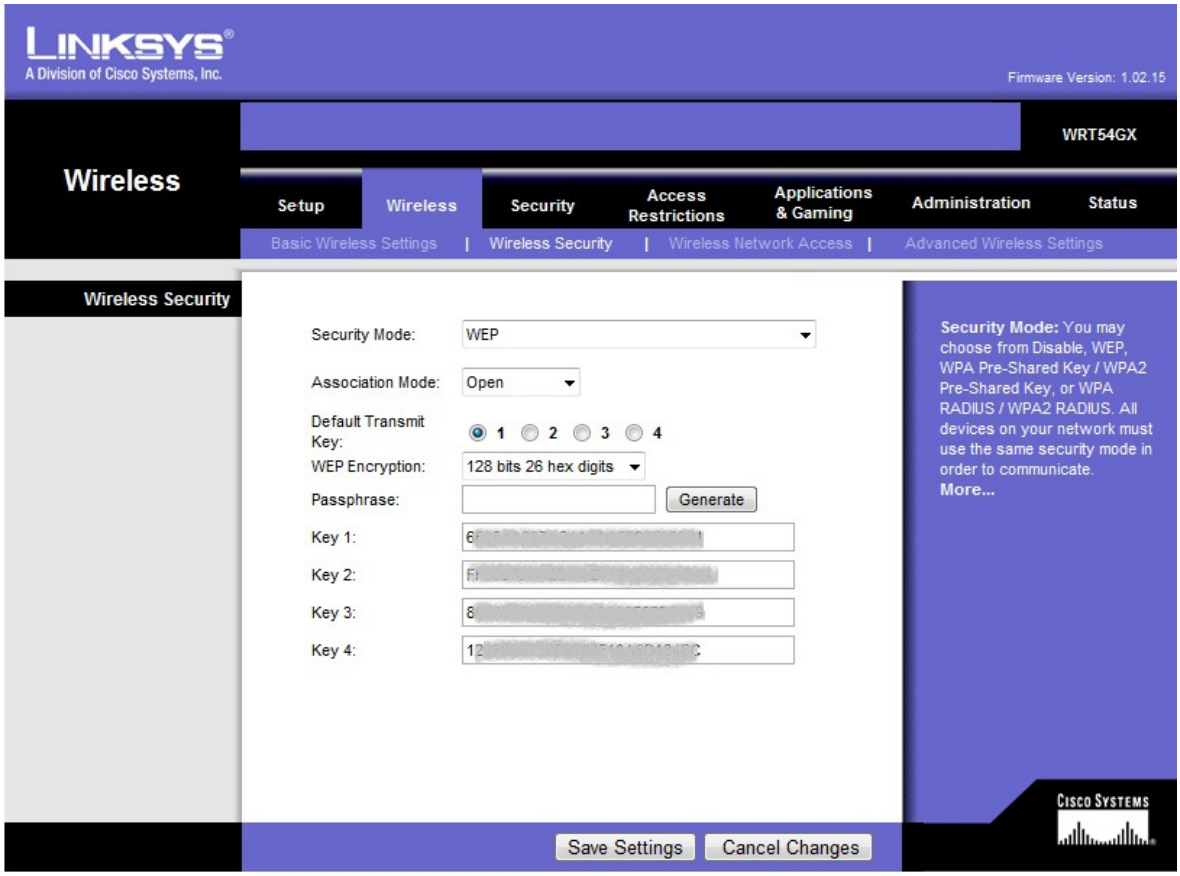
Po opätovnej konzultácii so spoločnosťou, bola priorita spraviť lepšie WiFi zabezpečenie. Bezdrôtová sieť sa skladá so štyroch WiFi prístupových bodov značky Linksys. Linksys je dcérskou spoločnosťou firmy Cisco.



Obr. 11 Schéma WiFi siete

Nastavenie prístupových bodov sa robí pomocou webového rozhrania. Podľa prieskumov firmy Nextlan: „ *Približne deväť z desiatich firemných bezdrôtových sietí Wi-Fi v Prahe a Brne má slabé zabezpečenie a sú jednoducho napadnuteľné hackermi. Podľa prieskumu spoločnosti Nextlan nemajú tieto siete buď vôbec žiadnu ochranu, alebo len slabú, ktorú sa dá bežne dostupnými prostriedkami prelomiť v priebehu niekoľkých desiatok minút. Firma to uviedla v tlačovej správe."* [11]

Z tejto správy plynie ponaučenie. Čím silnejšia ochrana, tým menšie riziko hrozí. V rámci zabezpečenia, sa našla bezpečnostná slabina, ktorá sa dá využiť. Mnoho ľudí dneska vie, ako prelomiť WEP ochranu u WiFi pripojenia. Riešením je použiť silnejšiu ochranu, napríklad WPA, WPA2, Rádius server. Dá sa nastaviť tiež, stupeň ochrany a to buď filtráciou pomocou MAC adries alebo IP adries. Za ďalšiu potencionálnu hrozbu považujem vysielanie SSID broadcastu, ktorý útočník vidí. SSID broadcast, je vysielanie mena WiFi siete. Šikovnejší útočníci si s tým poradia. Avšak tým, že vypneme túto funkciu, je znížené riziko.



Obr. 12 Webové rozhranie prístupového bodu Linksys

3.3 Analýza bezpečnosti serverov

Nesmie sa zabúdať na bezpečnosť serverov. Pri ich výpadku a ich nedostupnosti by následky boli fatálne. V spoločnosti sa používa komerčný software Microsoft Windows 2003, Windows 2008 Enterprise edition, tak aj sieťový operačný systém Linux pod licenciou GNU/GPL. Konkrétne CentOS a Debian. V DMZ zóne sú servery, na ktorých bežia webové, e-mailové a VoIP služby. Ostatné servre poskytujú podporu napríklad Antivírusu, súborového systému - RAID 5, atď.

Prieskum pomocou aplikácie nmap ukáže, ktoré porty a služby sú dostupné. Táto aplikácia beží pod Linuxom, vo verzii Backtrack. Backtrack je sada bezpečnostných nástrojov, ktorá slúži na analýzu bezpečnostného prostredia. Pomocou príkaza: **nmap 192.168.15.0/24**

Zistil som tieto otvorené porty:

Port	Služba
21	FTP
22	SSH
23	Telnet
25	E-mail
53	DNS
80	HTTP
139	Samba
443	HTTPS
445	Samba
631	Print
1027	IIS
3389	Vzdialená plocha
5060	VoIP

Tab. 1 Otvorené porty reprezentujúce služby

Z bezpečnostného hľadiska platí. Čím menej portov je otvorených, tým menšie riziko hrozí. Treba dbať nato, že nechať pustené len to, čo je nevyhnutné. Je nevyhnutné mať zapnutú podporu automatických aktualizácií na serveroch. Pretože obsahujú záplaty na bezpečnostné diery.

3.4 Analýza bezpečnosti dát pomocou softwaru

Spoločnosť mala požiadavku na software, aby bol čo najlepšie zabezpečený. Po dôkladnej analýze som zistil, že počítače majú nainštalované tieto operačné systémy:

- Windows XP SP1
- Windows XP SP2
- Windows XP SP3

- Windows Vista
- Windows 7
- Windows Embeeded

Užívatelia majú nastavenú dobrú bezpečnostnú politiku. Nemôžu inštalovať programy samovoľne. Majú to zakázané. Len so súhlasom nadriadeného a administrátora. Nie všetky počítače majú antivírusovú ochranu. Do budúcna ju treba doplniť, nainštalovať a zjednotiť verzie antivírusov. Ochrana počítačov, je riešená od spoločnosti Symantec. Je to komplet ochrana, včetne firewallu, antispyware programu, antivírusu. Spoločnosť má zakúpenú korporátnu multilicenciu.

Právo zápisu súborov majú v spoločnej zložke. Do budúcna sa toto riešenie bude musieť prerobiť z bezpečnostného hľadiska. Neuvádzajú sa detaily, kvôli bezpečnosti spoločnosti. Dočasne je vyriešený problém, s filtrovaním webového obsahu. Filter sa musí trošku poopraviť a aktualizovať zoznam zakázaných adries.

Hlavným problémom v dnešnej spoločnosti sú ľudia, pretože často krát v bezpečnosti zohrávajú hlavnú úlohu. Dobrým riešením je preto vytvoriť upozornenia, čo sa smie a naopak nie. Vytvorením pravidiel bezpečnosti, sa vyhneme nedorozumeniam, ktoré môžu nastať. Napríklad zakázať sťahovanie dát, chatovať s ľuďmi v pracovnom čase. Hlavným pravidlom pri prihlasovaní do domény, alebo programov, ktoré vyžadujú autentizáciu, je použitie silného heslo. Kombinovať znaky, aby heslo bolo dlhé a šanca na odhalanie hesla bude minimálna.

4 KYBERFORENZNÁ ANALÝZA DÁT, V PRÍPADE RELEVANTNÉHO ÚTOKU

Pole pôsobnosti kyberforenznej analýzy má dlhú a bohatú históriu. U.S. armáda a bezpečnostné orgány ako CIA, FBI v sedemdesiatych rokoch boli prví, čo začali používať túto metódu.

V skorých osemdesiatych rokoch, kriminálny vyšetrovatelia boli zapletení do kyberforenznej analýzy, bola to podpora vyšetrovania pre zločiny. Kyberforenzní vyšetrovatelia mali na starosti spočiatku drogy, vraždy a detskú pornografiu, ktorá sa vyskytovala v počítačoch. Páchatelia skladovali plány, dáta z účtovníctva, fotografie v počítačoch a kyberforenzné vyšetrovania poskytovali dôkazy, ktoré počítačový užívateľ používal v nejakom zločine.

V 21.storočí, počítače, sieť a celý kyberpriestor zažíva "boom" v náraste kriminality. V tomto storočí sa človek nevyhne práce so zariadeniami ako počítač, vreckový počítač, mobil. Človek ich používa denne, pri práci. Kyberforenzná analýza, sú vodítka, pomocou ktorých sa zistia určité súvislosti a slúži k hľadaniu potencionálnych útočníkov.

Pojem pochádza z kombinácie slov. Forenzný znamená súdny a Kyberpriestor - abstraktné ohraničenie priestoru, kde komunikujú zariadenia medzi sebou. Presnejšie povedané, je to súhrn metód, techník, nástrojov na hľadanie dôkazov vedúcich k potencionálnemu páchateľovi. Najčastejšie ide o analýzu digitálnych dát, ako detská pornografia, nelegálny obsah, odchytávanie dát v sieti a snaha zistiť páchateľa pri útoku. [12]

Metódy kyberforenznej analýzy:

- **Zber dát**
- **Analýza dát**
- **Prezentácia dát**

Zameranie v tejto práci, bude hlavne analyzovanie sieťovej komunikácie a rozbor dát. Kyberforenzní špecialisti majú mnoho možností, ako zrekonštruovať dáta zo sieťovej komunikácie. Môžu analyzovať sieťovo založené útoky, alebo potencionálne nebezpečenstvo. Dáta sú prenášané cez sieť, v tomto prípade globálny kyberpriestor. Pri odosielaní e-mailov nie je problém zistiť, z kade daný e-mail pochádza, akú má IP adresu samozrejme prečítať obsah správy.[12]

Sieťová kyberforenzná analýza je rekonštruovanie sieťových udalostí, s cieľom poskytnúť prehľad o tom, čo robia užívatelia, zariadenia a aplikácie. Rekonštrukciou sieťových udalostí znamená, poskladanie živý sieťových pripojení založených na príslušnej sieťovej službe, alebo aplikačným protokolom. Jednoduchý príklad môže byť, ak bezpečnostný tým potreboval zrekapitulovať celý webový obsah konkrétneho koncového užívateľa pre podporu vyšetrovania, tak mali by zrekonštruovať všetky HTTP a HTTPS pripojenia. K vykonaniu tejto rekonštrukcie predpokladáme, že bezpečnostný tým vykonával plnohodnotné odchytávanie paketov, na sieťovom zariadení kde bola analýza nevyhnutná. Užívatelia, zariadenia a aplikácie obsahujú všetko z OSI vrstvy číslo dva, až po vrstvu číslo sedem, ktoré generujú sieťovú prevádzku. Napríklad "užívatelia" zahrnujú nejaký sieťový objekt, ktorý môže reprezentovať užívateľa, alebo skupinu užívateľov v sieti, ako Microsoft Active Directory mená, Gmail e-mailové adresy, alebo Facebook chat. "Zariadenia" zahŕňajú pracovné stanice, servere alebo ostatné sieťové zariadenia, obsahujúce mená počítačov, MAC adresy, IP adresy a iné. "Aplikácie" zahŕňajú nezbytné charakteristiky a komponenty štandardných a neštandardných aplikácií operujúcich v rámci siete.[12]

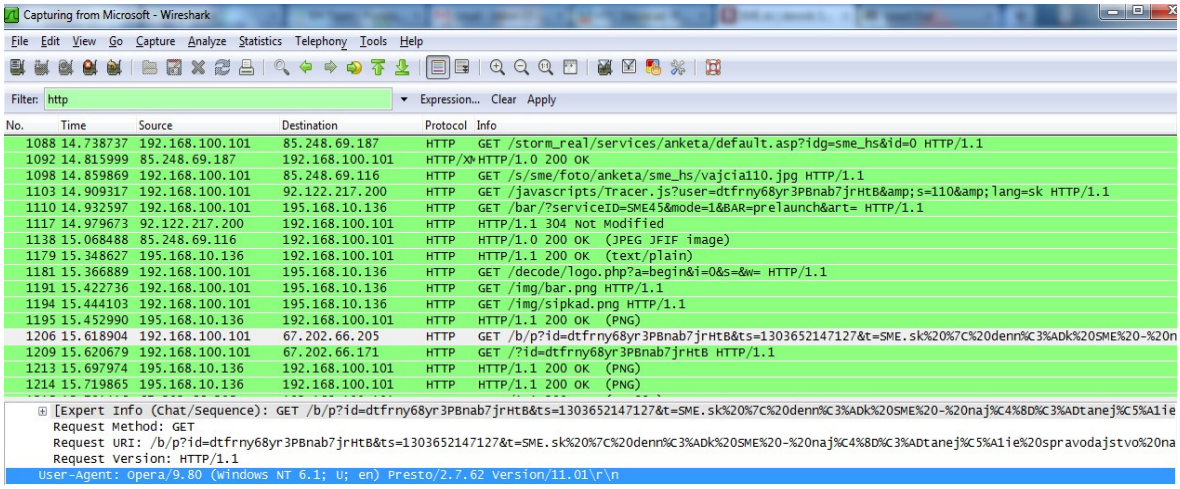
Zdroje dát pre analýzu:

- **Záznamy od ISP:** Poskytovatelia služieb v prípade relevantného útoku pomôžu s hľadaním páchateľa. Zistia IP adresu útočníka. Samozrejme aj adresy sa dajú sfalšovať a tak podvrhnúť IP adresu, ktorá ide cez cudzie proxy servre.
- **Záznamy serverov:** Servre obsahujú v sebe možnosť ukladania záznamu o priebehu sieťových relácii, poprípade čo sa udialo. Záznamy, nazývané v angličtine často krát ako logy, sa v Linuxových serveroch nájdeme v priečinku /var/logs. Analýzou záznamov, sa častkrát nájdu rôzne spojitosti. DNS záznamy poprípade sa budú hľadať.
- **Analyzátory:** Ich hlavnou úlohou je získavať čo najviac informácií v sieti. Sieťová karta sa nastaví do promiskuitného režimu a zachytávajú sa pakety. Je len na osobe, ktorá vykonáva analýzu, identifikovať nebezpečenstvo.
- **Smerovače, prepínače, firewally, proxy servre:** Z týchto sieťových zariadení existuje možnosť, získať nejaké indície vedúce k páchateľovi. Ak páchateľ nezametie stopy. Ale tieto možnosti sú obmedzené.

- **Monitorovanie siete:** Priebežným monitorovaním siete dosiahnem prevenciu. Pomáha zistiť prvotné náznaky nejakých problémov. Napríklad, ak monitorujeme priepustnosť siete každý deň a robíme si záznamy od toho, tak v prípade nadpriemerného prenosu dát už zistíme, že niečo nie je v poriadku.

Identifikácia útočníka nie je v mnohých prípadoch jednoduchá. Hlavným cieľom je eliminovať útok a v prípade zlyhania funkcií systému aj jej nasledovná obnova. Najlepšou metódou ako zistiť útočníka, kde sa nachádza, je zistenie IP adresy. Je to identifikačná adresa, pomocou ktorej zistíme, kde sa páchateľ nachádza. Existujú však určité bariéry, ktoré znemožňujú vypátrať útočníka. Sfalšovanie IP adresy je najčastejším problémom. Skúsení útočníci, zväčša menia IP adresy, aby tak ostali v anonymite. Obete tvoria ďalšie napadnuté počítače, alebo proxy servere, prostredníctvom ktorých útočia. Problém je, že útočníci používajú viacero IP adries a tak sa môžu maskovať a tým pádom sťažiť hľadanie. Existuje riešenie na falšovanie IP adries, spočíva v kontaktovaní o pomoc ISP poskytovateľa. Doporučuje sa kontaktovať, zložky činné v trestom konaní. A poslednou vecou je skúmať nejaké indície, vodítka, pomocou ktorých sa dopátrame na stopu útočníka.

Kyberforenzná analýza poskytuje širokú škálu nástrojov, ktoré sú na trhu. Od profi nástrojov pre analytikov, pre menej náročných existujú nekomerčné riešenie. Typickým príkladom softwaru je: **WireShark, NetWitness Investigator** a iné.



Obr. 13 Analyzátor WireShark

Na obrázku je sieťový analyzátor WireShark, pomocou ktorého sledujeme prevádzku sieťového pripojenia. Je tam vidieť zdroj IP adresy, cieľ IP adresy, čas, protokol, informácie a číslo paketu. Týmto programom zachytíme všetky sieťové aktivity. Tento

nástroj, doporučujem použiť v prípade relevantného útoku, spolu s kombináciou iných programov a snažiť sa zistiť čo najviac stôp vedúcich k páchateľovi.

Pri potencionálnom útoku, nevypíname servre, pretože by sa mohli stratiť dáta a tým pádom, by sme prišli o cenné informácie vedúce k útočníkovi. Odpojiť môžeme sieťové pripojenie a tak je šanca, že rozsah škôd bude menší.

5 SYSTÉM BEZPEČNOSTNÝCH OPATRENÍ A POSTUPOV K ZLEPŠENIU OCHRANY V SPOLOČNOSTI

5.1 Zabezpečenie siete

Túto kapitolu považujem za najťažšiu, pretože vyžaduje odborné skúsenosti a byť oboznámený s danou problematikou. Po konzultácii so spoločnosťou a po vzájomnej dohode čo potrebujú zabezpečiť, sa začalo s konfiguráciou zariadení. Najdôležitejšiu súčasť konfigurácie považujem core prepínače, firewally a potom edge prepínače. Z hľadiska bezpečnosti, sa nebudú uvádzať konkrétne detaily ako IP adresy a iné dôležité informácie, ktoré by môhli vážne narušiť, alebo poškodiť bezpečnosť. Niektoré z informácií, budú pozmenené.

Pre nastavenie bezpečnosti, sa v prepínačoch nastavilo niekoľko prvkov. Prihlasovacie meno a heslo na administráciu smerovačov, prepínačov, šifrovanie MD5, prihlasovanie cez telnet a SSH, VLANy. **V kapitole 3.1 Obr. 9 je prepojenie sieťových prvkov**. B strana, sieťových zariadení, slúži ako redundantný spoj pri výpadku. **Pre konfiguráciu prvkov, je uvedená konfigurácia v prílohe číslo jedna.**

Nastavil som core prepínače, edge prepínače, firewally. Nastavila sa správna konfigurácia na nich, aby sa oddelili jednotlivé **VLANy**. Na monitorovanie priepustnosti siete, slúži software What's Up Gold. Tento monitorovací nástroj nám zaistí integritu dát. Kontrola sieťových zariadení sa bude robiť aj pomocou protokolov Telnet, SSH a webové rozhranie. Pre zaistenie integrity siete bude zaistená každodenná podpora, dvadsaťštyri hodín, sedem dní v týždni.

Na zabezpečenie aktívnych prvkov a serverov, dátových rozvádzačov, boli použité zámky. V prípade, že by kľúč nemala kompetentná osoba, alebo rozvádzač by bol odomknutý, potencionálny útočník by mohol spôsobiť škody veľkého rozsahu. Napríklad poodpájať dátové káble, ukradnúť prepínač, smerovač, atď. Malo by to vplyv, na výpadky siete. Poprípade znefunkčnenie zariadení. Vstup do serverovne, bol taktiež konzultovaný so spoločnosťou a bude realizovaný v priebehu tohto roka pomocou access systému. Hľadá sa riešenie, ktoré sa použije. Dôvod je jednoduchý, bude sa vedieť kto, kde a kedy, vstúpil do objektu a v prípade výpadku sa bude vyvodzovať zodpovednosť.

5.2 Zabezpečenie WiFi siete

Po konzultácii so spoločnosťou, bolo na výber viacero riešení. Avšak existujúce riešenie bezpečnosti pomocou WEP kľúča, bolo nedostačujúce. O zabezpečení WiFi, bolo už veľa toho napísaného, či už v odborných prácach bakalárskych, diplomových, rigoróznych prác, aj v časopisoch a zborníkoch. V skratke povedané, potencionálny útočník nemá problém prelomiť WEP ochranu WiFi. Robil som aj pokusy doma, dešifrovanie kľúča nie je problém a nasledovné pripojenie do siete. MAC filtering sa dá ľahko oklamať, podsunie sa MAC adresa klienta, ktorý patrí do siete. Odborne sa to nazýva MAC poisoning. Taktiež, šikovnejší útočník uvidí vysielanie SSID.

Jednou z možností po úvahe, bolo zvýšenie ochrany na WPA, alebo WPA2. Toto novšie zabezpečenie poskytuje radu výhod, ako lepšie šifrovanie. Na prelomenie tejto ochrany, existujú hash tabuľky a za pomocou nich sa dá dešifrovať táto ochrana. Je skoro nemožné dešifrovať túto ochranu bez širokého spektra znalostí. Použitím tejto ochrany, zminimalizujeme riziko útokov na WiFi.

Po spoločnej konzultácii so spoločnosťou, sa dospelo k názoru, že by bolo vhodné použiť server na autentizáciu a autorizáciu. Použil sa **open-sourcový software Freeradius**. Tento spôsob zabezpečenia WiFi sa používa na Fakulte aplikovanej informatiky Tomáše Bati v Zlíne. Toto riešenie sa implementovalo do spoločnosti. Konfigurácia Freeradius servera, je v diplomovej práci vzadu v prílohe II.

5.3 Zabezpečenie serverov

Zabezpečenie serverov a služieb bežiacich na nich, majú na starosti firewally. Dôslednou analýzou serverov sa zistilo, že bolo potrebné nainštalovať **monitorovací software** pre zistenie dostupnosti, či daný server funguje. V prvej fáze sa uvažovalo o nainštalovaní nekomerčného softwaru Nagios, poskytujúci monitoring siete. Avšak problém bol v tom, že trvá veľmi dlho, kým sa doplnia všetky zariadenia na sieti a vytvorí sa zoznam.

Vyhral komerčný software **What's Up, verzia Gold**. Ďalšou výhodou je jednoduchá inštalácia tohto programu, podpora koncového užívateľa. Tento produkt bol potrebný, na monitorovanie serverov, smerovačov, prepínačov, priepustnosti na sieti, záťaže a keby sa naskytol nejaký problém.

Ochranu proti škodlivému kódu, zabezpečuje software **Symantec Endpoint verzia 11**. Pred tým sa naskytol problém, pretože verzia bola staršia, takže niektoré nové funkcie neboli obsiahnuté v staršej verzii. Z dôvodu podpory nových funkcií sa nainštalovala nová verzia 11. Na serveri, sa poskytuje podpora pre klientské počítače. Databáza škodlivého softwaru si sťahuje automaticky z internetu.

Dôležitým prvkom v oblasti bezpečnosti, je mať zapnutú podporu **automatických aktualizácií**. V opačnom prípade sa zvyšuje riziko, že dané servre sa môžu stať obeťami útokov. Je viac než doporučené, mať tieto aktualizácie zapnuté. Z hľadiska bezpečnosti, sa prekontrolovala podpora automatických aktualizácii, či je všade zapnutá.

Ďalším prvkom v oblasti bezpečnosti serverov, čo sa muselo dorobiť, bolo pridať **heslá do BIOSU**. Pretože po analýze tejto slabiny sa zistilo, že by to mohlo mať vážne následky. Heslá do BIOSU sa zvolili ťažké, aby bola ochrana čo najúčinnejšia. Taktiež sa vyplo bootovanie z USB a CD, aby sa nemohli robiť úpravy. V prípade potreby údržby, alebo inštalácie nového operačného systému, vie toto heslo len kompetentná osoba.

Posledným softwarom **Websense** pre server bola inštalácia. Tento software pracuje na báze **filtrácie webového obsahu**, čo sa nachádza vo web stránke. Ak klient pošle požiadavku pre server na nejakú zakázanú stránku, server skontroluje obsah, vyhodnotí tento obsah za nežiaduci a pošle klientovi upozornenie, že bol odopretý prístup. Pretože obsahoval nevhodný obsah. Táto filtrácia je zapnutá len prepínači, kde je kancelárska sieť.

5.4 Zabezpečenie dát pomocou softwaru

Po dôkladnej analýze softwaru, padlo rozhodnutie zosynchronizovať verzie operačných systémov Windows XP na service pack 3 z dôvodu bezpečnosti, pretože je to najnovšia verzia Windows XP. Obsahuje už záplaty, ktoré neboli obsiahnuté v nižších verziách. Potencionálny útočník, by tak mal šancu zaútočiť pomocou exploitov a narobil by značné škody v systéme. Najhoršia varianta je odcudzenie citlivých dát.

Po zosynchronizovaní operačných systémov, nastala fáza zapnutia automatických aktualizácií, lebo nie každý počítač mal zapnutú túto funkciu. Aktivovaním automatických aktualizácií, sa zabezpečí dostupnosť najnovších aktualizácií, ktoré prinášajú záplaty na diery. Pozor, pri bezpečnosti nepomôže mať aktualizovaný len operačný systém, ale je viac než vhodné aktualizovať aj software nainštalovaný na počítačoch.

Po aktualizácii OS, nastala fáza ochrany počítačov. Preinštalovali sa počítače, obsahujúce staršiu verziu programu Symantec End point 7 na novú verziu Symantec End point 11. Po reinštalácii ochranného produktu pre spoločnosť, sa nastavila automatická aktualizácia databázy škodlivého softwaru. Databázy sú uložené na lokálnom serveri, pre lepšiu dostupnosť.

S ďalším bezpečnostným riešením po konzultácii s firmou sa nahodil software Websense na server, pre filtrovanie užívateľského obsahu. Tento software pre koncových užívateľov, blokuje nami nastavené stránky v zozname, ktorý sa určil. Zakázané je pozerať porno, sex, chat, terorizmus a freemailové služby.

Po zvážení ďalších bezpečnostných opatrení, po konzultácii s firmou padlo rozhodnutie vybrať **šifrovací program**, ktorý by zabezpečil solídne šifrovanie citlivých firemných dát a podporoval aj steganografiu (viď kapitolu 2.8). Po dlhšej úvahe a konzultácii, v čase hospodárskej krízy kde sa šetria náklady, bola požiadavka na nekomerčný, alebo open-sourcový program. Rozhodnutie padlo na program **TrueCrypt**. Tento program je open-source, čo znamená že je nekomerčný, podporuje všetky operačné systémy, Windows 7/Vista/XP, Mac OS X, a Linux. Podpora FAT, NTFS, EXT3,EXT4,atď. **Jeho hlavné funkcie sú:** Vytvára virtuálny šifrovací disk a zavádza sa ako reálny disk. Kryptuje celú partíciu, alebo úložné zariadenie ako USB flash disk, alebo hardisk. Šifruje partíciu alebo disk, kde je operačný systém nainštalovaný, šifruje aj boot sektor. Šifrovanie je automatické, v reálnom čase za behu a je transparentný. Šifrovanie môže byť hardwarovo-akcelerované na moderných procesoroch. Poskytuje ukrývanie diskov pomocou steganografie a ukrývanie operačného systému. Podporuje tieto šifrovacie algoritmy: AES-256, Blowfish (448-bit key), CAST5, Serpent, Triple DES a Twofish. AES **šifrovací algoritmus**, poskytuje utajenie informácií, až do úrovne **prísne tajné** A za najdôležitejšiu výhodu sa pokladá jazykový balíček, ktorý tento program poskytuje. Čeština, slovenština, atď. Podľa štatistík z web stránky www.truecrypt.org/statistics ku dňu 10.4.2011 bolo stiahnutých 18,334,946 kópií tohoto softwaru.

Nie na každom počítači bude využívaný tento program. Bude využívaný pre šéfa spoločnosti, managerov a neskôr sa uvidí. Implementácia tohto programu. Nie je zložitá.

Návod na vytvorenie šifrovaného zväzku je zobrazený pomocou diagramu, ktorý sa nachádza vzadu v prílohe III.

6 VYHODNOTENIE A OVERENIE NÁVRHU V PRAXI

Pri vytváraní tejto práce, som konzultoval mnoho hodín so spoločnosťou o zabezpečení, čo chcú zabezpečiť, ako to chcú zabezpečiť a finálny termín zabezpečenia. Strávil som mnoho hodín skúmaním, badaním, čítaním kníh, manuálov, ako čo najlepšie predísť rizikám, ktoré by mohli nastať.

Dôkladnou analýzou sa zistili nedostatky, ktoré boli v spoločnosti. Bez tejto analýzy by som nevedel, čo treba zabezpečiť. Každé jedno zabezpečenie, potrebuje dôkladný rozbor. Po analýze nastalo zabezpečovanie sietí, WiFi siete, serverov a softwaru. Implementovali sa zaujímavé riešenia. Snažil som stláčať pre spoločnosť náklady tak, že som začal kombinovať nekomerčné riešenia spolu s komerčnými. Pri softwarových riešeniach na monitorovanie siete, som implementoval software What's Up Gold, NetFlow. Použil som komerčné riešenie, ktoré je vhodné na správu nečakaných udalostí, ako je nárast dátovej priepustnosti. Nie zrovna lacný software, ale výborný na správu, monitoring a zabezpečenie dostupností zariadení. Pre lepšiu bezpečnosť siete som implementoval a nakonfiguroval, hardwarový firewall od spoločnosti Juniper, ktorý zabezpečuje príchodzie a odchodzie spojenia. Správnou konfiguráciou firewallu som zabezpečil to, že sa znížili riziká na minimum a sú povolené len potrebné služby a nie nadbytočné. Zabezpečenie serverov, som vyhodnotil ako dostatočné, iba v pár prípadoch sa vypli nadbytočné služby. Ich novou konfiguráciou, sa dosiahlo lepšej stability a taktiež sa oddialilo riziko napadnutia útočníkom. Bezpečnosť na strane sieťových prvkov som zabezpečil pridaním hesiel do vstupu systému pre konfiguráciu sieťových zariadení, šifrovanie MD5, taktiež zmena služieb Telnet na SSH pre bezpečné spojenie. Vytvoril som virtuálne siete, na ktorých som nastavil bezpečnostnú politika podľa kritérií spoločnosti. Ako problém ktorý som ešte nedoriešil, považujem prístup na prepínače, smerovače pomocou ACL zoznamu, kde sa môžu prihlásiť oprávnené osoby, ktoré budú neskôr pracovať s citlivými údajmi. Spoločnosť musí doriešiť problém so vstupom do serverovne, kde majú prístup osoby s kľúčom a ten sa ľahko môže skopírovať, nevýhoda je to, že keď sa tam niečo stane, nikto nebude presne vedieť kedy, kde sa dotyčný človek nachádzal. Doporučujem prístupový systém, ktorý umožní zaznamenávať dáta s kariet osôb, kto, kde, kedy bol.

Pre zabezpečenie počítačov v spoločnosti som implementoval komerčný produkt End point od spoločnosti Symantec. Nevýhodou bolo vynaloženie finančných nákladov, na aktualizovanie verzie z nižšej, na vyššiu. Bezplatné riešenie bezpečnostných opatrení pre

osobné počítače som nedoporučoval, kvôli koncovej podpore pre užívateľov a dostupnosti služieb. Pri komerčných riešeniach existuje podpora. Nezabudol som zapnúť automatické aktualizovanie na všetkých počítačoch, serveroch, taktiež všetkých programov, pretože hrozí zneužitie bezpečnostnej slabiny. Zabezpečenie osobných dát, pre pár osobných počítačov, som urobil prostredníctvom nekomerčného softwaru TrueCrypt, ktorý umožňuje šifrovanie citlivých dát a tak posúva zabezpečenie na vyššiu úroveň, až do prísne tajných informácií podľa druhu šifry, ktorá je použitá v programe. Návod sa nachádza v diplomovej práci v prílohe číslo tri.

Podporu pre WiFi som implementoval a nakonfiguroval pomocou open-source programu FreeRadius server, ktorý je taktiež nasadený na fakulte aplikovanej informatiky v Zlíne. Jeho výhodou je to, že ide o bezplatné riešenie a z cela potlačuje riziko napadnutia, alebo odchytenie hesla prostredníctvom bezdrôtovej siete.

Samozrejme po vzájomných konzultáciách so spoločnosťou sa dospelo k stavu, kde každý bol spokojný. Všetky bezpečnostné riešenia uvádzané v práci, boli implementované. Zvýšila sa tak celková bezpečnosť pre spoločnosť. Za negatívum považujem nedostatok času na realizáciu týchto bezpečnostných opatrení. Na budúcom zabezpečení by sa mala podieľať len osoba, ktorá bola, bude oboznámená so systémom spoločnosti, pretože v prípade nových zmien, treba aplikovať nové bezpečnostné opatrenia.

ZÁVER

Čoraz častejšie počujeme slovo bezpečnosť. V dnešnej modernej dobe všade potrebujeme bezpečnosť, v tomto prípade bezpečnosť v kyberpriestore. Cieľom v tejto práci bolo ukázať široké spektrum rizík, možností ochrany na zabezpečenie systému, analýza systému v praxi a vhodná implementácia bezpečnostných opatrení na minimalizáciu rizík. Nie je možné dosiahnuť 100% ochranu v kyberpriestore, dajú sa však riziká potlačiť a znížiť. Aj najlepší experti na počítačovú bezpečnosť sú omylní, pretože vytvorili nejaký systém, ktorý bude mať chyby.

Dáta sú najcennejším artiklom v spoločnosti, tak som nemohol podceňovať riziká. Za hlavné body, považujem neustále inovovať programy, firmware sieťových zariadení, neustále monitorovanie aktivít v internete. Ale ta najdôležitejšia časť je samotný užívateľ! Ten môže priamo, alebo nepriamo ovplyvniť celkovú bezpečnosť systému. Mal by sa správať zodpovedne, voči svojmu okoliu a neohrozovať tak ostatných. Zaviedol by som školenia na bezpečnosť v informačných technológiách, alebo zúžil by som poskytovanie služieb na minimum.

V predloženej práci som splnil všetky body podľa zadania. Po konzultáciách so spoločnosťou som implementoval všetky bezpečnostné opatrenia vedúce k ochrane. Taktiež táto práca poslúži na študijné účely, pre ľudí ktorí sa chcú niečo nové naučiť a tak si rozšíriť obzor. Ako výhody som získal, nevyhnutnú prax s modernými technológiami, prehľad o celkovej bezpečnosti v kyberpriestore.

Môj osobný prínos v tejto práci vidím v tom, že som urobil pre spoločnosť celkový audit bezpečnosti. Snažil som sa poukázať na existujúce potencionálne riziká. Zabezpečil som sieťové prvky, WiFi sieť, servere a zabezpečil dáta pomocou softwaru. Pre spoločnosť som bol vhodným kandidátom, pre vybudovanie bezpečnostných opatrení a tak som spoločnosti ušetril náklady.

Za nevýhody, som považoval málo času na implementáciu bezpečnostných opatrení. Vždy, je čo zlepšovať. Z bezpečnostného hľadiska som nemohol poskytnúť všetky informácie o spoločnosti, ako meno a detaily, pretože ma viaže zmluva o mlčanlivosti.

CONCLUSION

Increasingly, we are hearing the word security. In the modern era, we need security everywhere, in this case, security in cyberspace. The objective in this work was to show a wide range of risk protection options to ensure the system analysis of the system in practice and appropriate implementation of safety measures to minimize risks. It is impossible to achieve 100% protection in cyberspace, although it is feasible to suppress and reduce risks. Even the best computer security experts are fallible, because they created a system that will have errors.

Data are most valuable item in the company, so I can not underestimate the risks. For the main points, I think constantly innovate programs, firmware, network equipment, constantly monitoring activities on the Internet. But the most important part is the actual user! This may directly or indirectly affect a total security system. It can be the responsibility, to their surroundings and not to jeopardize the other. I introduced training for security in information technology, narrowed or would like to provide services to a minimum.

In the present work I have fulfilled all the points what have been specified. After consulting with the company, I have implemented all security measures to protect the lead. Also, this work will be for educational purposes, for people who want to learn something new and to spread new horizons. As the benefits I have received, the necessary experience with advanced technologies, an overview of the overall security in cyberspace.

My personal contribution to this work, I know that I made for the company overall safety audit. I tried to highlight the existing potential risks. I ensured network elements, WiFi networks, servers and secure data using the software. For the company I was a good candidate for building security measures and so I saved a costs for them.

For drawbacks, I didn't find enought time to implement security measures. Always is an option for improvement. From a security point of view I could not provide any information about the company, as the name and details because I am bound by confidentiality agreement.

ZOZNAM POUŽITEJ LITERATÚRY

[1] JIROVSKÝ, Václav. *Kybernetická kriminalita : nejen o hackingu, crackingu, virech a troských koní bez tajemství.* První vydaní. Praha : Grada, 2007. 288 s s. ISBN 978-80-247-1561-2.

[2] MITRA, Ananda. Digital Security : *Cyber Terror and Cyber Security*. 1st edition. New Jersey : Wiley & Sons, 2005. 416 s. ISBN 978-0-8160-6791-6.

[3] *Cyberwar : The threat from the internet* [online]. [cit. 2011-04-27]. Dostupné z WWW: <http://www.economist.com/node/16481504>.

[4] *Computer Security: A Practical Definition* [online]. [cit. 2011-04-27]. Dostupné z WWW: <http://www.albion.com/security/intro-4.html>.

[5] PUŽMOVÁ, Rita. *Moderní komunikační sítě od A do Z.* Brno: Computer Press, 2006. 432 s. ISBN 80-251-1278-0.

[6] HASSELL, Jonnatan. *Radius*. 1st Edition. Sebastopol: O'Reilly, 2002. 190 s. ISBN 0596003226.

[7] STAMP, Mark. *Cyber Terror and Cyber Security*. 1st edition. New Jersey: Wiley & Sons, 2005. 416 s. ISBN 0471738484.

[8] LOVEČEK, Tomáš. *Bezpečnostná IT politika ako jeden zo základných dokumentov organizácie*. [online]. [cit. 2011-04-28]. Dostupné z WWW: <http://www.securityrevue.com/article/2006/04/bezpecnostna-it-politika-ako-jeden-zo-zakladnych-dokumentov-organizacie/>.

[9] *Šesť z desiatich počítačov je vystavených riziku zneužitia alebo straty dát* [online] [cit. 2011-05-01]. Dostupné z WWW: <http://www.eset.cz/cz/o-nas/pro-novinare/tiskove-zpravy/article/spolocnost-sest-z-desiatich-pocitacov-je-podla-harris-interactive-vystavenych-internetovym-hrozbam/>.

[10] LAYTON, P.Timothy. *Information Security: Design, Implementation, Measurement, and Compliance*. 1st edition. New York: Auerbach, 2006. 167s. ISBN 0849312701.

[11] *Prieskum: 9 z 10 Wi-Fi sietí v Prahe a Brne je slabo zabezpečených* [online]. [cit. 2011-05-01]. Dostupné z WWW: <http://pocitace.sme.sk/c/2650057/prieskum-9-z-10-wi-fi-sieti-v-prahe-a-brne-je-slabo-zabezpecenych.html>.

[12] BAYUK, Jeniffer. *Understanding information security investigations*. 1st edition. New York: Springer, 2010. 167s. ISBN 978-1-60761-771-6.

ZOZNAM POUŽITÝCH SYMBOLOV A SKRATIEK

CSMA	Carrier Sense Multiple Access
DMZ	Demilitarized Zone
DNS	Význam třetí zkratky.
FTP	File Transfer Protocol
GNU/GPL	General Public License
HTTP	Hyper Text Transfer Protocol
IDF	Intermediate Distribution Frame
IDS	Intrusion Detection System
IIS	Internet Information Services
IP	Internet Protocol
IPS	Intrusion Prevention System
MAC	Media Access Control
MDF	Main Distribution Frame
OS	Operating System
OSI	Open Systems Interconnection
SSH	Secure Shell
SSID	Service Set Identifier
TCP	Transmission Control Protocol
VoIP	Voice over Internet Protocol
WEP	Wireless Encryption Protocol
WPA	Wifi Protect Access

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

PRÍLOHA P I: KONFIGURÁCIA SIEŤOVÝCH PRVKOV

Konfigurácia kancelárskeho core prepínača:

Kancelarsky_Core_A #sh run

Building configuration...

Current configuration : 8835 bytes

hostname Kancelarsky_Core_A

enable secret 5 1AaSi$3Ddd2HcgJPHnYiGd8jHTx/

username admin privilege 15 password ***

no **aaa** new-model

vtp domain spolocnost

vtp mode transparent

power redundancy-mode redundant

spanning-tree mode pvst

spanning-tree extend system-id

spanning-tree vlan 2-15 priority 24576

vlan internal allocation policy ascending

vlan 2-15

interface GigabitEthernet3/11

description OA-Proxy

switchport access vlan 15

switchport mode access

interface GigabitEthernet3/12

description Websense-Mirror-Sensor

switchport access vlan 15

switchport mode access

interface GigabitEthernet3/13

description OA-Websense

switchport access vlan 15

switchport mode access

interface Vlan15

ip address 192.168.5.252 255.255.255.0

ip helper-address 192.168.1.1

ip helper-address 192.168.1.2

standby 5 ip 192.168.5.254

standby 5 preempt

monitor session 1 source interface Gi3/11

monitor session 1 filter packet-type good rx

monitor session 1 destination interface Gi3/12

Konfigurácia edge prepínača:

IDF-11#show run

Building configuration...

service password-encryption

hostname IDF-11

enable secret 5 1hi/C$4RNMHiPeliZ138WJw9Z4B.

username admin privilege 15 password 7 0005170B0D55

no **aaa** new-model

system mtu routing 1500

vtp domain spolocnost

vtp mode transparent

ip subnet-zero

spanning-tree mode pvst

spanning-tree extend system-id

vlan internal allocation policy ascending

vlan 1,15

interface FastEthernet0/1

 switchport access vlan 11

 switchport mode access

 spanning-tree portfast

.

.

.

interface FastEthernet0/24

switchport access vlan 11

switchport mode access

spanning-tree portfast

interface GigabitEthernet0/1

```
 switchport mode trunk
switchport nonegotiate

interface GigabitEthernet0/2
 switchport mode trunk
 switchport nonegotiate

interface Vlan1
 no ip address
 no ip route-cache
 shutdown

interface Vlan11
 ip address 192.168.15.1 255.255.255.0
 no ip route-cache

ip http server
ip http secure-server

control-plane

line con 0
 login local
 line vty 0 4
 login local
```

```
line vty 5 15
 login local
!
end
```

Konfigurácia Firewallu:

```
ssg20-> get config
Total Config size 4307:
unset key protection enable
set clock timezone 0
set vrouter trust-vr sharable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
unset auto-route-export
exit
set alg appleichat enable
unset alg appleichat re-assembly enable
set alg sctp enable
set auth-server "Local" id 0
set auth-server "Local" server-name "Local"
set auth default auth server "Local"
set auth radius accounting port 1646
set admin name "admin"
```

```
set admin password "nKv3LvrdAVtOcE5EcsGIpYBtniNbUn"
set admin auth web timeout 10
set admin auth dial-in timeout 3
set admin auth server "Local"
set admin format dos
set zone "Trust" vrouter "trust-vr"
set zone "Untrust" vrouter "trust-vr"
set zone "DMZ" vrouter "trust-vr"
set zone "VLAN" vrouter "trust-vr"
set zone "Untrust-Tun" vrouter "trust-vr"
set zone "Trust" tcp-rst
unset zone "Untrust" block
unset zone "Untrust" tcp-rst
set zone "MGT" block
unset zone "V1-Trust" tcp-rst
unset zone "V1-Untrust" tcp-rst
set zone "DMZ" tcp-rst
unset zone "V1-DMZ" tcp-rst
unset zone "VLAN" tcp-rst
set zone "Untrust" screen tear-drop
set zone "Untrust" screen syn-flood
set zone "Untrust" screen ping-death
set zone "Untrust" screen ip-filter-src
set zone "Untrust" screen land
set zone "V1-Untrust" screen tear-drop
```

```
set zone "V1-Untrust" screen syn-flood
set zone "V1-Untrust" screen ping-death
set zone "V1-Untrust" screen ip-filter-src
set zone "V1-Untrust" screen land
set interface "ethernet0/0" zone "DMZ"
set interface "ethernet0/1" zone "Untrust"
set interface "bgroup0" zone "Trust"
set interface bgroup0 port ethernet0/2
set interface bgroup0 port ethernet0/3
set interface bgroup0 port ethernet0/4
unset interface vlan1 ip
set interface ethernet0/0 ip 111.11.22.254/24
set interface ethernet0/0 route
set interface ethernet0/1 ip 192.168.1.1/22
set interface ethernet0/1 route
set interface bgroup0 ip 192.168.1.2/29
set interface bgroup0 nat
unset interface vlan1 bypass-others-ipsec
unset interface vlan1 bypass-non-ip
set interface ethernet0/0 ip manageable
set interface ethernet0/1 ip manageable
set interface bgroup0 ip manageable
set interface ethernet0/1 manage ping
set interface ethernet0/1 manage ssh
--- more ---              set interface ethernet0/1 manage telnet
```

```
set interface ethernet0/1 manage ssl
set interface ethernet0/1 manage web
set interface bgroup0 manage mtrace
set interface "serial0/0" modem settings "USR" init "AT&F"
set interface "serial0/0" modem settings "USR" active
set interface "serial0/0" modem speed 115200
set interface "serial0/0" modem retry 3
set interface "serial0/0" modem interval 10
set interface "serial0/0" modem idle-time 10
set flow tcp-mss
unset flow tcp-syn-check
unset flow tcp-syn-bit-check
set flow reverse-route clear-text prefer
set flow reverse-route tunnel always
set pki authority default scep mode "auto"
set pki x509 default cert-path partial
set crypto-policy
exit
set ike respond-bad-spi 1
set ike ikev2 ike-sa-soft-lifetime 60
unset ike ikeid-enumeration
--- more ---              unset ike dos-protection
unset ipsec access-session enable
set ipsec access-session maximum 5000
set ipsec access-session upper-threshold 0
```

```
set ipsec access-session lower-threshold 0
set ipsec access-session dead-p2-sa-timeout 0
unset ipsec access-session log-error
unset ipsec access-session info-exch-connected
unset ipsec access-session use-error-log
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
set vpn-group id 1
set url protocol websense
exit
set policy id 1 from "Trust" to "Untrust"  "Any" "Any" "ANY" nat src permit log
set policy id 1
exit
set firewall log-self
set nsmgmt bulkcli reboot-timeout 60
set ssh version v2
set ssh enable
set config lock timeout 5
unset license-key auto-update
set telnet client enable
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
```

```
unset add-default-route
set route 0.0.0.0/0 interface ethernet0/1 gateway 192.168.0.207
exit
set vrouter "untrust-vr"
exit
set vrouter "trust-vr"
exit
```

PRÍLOHA P II: KONFIGURÁCIA RADIUS SERVERA

Konfigurácia Radius servera:

----------EAP-TLS (wifi-wpa) (konfiguracia a install)

/var/run/ - beziace sluzby

radiusd.conf - hlavny configuracny subor

client - zoznam preposielacov- ap, switch (prostrednikov)

users - zoznam klientov - priamo pc, notebooky

----------freeradius -X

odmietnutie nedefinovaneho klienta - ap (def-radiusd,non-client,non-user)

Ignoring request to authentication address * port 1812 from unknown client 10.1.1.3 port 2049

Ready to process requests.

_____

_____

(instalacia kompilacie)

wget balik

tar -xvf freeradius-server-2.1.7.tar.gz -C /tmp/

apt-get install build-essential (kompilacia-nutne)

apt-get install libssl-dev (ssl kniznice-nutne)

cd /tmp/freeradius

./configure (--prefix=/usr/local/freeradius)

make

make install

(chybajuca kniznica - tak link "ln -s /usr/local/lib/libltdl.so.3 /usr/local/freeradius/1/lib/libltdl.so.3")

-test funkcie - spustenie ./sbin/radiusd -X

_____

_____

---------- Úprava skriptu pred generovaním certifikátu

********** Keygen

apt-get install bind9utils (obsahuje DNSSEC-keygen-nutný pre skripty CA, gen.náhodnych čísiel)

DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y

********** Generovaním certifikátu

------ CA. Root

-Upraviť skript CA-root.sh

Openssl = openssl (skusit spustiť "openssl")

CAPL = / usr / lib / ssl / misc / CA.pl (najst "find-name CA.pl")

KEYGEN = / DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y (najst Alebo neinštalovať "apt-get install bind9utils", "find-name * keygen")

-Generované CA.root

/ Root / CA-root.sh [password] (nejake heslo (pre zasifrovanie certifikačnú) v mojom prípade "rootpass")

(Potom sa to opytat ---- nemusi sa to vyplňovať - common name = leave this field blank)

("/ Root / CA-root.sh rootpass")

= Vysledkom je koreňový certifikát (certifikačná autorita) podpísaný sám sebou

------ CA. Server

-Upraviť skript CA-server.sh

KEYGEN = DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y

-Vytvoriť súbor pre rozšírenie xpextensions

nano / root / xpextensions (v skripte zameniť za extfile)

[Xpclient_ext]

extendedKeyUsage = 1.3.6.1.5.5.7.3.2

[Xpserver_ext]

extendedKeyUsage = 1.3.6.1.5.5.7.3.1

-Generovaný CA.server

/ Root / CA-server.sh server-name [password [root-password]]

(Server-name = nazov servera (zistíte prikaz "hostname"), password = nejaké ďalšie heslo pre tento certifikat (dáme "serverpass"), root-password = predchodzie heslo

root.certifikatov ("rootpass")

/ Root / CA-server.sh bfree serverpass rootpass

(Potom sa to opýta -môžeme vyplniť ale common name = fully-qualified domain-name of the RADIUS server)

(Ak to vyhodí chybu:. / DemoCA / serial: No such file or directory,,, atď, tak urobiť file serial "echo 00> / root / demoCA / serial" potom to pôjde)

= Výsledkom je certifikát servera podpísaný koreňovým certifikátom

------ CA. Client

-Upraviť skript CA-server.sh

KEYGEN = DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y

-Generované CA.client

/ Root / CA-client.sh client-name [password [root-password]]

(Client name - hostname klienta (názov počítača alebo doménové meno) password - heslo pre klientský certifikát (dáme "clientpass") root-password

- Heslo z CA.root ("rootpass"))

/ Root / CA-client.sh ntb-bron clientpass rootpass

(Na niečo sa opýta, common-name = meno pc klienta)

= Výsledkom je certifikát počítača, klienta, procedúru vykonávame toľkokrát, koľko máme klientov (užívateľov)

********** Inštalácia windows certifikátov

- Skopírovať xyz certifkátov, vygenerovaných z cert servera a nainštalovať ich

der / root.der (do dôveryhodných koreňových autorít)

p12/client-name.p12 (automaticky sa nakopíruje do osobných cert, zadáva sa heslo na rozšifrovanie, zadanej počas generovania (clientpass))

********** Server, úložisko certifikátov

(V podstate - Vytvorenie zložky, prekopírovanie certifikátu a zabezpečenie zmeny prístupových práv pricom radiusd je uzivatel, pod ním beží služba rádiusu)

"Mkdir / etc / wireless-auth"

"Cp pom / root.pem pom / server-name.pem / etc / wireless-auth"

Nepoužíva # "chown root: radiusd / etc / wireless-auth / *. pem"

Nepoužíva # "chmod 0640 / etc / wireless-auth / *. pem"

********** Server certifikáty pre freerad eap.conf

DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y> / etc / wifiauth / DH

DNSSEC-keygen-r / dev / urandom-a HMAC-MD5-b 128-n HOST HW_co45y> / etc / wifiauth / random

chown root: radiusd / etc / wifiauth / DH / etc / wifiauth / random

chmod 0640 / etc / wifiauth / DH / etc / wifiauth / random

********** Nastaviť EAP modul s certifikátmi

"Nano eap.conf"

MODULE CONFIGURATION

modules {

  # This is an EAP-based operation.

  EAP {

    default_eap_type = tls

    timer_expire = 60

    tls {

      private_key_password = "serverpass"

      private_key_file = / etc / wireless-auth / server-name.pem

      certificate_file = / etc / wireless-auth / server-name.pem

CA_file = / etc / wireless-auth / root.pem

dh_file = / etc / wireless-auth / DH

random_file = / etc / wireless-auth / random

fragment_size = 1024

include_length = yes

}

}

********** Pridať AP klientov

"Nano clients.conf"

client 192.168.11.33 {

secret = secret

shortname = linksys-test

nastype = other

}

********** Pridať typ užívateľov a ich autentifikáciu

"Nano users"

"Client-name" Auth-Type: = EAP

This is important: it makes RADIUS Reject users not found above

DEFAULT Auth-Type: = Reject

Reply-Message = "(Colourful note of Rejection)"

****

| Rootpass | root - pass

| Serverpass | sysadmin - pass

| Clientpass | "x" - pass

========== Revokácia certifikátu - kontrola revokovaných certifikátov

==========

==========

==========

--------- Revokácia certifikatov openssl

openssl ca-config openssl.horpol.cnf-REVOKE certs/client-1.crt

Revokácia

openssl ca-config openssl.horpol.cnf-gencrl-out crl / horpol-crl.pem

Vytvorenie crl listu - zoznam všetkých zrušených certifikátov

Pre ďalšie odvolanie stačí revokovať ďalší klientský certifikát a vyexportovať opät crl

-> Novšie crl obsahuje všetky (aj tie predchodzie) odvolanie na certifikáty

Pozor -----!!!! crl.pem!!! --- Koncovka a format PEM, inak to nefunguje (neprelinkuje sa c_rehash)

(Openssl crl-in crl / horpol-crl.pem-text)

Info - vypíše čitateľne CRL

--------- Príprava adresárov a súborov

mkdir / usr / local / freeradius / etc / raddb / certs / crl

Adresár pre crl - bude obsahovať CA certifikat a CRL list

cp crl / horpol-crl.pem / usr / local / freeradius / etc / raddb / certs / crl

Kopírovanie CRL listu

cp / usr / local / freeradius / etc / raddb / certs / bb / horpol-CA.crt / usr / local / freeradius / etc / raddb / certs / crl

Kopírovanie CA certifikatu

c_rehash / usr / local / freeradius / etc / raddb / certs / crl

Vykoná rehash certifikátov (Vytvoria sa hashe v podobe linku, k certifikátom)

(Resp - hash.0 (ca hash) a hash.r0 (hash CRL) - id hash je pre CA a CRL rovnako)

chmown root.root / usr / local / freeradius / etc / raddb / certs / crl / *

chmod 400 / usr / local / freeradius / etc / raddb / certs / crl / *

Bezpečnosť, na súbory by mal siahať len používateľ, pod ktorým beží freeradius

Konfigurácia freeradius

nano / usr / local / freeradius / etc / raddb / eap.conf

```
modules {
   # This is an EAP-based operation.
   EAP {
      default_eap_type = tls
      timer_expire = 60
```

```
        tls {
            private_key_password = "serverpass"
            ....
check_crl = yes
        CA_path = $ {cadir} / crl /
        }
    }
```

Pridať (alebo odkomentovať) parametre - check_crl = yes a CA_path = $ {cadir} / crl /

(Cesta kde je CA a CRL - / usr / local / freeradius / etc / raddb / certs / crl)

----> A malo by to ísť.

- Pri odvolaní ďalšieho cert (revokácia pomôže openssl) stačí potom len vygenerovať nový CRL súbor (openssl) a

nahradiť existujúce a vykonať c_rehash

-> Kontrola funkcie:

/ usr / local / freeradius / sbin / radiusd-X

Vygenerovaný certifikát CA-Server:

```
#!/bin/sh

OPENSSL=openssl
KEYGEN=usr/sbin/dnssec-keygen
PASSDIR=pass
DERDIR=der
```

```
P12DIR=p12
PEMDIR=pem
VALIDFOR=365

SNAME=$1
PASSWD=$2
ROOTPASSWD=$3

mkdir -p $PEMDIR $P12DIR $DERDIR $PASSDIR

if [ -z "${SNAME}" ]; then
        echo "WARNING: server name not specified. Using \"server\"."
        SNAME=server
fi

if [ -z "${PASSWD}" ]; then
        echo "No password specified, trying $PASSDIR/$SNAME.pass."
        if [ -a $PASSDIR/$SNAME.pass ]; then
                PASSWD=`cat $PASSDIR/$SNAME.pass`
        else
                echo "Not found. Generating password, see $PASSDIR/$SNAME.pass for contents."
                PASSWD=`$KEYGEN | head -c 32`
                cat /dev/null > $PASSDIR/$SNAME.pass
                echo $PASSWD >> $PASSDIR/$SNAME.pass
        fi
```

```
fi


if [ -z "${ROOTPASSWD}" ]; then
        echo "No root password specified, trying $PASSDIR/root.pass."
        if [ -a $PASSDIR/root.pass ]; then
                ROOTPASSWD=`cat $PASSDIR/root.pass`
        else
                echo "FATAL: No root certification password."
                exit
        fi
fi


$OPENSSL req -new -keyout $PEMDIR/newreq.pem -out $PEMDIR/newreq.pem -passin
\
   pass:$PASSWD -passout pass:$PASSWD
$OPENSSL ca -policy policy_anything -out $PEMDIR/newcert.pem -key
$ROOTPASSWD \
   -extensions xpserver_ext -extfile xpextensions -days $VALIDFOR -infiles
$PEMDIR/newreq.pem
$OPENSSL pkcs12 -export -in $PEMDIR/newcert.pem -inkey $PEMDIR/newreq.pem -
out \
   $P12DIR/$1.p12 -clcerts -passin pass:$PASSWD -passout pass:$PASSWD
$OPENSSL pkcs12 -in $P12DIR/$SNAME.p12 -out $PEMDIR/$SNAME.pem -passin \
   pass:$PASSWD -passout pass:$PASSWD
$OPENSSL x509 -inform PEM -outform DER -in $PEMDIR/$SNAME.pem -out
$DERDIR/$SNAME.der
```

```
rm -rf $PEMDIR/newcert.pem $PEMDIR/newreq.pem
```

Vygenerovaný certifikát CA-Root:

```
#!/bin/sh
OPENSSL=openssl
CAPL=/usr/lib/ssl/misc/CA.pl
KEYGEN=/usr/sbin/dnssec-keygen
PASSDIR=pass
DERDIR=der
P12DIR=p12
PEMDIR=pem
VALIDFOR=365
PASSWD=$1

mkdir -p $PEMDIR $P12DIR $DERDIR $PASSDIR

if [ -z "${PASSWD}" ]; then
        echo "No root password specified, trying $PASSDIR/root.pass."
        if [ -a $PASSDIR/root.pass ]; then
                PASSWD=`cat $PASSDIR/root.pass`
        else
                echo "Not found. Generating password, see $PASSDIR/root.pass for contents."
                PASSWD=`$KEYGEN | head -c 32`
                cat /dev/null > $PASSDIR/root.pass
                echo $PASSWD >> $PASSDIR/root.pass
```

```
        fi
fi

rm -rf demoCA

$OPENSSL req -new -x509 -days $VALIDFOR -keyout $PEMDIR/newreq.pem -out \
    $PEMDIR/newreq.pem -passin pass:$PASSWD -passout pass:$PASSWD
echo "${PEMDIR}/newreq.pem" | $CAPL -newca >/dev/null
$OPENSSL pkcs12 -export -in demoCA/cacert.pem -inkey $PEMDIR/newreq.pem -out \
    $P12DIR/root.p12 -cacerts -passin pass:$PASSWD -passout pass:$PASSWD
$OPENSSL pkcs12 -in $P12DIR/root.p12 -out $PEMDIR/root.pem -passin \
    pass:$PASSWD -passout pass:$PASSWD
$OPENSSL x509 -inform PEM -outform DER -days $VALIDFOR -in $PEMDIR/root.pem
\
    -out $DERDIR/root.der -passin pass:$PASSWD

rm -rf $PEMDIR/newreq.pem
```

Vygenerovaný certifikát CA-Klient:

```
#!/bin/sh

OPENSSL=openssl
KEYGEN=/usr/sbin/dnssec-keygen
PASSDIR=pass
DERDIR=der
P12DIR=p12
PEMDIR=pem
```

```
VALIDFOR=365

CLNAME=$1
PASSWD=$2
ROOTPASSWD=$3

mkdir -p $PEMDIR $P12DIR $DERDIR $PASSDIR

if [ -z "${CLNAME}" ]; then
        echo "WARNING: client name not specified. Using \"client\"."
        CLNAME=client
fi

if [ -z "${PASSWD}" ]; then
        echo "No password specified, trying $PASSDIR/$CLNAME.pass."
        if [ -a $PASSDIR/$CLNAME.pass ]; then
                PASSWD=`cat $PASSDIR/$CLNAME.pass`
        else
                echo "Not found. Generating password, see $PASSDIR/$CLNAME.pass for contents."
                PASSWD=`$KEYGEN | head -c 16`
                cat /dev/null > $PASSDIR/$CLNAME.pass
                echo $PASSWD >> $PASSDIR/$CLNAME.pass
        fi
fi
```

```
if [ -z "${ROOTPASSWD}" ]; then
        echo "No root password specified, trying $PASSDIR/root.pass."
        if [ -a $PASSDIR/root.pass ]; then
                ROOTPASSWD=`cat $PASSDIR/root.pass`
        else
                echo "FATAL: No root certification password."
                exit
        fi
fi

$OPENSSL req -new -keyout $PEMDIR/newreq.pem -out $PEMDIR/newreq.pem -passin
\
   pass:$PASSWD -passout pass:$PASSWD
$OPENSSL ca -policy policy_anything -out $PEMDIR/newcert.pem -passin \
   pass:$PASSWD -key $ROOTPASSWD -extensions xpclient_ext -days $VALIDFOR \
   -extfile xpextensions -infiles $PEMDIR/newreq.pem
$OPENSSL pkcs12 -export -in $PEMDIR/newcert.pem -inkey $PEMDIR/newreq.pem -
out \
   $P12DIR/$CLNAME.p12 -clcerts -passin pass:$PASSWD -passout pass:$PASSWD
$OPENSSL pkcs12 -in $P12DIR/$CLNAME.p12 -out $PEMDIR/$CLNAME.pem -passin
\
   pass:$PASSWD -passout pass:$PASSWD
$OPENSSL x509 -inform PEM -outform DER -in $PEMDIR/$CLNAME.pem -out \
   $PEMDIR/$CLNAME.der

rm -rf $PEMDIR/newcert.pem $PEMDIR/newreq.pem
```

PRÍLOHA P III: DIAGRAM PROGRAMU TRUECRYPT