Řízení informační bezpečnosti a bezpečnosti dat ve firemní síti.

Informative data safety control in the company network

Bc. Pavel Kučera

Diplomová práce
2009

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
Ústav aplikované informatiky
akademický rok: 2008/2009

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Pavel KUČERA**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Informační technologie**
Téma práce:	**Řízení informační bezpečnosti a bezpečnosti dat ve firemní síti - Pavel Kučera**

Zásady pro vypracování:

1. **Proveďte analýzu informačních zdrojů a literární rešerší na téma řízení informační bezpečnosti**
2. **Popište principy síťové komunikace a nástroje pro jejich zabezpečení.**
3. **Definujte cíle práce a navrhněte teoretická řešení.**
4. **Formou projektu realizujte uvedené cíle.**
5. **Kriticky vyhodnoťte výsledky práce a konfrontujte je s bodem 3.**

Rozsah práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LEE, Barken. Jak zabezpečit bezdrátovou síť Wi-Fi. Jiří Veselský. 1. vyd. [s.l.] : Computer press, 2004. 174 s. ISBN 80-251-0346-3.**
2. **NORTHCUTT, Stephen, et al. Bezpečnost počítačových sítí. [s.l.] : [s.n.], 2005. 592 s. ISBN 80-251-0697-7.**
3. **LUDVÍK, Miroslav, ŠTĚDROŇ, Bohumír. Teorie bezpečnosti počítačových sítí. 1. vyd. [s.l.] : Computer Media, 2008. 98 s. ISBN 80-86686-35-3.**
4. **THOMAS, M. Zabezpečení počítačových sítí - bez předchozích znalostí. David Krásenský. 1. vyd. [s.l.] : Computer press, [2005]. 338 s. ISBN 80-251-0417-6.**
5. **LOCKHART, Andrew. Bezpečnost sítí na maximum. Jiří Veselský. 1. vyd. [s.l.] : Computer press, [2007]. 276 s. ISBN 80-251-0805-8.**
6. **SMITH, Ben, et al. Zabezpečení systému a sítě Microsoft Windows. [s.l.] : Computer press , 2005. 700 s. ISBN 80-251-1260-8.**
7. **SIMMONS, Curt, CAUSEY, James. Mistrovství v sítích Microsoft Windows XP. [s.l.] : Computer Press, 2005. 624 s. ISBN 80-251-0583-0.**
8. **ODOM, Wendell. Počítačové sítě . [s.l.] : Computer Press, 2005. 384 s. ISBN 80-251-0538-5.**

Vedoucí diplomové práce: **doc. Mgr. Roman Jašek, Ph.D.**
Ústav aplikované informatiky

Datum zadání diplomové práce: **20. února 2009**

Termín odevzdání diplomové práce: **27. května 2009**

Ve Zlíně dne 13. února 2009

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Práce řeší problematiku systémového managementu bezpečnosti a jeho zavádění do moderní společnosti včetně implementace bezpečnostních IT technologií do firemní sítě.

Klíčová slova:

Sítě, bezdrátové sítě, zabezpečení, přístupový bod, hesla, zařízení, wifi, bezpečnost, uživatel.

ABSTRACT

This thesis solves the questions of system security management and its introduction to modern society including the implementation of security IT technologies into company net.

Keywords:

Nets, wireless nets, security, access point, passwords, facilities, wifi, safety, user.

Poděkování

Děkuji vedoucímu diplomové práce doc. Mgr. Romanovi Jaškovi, Ph.D.za velmi užitečnou pomoc a cenné rady při zpracování diplomové práce.

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.

Ve Zlíně …….

Podpis diplomata

OBSAH

ÚVOD **9**
I TEORETICKÁ ČÁST **10**
1 PASIVNÍ PRVKY POČÍTAČOVÉ SÍTĚ **11**
1.1 KABELÁŽ 11
2 AKTIVNÍ PRVKY POČÍTAČOVÉ SÍTĚ **12**
2.1 SWITCHE 12
2.2 ROUTER 12
2.3 ACCES POINT 13
II PRAKTICKÁ ČÁST **16**
3 BEZPEČNOST PRO NAVRHOVANOU SÍŤ **17**
4 WIFI A HROZBY V BEZDRÁTOVÝCH SÍTÍCH **20**
4.1 ÚTOKY 21
4.2 PIRÁTSKÉ PŘÍSTUPOVÉ BODY 22
4.3 NESPRÁVNĚ KONFIGUROVANÉ PŘÍSTUPOVÉ BODY 24
4.4 ZNEUŽÍVÁNÍ SÍTĚ 24
4.5 ZABEZPEČENÍ BEZDRÁTOVÝCH SÍTÍ 25
4.5.1 Identifikátor SSID 25
4.5.2 Připojení zařízení k přístupovému bodu 25
4.5.3 WEP (Wired Equivalent Privacy) 26
4.5.4 WPA a WPA2 28
4.5.5 WPS 29
4.5.6 Filtrování adres MAC 30
4.5.7 Protokol EAP (Extensible Authentication Protocol) 31
4.5.8 Zvýšení bezpečnosti bezdrátových sítí 34
5 SERVER **35**
6 HESLA A BEZPEČNOSTNÍ ZÁSADY **36**
6.1 DEFINICE DŮVĚRY 39
6.2 ZÁSADY PŘÍPUSTNÉHO UŽÍVÁNÍ 42
6.3 AKTIVITY V ELEKTRONICKÉ POŠTĚ A PŘI KOMUNIKACI 43
6.4 ZÁSADY PRO PRÁCI S HESLY 44
7 FIREWALL **48**
7.1 PRAVIDLA FIREWALLU 48
8 OPERAČNÍ SYSTÉMY **50**
9 VIROVÁ OCHRANA **51**
10 ZÁLOŽNÍ ZDROJ UPS **53**

11 DOSAŽENÉ CÍLE 55
ZÁVĚR 57
CONCLUSION 59
SEZNAM POUŽITÉ LITERATURY 61
SEZNAM OBRÁZKŮ 64
SEZNAM TABULEK 65

ÚVOD

Mým úkolem je navrhnout maximálně funkční, výkonnou a zabezpečenou firemní síť pomocí dostupných technologií v podniku, který se rozprostírá na území rozlohou cca 500m^2. Velký důraz jsem měl klást i na bezpečnost s ohledem na cenu a výkon sítě. A také další požadavky, jako rychlost sítě, v některých úsecích nutná neexistence kabelových rozvodů a nutné nahrazení bezdrátovými spoji, výkon serverů, zabezpečení před útoky hackerů a možné virové infiltrace, některé spoje budou současně využívat i na telekomunikační síť, rozpočet, internetové připojení, možnost bezdrátového připojení v některých částech podniku, zajištění nepřetržitého zdroje napájení. Návrh počítačové sítě je vždy individuální pro každého zájemce (firmu) a nedá se použít nějaký standardní model. Každý zájemce má svoje specifikace, které musí síť splňovat, aby byla vyhovující: rychlost, kabeláž, topologie, přístupová metoda atd.. Dalším velmi významným faktorem, který musíme zohlednit je finanční rozpočet, ze kterého vyplívá problém, že musíme hledat kompromisy mezi poměrem cena / výkon.

Klíčové požadavky na síť LAN jsou:
• spolehlivost - síť musí být neustále k dispozici a přístupná uživatelům v každém okamžiku
• škálovatelnost - tj. možnost poskytnout různé služby s různou šířkou pásma.
uvnitř sítě, detekce a eliminace virů
• redundance řídící jednotky a napájecího zdroje centrálního uzlu.
• jednotný management celé sítě

Součástí každé počítačové sítě je i přiměřená technická podpora:
• odstraňování poruch
• dálkové změny parametrů a konfigurace
• preventivní údržba
• hot-line

I. TEORETICKÁ ČÁST

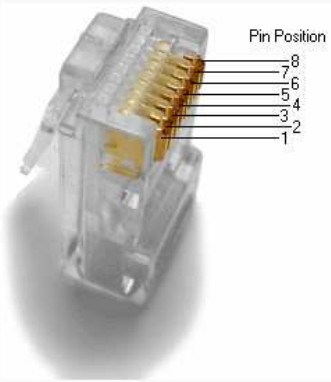
1 PASIVNÍ PRVKY POČÍTAČOVÉ SÍTĚ

Pasivní prvky jsou prvky, které nereagují na signál který přes ně prochází. (kabeláž, hub)

1.1 Kabeláž

Obvykle se používají zapojení s označeními T568A nebo T568B, která jsou definována v TIA/EIA-568-B.

Ethernet se většinou přenáší po kabelech typu „kroucená dvojlinka“ kategorie 5e nebo kabely kategorie 6, které jsou určeny pro gigabitový ethernet, ale jsou současně zpětně kompatibilní s kategoriemi 3, 5 a 5e.[10]

Pin	Křížené zapojení (varianta A)	Standardní zapojení (varianta B)	Označení pinů na konektoru	Gigabit ethernet (varianta A)	Gigabit ethernet (varianta B)
1	zeleno-bílý	oranžovo-bílý		oranžovo-bílý	zeleno-bílý
2	zelený	oranžový		oranžový	zelený
3	oranžovo-bílý	zeleno-bílý		zeleno-bílý	oranžovo-bílý
4	modrý	modrý		modrý	hnědo-bílý
5	modro-bílý	modro-bílý		modro-bílý	hnědý
6	oranžový	zelený		zelený	oranžový
7	hnědo-bílý	hnědo-bílý		hnědo-bílý	modrý
8	hnědý	hnědý		hnědý	modro-bílý

Obr. 1 - Označení pinů na konektoru a způsoby zapojení.[10]

2 AKTIVNÍ PRVKY POČÍTAČOVÉ SÍTĚ

Aktivní prvky, jako například switch, nebo router nějakým způsobem reagují na signál, který přes ně prochází. Lokální sítě se propojují pomocí aktivních prvků.

2.1 Switche

Vlastností switchů je, že analyzují procházející pakety a podle informací v nich obsažených (adres, identifikátorů apod.) rozhodují, kam paket předat dál.[11]

LAN přepínače poskytují bezkolizní spojení s datovými zařízeními (stanice, servery ,...). Přepínače můžeme rozdělit na:
• přepínače pracovních skupin (workgroup switch) - na každém portu přepínače je pouze jedno PC.
• páteřový přepínače (backbone switch) - k jedenu portu přepínače se připojí celý segment

Switch je "inteligentnější zařízení". Obsahuje vnitřní paměť, v níž si uchovává všechny síťové adresy (MAC = Media Access Control - hardwarová adresa, která jednoznačně identifikuje každé zařízení v síti) připojených počítačů. Pokud tedy switch přijme datový rámec, ví přesně, na kterém portu je připojen počítač, kterému je rámec určen a vyšle ho jen na tento port. To samozřejmě velmi zrychluje komunikaci v síti a navíc switch může pro komunikaci s připojeným počítačem využít celou šířku komunikačního pásma. Management switchů: Do managmentového prostředí se dostaneme zadáním IP adresy jednoho ze switchů a vyplněním přihlašovacích údajů. (Login, Password) do webového prohlížeče. Připojit lze také přes terminálového klienta.

2.2 Router

Směrovač (router) je síťové zařízení, které zprostředkovává přenos dat mezi dvěma nebo několika počítačovými sítěmi v procesu nazvaném směrování (anglicky routing). Směrovač propojuje počítačové sítě na úrovni vrstvy 3 modelu OSI.

Obr. 2 – OSI model [12]

Směrovač je osazen dvěma nebo více síťovými rozhraními, které mohou, ale nemusí být stejného typu. Směrovač analyzuje adresu každého datagramu, který dostane na jednom ze svých síťových rozhraní od jiného síťového zařízení a na základě stavu sítí na jiných síťových rozhraních rozhoduje, kterému dalšímu síťovým zařízením má datagram poslat, aby se dostal do bodu určení.

Směrovače navzájem komunikují a informují se o stavu sítě a směrování prostřednictvím zvláštních komunikačních protokolů.

2.3 Acces point

Bezdrátový přístupový bod (anglicky wireless access point - WAP, nebo jen access point - AP) je zařízení, které vzájemně propojuje bezdrátové síťové komunikační zařízení, čímž vytváří bezdrátovou síť. Bezdrátový přístupový bod funguje jako fyzický opakovač (repeater) nebo jako směrovač (router).

Přístupový bod se obvykle připojuje k pevné síti typu Ethernet, což umožňuje přenášet data mezi bezdrátovými a drátěnými zařízeními. Několik přístupových bodů lze navzájem propojit a vytvořit tak větší síť, která umožňuje "roaming". Naproti tomu síť, v níž se klientské zařízení komunikují přímo navzájem, bez přístupových bodů, se nazývá ad-hoc síť.

Tato zařízení poskytují způsob jak se v typických ethernetových sítích zbavit kabelů. Zatímco instalace kabeláže v kanceláři, doma nebo ve škole často vyžaduje natažení mnoha kabelů přes stěny a stropy, bezdrátové sítě umožňují kabeláž snížit nebo zcela eliminovat.

Navíc bezdrátové sítě poskytují uživatelům větší pohyblivost, čímž osvobozují jednotlivce od omezení počítačů "přikáblovaných" ke stěně.

Výhody / nevýhody bezdrátového připojení (Wi-Fi)

Výhody:

• Na rozdíl od paketových rádiových systémů, Wi-Fi využívá nelicencované rádiové pásmo a individuální uživatel nepotřebuje souhlas místních úřadů.

• Umožňuje vybudovat LAN bez kabelů, a tak snížit náklady na výstavbu či rozšiřování sítě. Bezdrátové sítě jsou výhodné v prostorách, kde nelze použít kabely - např.. ve vnějších prostorách nebo v historických budovách.

• Wi-Fi produkty jsou na trhu široce dostupné. Různé značky přístupových bodů a klientských síťových adaptérů mezi sebou spolupracují na základní úrovni.

• Konkurence mezi výrobci významně snížila ceny.

• Wi-Fi sítě podporují roaming, díky kterému se může mobilní klientská stanice (např. přenosný počítač) přesouvat od jednoho přístupového bodu k druhému bez ztráty spojení současně s pohybem uživatele v budově nebo oblasti.

• Několik přístupových bodů a síťových adaptérů podporuje různé stupně kryptování, díky čemuž je komunikace zajištěna před zachycením nechtěnou osobou.

• Wi-Fi je celosvětová skupina standardů. Na rozdíl od mobilní telefonie stejný Wi-Fi klient pracuje v různých zemích na celém světě.

Nevýhody:

• Použití Wi-Fi pásma 2.4 GHz ve většině zemí nevyžaduje licenci za předpokladu, že zůstanete pod limitem 100 mW a akceptujete rušení z jiných zdrojů včetně rušení, které způsobí odpojení vašich zařízení.

• Vysoká spotřeba v porovnání s některými jinými normami snižuje životnost baterií a způsobuje přehřívaní zařízení.

• Nejpoužívanější bezdrátový kryptovací standard Wired Equivalent Privacy (WEP) je prolomitelný, i když je správně nakonfigurován (příčinou je generování slabého klíče). Ačkoliv většina novějších bezdrátových produktů podporuje zdokonalený protokol Wi-Fi Protected Access (WPA), množství přístupových bodů první generace se nedá upgradovat v terénu a musí se vyměnit. Standard 802.11i (WPA2), který je dostupný v nejnovějších

zařízeních, dále vylepšuje bezpečnost. Oba novější protokoly vyžadují silnější hesla než používá většina uživatelů. Mnohé firmy aplikují dodatečné úrovně šifrování (např. VPN), aby se ochránilo před zachycením komunikace.

• Wi-Fi sítě mají omezený dosah. Typický domácí Wi-Fi směrovač používající 802.11b nebo 802.11g může mít dosah 45 m v budově a 90 m mimo budovy. Dosah se přitom mění, protože WiFi nemá výjimku ze zákonů šíření rádiových vln. WiFi ve frekvenčním pásmu 2.4 GHz má lepší dosah než WiFi v pásmu 5 GHz a menší dopad než nejstarší WiFi (a před-WiFi) 900 MHz pásmo.

• Vzájemné působení uzavřených (kryptování) přístupových bodů a otevřených přístupových bodů na stejném nebo sousedním kanálu může zabránit přístupu klientů v oblasti k otevřeným přístupovým bodem. To může způsobit problém v problémy oblastech jako např.. ve velkých budovách, kde několik obyvatel provozuje Wi-Fi přístupové body.

• Přístupové body se dají využít na zcizení osobních informací vysílaných Wi-Fi klienty.

• Problémy v součinnosti mezi produkty různých značek nebo odchylky od standardů mohou způsobit omezení připojitelnosti nebo nižší přenosovou rychlost.

• Bezplatné přístupové body (nebo nesprávně nakonfigurovány přístupové body) může záškodník využít na anonymní útok, který se nedá vystopovat za majitelem přístupového bodu.

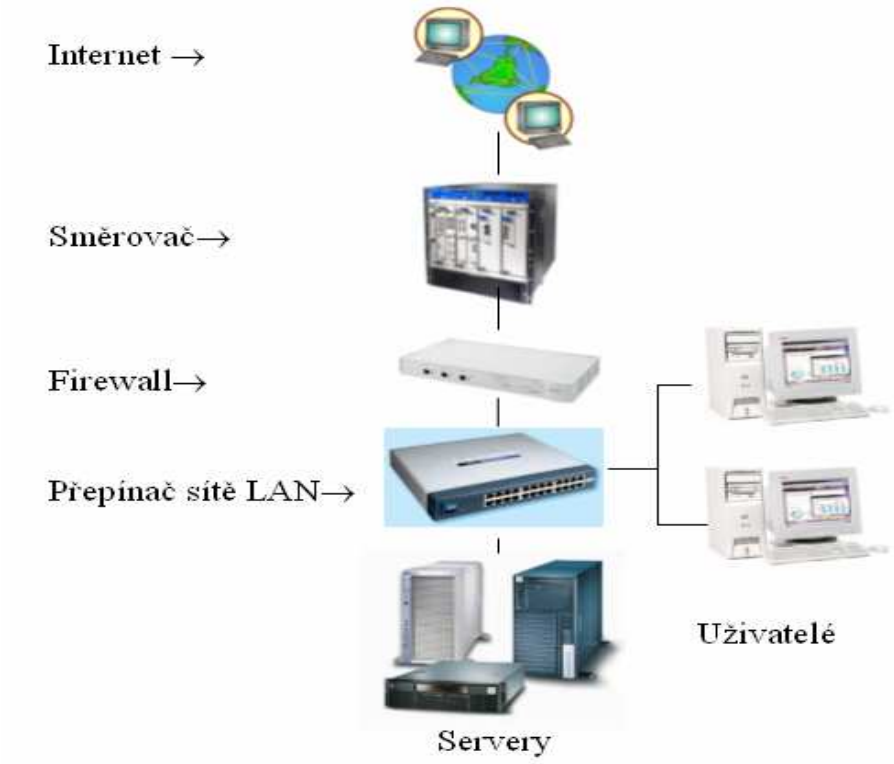
II. PRAKTICKÁ ČÁST

3 BEZPEČNOST PRO NAVRHOVANOU SÍŤ

Bezpečnost sítě má mnoho stránek a různých úhlů pohledu; záleží vždy na tom, jakým potenciálním útokům a hrozbám je síť vystavena. Také různých zdrojů informací i názorů existuje přímo neskutečné množství - a každý nám může dát jinou odpověď. Tím chci říci, že odborníci v jednotlivých podoborech návrhu sítí toho o síťové bezpečnosti napsali tolik, že nemá smysl se pokusit o nějaké zhodnocení úplně všech dostupných informací.

Důležité pojmy v zabezpečení sítí jsou:

- Vrstvená bezpečnost. Jen jedno obranné místo proti útoku nestačí. Za dobře navrženou můžeme považovat jen takovou síť, jejíž zabezpečení je implementováno konzistentně ve všech částech. Princip vrstvené bezpečnosti sítě je tou nejdůležitější myšlenkou při zabezpečování sítí.



Obr.3 - Vrstvené zabezpečení sítě –
V každé z vrstev je implementováno zabezpečení.

- Řízení přístupu. Za provoz sítě jsme v roli správce zodpovědní my sami, a proto také musíme určit, kdo bude mít povolen přístup do sítě. Jedním z nejdůležitějších doporučovaných postupů je, vycházet při veškerých rozhodnutích o přístupu ze zásady: „všechno zablokovat, a potom výslovně povolit jen to, co tento člověk

potřebuje ke své práci". Při rozhodování o přístupu a oprávněních je velmi vhodné vycházet z role daného uživatele v organizaci. Vývojář webových stránek potřebuje například do webového serveru společnosti zcela zřejmě právo úplného přístupu, zatímco administrativní pracovnice nikoli.

- Uvědomění uživatelů.. Školení uživatelů a posílení jejich uvědomění v otázkách bezpečnosti je velmi důležité; jen tak pochopí její význam a budou spolupracovat a podporovat zásady zabezpečení.
- Monitorování. Snad jednou z nejčastěji opomíjených stránek bezpečnosti je monitorování či sledování. Mnohé organizace se domnívají, že zkrátka stačí si jednou síť zabezpečit a mají vystaráno. To ale pravda není; každý musí systémy průběžně monitorovat a ověřovat, jestli jsou stále bezpečné a odolné vůči útokům.
- Aktualizace systémů. Upgrade, aktualizace či záplaty v systémech jsou také jedním z úkolů, jež zaneprázdnění systémoví administrátoři často přehlížejí. Mnohé novější operační systémy dokáží naštěstí automaticky připomínat stahování aktualizací. Základní myšlenka je jasná: vždycky je potřeba sledovat, jestli pro daný systém nejsou k dispozici nějaké aktualizace, protože hackeři nikdy nespí a stále hledají nové možnosti zneužití. Podobné funkce najdeme například i v systémech Apple.

Bezpečnostní politika je soubor pravidel, jejichž dodržování má zaručit počítačovou bezpečnost. Jelikož bezpečnost je příliš důležitá na to, aby byla dobrovolná, musí být prosazována operačním systémem nebo speciálními aplikacemi a zařízeními, které musí být navrženy tak, aby se nedali obejít (proxy servery, firewally, ...)
Každý informační systém by měl mít stanovenou jasnou a kompletní bezpečnostní politiku, která určuje, kdo má jaká práva. Počítače na Internetu (nebo jakékoli jiné síti) jsou také informační systémy, jejichž hodnota může být mnohem větší než jen hodnota "železa"! Proto pokud se připojíte na Internet, musíte si vypracovat i bezpečnostní politiku. Jinak jsou vaše data v ohrožení.

Základní body pro tvorbu bezpečnostní politiky:
1. to, co není výslovně povoleno, je zakázáno!
2. nedávejte uživatelům a aplikacím více práv, než potřebují pro svou činnost
3. nikdy se nespoléhejte na jediný ochranný prostředek. Například omezení přístupu

můžete používat TCP wrapper, ale zkombinujte ho i s firewallem.

4. pravidelně aktualizujte software a zálohujte data!

Při tvorbě bezpečnostní politiky nezapomenout zohlednit i to, že absolutní většina (80% a více) útoků pochází z vnitřní sítě, tedy ze sítě, kterou obvykle chráníme proti útokům zvenčí. Pokud je ochrana založená pouze na ochraně "hranice" mezi sítěmi, kterou obvykle zajišťuje firewall, a nebere v úvahu chyby v aplikacích na serverech (neaktualizují se), ve skutečnosti jsou servery stejně zranitelné - z vnitřní strany (a my o tom nevíme, a co je horší, ani nás to nenapadne).

Bezpečnostní slabiny:

• zranitelné místo ("vulnerability"): slabina v bezpečnostním systému (aplikaci, operačním systému ,...), která může být využita

• hrozba ("threat"): okolnost, která má potenciál způsobit ztrátu nebo škodu

• útok ("attack"): aktivita, která využívá zranitelné místo na průnik do systému.

• ochrana: ochranné opatření, jehož úkolem je redukce slabin. [4]

4 WIFI A HROZBY V BEZDRÁTOVÝCH SÍTÍCH

Ohrožení bezdrátových sítí má nejrůznější podobu — někdo se může připojit k bezdrátovému přístupovému bodu (Wireiess Access Point, WAP) bez oprávnění, anebo může pomocí vhodného nástroje odposlouchávat pakety přímo „ze vzduchu" a snažit se je dekódovat. Řada uživatelů bezdrátových sítí nemá přitom nejmenší tušení, jakým nebezpečím se při pouhém zapojení přístupového bodu do pevné sítě vystavují. Pokusím se proto popsat nejčastější typy hrozeb, k nimž vede zapojení bezdrátových komponent do sítě.

Protože přenos dat v bezdrátové síti WLAN běží otevřeným prostorem, „vzduchem", je celá síť otevřená i vůči potenciálním vetřelcům a útokům, které mohou přijít odkudkoli. Provoz v bezdrátové síti je navíc veden po rádiových vlnách, jež prostupují i zdmi budov. Zaměstnanci mohou sice pohodlně pracovat třeba s notebookem někde na trávníku, ale stejně tak se do sítě mohou dostat i hackeří - ať už sedí nenápadně na parkovišti, nebo se pohybují po ulici.

Bezdrátová komunikace probíhá formou vysílání rádiových vln, a proto můžeme pouhým naslouchánim přenosů snadno odposlechnout všechny nešifrované zprávy. Na rozdíl od pevných sítí LAN není totiž uživatel bezdrátové sítě omezen jen na vlastní prostory firmy ani na jeden přístupový bod — výjimkou jsou jedině nepokryté oblasti. Dosah bezdrátové sítě LAN se může být pohybovat i daleko za obvodové zdi kancelářské budovy, kde tím pádem umožňuje i neoprávněný přístup z veřejných míst, jako je parkoviště nebo kancelář jiné firmy. Útočníkovi, který se chce dostat na nechráněný přístupový bod, tak úplně stačí být v jeho dosahu, a nepotřebuje žádné speciální vědomosti či vybavení. Prakticky u každého zákazníka, jenž požaduje návrh sítě do pronajatých prostor v nějaké větší, společné budově, se setkáme s některým ze dvou případů:

- Sousední firma má otevřenou bezdrátovou síť.
- Sousední uživatel se neoprávněně napojil do bezdrátové sítě cizí firmy.

Pomocí vhodné aplikace pro odposlech paketů (packet sniffer) není problém sledovat veškerý provoz, který prochází určitým ethernetovým připojením (ať už vede do pevné nebo bezdrátové sítě). Takový nástroj zachycuje veškeré pakety, jež prochází přes jedno nebo několik spojení v síti Ethernet, a umožňuje jejich pozdější kontroly; odposlechové

aplikace vezmou paket, analyzují jej a zjistí jeho datovou zátěž. Jednou z největších hrozeb je zde zcela jednoznačně krádež identity (totožnosti) právoplatného, oprávněného uživatele.

Pomocí odposlechu paketů se dá snadno napadnout běžné, známé chování uživatelů. Člověk zkrátka přijde do práce, pustí si počítač, a jako jednu z prvních věcí si zkontroluje příchozí poštu. Většina e-mailových serverů nevyžaduje žádné šifrování, a protože ani bezdrátová síť zde nepřenáší žádná data v šifrované podobě, vysílá se i uživatelské jméno a heslo v prostém textu. Útočník s odposlechovým nástrojem tak může snadno odcizit identitu uživatele a později se kdykoli bez vědomí poškozeného přihlásit k poštovnímu serveru.

Pokud jste už něco o odposlechu paketů slyšeli a víte, jaké informace se z nich dají zjistit, nejspíš vás teď zarazí, že popsaných nástrojů existuje celá řada a že jsou některé dokonce zadarmo - a navíc, že jsou bezdrátové sítě tak zranitelné. A pokud se s odposlechem setkáváte poprvé, bude pro vás možná šokem, jaké obrovské množství informací se může skrývat v datové části paketu. Představte si, že se jako doménový administrátor přihlašujete k doménovému serveru, nebo že se přihlašujete do elektronické bankovní aplikace k osobnímu účtu - a vidíte, jak nebezpečná může být krádež informací.

4.1 Útoky

Hrozbou pro bezdrátovou síť může být i útočník, kterému se přímý přístup získat nepodaří - může totiž síť zaplavit neboli zahltit množstvím statického šumu, díky němuž začne docházet ke kolizím bezdrátového signálu a ke vzniku chyb kontrolního součtu CRC. Tyto útoky spadají do kategorie odepření služeb (Denial of Service, DoS) a v konečném důsledku dokáží celou bezdrátovou síť vyřadit z provozu nebo ji výrazně zpomalit, stejně jako klasické útoky DoS zasahují do pevných sítí. Uvedená hrozba je na první pohled jasná a těžko se jí vyhnout - ostatně ani v pevné síti nejsme vůči virům, útokům a dalším problémům nijak výrazněji chráněni.

Bezdrátový přístup dnes nabízí řada restaurací, hotelů, obchodních či podnikatelských center, bytových komplexů i jednotlivců, přičemž ale nemají téměř žádnou nebo vůbec žádnou ochranu. V těchto situacích se můžeme snadno dostat i do jiných počítačů,

připojených ke stejné bezdrátové síti LAN; vzniká tak hrozba neoprávněného odhalení citlivých informací a krádeže systémových prostředků. Pokud si uživatel vezme svůj firemní notebook domů a zde s ním pracuje v prostředí bezdrátové sítě, je nakonec v ohrožení i vlastní firemní síť.[1]

4.2 Pirátské přístupové body

Bezdrátový přístupový bod si může uvést do provozu každý, kdo má přístup k vhodnému síťovému připojení, ve firemní i domácí síti. Většina bezdrátových zařízení pracuje skutečně v domácnostech a lidé s notebookem tak mohou pracovat v libovolné místnosti. To, že se s bezdrátovými technologiemi pracuje tak snadno, by ale mělo být pro každého síťového administrátora varováním.

K instalaci malé bezdrátové sítě WLAN stačí do pevné sítě zapojit obyčejný bezdrátový přístupový bod a použít notebook s WIFI kartou. Zaměstnanci si díky tomu velice často spouštějí neoprávněné, neschválené bezdrátové sítě, protože „oficiální" počítačové oddělení přijímají často nové technologie příliš pomalu. Neoprávněné přístupové body se označují také jako pirátské (rogue access point).

Podstatou bezdrátové technologie je nabídnout lidem svobodu pohybu za současné možnosti připojení k síťovým prostředkům. Kouzlo této svobody je například mezi zaměstnanci firem natolik lákavé, že si bezdrátové zařízení koupí za své náklady a v kanceláři je „napíchnou" do firemní sítě. [4]

Síťoví administrátoři dělají všechno pro to, aby ochránili podnikovou síť před útočníky a dalšími „zločinci", a najednou se objeví úplně nezabezpečený vstup do „nejposvátnějších" míst - do samotné počítačové sítě firmy.

Ve firmě, která je dobře vybavena potřebnou dokumentací, platí několik souborů zásad zabezpečení, jež usměrňují veškeré typy chování uživatele připojeného do sítě. Pirátské přístupové body ale tyto zásady porušují a otevírají vrátka nejrůznějším závadným aktivitám.

Abychom ale vůči zaměstnancům, kteří se tohoto „těžkého hříchu" dopustí, byli spravedliví, musíme v písemných zásadách zabezpečení jasně stanovit, že:

- Síťová zařízení smí připojovat jen oprávněný zaměstnanec počítačového oddělení (IT).
- Veškerá zařízení, připojovaná do firemní sítě, a zejména pak bezdrátové přístupové body, musí vyhovovat platným zásadám zabezpečení.
- Jakékoli zařízení, které nainstaloval jiný zaměstnanec než oprávněná osoba z oddělení IT, buďto propadne do vlastnictví firmy, nebo bude vyřazeno z provozu.

Hledání pirátských přístupových bodů je dnes o něco snazší než dříve, a to díky volně dostupnému softwaru. Stejný softwarový nástroj, jenž mají v oblibě hackeři, je tak oblíbeným a užitečným pomocníkem specialistů na bezpečnost sítí, kteří s neoprávněnými bezdrátovými přístupovými body naopak bojují.

I útočníci mají nicméně svoje „doporučené postupy", které si mezi sebou vyměňují - nakonec ale takové WarDriving znají i všichni slušní konstruktéři sítí a tímto sledováním chrání sítě zákazníků.

Postupy útočníků:

- Než do sítě zapojíme přístupový bod, musíme si ujasnit, čeho chceme dosáhnout.
- Na používání přístupového bodu se připravíme; To znamená, že jej zapojíme na takové místo, kde ani se zapnutým notebookem nebudeme budit pozornost a podezření.
- Přístupový bod namontujeme co nejméně nápadně, ale zároveň tak, abychom se k němu mohli co nejlépe připojit.
- Vypneme nesměrové vysílání SSID, aby nás lidé z IT oddělení v cílové organizaci neodhalili bez odposlechu paketů.
- Dále v přístupovém bodu vypneme všechny funkce pro správu sítě, jako jsou protokoly SNMP, HTTP a telnet.
- Pokud možno se postaráme, aby se fyzická adresa MAC přístupového bodu neobjevila v žádné tabulce ARP.

Dále je důležité poznamenat, že existují různá zařízení pro rušení rádiových signálů - ta jsou na světě podstatně déle než nějaké bezdrátové sítě. A protože bezdrátové vysílání je rádiové, dá se rušit velice snadno. [4]

4.3 Nesprávně konfigurované přístupové body

Nesprávné konfiguraci přístupových bodů bychom sice měli být schopni zabránit, jinak ale představují významnou díru do bezpečnosti bezdrátové sítě WLAN. Řada přístupových bodů tak podle prvotní, tovární konfigurace otevřeně vysílá své SSID všem oprávněným uživatelům; někteří síťoví administrátoři pak SSID nesprávně používají v roli hesla pro ověření oprávněnosti uživatele. Protože ale SSID se vysílá nesměrově, znamená tato konfigurace velmi závažnou chybu; případný vetřelec se může SSID velice snadno zmocnit a vydávat se za právoplatného uživatele sítě.

Identifikátory SSID fungují jako velmi primitivní heslo a často se používají k rozpoznávání oprávněných bezdrátových zařízení; musíme je proto za hesla považovat a pracovat s nimi v souladu se zásadami práce s hesly.

4.4 Zneužívání sítě

Oprávněný uživatel může integritu sítě narušit také jejím zneužíváním, při němž zabírá velké množství dostupných přenosových kapacit či šířku pásma, snižuje tak rychlost připojení a sráží celkovou výkonnost bezdrátové sítě. Pokud si pár uživatelů začne po bezdrátové sítí vyměňovat nahrávky v MP3, mohou tak způsobit výrazný pokles produktivity ostatních. Ti uživatelé, kteří chtějí v práci skutečně pracovat, si pak nakonec stěžují, že je síť pomalá, nebo že v ní ztrácejí spojení. Podle obecných zkušeností se tyto problémy velice těžko odhalují a lokalizují, zejména pokud firma šetří na nepravém místě a místo přístupových bodů určených do firemní sítě koupí levnější zařízení pro domácí použití - ta ale nejsou vybavena potřebnými nástroji.

Dalším bezpečnostním rizikem, a konec konců i problémem pro výkonnost bezdrátové sítě s neoprávněnými přístupovými body, nesprávným zabezpečením a častým zneužíváním jsou nedbalé a úmyslné operace loajálních i nespokojených zaměstnanců. Opět se tak dostáváme k pravdivému zjištění, podle něhož za většinou případů narušení bezpečnosti stojí uživatelé vnitřní sítě, kterým důvěřujeme.

4.5 Zabezpečení bezdrátových sítí

WEP- se vysvětluje jako Wired Equivalent Protocol, Wireless Encryption Protocol, nebo také Wired Equivalent Privacy. Ať už si ale zkratku vyložíme jakkoli, je WEP šifrovacím algoritmem, který slouží k šifrování přenosů dat mezi uživatelem a bezdrátovým přístupovým bodem.

Při svém zrodu neobsahovala norma 802.11b žádné obsáhlé bezpečnostní nástroje, vhodné pro podnikové sítě a profesionální použití. Dnes již v něm ale jistá základní bezpečnostní opatření jsou a bezdrátová síť tak může být alespoň trochu zabezpečena. Pomocí každé z bezpečnostních funkcí můžeme síť buďto lépe zabezpečit, nebo ji více otevřít pro případné útočníky.

4.5.1 Identifikátor SSID

Přístupový bod vysílá implicitně identifikátor SSID každých několik sekund v takzvaném majákovém rámci (beacon frame). Takto může oprávněný uživatel snadno najít správnou síť, ale zároveň se do ní dostane i neoprávněný hacker. Právě díky této funkci dokáže většina softwarových detekčních nástrojů najít bezdrátovou síť bez předchozí znalosti SSID.

Hodnotu parametru SSID v síti je třeba považovat za první úroveň zabezpečení. Ve své základní, tovární podobě nemusí SSID poskytovat žádnou ochranu proti neoprávněnému přístupu k síti; pokud jej ale změníme na hůře uhodnutelný text, nedostanou se vetřelci do sítě tak snadno.

Hodnoty SSID se dají snadno najít na Internetu, takže je dobré je nejen změnit, ale především nesměrové vysílání SSID vypnout.

4.5.2 Připojení zařízení k přístupovému bodu

Než muže začít jakákoli komunikace mezi klientem a přístupovým bodem v bezdrátové síti, musí obě zařízení zahájit dialog. Tomuto procesu se říká přidružení neboli asociace. Do návrhu normy 802.11b doplnilo přitom sdružení IEEE funkci, podle níž může bezdrátová síť vyžadovat autentizaci klientského zařízení, která musí proběhnout ihned po jeho přidružení, ale ještě před započetím vysílání z přístupového bodu. Cílem bylo samozřejmé vytvořit další vrstvu zabezpečení; autentizace může probíhat se sdíleným

klíčem nebo s otevřeným klíčem.

Jedinou použitelnou metodou je ale autentizace s otevřeným klíčem, protože autentizace se sdíleným klíčem je chybná; je to sice podivné, ale toto doporučení vychází z toho, že budeme mít v síti ještě jiné šifrování.

4.5.3 WEP (Wired Equivalent Privacy)

WEP není a ani neměl být žádným bezpečnostním algoritmem; jeho úlohou nebyla ochrana dat ani před skriptovými amatéry, ani před inteligentnějšími útočníky, kteří se v sítí zajímají o důvěrné údaje. Protokol WEP není postaven jako nějaká zvlášť pevná ochrana, ale pouze zajišťuje, abychom si přechodem z pevné sítě „do vzduchu" nesnížili bezpečnost dat (proto se také většinou vykládá jako Wired Equivalent Privacy, tedy „míra soukromí, ekvivalentní s pevnou sítí")- Problém je, že mnozí lidé vidí v jeho zkratce písmeno „E" jako „Encryption", šifrování. Úkolem WEP je vyřešit slabší zabezpečení bezdrátového přenosu oproti klasické pevné síti; to znamená, že s protokolem WEP jsou data stejně bezpečná, jako na pevné, ale nešifrované síti typu Ethernet.

činnosti WEP:

- Bez šifrování
- 40bitové šifrování
- 128bitové šifrování

WEP je nepovinný šifrovací standard, závislý na dohodě; jeho konfiguraci musíme ovšem provést ještě před připojením uživatele do bezdrátové sítě. Po konfiguraci bezdrátového přístupového bodu i klientského zařízení uživatele již veškerá bezdrátová komunikace probíhá šifrovaně; tím vzniká bezpečné spojení, jehož „rozbití" je poměrně obtížné, i když nejnovější hackerské nástroje již získávají značný náskok. Pokud se uživatel chce k bezdrátovému přístupovému bodu připojit pomocí WEP, musí jej nejprve na svém počítači zapnout a zadat „přístupovou frázi" neboli „klíč", který je společný pro komunikaci uživatele a přístupového bodu.

Záměrem standardu WEP (Wired Equivalent Privacy) bylo tedy nabídnout uživatelům bezdrátové sítě stejné zabezpečení, jako na klasické pevné síti. Při zapnutém WEP se data paketu během přenosu z přístupového bodu do klientského zařízení nejprve zašifrují pomocí tajného 40bitového čísla a šifrovacího algoritmu RC4. Výsledný zašifrovaný paket

se pak odešle do klientského zařízení, které po přijetí dat pod ochranou WEP spustí zpětný chod algoritmu RC4 a pomocí stejného 40bitového čísla paket dešifruje. Tento proces pracuje samozřejmě i v opačném směru, kdy chrání data při přenosu z klientského zařízení do přístupového bodu. Stejným způsobem funguje také 128bitová verze Šifrování; vzhledem k jistým chybám v protokolu WEP se přitom doporučuje používat vždy silnější 128bitové šifrování.[1]

Protokol WEP chrání bezdrátový provoz pomocí šifrovacích služeb, které pracují s kombinací „tajného" klíče WEP a 24bitového náhodně generovaného Čísla (takzvaný inicializační vektor, IV). Tento 24bitový vektor se dále spojí se 40- nebo 104bitovou přístupovou frází WEP a dohromady tak dostaneme plných 128, bitů Šifrovací síly a ochrany.

Se současnými vadnými implementacemi protokolu WEP je bohužel spojeno několik významných problémů:

- První slabou stránkou protokolu WEP je zřejmé omezení číselného rozsahu 24bitového inicializačního vektoru (IV). Výsledkem je 2^{24} = l6 777 216 možných hodnot; to se na první pohled může zdát hodně, ale toto číslo je spíše zavádějící. Problém je, že vzhledem k tomuto poměrně malému číslu se hodnoty a tedy i klíče začnou za relativně nedlouhou dobu opakovat - odtud také útočníci zjistí klíč WEP.
- Druhým slabým místem je, že ne všech zmíněných l6 miliónů hodnot je stejně dobrých; Číslo 1 je tak například pro šifrování nevhodné. Pokud se útočníkovi s pomocí vhodného nástroje podaří najít slabé hodnoty inicializačního vektoru, může bezpečnost WEP prolomit.
- Třetí slabinou je rozdíl mezi 64bitovým a 128bítovým šifrováním. Na první pohled se zdá, že 128bitové musí být dvakrát tak bezpečné - pravda to ale není. Obě úrovně Šifrování pracují totiž se stejným, 24bitovým inicializačním vektorem, který je sám o sobě slabý. Ani 128bitové Šifrování neznamená tedy vyšší bezpečnost sítě.

Všechny tyto věci se samozřejmě dají „zvládnout" pomocí volně dostupných nástrojů, které si hackeři mohou stáhnout z různých míst.

4.5.4 WPA a WPA2

WPA šifruje informace a také ověřuje, zda nedošlo ke změně klíče zabezpečení sítě. Protokol chráněného přístupu WPA také ověřuje uživatele a pomáhá zajišťovat, aby přístup k síti získali pouze autorizovaní uživatelé.

Existují dva typy ověřování pomocí protokolu WPA: WPA a WPA2. Protokol WPA pracuje se všemi adaptéry bezdrátové sítě, ale nemusí pracovat se staršími směrovači nebo přístupovými body. Protokol WPA2 poskytuje větší zabezpečení než protokol WPA, ale nepracuje s některými staršími síťovými adaptéry. Protokol WPA je vytvořen k použití se serverem pro ověřování 802.1X, který jednotlivým uživatelům distribuuje různé klíče.

Pro autentizaci a management klíčů WPA používá 802.1x, pro kontrolu integrity zpráv se zavádí nový mechanismus MIC (Message-Integrity Check) a pro utajení dat nový protokol TKIP (Temporal Key Integrity Protocol) používající pro silnější zabezpečení dynamicky se měnící klíč pro každý paket a prodlouženou délku vektoru IV na 48 bitů. Výhodou WPA jsou dynamické klíče, které jsou výhodné pro podnikové sítě, ale vyžadují složitější síťovou infrastrukturu se serverem RADIUS (802.1x). Nezapomíná se ovšem ani na jednodušší implementace např. v domácích sítích, kde se používají předem nastavené sdílené klíče.

IEEE 802.11i, bezpečnostní doplněk pro všechny bezdrátové LAN podle 802.11a/b/g, byl schválen až v roce 2004. Na základě povinných prvků normy certifikuje WiFi Alliance produkty pod označením WPA2. V současné době je již certifikace podle WPA2 povinná, takže všechny certifikované produkty WLAN musí nejvyšší úroveň zabezpečení podporovat. 802.11i/WPA2 charakterizuje vzájemná autentizace na základě 802.1x nebo na základě PSK a silné šifrování na bázi AES volitelně však také RC4 pro zpětnou slučitelnost s WPA (TKIP).

I když vyšší stupně zabezpečení v podobě WPA a 802.1x mají také známé slabiny, rozhodně se vyplatí nešetřit na řešení zabezpečení WLAN, a tím chránit vstup do celé podnikové sítě. WiFi je totiž pouze tak bezpečná jako její nejméně zabezpečený připojený klient. V situaci, kdy se WEP nelze vyhnout (starší a menší zařízení), je jedinou možností umístit zařízení s WEP na separátní virtuální LAN (subnet) a povolit výhradně očekávaný provoz ze známých stanic. V případě nasazení je pak minimálně vhodné nastavit

upozornění při útocích na WEP, na něž je možné rychle zareagovat prostřednictvím vypnutí napadeného AP, překlíčováním zařízení a fyzickou lokalizací útočníka. [13]

4.5.5 WPS

Průzkum JupiterResearch zjistil, že 40 % uživatelů si neaktivuje bezpečnostní prvky ve své WiFi (stěžují si na složitost) nebo o nich vůbec neví, a z nich polovina spoléhá na firewall. Podle průzkumu WiFi Alliance/Kelton Research dokonce 44 % uživatelů považuje konfiguraci zabezpečení WLAN za středně až značně obtížnou. Proto WiFi Alliance učinila vstřícný krok pro zvýšení bezpečnosti domácích sítí právě z hlediska zjednodušení vlastní konfigurace. Zavedla volitelný program *WiFi Protected Setup*™ (WPS), který podporuje snadnou konfiguraci silných zabezpečovacích prvků (WPA2) tak, aby běžní uživatelé měli šanci svoji WiFi správně zabezpečit a nebyli odrazeni složitým procesem nastavení bezpečnostních mechanismů. [13]

Nejjednodušší varianta WPS podporuje konfiguraci autentizace, kdy směrovač poskytne klientům šifrovací klíče pro WPA/WPA2 na základě stisknutí „jediného knoflíku“ nebo zadáním PIN (ten je generovaný softwarově a zobrazený na monitoru nebo předprogramovaný v klientském zařízení a vytištěný na přiložené kartě/nálepce). Vyšší stupeň WPS bude využívat tokeny nebo bezkontaktní karty, na nichž jsou informace potřebné pro konfiguraci zabezpečení uloženy, takže není již třeba zadávat žádné kódy či hesla ručně. Přiblížení karty nebo tokenu k bezdrátovému zařízení iniciuje výměnu klíčů.

Nejvyšší variantou WPS je využití USB paměti flash, jejímž prostřednictvím se manuálně přenesou potřebné informace do všech klientských zařízení v síti. Místo manuálního zadávání kódů se kopírují automaticky informace z tokenu nebo paměti. Tato možnost se zatím jeví jako nejbezpečnější, protože uživatel musí všechna zařízení, která se mají připojit, fyzicky obejít. Uživatel má pochopitelně možnost i s WPS nahlédnout do konfigurace sítě a jejích bezpečnostních parametrů na směrovači a na přístupovém bodě, což bude třeba v případech sítí s kombinací nových zařízení a starších bez WPS. Pro starší zařízení (s podporou WPA nebo WPA2) má být WPS k dispozici prostřednictvím stávajícího klientského softwaru a webové konfigurace WPA klíčů (autentizace na základě PIN). Pro konfiguraci na základě stisku knoflíku bude třeba pro starší zařízení firmware.

Bezpečnost WiFi nelze oddělit od celkového řešení bezpečnosti sítě. Nejde jen o zabezpečení bezdrátové komunikace na nejnižších vrstvách (fyzické a spojové), ale o řešení bezpečnosti na všech vrstvách síťové architektury, od fyzického zabezpečení po VPN. Bezpečnostní politika musí mít dostatečný nadhled nad všemi součástmi podnikové sítě. Přitom vždy zůstává přítomen neopominutelný lidský faktor, který může náhodou, nevědomky, nebo záměrně způsobit bezpečnostní problém různého dopadu a rozsahu. "Social engineering" je velice účinná metoda hackerů, na kterou jsou všechny bezpečnostní technologie krátké: důvěřivý zaměstnanec může útočníkovi leccos užitečného prozradit nebo mu jinak nechtěně napomoci k přístupu do budovy či sítě. Žádné bezpečnostní řešení v síti proto nemůže být stoprocentní. Ani silná norma 802.11i nezaručuje, že její implementace odolá všem budoucím útokům. Zařízení s WPA2 jsou ale dostatečně dobře technicky vybavena pro dnešní bezpečnostní situace, s nimiž se potýkají zejména podnikové sítě. Nicméně technické možnosti zařízení nestačí, vždy bude na koncovém uživateli, aby se seznámil s bezpečnostními mechanismy, porovnal je se svými potřebami, pečlivě a samozřejmě správně nakonfiguroval příslušnou podporu pro zvolené bezpečnostní řešení. Bezpečnost WLAN prostě nikdy nebude řešitelná pouhým důvěřivým a uživateli tolik oblíbeným přátelským přístupem plug'n'play. S komplexní bezpečností jde přece ruku v ruce složitost. [14]

4.5.6 Filtrování adres MAC

Metoda filtrování fyzických adres MAC představuje další možnost zabezpečení sítí nad normu 802.11b. Adresa MAC síťové karty je 12ciferné hexadecimální číslo, které je jedinečné mezi všemi síťovými kartami na světě. Protože svoji adresu MAC má i každá bezdrátová karta sítě Ethernet, můžeme v přístupovém bodu snadno omezit povolení přístupu jen pro jistou množinu oprávněných zařízení a kohokoli cizího tak snadno vykázat ze sítě.

Filtrování adres MAC není ale bohužel úplně bezpečné, a plně se na ně spoléhat by bylo hrubou chybou.

Nevýhody filtrování adres MAC:

- Někdo musí udržovat databázi adres MAC všech bezdrátových zařízení v síti. Pokud jich máme v síti třeba deset nebo dvacet, není to problém; jakmile máme ale v rozsáhlejší podnikové síti sledovat stovky různých fyzických adres MAC, bude

stejný úkol dosti obtížný.

- Adresy MAC se mohou měnit; cílevědomý útočník může proto pomocí bezdrátového odposlechu zjistit, jaká adresa MAC má povolen přístup, a nastavit si ji ve svém vlastním počítači. Šifrování pracuje v síťové vrstvě 2, takže fyzické adresy MAC jsou při odposlechu paketů stále viditelné. [4]

4.5.7 Protokol EAP (Extensible Authentication Protocol)

Sdružení IEEE schválilo důležitou normu 802.1X, která hovoří o zabezpečení na úrovni portů. Záměrem tohoto schválení bylo sice původně standardizovat bezpečnost portů v pevných sítích, ale záhy se zjistilo, že se dá bez problémů aplikovat také na bezdrátové sítě. Vznikl tedy bezpečnostní protokol EAP (Extensible Authentication Protocol), který pracuje ve vrstvě 2 (tedy ve vrstvě adres MAC), aktivuje se v autentizační fázi celého procesu zabezpečení, a spolu s dalšími bezpečnostními opatřeními zajišťuje třetí a poslední vrstvu zabezpečení bezdrátové sítě. Podle normy 802.1X tak při žádosti zařízení o komunikaci s přístupovým bodem probíhají v protokolu EAP následující operace:

1. Přístupový bod si od klienta vyžádá autentizační informace.
2. Uživatel zadá požadované informace pro autentizaci.
3. Poté přístupový bod odešle autentizační informace od klienta do standardního serveru k autentizaci a autorizaci.
4. Jakmile proběhne autentizace na serveru, dostane klient povolení připojit se a vysílat data.

Obr. 4 - Ověření pomocí funkce NetworkLogin 802.1x[13]

V rámci protokolu EAP se používají následující metody autentizace:

- EAP-MD5
- EAP-Cisco Wireless (také označováno jako LEAP)
- EAP-TLS
- EAP-TTLS

Metoda EAP-MD5 se při odesílání autentizačních informací na server opírá o haš (otisk) MD5, vytvořený z uživatelského jména a hesla. Tato metoda nezajišťuje žádnou správu klíčů ani nenabízí dynamické generování klíčů WEP, a proto vyžaduje statické klíče WEP; má proto jistá omezení:

- Protože není k dispozici žádné dynamické generování klíče WEP, neznamená protokol EAP oproti WEP žádné vyšší zabezpečení; útočníci mohou i nadálé odposlouchávat síť a snadno dešifrovat klíč WEP.
- EAP-MD5 nenabízí žádné prostředky, kterými by si klientské zařízení ověřilo, že vysílá informace do správného přístupového bodu; klient tak může mylně vysílat i do pirátského přístupového bodu.

Znamená to, že EAP-MD5 nenabízí oproti samotnému standardu 802.1X žádné funkce navíc, a proto se ze všech metod EAP považuje za nejméně bezpečnou. [1]

Metodu EAP-Cisco Wireless (označovaná častěji také jako LEAP) vyvinula na základě normy 802.1X firma Cisco a je základem velké části oficiálně schválené verze EAP. Podobně jako EAP-MD5 i metoda LEAP od klientského bezdrátového zařízení přebírá uživatelské jméno a heslo, a předává je k autentizaci na server. Firma Cisco doplnila kromě požadavků samotné normy i další podporu a přinesla tak do metody vyšší bezpečnost:

- Metoda LEAP provádí autentizaci klienta; pro každé klientské připojení se dynamicky generují jednorázové klíče WEP. To znamená, že každý klient bezdrátové sítě pracuje s jiným dynamicky vygenerovaným klíčem, který nikdo nezná - dokonce ani samotný uživatel.
- LEAP podporuje jednu funkci protokolu, kterou jsou časové limity komunikačních relací; to znamená, že se klient musí každých několik minut přihlásit znovu. Uživatel ale naštěstí nemusí dělat nic zvláštního. Přidáme-li k této funkci

dynamické klíče WEP, budou se v důsledku toho klíče WEP měnit tak často, že se útočníkům nepodaří je včas prolomit.

- LEAP provádí vzájemnou autentizaci, tedy klienta vůči přístupovému bodu i naopak přístupového bodu vůči klientu; tím se vytváří ochrana proti instalaci pirátských přístupových bodů do sítě.

U autentizační metody LEAP je známo omezení; pro autentizaci klientu i přístupového bodu se používá protokol MS-CHAPv1, který obsahuje známá zranitelná místa.

Metodu EAP-TLS vyvinula firma Microsoft a její popis je uveden v dokumentu RFC 2176. Namísto kombinace uživatelského jména a hesla provádí tato metoda autentizaci pomocí certifikátů X.509; informace veřejného klíče v PKI se zde do EAP přenášejí pomocí zabezpečení transportní vrstvy. Podobně jako LEAP nabízí i verze EAP-TLS dvě důležité funkce:

- Dynamické generování jednorázového klíče WEP
- Vzájemná autentizace zařízení

A mezi nevýhody metody EAP-TLS patří:

- Pro jeho činnost je nutný protokol PKI, který ale většina firem neprovozuje.
- Je možné využít také službu Microsoft Active Directory a server certifikátů, tato změna je ale obtížná.
- Jestliže máme implementovánu PKI s certifikáty VeriSign, nejsou u ní k dispozici všechna pole požadovaná metodou EAP-TLS.

Tuto metodu má smysl uvádět do provozu jen v případě, že se při její implementaci budeme přesně držet doporučení firmy Microsoft. [1]

Autentizační metodu EAP-TTLS zavedla firma Funk Software, a to jako alternativu k EAP-TLS. Bezdrátový přístupový bod se i zde musí autentizovat vůči klientu pomocí serverového certifikátu, ale uživatelé odesílají pro přihlášení jen uživatelské jméno a heslo. Tyto přihlašovací informace (jméno a heslo) pak EAP-TTLS předává k ověření pomocí libovolného mechanismu výzvy a odpovědi, určeného administrátorem (PAP, CHAP, MS-CHAPv1, PAP/tokenová karta, nebo EAP). Jedinými nedostatky této metody je:

- Je o něco méně bezpečná než dvojité certifikáty EAP-TLS.
- Přesně stejným způsobem pracuje i standard firem Microsoft a Cisco - „chráněná" verze Protected EAP (PEAP).

4.5.8 Zvýšení bezpečnosti bezdrátových sítí

- Bezdrátovou síť umístíme za samostatné směrované rozhraní, které se stane jejím „hrdlem", a které můžeme v případě problémů okamžitě „odstřihnout".
- Budeme sledovat pirátské přístupové body a s nimi spojená potenciální zranitelná místa.
- Fyzicky i logicky zabezpečíme přístupové body, aby se k nim nemohl někdo nepozorovaně dostat a změnit jejich konfiguraci.
- Změníme výchozí identifikátor SSID a zvolíme namísto něj nahodilý řetězec, z něhož nelze odvodit žádné informace o mateřské firmě či síti.
- Vypneme aktivní nesměrové vysílání hodnoty SSID.
- Každých 10 minut a méně budeme rotovat klíče nesměrového vysílání.
- Zapneme šifrování a autentizaci, což může znamenat vytvoření virtuální privátní sítě nad bezdrátovými zařízeními.
- Pro správu klíčů a autentizaci využijeme protokol 802.1X.
- Posoudíme všechny dostupné protokoly EAP a rozhodneme se, který z nich je pro dané prostředí nejvhodnější.
- Nastavíme časový limit komunikační relace, a to na 10 minut a méně.
- Zavedeme vhodné zásady zabezpečení bezdrátové sítě a budeme vyžadovat jejich dodržování.
- Implementujeme proaktivní bezpečnostní opatření, mezi něž patří ochrana proti vniknutí. [1]

5 SERVER

Server poskytuje služby a prostředky klientům.V síti může být libovolný počet serverů a pracovních stanic (omezení klade konkrétní implementace). Serverů bývá řádově méně než klientů. Pokud je serverů v síti více, mohou se navzájem v poskytování služeb a prostředků doplňovat.

Rozdíl v součástech mezi serverem a pracovní stanicí:

komponent	SERVER	Běžný PC	poznámka
CPU	Serverový CPU (XEON, OPTERON)	Běžný CPU (Pentium 4, ATHLON)	Serverové CPU jsou odlišné od klasických hlavně výkonem a liší se i paticí.
RAM	RAM s ECC	RAM bez ECC	Serverové paměti využívají navíc kontrolní paritu aby se předešlo chybám
HDD	SCSI	SATA , PATA	SCSI disky mají oproti běžným diskům větší výkon a delší životnost
ZDROJ	Redundantní zdroj	Klasický zdroj	Servery používají redundantní zdroje, to znamená, že je v serveru víc zdrojů. V případě výpadku jednoho zdroje nahradí činnost další zdroj. Server běží bez pádu.Vadný zdroj se dá za běhu vyměnit.
Operační systém	Serverový systém Win 2003/2000 Server , UNIX	WIN XP , WIN VISTA, Linux	Serverové OS se liší hlavně škálovatelností a službami , které poskytují.

Tabulka 1. - rozdíl server/pracovní stanice

6 HESLA A BEZPEČNOSTNÍ ZÁSADY

Mít jasně stanovené zásady zabezpečení neboli bezpečnostní politiku je naprosto nejdůležitějším prvním krokem při zabezpečení a ochraně sítě. Tyto zásady rámcově určují, co je přijatelné a správné chování uživatele ve firemní síti a na základní úrovni tak zásady tvoří jakousi „zákonnou normu", podle níž posuzujeme všechno ostatní. Zásady zabezpečení jsou tedy do značné míry podobné různým pravidlům a zákonným normám, kterými se řídíme v našem každodenním životě. Pravidla nám ale nesmí bránit v provádění běžných a rozumných věcí. Stejně tak i zásady zabezpečení stanovují, jaké chování je a není uvnitř i vně sítě přípustné.

Bezpečnostních zásady:

- Zásady zabezpečení určují očekávané postupy.
- Definují vhodné chování v síti.
- Představují základ pro případný postih ze strany osobního oddělení za nepřípustné chování.

Pokud máme ve firmě stanovené zásady zabezpečení sítě, je z nich každému uživateli naprosto jasné, kdo je za co odpovědný, a jaké zásady a procesy platí pro jednotlivá firemní oddělení. Oddělení služby zákazníkům bude například znát své povinnosti při ochraně citlivých údajů o zákaznících, osobní oddělení ví, co se očekává od zaměstnanců, a oddělení výroby a vývoje ví, jak chránit výsledky nákladného výzkumu. Nejdůležitější ale samozřejmě bude, co zásady zabezpečení znamenají pro počítačové neboli IT oddělení; jeho zaměstnanci tak musí vědět, jak mají konfigurovat servery, jaké nástroje budou potřebovat, jaká pravidla mají být nastavena na firewallech, jak mají vypadat virtuální privátní sítě VPN a tak dále.

Nejběžnější typy zásad zabezpečení:

- Přípustné šifrování

Stanovuje pravidla, která omezují šifrování jen na obecně známé, prověřené a účinné algoritmy. Navíc určuje potřebné postupy, které zajišťují naplnění příslušných zákonů a nižších předpisů.

- Přípustné užití

Vymezuje osoby, které smí pracovat s počítačovým zařízením a sítěmi ve vlastnictví

společnosti. Týká se firemních počítačů, umístěných ve firemních prostorách i v domácnostech zaměstnanců.

- Analogové linky

Popisuje způsoby přípustného využívání analogových telefonních

linek a linek ISDN a nařizuje příslušné zásady a postupy pro schvalování. Pro linky, určené výhradně k faxování a příjmu hovorů, a linky zapojené do počítačů platí samostatná pravidla.

- Standardy poskytovatelů aplikačních služeb

Vyjadřuje požadavky firmy na poskytovatele aplikačních služeb (Application Service Providers, ASP). Tito poskytovatelé zajišťují společně softwarové, hardwarové i síťové technologie. Součástí těchto zásad jsou také samostatné standardy poskytovatelů. Definuje kritéria minimální bezpečnosti, kterou musí splňovat každý poskytovatel aplikačních služeb (ASP).

- Audit

Členům oddělení informační bezpečnosti přiděluje oprávnění k výkonu bezpečnostního auditu nad libovolným systémem, který je ve vlastnictví společnosti nebo který je v jejích prostorách nainstalován.

- Automaticky přeposílaná pošta

Zakazuje neoprávněné i neúmyslné prozrazování citlivých firemních informací.

- Přístupové informace

Určuje požadavky na bezpečné ukládání a načítání uživatelských jmen a hesel k databázím (neboli přístupových informací), které budou využívat programy při přístupu k databázi provozované na firemní síti.

- Vytáčený přístup

Stanovuje pravidla pro ochranu elektronických informací před neúmyslným ohrožením, jestliže oprávněný zaměstnanec pracuje nad vytáčeným připojením.

- Extranet

Určuje zásady, podle nichž se do firemní sítě smí připojit cizí organizace za účelem provádění transakcí.

- Citlivost informací

Napomáhá zaměstnancům určit, které informace smí sdělovat cizím osobám (mimo zaměstnanců), a také relativní citlivost informací, které se bez oprávnění sdělovat nesmí.

- Bezpečnost vnitřních laboratoří

Definuje požadavky informační bezpečnosti v laboratořích, které zabraňují v ohrožení důvěrných informací a technologií, a také ochraňují provozní služby a ostatní zájmy firmy před pokusnými laboratorními aktivitami.

- Antivirová ochrana

Vymezuje požadavky, jež musí splňovat všechny počítače připojené do podnikové sítě s ohledem na účinnou detekci virů a jejich prevenci.

- Hesla

Zavádí standardy pro vytváření silných hesel, ochranu hesel a frekvenci změn hesel.

- Vzdálený přístup

Definuje standardy pro připojení libovolného hostitele do firemní sítě. Tyto standardy sledují minimalizaci různých potenciálních hrozeb, jako je ztráta citlivých nebo důvěrných firemních dat, duševního vlastnictví, poškození image firmy na veřejnosti, poškození kriticky důležitých vnitřních systémů atd.

- Posuzování rizik

Zmocňuje oddělení informační bezpečností k provádění pravidelného posuzování rizik bezpečnosti informací, jehož účelem je zjištění zranitelných míst v síti a zahájení nápravných opatření.

- Zabezpečení směrovačů a přepínačů

Popisuje povinnou minimální bezpečnostní konfiguraci všech směrovačů a přepínačů, připojených do ostré provozní sítě, nebo používaných v jakémkoli ostrém provozním prostředí.

- Zabezpečení serverů

Vymezuje standardy pro základní konfiguraci interních serverů, které jsou ve vlastnictví a/nebo provozu firmy, případně které pracují ve webovém hostovaném prostoru.

- Virtuální privátní sítě

Stanovuje zásady vzdáleného přístupu přes síť VPN s IPSec nebo L2TP do vnitřní firemní sítě.

- Bezdrátová komunikace

Určuje pravidla pro přístup do podnikové sítě prostřednictvím zabezpečených mechanismů bezdrátové komunikace.

6.1 Definice důvěry

Každý ze zaměstnanců daného oddělení či firmy musí nejenže znát obsah příslušných zásad, ale především se jimi také řídit. Zásady zabezpečení mají skutečně vliv na všechny skupiny uživatelů v organizaci:

- Běžný uživatel. Na obyčejného uživatele, který přistupuje k síťovým prostředkům, mají stanovené zásady největší vliv.
- Týmy ve vedení firmy. Tato skupina má největší zájem na ochraně podnikových prostředků a dat, přičemž je pro ni zároveň důležité, za jakou cenu budou tato opatření prováděna.
- Účetní a právní oddělení, investoři. Odpovědnost firmy pří ochraně svých vlastních aktiv je závislá na popisovaných zásadách (bezpečnostní politice); každý z této skupiny si musí uvědomit, jaký pozitivní dopad mají přijaté zásady.
- Týmy pro vedení bezpečnosti. Role této skupiny je definována v samotných zásadách a jejím úkolem je zajišťování platnosti zásad zabezpečení.[4]

Důvěra je ústředním motivem mnoha různých stránek věnovaných bezpečnosti, a jako taková musí být pro nás naprosto prvořadá i při návrhu konkrétní bezpečnostní politiky či zásad zabezpečení. Kdyby byl svět dokonalý, neměli bychom s důvěrou žádné problémy zkrátka bychom mohli důvěřovat každému a nikdo by také nikdy nedělal nic nedovoleného. To je ale bohužel velmi vzdálená utopie, která navíc nebere v úvahu další faktory, jako jsou například možné chyby v síťových prostředcích. I zde se dá říci, že důvěřovat různým prostředkům v síti je v zásadě v pořádku, ale nesmíme zapomenout, že ani v hardwaru a softwaru se zkrátka chybám nevyhneme.

Zásady zabezpečení bychom naopak mohli postavit na myšlence, že nebudeme důvěřovat vůbec nikomu, a to ani zaměstnancům vlastní organizace. Takovéto zásady by ale také nefungovaly; je všeobecně známo, že pokud se uživatelům nějaké zásady zdají příliš svazující, tím častěji je obcházejí. V zásadách zabezpečení musíme proto nastolit vhodnou

rovnováhu mezi důvěrou a bezpečností; každá organizace má tento rovnovážný bod někde jinde, ale určité zabezpečení potřebuje každý.

Při stanovení úrovně důvěry, musíme zvážit následující otázky a během dalšího návrhu zásad na nich dále stavět.

- Určit, kdo smí dostat právo přístupu do jednotlivých částí sítě.
- Vymezit, k jakým prostředkům smí tito uživatelé přistupovat a jak.
- Vyvážit důvěru mezi osoby a technické prostředky.
- Povolit přístup podle úrovně důvěry uživatelů a prostředků.
- Pomocí vhodných prostředků zajistit, že důvěra nebude narušena.
- Definovat odpovídající používání sítě a jejích prostředků.

Kromě tohoto stručného seznamu je třeba zvážit celou řadu dalších věcí, včetně celkové firemní politiky a také zvyklostí uživatelů a jejich reakcí. Žádná bezpečnostní politika nemůže počítat úplně se vším, přesto je ale důležité si uvědomit, že mezi lidmi vyvolává také nějakou reakci.

Zásady zabezpečení by měly především zdůrazňovat, co je povoleno, nikoli co je zakázáno; podle potřeby mohou uvádět příklady správného (povoleného) a nesprávného (zakázaného) chování. Takto není pochyb o významu zásad; obecně platí, že jakékoli chování, které není v zásadách zabezpečení výslovně povoleno, je zakázáno. Zásady zabezpečení by měly popisovat také způsoby dosažení stanovených cílů.

Důvěřovat můžeme úplně každému, nebo naopak vůbec nikomu; ani jeden z těchto extrémů ale při nastolení rovnováhy mezi produktivitou práce a bezpečností nefunguje. Každý uživatel má na potřebné zabezpečení sítě jiný náhled a každý cítí také trochu jiné obavy. Uživatel se může například obávat, že kvůli bezpečnosti bude jeho práce obtížnější, nebo se může bát trestu i za nějaký chybný krok či drobné opomenutí. Žádný člověk ale každopádně nemá rád, když mu někdo nebo něco brání v normální prácí. Všechny tyto postoje jsou docela běžné, normální emoční reakce, a proto jim musíme porozumět a v zásadách zabezpečení je správně ošetřit, jinak se nepodaří docílit vyvážené ochrany firmy.

Jestliže do návrhu zásad zabezpečení zapojíme zástupce z různých skupin zaměstnanců, vyhneme se tím případným osobním sporům. V podstatě je to jakési „sociální inženýrství" v dobrém slova smyslu - pokud se návrhu zásad účastní „zástupci lidu", přijmou jejich

výslednou podobu snáze.[5]

Účelem těchto zásad zabezpečení je stanovit pravidla přípustného užívání počítačového vybavení ve firmě. Tato pravidla slouží k ochraně firmy i jejích zaměstnanců; nepřípustné užívání systémů může vystavovat společnost různým rizikům, například virovým útokům, napadení síťových systémů a služeb i právnímu postihu.

Tyto zásady zabezpečení platí pro každého zaměstnance, dodavatele, konzultanta, dočasného pracovníka a pro ostatní osoby ve firmě, včetně osob spojených s příslušnými cizími subjekty. Dále platí pro veškerá zařízení, která jsou ve vlastnictví firmy nebo jsou jí pronajatá, a také pro každé osobní zařízení, které může přijít do styku s podnikovou infrastrukturou IT.

Snahou týmu podnikové bezpečnosti firmy je zajistit přiměřenou úroveň soukromí, uživatelé si nicméně musí být vědomi, že veškerá data, která v podnikových systémech vytvoří, zůstávají vlastnictvím firmy. Vzhledem k nutnosti ochrany sítě nemůže vedení firmy zaručit důvěrnost žádných informací, uložených na síťovém zařízení v majetku firmy.

Příklady důvěrných informací jsou mimo jiné:

Soukromé nebo důvěrné firemní informace, podnikové strategie a záměry, informace citlivé vzhledem ke konkurenci a konkurenční analýzy, data podléhající obchodnímu tajemství, patenty, výsledky testů, specifikace a provozní parametry, seznamy zákazníků a údaje o nich.

Zaměstnanci musí všemi vhodnými prostředky zabránit neoprávněnému přístupu k těmto a podobným informacím. Má-li zaměstnanec podezření z úniku těchto informací mimo společnost, musí bezprostředně uvědomit tým podnikové bezpečnosti.

Hesla je třeba uchovávat v tajnosti a bezpečí; zaměstnanci nesmí účet půjčovat nikomu jinému. Každý oprávněný uživatel je odpovědný za bezpečnost svého vlastního účtu i hesla. Systémová hesla je dobré měnit nejméně jednou za čtvrtletí, uživatelská hesla pak každých šest měsíců.

Veškeré osobní počítače, notebooky a pracovní stanice musí být zabezpečeny pomocí spořiče obrazovky s ochranou heslem a s automatickou aktivací nejpozději po 10 minutách nečinnosti, nebo se uživatel při vzdálení od počítače musí odhlásit.

Také informace umístěné na přenosných počítačích jsou zvláště zranitelné, a proto je nutné s nimi zacházet mimořádně opatrně.

Veškeré počítačové systémy, které zaměstnanec používá a které jsou připojeny k Internetu, intranetu nebo extranetu ve firmě, ať už jsou v majetku zaměstnance nebo firmy, musí být neustále kontrolovány schváleným antivirovým softwarem s aktuální databází virů.

Tato část zásad se týká mimo jiné i osob, které mají ve zvyku číst e-mail z různých počítačů na různých fyzických místech. Představte si například zaměstnance, jenž bude v práci číst poštu ze svého soukromého, bezplatného účtu webového e-mailu a nevědomky si stáhne zavirovaný soubor. Cílem uvedeného pravidla je zajistit, že i takovýto virus bude zachycen ve vhodném antiviru. Pokud ale zaměstnanec přistupuje ke stejnému webovému e-mailu z domácího počítače, jehož prostřednictvím se následně připojuje i do podnikové sítě, je třeba důkladně zvážit možné důsledky a ohrožení firemních systémů.

Při otevírání e-mailových příloh od neznámých odesílatelů, které mohou obsahovat viry, e-mailové bomby nebo trojské koně, si uživatelé musí počínat maximálně opatrně. V případě pochybností je uživatel povinen zkontrolovat dokument ručně a před otevřením přílohy se spojit s týmem podnikové bezpečnosti. [1]

6.2 Zásady přípustného užívání

Tyto aktivity jsou bez jakýchkoli výjimek přísně zakázány:

Porušování práv libovolné osoby či společnosti, chráněných autorskými zákony, obchodním tajemstvím, patentovým nebo jiným duševním vlastnictvím, případně podobnými zákony a nařízeními, včetně instalace a distribuce odcizeného či „pirátského" softwaru, jehož užívání není kryto odpovídající licencí.

Neoprávněné kopírování materiálu podléhajícího autorským právům, jako je mimo jiné i digitalizace a distribuce fotografií z časopisů, knih a jiných zdrojů krytých autorským právem, hudby chráněné autorským právem, a také instalace softwaru krytého autorským právem, pro který nemá společnost ani koncový uživatel potřebnou aktivní licenci, je přísně zakázána.

Zavádění škodlivých či zlomyslných programů do sítí a serverů (například virů, červů, trojských koňů, e-mailových bomb atd.).

Prozrazení hesla k uživatelskému účtu jiným osobám nebo svolení k využívání účtu jinou osobou. Vykonává-li zaměstnanec svou práci doma, spadají mezi tyto osoby i ostatní členové rodiny a společné domácnosti.

V rámci zásad je vhodné také stanovit, že se nikdo ve firmě nesmí na podobu hesla ptát. Při technických závadách může administrátor heslo pouze vymazat (nahradit výchozí hodnotou).

Jednání, které má za následek prolomení bezpečnosti nebo narušení síťové komunikace. Mezi prolomení bezpečnosti patří mimo jiné přístup k datům, která nejsou určena danému zaměstnanci, nebo přihlášení k serveru či pod účet, k němuž není zaměstnanec oprávněn přistupovat, ledaže se jedná o úkoly spojené s plněním pracovních povinností. Za „narušení" považujeme odposlech v síti, záplavy dotazů ping, falšování paketů, odepření služeb a falšování směrovacích informací za nekalými úmysly.

Jakákoli forma monitorování sítě, při němž zaměstnanec zadržuje či odposlouchává data, která pro něj nejsou určena, ledaže toto monitorování spadá pod normální pracovní povinností zaměstnance.

Obcházení mechanismů autentizace uživatelů či bezpečnosti libovolného hostitelského systému, sítě nebo účtu.

Spouštění jakýchkoli programů, skriptů a příkazů, nebo odesílání jakýchkoli zpráv, jejichž cílem je narušování nebo zablokování terminálové relace jiného uživatele, a to lokálně, v Internetu, intranetu i extranetu. [4]

6.3 Aktivity v elektronické poště a při komunikaci

Zakázané činnosti v zabezpečené síti: Odesílání nevyžádaných zpráv elektronické pošty, hromadné pošty nebo jiného reklamního materiálu jednotlivcům, kteří je výslovně nepožadovali (e-mailový spam).Jakákoli forma obtěžování, a to elektronickou poštou, telefonem a jinými prostředky, a to v libovolném jazyce, s jakoukoli frekvencí a při jakékoli velikosti zpráv. Neoprávněné používání nebo falšování informací v záhlaví elektronické posty.Vyžadování e-mailových zpráv, určených pro kteréhokoli jiného uživatele či adresu, se záměrem obtěžování či shromažďování odpovědí. Vytváření a rozesílání řetězových dopisů, pyramidových her a podobných. Podávání stejných či podobných zpráv nepracovního charakteru do velkého množství diskusních skupin (spam v

diskusních skupinách).

Lidé bývají z uvedených zásad a podobných dokumentů často otráveni a myslí si, že po nich zaměstnavatel zase něco nového chce; ve skutečnosti tak ale přispívají k naplňování cílů firmy. Jen pokud přijmeme tuto základní pravdu, budou nám zásady zabezpečení sloužit pří ochraně celé společnosti, jejích zaměstnanců a všech partnerů.

6.4 Zásady pro práci s hesly

Hesla jsou velmi důležitou stránkou zabezpečení počítačů a tvoří první „obrannou linii" uživatelských účtů. Nevhodně zvolené heslo může nakonec vést i k narušení bezpečnosti celé podnikové sítě firmy. Vzhledem k tomu je každý zaměstnanec (i každý z uživatelů mezi dodavateli a odběrateli firmy, kteří mají do firemních systémů přístup) odpovědný za správný výběr hesla a jeho zabezpečení.

Úkolem těchto zásad je stanovit standard pro vytváření silných hesel, mechanismy ochrany hesel, a definovat způsob jejich měnění.

Hesla k uživatelským účtům je potřebné pravidelně měnit, protože útočník se je pokouší prolomit jako první. Většina systémů vyzývá po uplynutí určité doby uživatele ke změně hesla automaticky; mnohé z novějších operačních systémů provádějí nad heslem dokonce určité testy a zakazují uživateli volit heslo, které se dá snadno uhodnout nebo nalézt ve slovníku.

Tyto zásady zabezpečení platí pro každou osobu, která je odpovědná za určitý účet nebo za libovolný jiný typ přístupu, jenž podporuje nebo vyžaduje zaslání hesla, a to na libovolném systému, který je umístěn v prostorách firmy, který má přístup k síti, nebo na kterém jsou uloženy neveřejné informace společnosti.

Pojem účtu je možné v definici rozšířit také na elektronickou poštu, elektronické zámky, službu FTP, sdílené diskové jednotky atd. Určité zásady pro práci s hesly musí platit pro přístupová hesla ke všem těmto prostředkům.

Obecné zásady:

- Veškerá systémová hesla (například účty root, enable, Administrátor ve Windows NT, účty pro správu aplikací apod.) se musí změnit alespoň jednou za čtvrtletí.
- Veškerá provozní systémová hesla musí spadat pod globální databázi správy hesel.

Ne každá organizace sleduje hesla v něčem takovém jako je „globální databáze správy hesel" a většina z nich v podstatě nic takového nepotřebuje. Hesla a frekvenci jejich změn nicméně jistým způsobem sledovat musíme; jen tak zajistíme dodržování stanovených zásad. Přístup k jakémukoli nástroji musí být pochopitelně přísně střežen.

Veškerá uživatelská hesla (například pro přístup k e-mailu, k webu, ke stolním počítačům apod.) musí být změněna nejméně jednou za šest měsíců; doporučený interval změn je jednou za čtyři měsíce.

Uživatelské účty s oprávněními systémové úrovně, přidělovanými pomoct členství uživatele ve skupinách či pomocí jiných programů (například administrátor a root) musí mít jedinečné heslo, různé od hesel všech ostatních účtů dané osoby. Hesla nesmí být zapisována do zpráv elektronické pošty ani do jiné elektronické komunikace.

Heslo nesmí žádný uživatel prozradit nikomu jinému, bez ohledu na pozici případného žadatele v organizaci.

Skupinové heslo (community string) nesmí mít standardní výchozí hodnotu jako „public", „private" a „system", a musí být různé od hesel pro interaktivní přihlášení.

Je doslova šokující, kolik firem se tato výchozí hesla nenamáhá změnit.

Hesla se v systémech firmy používají k nejrůznějším účelům například hesla k uživatelským účtům, k webovým účtům, k e-mailovým účtům, ke spořičům obrazovky, k hlasové poště a pro místní přihlášení ke směrovačům. Jen málokterý systém podporuje přitom jednorázové tokeny (neboli dynamická hesla s jednorázovou platností), a proto si každý uživatel musí umět zvolit dostatečně silné heslo.

Takto vypadá typické slabé, nevhodné heslo:

- Heslo je kratší než osm znaků.
- Heslo se dá přímo najít v jazykovém slovníku (českém, anglickém nebo i jiném).
- Heslo je běžným výrazem, jako například: Jméno člena rodiny, domácího zvířete, přítele, spolupracovníka, filmové postavy apod.
- Výrazy a názvy z oblasti počítačů, příkazy, servery, firmy, hardware, software.
- Snadno uhodnutelné vzorky písmen a číslic, jako například aaabbb, 123321 a podobně.
- Libovolný z výše uvedených výrazů, zapsaných pozpátku.
- Libovolný z výše uvedených výrazů, před nebo za kterým je jediná číslice (například

heslo5, 4heslo).

- Jména sportovních klubů a hráčů.

Wordlist neboli seznam slov je jednoduchá množina slov, například běžná slova ze slovníku, jména sportovních klubů, odborné výrazy, slangové výrazy, jména a podobně; na Internetu je najdeme pro různé jazyky.

Útočníci zkoušejí tyto seznamy slov jako první krok při útoku; hledají přitom účet, jehož heslo se dá z některého výrazu snadno odvodit. Pro jistotu zkoušejí také vkládat do slov číslice. A právě proto je nutné přijmout výše uvedenou část zásad.

Silná, správně vytvořená hesla můžeme naopak charakterizovat takto:

- Obsahují malá i velká písmena
- Obsahují číslice a interpunkční znaménka (například 0-9, !®#$%a&*()_+ I — =V<)G:V<>?,./)
- Mají délku nejméně osm alfanumerických znaků
- Nejsou tvořena žádným slovem z běžného slovníku, slangu, dialektu, odborné hantýrky apod.
- Nejsou odvozena ze žádných osobních údajů, jmen členu rodiny atd.

Takto vytvořená hesla se nesmí zapisovat na papír ani ukládat v elektronické podobě. Vytvářejte proto taková hesla, která si snadno zapamatujete; zkuste například vyjít z určité fráze, názvu hudební skladby nebo jiného slovního spojení a vhodně je přetvořit (třeba prvními písmeny a dalšími úpravami). [4]

Pro účty v systémech firmy si nevolte stejné heslo jako pro jiný, cizí systém (například pro osobní účet u poskytovatele Internetu, pro vstup do bankovního účtu, obchodování s cennými papíry atd.). Pokud možno nepoužívejte také stejné heslo u několika různých systémů, jiné heslo si například definujte pro vývojové oddělení a jiné pro běžnou podnikovou síť.

Hesla nikomu nedávejte k dispozici, ani administrativním pracovníkům či sekretářkám. Všechna hesla se považují za citlivé a důvěrné údaje firmy a je třeba s nimi takto i zacházet.

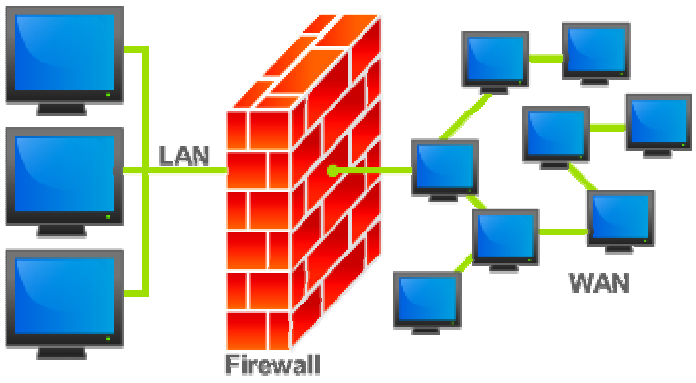
Následující věci jsou zakázány:

- NIKOMU neříkejte heslo po telefonu.
- Nezapisujte heslo do e-mailové zprávy.
- Neříkejte heslo svému nadřízenému.
- Nemluvte o svých heslech před druhými.
- Nenapovídejte nikomu ani formát hesla (třeba „celé jméno mé manželky").
- Nepište heslo na dotazníky či bezpečnostní formuláře.
- Nesdělujte heslo členům rodiny.
- V aplikacích nepoužívejte funkci „Zapamatovat si heslo“ (například Outlook, Netscape Messenger).

Uživatelé se vždycky snaží platná omezení a zásady obcházet, a ani zásady pro hesla nejsou žádnou výjimkou - kdo by byl nadšený z toho, že si musí pamatovat nějaká složitě konstruovaná hesla. Každý uživatel si tedy bude muset chtě nechtě zapamatovat nejen komplikované heslo, ale i celé tyto zásady, a řídit se jimi. Nezapomeňte, že zabezpečení hesel je prvním krokem v ochraně každé sítě, a proto je i pro zajištění bezpečnosti organizace jako celku důležité začít od hesel a od uživatelských postojů k nim.[1]

7 FIREWALL

Firewall je síťové zařízení a nebo software, jehož úkolem je oddělit sítě s různými přístupovými právy (typicky např.. Internet a Intranet) a kontrolovat tok dat mezi těmito sítěmi. Kontrola údajů probíhá na základě uplatňování pravidel, které stanoví podmínky a akce. Podmínky se stanovují pro údaje, které lze získat z datového toku (např. zdrojová, cílovou adresu, zdrojový nebo cílový port a různé jiné). Úkolem firewallu je vyhodnotit podmínky a pokud je podmínka splněna, provede se akce. Dvě základní akce jsou "povolit datový tok" a "zamítnout datový tok". Po provedení této akce firewall přestane paket zpracovávat. Existují však i jiné akce, které neurčují osud paketu a slouží např.. na logování hlaviček paketu, změnu hlaviček paketu a podobně. Další vlastností firewallu, která se často používá, i když nejde o filtrování, je schopnost překladu adres (Network Address Translation - NAT). NAT umožňuje měnit zdrojové a cílové adresy v paketech, čím se nejčastěji umožňuje komunikace se sítěmi s privátními adresami (např. 10.111.1.1/254). I překlad adres probíhá pomocí pravidel. Podle toho, na níž vrstvě firewall analyzuje síťový provoz, rozlišujeme v zásadě dva firewally: Aplikační proxy server a paketový filtr.



Obr. 5 – Činnost firewallu[14]

7.1 Pravidla firewallu

Základem každého filtrovacího pravidla je jedna nebo více podmínek, které umožňují vybrat paket. Pokud paket vyhoví podmínkám, provede se akce, která je součástí definice pravidla. Pokud je nesplní, pokračuje se ve vyhodnocovaní dalšího pravidla v řetězu pravidel. Pokud paket nesplňuje ani jednu podmínku, dostane se na konec řetězu pravidel a provede se akce, která je specifikována jako "standardní politika" (default policy).

S paketem lze provádět následující akce:

ACCEPT: paket bude akceptován
DROP: paket bude zahoděn. Odesílatel paketu se o tom ani nedozví
QUEUE: pošle paket na zpracování uživatelskému procesu
RETURN: přestane vyhodnocovat pravidla v tomto řetězu a pokračuje ve vyhodnocování pravidel v řetězu, s níž se sem dostal. (návrat z funkce nebo procedury)
jméno_řetězce: paket bude dále zpracovávat v řetězu pravidel "jméno_řetězce"
jméno_rozšíření: paket se předá na zpracování nějakému rozšíření (modulu) firewallu.
DNAT: umožní modifikovat cílovou adresu příchozího paketu
REDIRECT: umožní přesměrovat paket na samotný firewall (používá se např.. Při transparentním proxy)

8 OPERAČNÍ SYSTÉMY

Každý operační systém (Windows, Linux / Unix, MAC) ma svoje slabiny a neexistuje 100% bezpečný operační systém. Každý operační systém má své slabiny / díry, které dokáží pomoci k průchodu do operačního systému a způsobit pád operačního systému, případně celé sítě. Proto je nutné pravidelně aktualizovat operační systémy (instalovat bezpečnostní záplaty, které vydávají tvůrci operačního systému), což vede k lepšímu zabezpečení systému. O aktualizaci na platformě Windows se stará služba WSUS (Windows Server Update Services), která stahuje vybrané aktualizace a poskytuje jejich pracovním stanicím, serverům. Výhoda linuxových aktualizací je ta, že nevyžadují restartování systému jako je to třeba na platformě Windows.

9 VIROVÁ OCHRANA

Počítačový vir v oblasti počítačové bezpečnosti označuje program nebo kód, který se dokáže sám šířit bez vědomí uživatele. Aby se mohl množit, vkládá kopie svého kódu do jiných spustitelný soubor nebo dokumentů. Takový program se tedy chová obdobně jako biologický virus, který se šíří vkládáním svého genetického kódu do živých buněk. Analogicky se procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů tzv.. malware, škodlivého softwaru. Obecně se jako viry (nesprávně) označují i např. červi a jiné druhy malware.

Zatímco některé viry mohou být cíleně ničivé (např. mazat soubory na disku), mnoho jiných virů je relativně neškodných, popřípadě pouze obtěžujících. U některých virů se ničivý kód spouští až se zpožděním (např. v určitý den či po nakažení určitého počtu jiných hostitelů), což se někdy označuje jako (logická) bomba. Další negativní dopad virů je jejich samotná reprodukce, která zatěžuje počítačové systémy a obsazuje jejich zdroje.

Dnes jsou klasické počítačové viry na ústupu oproti červům a spywaru které se šíří prostřednictvím počítačových sítí, zejména internetu. Některé antivirové programy a další specializované programy se proto snaží chránit počítač i před jinými, nevirovými hrozbami.
Ochrana proti virům
Ochranu v naší firmě zajišťuje antivirový program od společnosti ESET, NOD 32. NOD32 je antivirový software od slovenské firmy Eset. Serverové verze jsou pro systémy Windows, Linux, FreeBSD, jakož i pro jiné platformy. Nástroje pro vzdálený přístup na mnohouživatelské instalace jsou k dispozici za příplatek.

NOD32 byl oceněn jako jeden z nejlepších antivirů v magazínu Virus Bulletin, kde současně dosáhl nejnižší chybovost. Používá Heuristická analýza v kombinaci s pravidelně aktualizovanou virovou databází. NOD32 vyniká v tzv.. Int-The-Wild virech. Čtvrtá generace umožňuje detekci malware, červů a trojanů.

Důležité vlastnosti antivirového systému NOD32:

- rezidentní skener
- skenování webových stránek (HTTP)

- skenování příchozí pošty (POP3)
- detekce malware pomocí vzorků a heuristické analýzy
- detekce adware a spyware
- skenování obsahu archivů, samorozbalovacích archivů a runtime archivů
- skenování obsahu dokumentů Microsoft Office
- skenování pošty uložené v Microsoft Outlook
- skenování pošty procházející přes Microsoft Exchange Server a Lotus Domino
- automatická aktualizace virové databáze z internetu
- administrátorská konzole[15]

NOD 32 je nastaven tak aby se spouštěl po spuštění systému. Aktualizace je nastavena na každou hodinu, aby měli uživatelé vždy aktuální verzi virové databáze. Dále jsou na internetové bráně nastavené stránky, na které uživatelé nemohou přistupovat (free maily, stránky s pornografickým obsahem, stránky, které poskytují nelegální stahování programů). Jedná se o stránky kde je riziko infiltrace vysoké.
Virové riziko sledujeme na stránce www.virovyradar.cz kde se nacházejí aktuální rizika infiltrace, které se šíří internetem.
Vypnutí programu NOD 32 je chráněno a je možné jen po zadání hesla (které běžný uživatel nezná a tak si nemůže svévolně vypnout antivirovou ochranu a vystavit počítač hrozbě).

10 ZÁLOŽNÍ ZDROJ UPS

Pro záložní zdroj se používá označení UPS (nepřerušitelný zdroj energie.) UPS slouží k bezpečnému uložení rozpracovaných úkolů v počítači. UPS nabízí neocenitelné služby. Pokud se v elektrické síti vyskytnou různé rušení, napěťové rázy, přepětí a poklesy napětí, o potřebnou filtraci nebo vyrovnání. V případě že napájení z veřejné sítě zcela selže, UPS zajistí napájení počítače a prostřednictvím komunikačního kabelu i jeho korektní vypnutí v době nepřítomnosti. Je třeba mít vždy na vědomí, že záložní zdroj ochrání připojené zařízení před nestabilitou, výpadky a rušením z napájecí sítě pouze s určitým stupněm spolehlivosti. To, co se potom může stát na trase mezi spotřebičem a záložním zařízením však záložní zdroj nijak neovlivní. S ohledem na skutečnost, že sám záložní zdroj je zařízení s určitou definovanou poruchovosti, je zřejmé, že je třeba systémy záložního napájení brát komplexně s ohledem na význam chráněných zařízení, s ohledem na servis, údržbu a pravidelné revize celého systému napájení i jednotlivých záložních zdrojů, s minimálními dopady na spolehlivost napájení připojených spotřebičů. Součástí komplexního řešení je pak v neposlední řadě přehlednost a management celého systému záložního napájení. UPS rozdělujeme na 2 typy: Smart UPS a obyčejné UPS.

Výhody:

• Záložní systém plní svou hlavní funkci spolehlivě chrání připojená zařízení.

• Jednoduchost a přehlednost systému záložního napájení

• Jednoduchá a v standardu obsažena možnost komunikace se zdroji UPS

Nevýhody:

• Omezená doba provozu daná kapacitou záložních baterií. Slouží pouze k regulérního ukončení a nastavení výchozí pozice pro opětovný rozjezd provozu. Není určen pro pracoviště s trvalým provozem.

• Nutná komunikace s nadřízeným systémem nebo signalizace. Záložní systém je většinou umístěn v prostorech bez trvalé obsluhy a bez jakékoli komunikace či signalizace se pouze oddaluje o pár minut výpadek, kdy nastane vyčerpání kapacity baterií.

• Systém není příliš vhodný pro zajištění nepřetržitých provozů. Vzhledem k údržbě systému je vhodný spíše pro provoz 5 dní v týdnu.

• Délka vedení mezi centrální UPS a samotným kritickým spotřebičům. Centrální UPS neochrání kritickou zátěž před manipulací v rozvaděčích (vypnutí jističe), přerušením

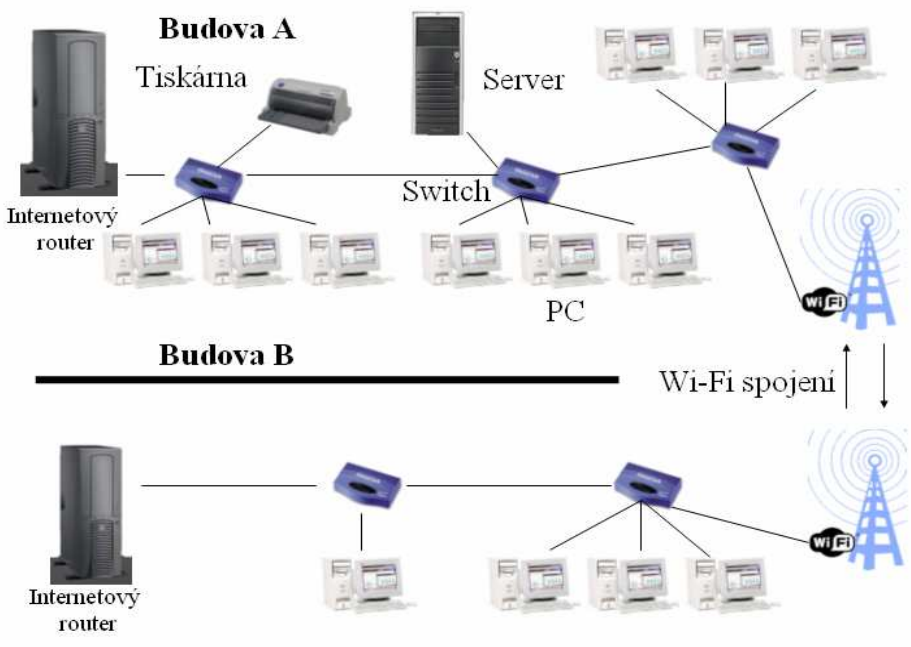
kabelu (zkrat) a před přechodovými jevy na zálohovaných rozvodech, přepětí.

• Pravidelné revize rozvaděčů a kabelových rozvodů znamenají vyřazení zařízení.[17]

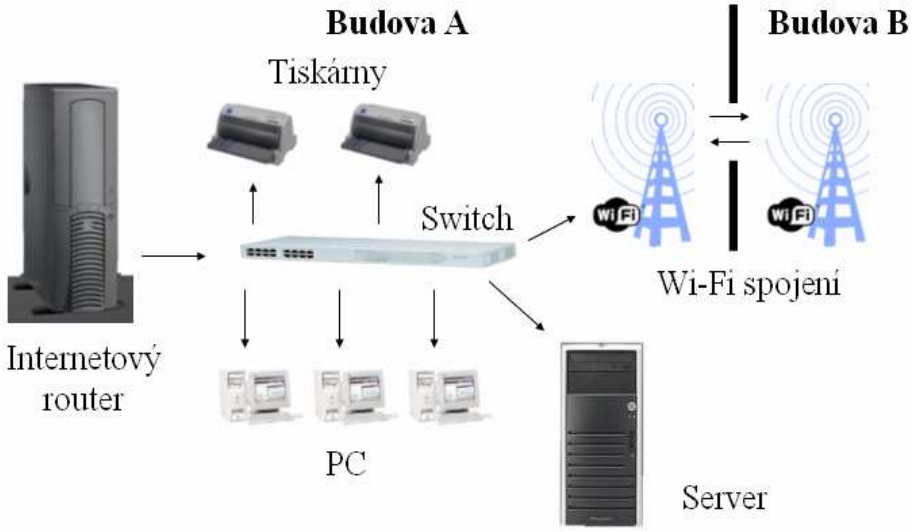
11 DOSAŽENÉ CÍLE

Cílem práce bylo vytvořit bezpečnou plně fungující firemní síť. Prvním mým krokem bylo celou síť přestavět z původního často kolizního a nijak neudržovaného stavu. Přestavění původní sítě na obr.6 na stávající řešení obr.7 znamenalo "přetahat" veškeré kabelové rozvody a zrušit původní strukturu sítě, kterou tvořilo několik switchů vzájemně propojených. Při poruše zařízení nebo kabelu nefungovala celá síť. Použité switche byly spíše určeny pro domácí použití a ne pro firemní účely. Síť vykazovala velkou chybovost, rychlost byla také omezena. O nepřehlednosti a způsobu zapojení ani nemluvím – najít v síti chybu a opravit ji vždy znamenalo nejen velkou časovou ztrátu, ale také ztrátu finanční. V síti neexistovala žádná správa dat, nebyly nastavené žádná přístupová práva a propojení budov pomocí wifi nebylo také nijak zabezpečeno. Situace byla tak vážná, že si kdokoliv z okolí při vyvinutí malého úsilí mohl prohlížet firemní data jako jsou učetní podklady, vnitřní normy, ale také mnohem důležitější data, například výkresovou dokumentaci, technologické postupy a v nejhorším případě data k bankovním účtům. Podobná situace byla i uvnitř firmy. Uživatelé firemních PC měli přístup prakticky kamkoliv. Bylo potřeba nastavit přístupová práva podle zaměření, vytvořit veřejné adresáře atd. V síti také chyběl záložní zdroj, to znamená, že při náhlém výpadku el. proudu se stala síť nefunkční a následky si dokáže každý z nás představit. Nové skutečně realizované řešení odstranilo všechny výše uvedené problémy. Hhlavní slabinu firemní sítě tj. propojení budov A a B pomocí wifi. Bylo rekonstruováno použitím novější technologií podporujicích protokol WPA2, který je oproti původnímu WEP bezpečnější. Původně používaná siť na frekvenci 2,4 GHz byla v této oblasti rušena, tím vznikaly komplikace jako kvalita připojení atd. Síť byla nahrazena modernější technologii 5 GHz která není tak náchylná na rušení. Bylo vypnuto směrové vysílání SSID a také byl použit filtr MAC adres. Jednotlivé uživatelské stanice byly nakonfigurovány tak, že k nim měl přístup pouze oprávněný uživatel. Firemní PC nyní požadují pro přihlášení heslo a jsou také zapnuty spořiče obrazovek chráněné heslem. V celé síti je nainstalován anitivirový software NOD 32, který chrání data před viry. Jsou nastavena určitá pravidla, které musí zaměstnanci dodržovat.Všichni pracovníci byli proškoleni v oblasti bezpečnosti dat a bylo jim vysvětleno, jak je bezpečnost firemních, ale také osobních dat důležitá. Tím však bezpečnost firemních dat pořád není stoprocentí. Vedení společnosti by mělo klást důraz na neustálé obnovování zabezpečení, co se týká hardwaru, softwaru ale také sociálního

inženýrství. Zabezpečení je široký pojem a mně se podařilo v naší firmě zavést alespoň standard, který je podle mého názoru nutný. Seznámil jsem vedení firmy i zaměstnance s hrozbami a prevencí proti nim. I přes časovou náročnost práce a při plném provozu firmy jsem až na malé vyjímky všechny požadavky splnil. Teď již zůstává na vedení firmy, aby byla dodržena stanovená pravidla a tím se i uchovala bezpečnost dat.



Obr. 6 – Původní řešení firemní sítě



Obr. 7 – Nové řešení firemní sítě

ZÁVĚR

Síť byla zabezpečena a bez problémů ověřena řadou programů. Hlavní prvky použité při stavbě byly metalická kabeláž kategorie a prvky propojení wifi. Server byl navrženy tak, aby výkonově vyhovoval počtu uživatelů v podniku. Během instalace se vyskytly pouze základní problémy. (špatné konektory přeseknuté kabely). Síť je funkční, stabilní a zabezpečená proti průnikům zvenčí a proti virové a spyware infiltraci.

Při komerční řešeních od Microsoftu si musíme dát pozor na přísné dodržování licenčních politik jinak jsme vystaveni možnému trestnímu stíhání za porušování autorských práv (jedna licence se dá použít jen jednou více násobné použití nepřipadá v úvahu, při některých typech licencí je licence vázána na určitou hardwarové část a nemůže migrovat). Při návrhu sítě jsem volil použití volně šiřitelný produktů tak i komerčních produktů tak, aby byla zachována plná funkčnost, bezpečnost a kvalita přenosu dat, a aby nevznikaly konflikty, nebo nefunkční stavy sítě. Rychlost sítě je 100 mb/s a při bezdrátových spojích 54 mb/s. Při kompletaci sítě dělal největší problém umístění některých částí ve velmi členitém terénu. Vedení společnosti bylo spokojeno s poskytnutým řešením. Počítačová síť je souhrn technických zařízení, které musí být nainstalovány správně, aby se dostavil výsledný efekt. Dále musí být dosažena vzájemná kompatibilita komponentů aby se docílilo maximální propustnosti sítě. Velký důraz je kladen i na kvalitu provedení spojů, neboť ty bývají většinou nejporuchovějším elementem v počítačové síti. Proto je vhodné mít měřicí přístroje, kterými si dokážeme ověřit bezvadnost spojů a vyvarujeme se nefunkčnosti hned po instalaci. Není vhodné volit komponenty od neznačkových výrobců ale třeba se zaměřit při návrhu pro podnikovou sféru na renomovaných výrobců, jejichž výrobky jsou ověřeny dlouholetým používáním (CISCO, 3COM, NETGEAR ....). Samotná hardwarová instalace může být bezchybná ale pokud není síť i dostatečně dobře nakonfigurováno tak nikdy nelze dosáhnout výsledného efektu a plného výkonu zařízení. Musíme si uvědomit, že výpadek počítačové sítě ohrozí fungování podniku a tím i finanční ztrátu pro firmu, a proto bychom měli klást důraz i na zařízení, které napomáhají eliminovat některé výpadky sítě. Hlavně servery a switche by měly zůstat funkční i když nastane výpadek el. energie. V naší firmě jsem to vyřešil instalací záložních energetických zdrojů (UPS), které poskytnou energii nejméně 30 min při plném výkonu.
Rovněž je nutné mít síť zabezpečenou proti hackerskými průnikům a virovými infiltracemi

a proto je třeba školit uživatele, co si můžou dovolit a co je zakázáno. Při dodržování všech pravidel, které stanoví síťový administrátor, by měla síť v konečném důsledku pracovat správně.

Síť, kterou popisuji v mé diplomové práci, jsem navrhl a následně dokončil pro firmu, v níž pracuji Trefal spol. s r.o. Příčinou modernizace sítě byla podmínka zvětšit rychlost zastaralé sítě pro využívání nových informačních technologií, které se mají zavádět v podniku (informační systém QI). Hlavním požadavkem, který byl kladen na síť byl ten, aby byla co v největší míře zajištěna bezpečnost, rychlost a kvalita přenášených dat. Při navrhování jsem se snažil zaměřit na moderní technologie, které se používají běžně ve světě a jsou zárukou kvality a bezpečnosti a bezproblémové instalace a dalšího rozvoje sítě. Nastavení sítě a serveru byly řešeny tak, aby poskytovaly co největší bezpečnost pro podniková data, a aby zamezil neoprávněný přístup do sítě. Síť je navržena tak, aby se dala plně řídit a tím v co nejkratší době lokalizovat a následně odstraňovat vzniknuté chyby. Síť se v praxi osvědčuje jako bezproblémová a plně funkční. Výpadky vznikají minimální a jsou snadno odstranitelné. Síť a server byly dimenzovány tak, aby poskytovaly určitou rezervu a kapacity pro případné rozšiřování sítě z důvodu stálé modernizace podniku a výrobních možností, při nichž je využití informačních technologií nezbytné.

CONCLUSION

The net was secured and with no problems tested by number of programs. Main elements used for the net construction were metallic wiring category and elements for wifi connection. The server was designed to be suitable performance wise for number of user in the company. During the installation appeared only basic problems (wrong connectors, cut wiring etc) The net is functioning, stable and secured against penetration from the outside, against viruses and spyware infiltration.

When using commercial solutions from Microsoft we have to be careful about strict abiding with licensing politics otherwise we could be exposed to possible criminal prosecution for copyright violation (one license can only be used once, multiple usage is out of question; some types of licenses are bound to certain hardware part and cannot migrate) When projecting the net I have chose use of shareware the way full functionality, security and quality of data transfer was kept and didn´t arise any conflicts or non functioning states of the net. Speed of the net is 100 mb/s and for wireless connections it is 54 mb/s. The biggest problem during the net completion was placement of some parts in very broken terrain. Company management was satisfied with proposed solution. Computer net is complex of technical units which must be installed correctly to achieve consequential effect. Furthermore, mutual compatibility of components must be reached in order to contrive maximal net transmission. A huge stress is laid on the quality of connection implementation, because these are usually most defective part in the computer net. That is why it is useful to have measuring devices which are able to check impeccability of connections and will prevent malfunction right after installation. It is not advisable to use components from unbranded manufacturers but it is important when preparing the solution for business sphere to concentrate to renowned manufacturers whose products are tested by long time usage (CISCO, 3COM, NETGEAR ....). Hardware installation itself can be flawless but if the net is not well enough configured there will never be reached consequent effect and full performance of the facility. We have to take in the account that the drop out of computer net will jeopardize function of the company and also it can mean financial loss for the company, so we should insist on facilities which help to eliminate some of net drop outs. Mainly servers and switches should stay working even during the electricity drop out. In our company I have solved this by installation of backup energy servers (UPS), which

will give the energy for at least 30 minutes while working in full swing. It is also necessary to have the net secured against hacking penetration and against virus infiltrations so that is why it is needed to have users trained in what is allowed and what is forbidden. When keeping all the rules which are given by net administrator the net should be working correctly.

The net I´m describing in my graduation thesis was designed and subsequently completed for the Trefal spol. s. r.o., company where I currently work. The reason for updating the net was the condition to increase the speed of outworn net in order to use new informative technologies, which should be implemented in the company (information system QI). The main request for this net was ensuring of security, speed and quality of transferred data at the most. When designing the solution I have tried to aim to modern technologies, which are commonly used all around the world and are the warranty of quality and security and smooth installation and further net development. Setting of the net and the server were solved to give highest possible security for company data and also the way to prevent unauthorized access to the net. The net is designed to be fully operated and that way able to locate and sequentially remove accrued errors. In the practice the net seems to be without problems and is fully functional. Drop out arise minimally and are easily removable. The net and the server were seized the way to give certain reserves and capacity for possible expansion of the net for the reason of constant modernization of the company and its manufacturing possibilities for which is needed use of informative technologies.

SEZNAM POUŽITÉ LITERATURY

[1] LEE, Barken. *Jak zabezpečit bezdrátovou síť Wi-Fi*. Jiří Veselský. 1. vyd. [s.l.] : Computer press, 2004. 174 s. ISBN 80-251-0346-3.

[2] NORTHCUTT, Stephen, et al. *Bezpečnost počítačových sítí*. [s.l.] : [s.n.], 2005. 592 s. ISBN 80-251-0697-7.

[3] LUDVÍK, Miroslav, ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí.* 1. vyd. [s.l.] : Computer Media, 2008. 98 s. ISBN 80-86686-35-3.

[4] THOMAS, M. *Zabezpečení počítačových sítí -- bez předchozích znalostí*. David Krásenský. 1. vyd. [s.l.] : Computer press, [2005]. 338 s. ISBN 80-251-0417-6.

[5] LOCKHART, Andrew. *Bezpečnost sítí na maximum*. Jiří Veselský. 1. vyd. [s.l.] : Computer press, [2007]. 276 s. ISBN 80-251-0805-8.

[6] SMITH, Ben, et al. *Zabezpečení systému a sítě Microsoft Windows*. [s.l.] : Computer press , 2005. 700 s. ISBN 80-251-1260-8.

[7] SIMMONS, Curt, CAUSEY, James. *Mistrovství v sítích Microsoft Windows XP*. [s.l.] : Computer Press, 2005. 624 s. ISBN 80-251-0583-0.

[8] ODOM, Wendell. *Počítačové sítě* . [s.l.] : Computer Press, 2005. 384 s. ISBN 80-251-0538-5.

[10] *RJ- 45: Zapojení* [online]. [cit. 2009-4-27]. Dostupný z WWW:

<http://encyklopedie.seznam.cz/heslo/497824-rj-45#Zapojen.C3.AD_kabel.C5.AF>.

[11] *Swith: switch* [online]. [cit. 2009-1-15]. Dostupný z WWW:

<http://encyklopedie.seznam.cz/heslo/178107-switch>.

[12] *Počítačové sítě: Referenční model ISO/OSI* [online]. [cit. 2009-5-7]. Dostupný z WWW: <http://dmp.wosa.iglu.cz/?strana=iso>.

[13] *Jaké jsou k dispozici metody zabezpečení bezdrátové sítě?* [online]. [cit. 2009-4-18]. Dostupný z WWW:

<http://windowshelp.microsoft.com/Windows/cs-CZ/Help/b385cc8a-af25-489e-a82e-decf6df26b681029.mspx#EO>.

[14] *BEZPEČNOST: wifi* [online]. [cit. 2009-2-10]. Dostupný z WWW:

< http://www.lupa.cz/clanky/bezpecnost-wifi-zalezi-jen-na-vas/>.

[15] *Firewall: firewall* [online]. [cit. 2009-5-12]. Dostupný z WWW:

< http://encyklopedie.seznam.cz/heslo/128845-firewall>.

[16] *NOD 32: Eset* [online]. [cit. 2009-4-1]. Dostupný z WWW: <http://www.eset.cz/produkty/eset-smart-security-business-edition>.

[17] *Datové sítě LAN: Napájení* [online]. [cit. 2009-5-1]. Dostupný z WWW: <http://www.enetsystem.net/index_201.htm>.

Seznam použitých symbolů a zkratek

WLAN	Wireless local Area Network.
LAN	Local Area Network.
PC	Personal computer.
MAC	Media access control
IP adresa	Internet protocol
WAP	Wireless Application Protocol
AP	Access point
Ad-hoc	Přímé rádiové spojení
WiFi	Standard pro lokální bezdrátové sítě
WEP	Wired Equivalent Privacy
TCP/IP	Komunikační protokol
CRC	Cyclic redundancy check
DoS	Denial of Service
IT	Information Technology
SSID	Service Set Identifier
ARP	Address Resolution Protocol
HTTP	Hyper Text Transfer Protocol
IEEE	Institute of Electrical and Electronics Engineers
RC4	Šifrovací metoda
VPN	Virtual private network
MD5	Message Digest algorithm 5
PKI	Public Key Infrastructure
ISDN	Integrated Services Digital Network

SEZNAM OBRÁZKŮ

Obr. 1 - Označení pinů na konektoru a způsoby zapojení……..11

Obr. 2 – OSI model……..……13

Obr.3 - Vrstvené zabezpečení sítě…… ……..17

Obr. 4 - Ověření pomocí funkce NetworkLogin 802.1x…… ……31

Obr. 5 – Činnost firewallu…… …… ……48

Obr. 6 – Původní řešení firemní sítě…… ……56

Obr. 7 – Nové řešení firemní sítě…….56

SEZNAM TABULEK

Tabulka 1. - rozdíl server/pracovní stanice……35