Univerzita Pardubice

Fakulta ekonomicko-správní

Obrana proti neoprávněnému získávání dat z firemní nebo domácí počítačové sítě

Jana Pochylá

Bakalářská práce
2014

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2014/2015**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Ing. Jana Pochylá**
Osobní číslo:	**E12690**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Obrana proti neoprávněnému získávání dat z firemní nebo domácí počítačové sítě**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Jakým způsobem lze nyní získávat data z firemní nebo domácí počítačové sítě. Jaká je možná obrana proti takovýmto útokům. Uvažovat bezdrátovou síť, drátovou síť a případně žádnou síť (tj. samostatný počítač). Ekonomické výhody a nevýhody. Sestavení vhodně obecného manuálu pro firmu, domácnost či státní správu - jak realizovat zabezpečení na vhodné úrovni, jaké budou náklady, jak lze kontrolovat, že obrana funguje a případně jak detekovat útok a jak se mu bránit.

Rozsah grafických prací:

Rozsah pracovní zprávy: **cca 35 stran**

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

Seznam odborné literatury:

1. **HORÁK, Jaroslav, KERŠLÁGER, Milan. Počítačové sítě pro začínající správce. Brno: Computer Press, 2006. 211 s. ISBN 80-251-0892-9.**
2. **PUŽMANOVÁ, Rita. Bezpečnost bezdrátové komunikace. Praha: Computer Press, 2005. 184 s. ISBN 80-251-0791-4.**
3. **SPURNÁ, Ivona. Počítačové sítě praktická příručka správce sítě. Kralice na Hané: Computer Media, 2010. 180 s. ISBN 978-80-7402-036-0.**
4. **DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer press, 2004. 200 s. ISBN 80-251-0106-1.**

Vedoucí bakalářské práce: **Ing. Martin Novák**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. října 2014**

Termín odevzdání bakalářské práce: **30. dubna 2015**

L.S.

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

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 1. října 2014

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracovala samostatně. Veškeré literární prameny a informace, které jsem v práci využila, jsou uvedeny v seznamu použité literatury.

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

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně.

V Pardubicích dne 27. dubna 2015 Jana Pochylá

PODĚKOVÁNÍ:

Tímto bych rád poděkovala svému vedoucímu práce Ing. Martinu Novákovi za jeho/její odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce.

ANOTACE

Tato práce bude sloužit čtenářům pro pochopení základních prvků ochrany dat v počítačové síti. Po přečtení by měl být čtenář schopen nastavit si základní prvky sloužící k ochraně dat před útočníky na svém vlastním počítači nebo v rámci malé počítačové sítě.

KLÍČOVÁ SLOVA

Obrana dat, počítačová bezpečnost, šifrování, autentizace, antivirový program)

TITLE

Defense against unauthorized data retrieval from home or business network.

ANNOTATION

This work will serve readers for understanding of basic elements of data protection in computer network. After reading this bachelor thesis the reader should be able to set basic elements which are destined for data protection on a home computer or within small computer network.

KEYWORDS

Data defense, computer security, encryption, authentization, antivirus

OBSAH

ÚVOD 8

1 POČÍTAČOVÁ SÍŤ 9

1.1 Rozdělení sítí 9

1.2 Prvky sítí 9
1.2.1 Hardwarové prvky 10
1.2.2 Softwarové prvky 11

2 ZABEZPEČENÍ DAT 12

2.1 Fyzické mechanismy bezpečnosti 12

2.2 Hardwarové mechanismy bezpečnosti 13

2.3 Administrativní mechanismy bezpečnosti 13

2.4 Softwarové mechanismy bezpečnosti 13

3 HROZBY POČÍTAČOVÉ BEZPEČNOSTI 14

3.1 Útočníci 14

3.2 Druhy útoků 14
3.2.1 Pasivní útoky 14
3.2.2 Aktivní útoky 15
3.2.3 Útoky na dostupnost služeb 15
3.2.4 Útoky na převzetí moci 15

4 OCHRANA DAT 16

4.1 Autentizace 16
4.1.1 Autentizační metody 17
4.1.2 Autentizační protokoly 18
4.1.3 Útoky na autentizační protokoly 19

4.2 Šifrování 19
4.2.1 Symetrické a asymetrické šifrování 19
4.2.2 Útoky na šifrovací algoritmy 20
4.2.3 Šifrování v MS Windows 21

4.3 Ochrana proti škodlivému softwaru 21

4.4 Firewall 23

4.5 Zabezpečení používaných protokolů 24
4.5.1 Vzdálená správa - Telnet a SSH 24
4.5.2 Přenos souborů – FTP a SecureFTP 25
4.5.3 Web – HTTP a HTTPS 25
4.5.4 Elektronická pošta 25

4.6 Zabezpečení dat u bezdrátové sítě 25
4.6.1 WEP 26
4.6.2 IEEE 802.11i 26

4.7 Virtuální privátní síť 27

4.8 Zálohování 29

5 POKYNY K VYTVOŘENÍ ZABEZPEČENÉ DOMÁCÍ POČÍTAČOVÉ SÍTĚ ... 30

5.1 Výběr potřebného hardwaru 30

5.2 Zásady zabezpečení sítě 31

5.3 Zásady počítačové bezpečnosti 31

5.4 Zásady bezpečného chování 32

6 NÁVRH DOMÁCÍ POČÍTAČOVÉ SÍTĚ 34

6.1 Ochrana sítě před útoky 39
6.1.1 Router 39
6.1.2 Firewall 41
6.1.3 Ochrana proti škodlivému softwaru 43
6.1.4 Správa uživatelských účtů 44
6.1.5 Šifrování 44
6.1.6 Virtuální privátní síť 46
6.1.7 Zálohování dat 48

ZÁVĚR 49

POUŽITÁ LITERATURA 50

SEZNAM PŘÍLOH 54

SEZNAM TABULEK

Tabulka 1: Srovnání WEP, WPA a WPA2 27
Tabulka 2: Odolnost proti útokům na počítačové sítě 27
Tabulka 3: Srovnání routerů 35
Tabulka 4: Kritéria rozhodování 35
Tabulka 5: Rozhodovací tabulka 36
Tabulka 6: Náklady na domácí počítačovou síť 39

SEZNAM ILUSTRACÍ

Obrázek 1: Jednoduchá počítačová síť 10
Obrázek 2: Autentizační protokol PAP 18
Obrázek 3: Autentizační protokol CHAP 18
Obrázek 4: Firewall 23
Obrázek 5: Hardwarový firewall 23
Obrázek 6: Znázornění vzdáleného přístupu 28
Obrázek 7: VPN pro spojení pracovišť 28
Obrázek 8: Logické schéma sítě 34
Obrázek 9: Brainstormingový model 36
Obrázek 10: Hierarchický model 36
Obrázek 11: Porovnání variant 37
Obrázek 12: Porovnání variant dle jednotlivých kritérií 37
Obrázek 13: Nastavení zabezpečení na routeru Netgear R6300-100PES 41
Obrázek 14: Nastavení firewallu 42
Obrázek 15: Nastavení povolení programů 42
Obrázek 16: Windows Defender 43
Obrázek 17: Šifrování složky pomocí EFS 45
Obrázek 18: Šifrování dat pro více uživatelů 46
Obrázek 19: Pokročilé nastavení VPN 47
Obrázek 20: Připojení k NAS serveru přes VPN 47
Obrázek 21: SWOT analýza autentizace znalostí ..... - 55 -
Obrázek 22: SWOT analýza autentizace vlastnictvím ..... - 56 -
Obrázek 23: SWOT analýza autentizace vlastností ..... - 57 -

SEZNAM ZKRATEK A ZNAČEK

AAA	Authenication, Authorization, Accounting
AHP	Analyticko-hierarchická metoda
BCM	Business Continuity Management
CDP	Critical Decision Plus
EAP	Extensible Authentication Protocol
EAS	Advanced Encryption Standard
EFS	Encryption File System
FEK	File Encryption Key
FTP	File Transfer Protocol
HTTP	HyperText Ttransfer Protocol
LAN	Local Area Network
MAN	Metropolitan Area Network
NAS	Network Attached Storage
OS	Operační systém
PGP	Pretty Good Privacy
SSH	Secure Shell
SWOT	Analýza silných a slabých stránek, příležitostí a hrozeb
TKIP	Temporal Key Integrity Protocol
UTM	Unified Threat Management
VPN	Virtuální privátní síťě
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
WPA	WIFI Protected Access

ÚVOD

Předmětem této bakalářské práce je obrana dat v počítačové síti. Cílem práce je poskytnout přehled o možných způsobech, jak se bránit proti neoprávněnému získávání dat, zaměřuje se tedy na obranu před útoky, jejichž strůjci jsou lidé. Práce je zaměřena na pochopení základních prvků, jak je možné data chránit a jak tyto jednotlivé prvky fungují. Cílem je také poskytnout návod, jak si zabezpečit domácí počítačovou síť.

Na začátku práce jsou popsány jednotlivé prvky počítačové sítě, a to jak hardwarové, tak i softwarové. Dále jsou pak popsány jednotlivé mechanismy, které slouží k ochraně dat. Pro obranu dat neslouží pouze softwarové prostředky v rámci počítačové sítě, ale i fyzické, technické a administrativní mechanismy ochrany dat. Ve třetí kapitole jsou popsány také možné druhy útoků a také samotní útočníci.

Tyto teoretické znalosti jsou potom uplatněny při samotném návrhu domácí počítačové sítě. Návrh je rozdělen do dvou částí, v první části jsou popsány pokyny, na které je potřeba se zaměřit při vytváření zabezpečené počítačové sítě. Ve druhé části je pak popsáno nastavení jednotlivých prvků sloužící k zabezpečení počítačové sítě a praktický postup naplnění pokynů z první části.

1 POČÍTAČOVÁ SÍŤ

Počítačová síť je pojem pro propojení několika počítačů a sdílení hardwarových prostředků. Mezi hlavní důvody vytváření počítačových sítí je možnost sdílení a přenášení dat mezi uživateli sítě, a to bez potřeby přenášení dat za použití např. flash disků, možnost komunikace mezi jednotlivými počítači nebo sdílení hardwarových prostředků, jako je např. tiskárna nebo skener.

Základem počítačové sítě je tedy sdílení výpočetních prostředků, které jsou v síti k dispozici. Pod pojmem „sdílení“ se rozumí „dát něco k dispozici“ (ne se s někým o něco dělit). Sdílením se u počítačových sítí myslí proces, při němž počítač zapojený do sítě dává uživatelům ostatních počítačů k dispozici prostředky, které sám vlastní, a ostatní uživatelů mohou sdílené prostředky používat. [2]

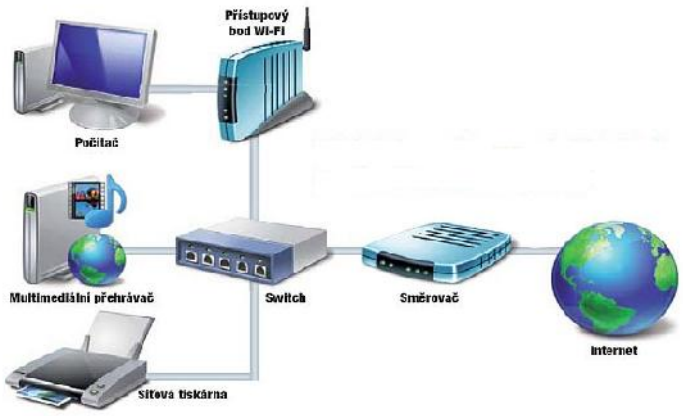
1.1 Rozdělení sítí

Nejčastější dělení sítí je dle jejich velikosti. Dle základního dělení lze rozlišit sítě LAN, sítě MAN a sítě WAN. Sítě LAN, neboli Local Area Network, jsou ty nejmenší sítě, které se rozprostírají pouze v rámci jednoho lokálního místa, jako je místnost, budova či podnik a zajišťují sdílení lokálních prostředků. Právě tímto typem sítě se věnuje tato bakalářská práce. [1, 2]

Sítě MAN, Metropolitan area Netwok, jsou sítě na území jednoho města. Nejrozsáhlejší typ sítě je WAN, neboli Wide Area Network, která se skládá z jednotlivých LAN a MAN sítí. Do této skupiny patří i světově nejrozšířenější síť, internet. [1, 2]

1.2 Prvky sítí

Počítačová síť je tedy souhrn hardwarových a softwarových prvků, které zprostředkovávají vzájemnou spolupráci počítačů. [1]



Obrázek 1: Jednoduchá počítačová síť

Zdroj:Upraveno podle [1]

Jedním ze základních prvků každé počítačové sítě je počítač. Každý počítač tak musí obsahovat hardware, kterými jsou síťové karty a software podporující síťovou spolupráci, aby byl počítač schopný vidět a používat vzdálené prvky sítě a byl schopný nabídnout ke spolupráci vlastní zdroje. V současné době jsou tyto síťové karty běžnou výbavou počítačů a softwarové vybavení je součástí ve všech používaných verzích operačních systémů Windows. Jednotlivé počítače jsou pak propojeny drátově (kabely) nebo bezdrátově (vzduchem). [1, 2, 4]

1.2.1 Hardwarové prvky

Do kategorie hardwarových prvků počítačové sítě patří:

- Síťová karta (adaptér);
- Přenosová, spojovací média;
- Aktivní síťové prvky; [1, 4]

Síťová karta je součástí základní desky počítače a vytváří rozhraní pro připojení k síti. Funguje na principu příjmu a vysílání signálů (elektrických nebo optických) z kabeláže nebo do kabeláže. [1, 4]

Základní prvkem **přenosových a spojovacích médií** je kabel. Rozlišujeme dva základní typy kabelů, a to metalické a optické kabely. Metalické kabely jsou založeny na měděném vodiči, kterým se přenáší elektrické signály. Nejpoužívanějším typem je kroucená dvojlinka skládající se z 8 vodičů ve 4 párech. U optických kabelů se k přenosu dat využívají světelné impulsy ve světlovodivých vláknech, tzv. optických vláken. Vlákna musí být minimálně dvě,

pro každý směr jeden. U bezdrátových sítí se pro přenos dat využívá vzduchu, kdy se vzduchem šíří elektromagnetické vlnění, které nahrazuje metalické kabely. [1, 4]

K fungování sítě však nestačí pouze jednotlivé počítače, které jsou propojené kabely nebo vzduchem. Je potřeba dalších prvků, které kontrolují činnost sítí, jako například výběr trasy nebo kontrola správnosti paketů a další, proto se jim říká **aktivní prvky**. Patří sem například zesilovač nebo switch, který poskytuje každému uzlu vlastní kanál, odděluje tak komunikaci stanic od zbytku sítě. Podobně jako switch funguje i bridge (most). Nejinteligentnějším aktivním prvkem je router (směrovač). Umožňuje propojit jednotlivé sítě, omezovat přístupové práva, budovat na něj firewally a připojit se přes něj na internet. [1, 4]

1.2.2 Softwarové prvky

Software dává síťovému hardwaru život a vzniká tak provozuschopná síť. Základním kritériem pro rozdělení síťového softwaru je úloha serveru. Podle toho rozlišujeme síť peer-to-peer a síť klient-server. [1, 2, 4]

1.2.2.1. Síť peer-to-peer

V případě sítě peer-to-peer jsou si všechny síťové stanice rovny. Jednotlivé počítače tak mezi sebou nabízejí své služby. Jedná se o levnější variantu, vhodnou ale spíše pro domácí nebo malé podnikové sítě. Není potřeba kupovat žádné síťové operační systémy, protože síť peer-to-peer je obsažena v MS Windows. [1, 4]

1.2.2.2. Síť klient-server

Server je počítač nebo program, který zabezpečuje služby pro klienty. U serveru se soustředí data, služby, údaje o uživatelích. Vzhledem k množství zpracovávaných dat musí být tento počítač kvalitní a rychlý. Navíc vyžaduje i speciální síťový operační program, který organizuje ukládání dat, přiděluje přístupové práva, a jak se bude počítačová síť chovat k jednotlivým uživatelům a prostředkům.

Mezi nejznámější a nejpoužívanější síťových operačních systémů patří:

- Microsoft Windows – nejnovější verze Windows Server 2012 R2;
- UNIX/Linux – např. Gentoo nebo Debian;
- Novell – Novell NetWare 6. [1, 4]

2 ZABEZPEČENÍ DAT

Informační technologie zasahují v současnosti do všech oblastí lidské činnosti a život bez nich si již nedokážeme představit. S jejich rostoucí úlohou v lidské společnosti, roste také množství informací a dat, které tyto technologie uchovávají, a roste také hodnota těchto dat.

Proto je také potřeba zabezpečit důvěrnost dat, což znamená zabezpečení přístupu k datům pouze těm, kteří k tomu mají oprávnění, a aby nebyly nekontrolovaným způsobem vyzrazeny. U domácí počítačové sítě je důležité zabránit proniknutí do sítě cizím uživatelům. Ve firmách je však potřeba zajistit i vnitřní bezpečnost, protože útok na počítačovou síť mohou provést i vlastní zaměstnanci.

K zabezpečení počítačové sítě neslouží pouze softwarové prostředky na počítači nebo v rámci sítě, ale kombinace více druhů bezpečnostních mechanismů, mezi které patří fyzické, hardwarové, administrativní a softwarové mechanismy. [34, 35]

2.1 Fyzické mechanismy bezpečnosti

Fyzické bezpečnostní mechanismy slouží k fyzické regulaci přístupu k datům, tedy fyzické zabezpečení sítě. Tyto mechanismy mají zabránit útočníkovi, aby se fyzicky dostal k počítačovému systému, kde by si potom mohl dělat, co chce. Všechna data jsou totiž vždy uložena na nějakém nosiči a právě přístup k těmto nosičům je důležité chránit. [34, 35]

Fyzickou ochranu lze rozdělit na čtyři oblasti, od všeobecných mechanismů ke konkrétním mechanismům pro jednotlivá zařízení, a to na:

- zajištění perimetru;
- kontrola přístupu;
- vnitřní bezpečnost;
- ochrana před vniknutím do zařízení. [34, 35]

Mechanismy k zajištění perimetru slouží k zjištění nepovoleného překročení hranice prostoru, ve kterém se nachází prvky počítačové sítě. Jedná se tedy o zajištění hranic a to pomocí například kamerových systémů, které se montují na plot či zeď. Mechanismy ke kontrole přístupu slouží k zajištění kontroly při vstupu do chráněné oblasti, jedná se například o vstupní brány, zajištění oken nebo dveří a další. Nejedná se o kontrolu přístupu k samotným datům. Mechanismy vnitřní bezpečnosti již slouží k ochraně prostorů, které obsahují citlivá data. Jedná se o zabezpečení jednotlivých místností, jako může být třeba serverovna.

Posledním, doplňkovým mechanismem, je ochrana před vniknutím do jednotlivých zařízení (např. počítačů). Jedná se o zámky na počítače, použití plomby a další. [34, 35]

2.2 Hardwarové mechanismy bezpečnosti

Hardwarové mechanismy bezpečnosti bývají také často označovány jako technické mechanismy bezpečnosti. Do této oblasti patří například šifrovače nebo autentizační a identifikační karty. Při hardwarovém šifrování odpadá nutnost instalace šifrovacího softwaru a tedy omezení vlivu na jeho výkon. Samotné šifrování zajišťuje elektronika pevného disku. Obslužný software je potřeba pro zapnutí nebo vypnutí bezpečnostních funkcí pevného disku. Může vykonávat další doprovodné funkce jako správu hesel, samotné šifrování však tento software neprovádí. [8, 34, 35]

2.3 Administrativní mechanismy bezpečnosti

Tyto mechanismy slouží k vytvoření systému opatření při nakládání s důležitými informacemi, jako je jejich evidence, zpracování, přenášení nebo ukládání. Jedná se tedy o stanovení administrativních pravidel při práci s daty. [34, 35]

Do této skupiny patří pravidla pro tvorbu hesel, právní normy, zákony, vyhlášky nebo předpisy. Základním dokumentem firmy upravující bezpečnost informací je bezpečnostní politika, ve které firma stanovuje, co chce chránit, proč to chce chránit, jak to chce chránit, jaké má mechanismy, aby zjistila, že je to opravdu chráněno a co se má udělat, pokud to tak není. [34, 35]

Někdy bývá úloha administrativní bezpečnosti zpochybňována, protože dodržování těchto pravidel je firma schopna si vynutit pouze na zaměstnancích, kteří jsou motivováni k jejich dodržování (loajálnost k firmě, snaha udržet si místo a další), což se od útočníka nedá očekávat. Toto však neplatí u utajovaných informací, které jsou upraveny zákonem. [34, 35]

2.4 Softwarové mechanismy bezpečnosti

Softwarové bezpečnostní mechanismy jsou někdy také označovány jako logické bezpečnostní mechanismy. Do této skupiny patří například řízení přístupu v daném operačním systému (OS), kryptografie, kódování, údržba programů, ochranné nástroje v OS, protokoly, hesla, autentizace a další. Jedná se tedy o ochranu dat v logické vrstvě. Této oblasti se blíže věnuje čtvrtá kapitola. [34, 35]

3 HROZBY POČÍTAČOVÉ BEZPEČNOSTI

V této kapitole budou rozebrány hrozby lidského faktoru, tedy úmyslné útoky lidí se špatnými úmysly.

3.1 Útočníci

Jednotlivé útočníky lze rozdělit do dvou základních skupin. Může se jednat o **interního útočníka**, tedy o osobu, která je připojená na danou počítačovou síť. Většinou se tedy jedná o zaměstnance u firemní počítačové sítě. Tento zaměstnanec tak může činit sám za sebe, nebo k takovéto škodlivé činnosti může být různými metodami nucen. Nejčastěji se jedná pouze o nechtěné nehody, které jsou způsobeny nedostatečnými znalostmi zaměstnanců v oblasti informačních technologií. Proti těmto útoků se lze bránit omezování přístupových práv tak, aby měli zaměstnanci přístup pouze k těm datům, které potřebují k výkonu své práce, zvyšováním loajality pro omezení úmyslných útoků a zvyšováním spolehlivosti pro neúmyslné útoky. [3, 5]

Druhou skupinou útočníků jsou **externí útočníci**, kteří na počítačovou síť útočí z vnějšku a nemají k ní fyzický přístup. Tento útočník se může nacházet kdekoliv na světě. Při útoku pak musí překonat jednotlivé bezpečností opatření sítě (firewall, bezpečnostní protokoly a další). U těchto útoků je horší vystopovatelnost útočníka a také složitější trestní stíhání. Možné způsoby ochrany proti těmto útočníkům a jejich útoky budou rozebrány v další části této kapitoly. [3, 5]

3.2 Druhy útoků

Podle toho, čeho se snaží útočník svým útokem dosáhnout, lze jednotlivé útoky rozdělit na aktivní útoky, pasivní útoky, útoky na dostupnost služeb a útoky na převzetí moci. [3, 5]

3.2.1 Pasivní útoky

Při těchto útocích se snaží útočník pouze získat data a to bez jakékoliv modifikace probíhající komunikace. Tím je také horší takovéhoto útočníka vystopovat. Jedná se tedy o odposlouchávání dat a útok na důvěrnost dat. K tomu lze využít několik prostředků. Jedná se například o trojského koně, pomocí kterého se útočníkovi podaří získat kontrolu nad nějakým komunikačním systémem. Například se může jednat o program, který zaznamenává stisky kláves. Druhým možným prostředkem je fyzický odposlech, pokud se útočníkovi podaří získat fyzický přístup k přenosovému médium. Může je jednat o umístění

odposlechového zařízení například k telefonu. Do této skupiny útoků patří také zjišťování informací z fyzické dokumentace. Je proto nutné dát si pozor i na informace, které skončí v odpadkovém koši a raději používat skartační zařízení. [3, 5]

Ochranou proti těmto útokům je používání šifrování, používání prvků počítačové ochrany, jako jsou antivirové programy nebo firewall a používání prvků fyzické zabezpečení. [3, 5]

3.2.2 Aktivní útoky

Při aktivních útocích se útočník nesnaží pouze o odposlech komunikace, ale i o její změnu. Může se jednat o změnu v přenášených datech, například změna čísla účtu při převodu peněz. Možnou ochranou je používání kontrolních součtů, pomocí kterých lze zjistit, zda se data při přenosu změnila. Další možnou formou je, že se útočník snaží předstírat, že je sám odesílatelem daných dat. Toho lze dosáhnout ukradením cizí identity. Obranou je zase používáním důsledné autentizace a zabezpečených komunikačních protokolů. [3, 5]

3.2.3 Útoky na dostupnost služeb

Jedná se o útoky, při kterých se útočník snaží buď úplně zničit přenášená data, nebo se snaží o přetížení systému tak, že zahltí systém neustálými požadavky. Systém tyto požadavky zamítá jako neoprávněné a tím je zahlcen natolik, že není schopný vyřizovat požadavky oprávněných uživatelů. Tento typ útoků se nazývá DoS – Denial of Service, útok na odmítnutí služeb. Obranou proti tomuto útoku je například rozdělení práce mezi více serverů nebo zablokování přístupu konkrétní IP adresy. Modifikací DoS je dDoS – Distributed Denial of Service, kdy útočník využívá k útoku v jeden okamžit velké množství počítačů. [3, 5]

3.2.4 Útoky na převzetí moci

Při těchto útocích se snaží útočník získat kontrolu nad jednou z komunikujících stran, může se jednat o jednotlivý počítač. Útočník tak získá přístup k datům na daném počítači, nebo jej může použít k dalšímu útoku. [3, 5]

Převzít moc může tak, že se podaří útočníkovi získat fyzický přístup k počítači, nebo může moc převzít pomocí vzdáleného útoku využitím programů, které se mu podaří nainstalovat na počítači například pomocí trojského koně. Další možností je využití chyb programů, které jsou na počítači již nainstalované. Proti těmto útokům se dá chránit zlepšením fyzického zabezpečení, zavedení autentizace, používání antivirových programů nebo zavedení pravidel chování na internetu. [3, 5]

4 OCHRANA DAT

Pro zabezpečení sítě před neoprávněným získáváním dat existuje několik možností, které se vzájemně prolínají a navazují na sebe. Důležité je zamezit neoprávněnému přístupu k datům. Jedná se tedy o ochranu fyzického přístupu k nosičům dat, o které bylo psáno ve druhé kapitole a ochrana logického přístupu k datům. Proto je důležité správně identifikovat a autentizovat uživatele.

Samozřejmě existuje možnost, že se přes tuto ochranu dostane neoprávněný uživatel, proto je potřeba data v síti šifrovat pomocí kódovacích prostředků. Pokud se tak do sítě dostane i neoprávněný uživatel, nebude schopný bez klíče zjistit obsah dat. Takto chráněná by měla být i data při jejich přenosu. Všechny zmíněné ochrany jsou zbytečné, pokud se data v síti přenáší v nezabezpečené podobě, mohou tak být odposlouchávána nebo modifikována. Je možností, že útočník nechce data pouze získat a přečíst, ale může se je pokusit zničit. Proto je důležitá ochrana dat i před zničením, například jejich zálohováním.

Díky připojení k internetu jsou počítačové sítě snadným terčem, útočník totiž nemusí ani nikam chodit, aby se do sítě dostal, a může tak sedět na opačné straně světa. Útočník tak může útočit na samotný počítač nebo odposlouchávat data při přenosu.

Podle útočníků lze rozdělit hrozby ochrany dat proti jejich neoprávněnému získávání ze sítě do tří hlavních oblastí.

1. Hrozby od jiného uživatele, který používá můj nebo jiný počítač v síti.
2. Hrozby od jiného uživatele, který přistupuje k síti z vnější sítě (internet).
3. Hrozby od programu, který se do sítě dostane z internetu a může se v něm pustit.

4.1 Autentizace

Na začátek je důležité vysvětlit si tří základní pojmy, které spolu souvisí a bývají často zaměňovány – identifikace, autentizace a autorizace. U identifikace uživatel tvrdí, že je skutečně tím, za koho se vydává (jedná se například o zadání jména a příjmení). Autentizace je ověření identity uživatele nebo entity v subsystému (např. zadáním hesla), tedy předložení důkazu, že je tou osobou, kterou tvrdí, že je. Autorizace je proces ověření práv pro přístup do určité oblasti, jedná se tedy o oprávnění pro určitou činnost (uživatel je přijat nebo odmítnut). Autentizace je tedy základním předpokladem pro autorizaci. Jedná se o dva na sebe navazující kroky. Systém tedy nejprve rozezná daného uživatele od ostatních a pak mu přidělí určitá práva. [3, 9]

Vlastní autentizace se skládá z několika fází. Nejprve je důležitá registrace uživatele, přiřazení autentizační informace a definice jeho přístupových práv. Ve druhé fázi je od uživatele získána autentizační informace (heslo, data z karty a další). V poslední fázi pak systém rozhodne o autorizaci uživatele. [3, 9]

4.1.1 Autentizační metody

Důležité je zvolit si vhodnou autentizační metodu, která poslouží jako ochrana před falšováním identity. Metoda by měla být dostatečně spolehlivá (určitý kompromis mezi chybou přijetí neoprávněného uživatele a chybou odmítnutí oprávněného uživatele), rychlá, důvěryhodná a nesmí být možné měnit zadání a výstupy autentizace. Autentizační metody znamenají způsob, jak je od uživatele získána autentizační informace. Mezi základní metody patří autentizace znalostí, vlastnictvím a vlastností. [3, 9]

Mezi nejstarší a nejrozšířenější způsob je autentizace znalostí, tedy že se ověřuje identita uživatele tím, že něco zná. Asi nejrozšířenější je zadání přihlašovacího jména a hesla. Může se jednat o alfanumerická hesla nebo numerické PINy. Tato metoda klade vysoké nároky na uživatele, který si toto heslo musí pamatovat. Důležité faktorem bezpečnosti hesla je také kvalita a jeho obměňování.

Druhou metodou je autentizace vlastnictvím. Při této metodě se využívá autentizační předmět, který musí uživatel vlastnit a při autentizaci předložit. Mezi nejpoužívanější formy autentizačních předmětů patří čipová nebo magnetická karta nebo USB Token. Mezi největší nevýhodu a rizikem použití této metody je právě nutnost daný předmět vlastnit a mít jej u sebe. Uživatel jej může ztratit nebo mu jej může kdokoliv ukrást. Daná osoba se tak může bez problémů dostat k potřebným datům. [3, 9]

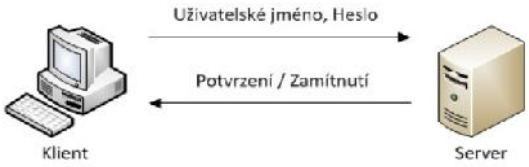
Třetí autentizační metodou je prokázání vlastností, tedy biometrická autentizace. Při této metodě se ověřuje pravost specifických fyziologických nebo biologických vlastností uživatele. Autentizační informace se získává z jedné z měřitelných charakteristik lidského těla, jako je otisk dlaně nebo prstu, obraz oční sítnice nebo duhovky, vzorek hlasu, písma nebo rytmus psaní na klávesnici. [3, 9]

Všechny metody mají své výhody a nevýhody, proto je vhodné nepoužívat pouze jednu metodu, ale jejich kombinaci. Příkladem může být výběr peněz z bankomatu, kdy je nutné předložit magnetickou kartu a zadat poté ještě PIN. V příloze A jsou zhodnoceny jednotlivé metody pomocí SWOT analýzy.

4.1.2 Autentizační protokoly

Vzhledem k tomu, že se během komunikace nachází uživatel obvykle fyzicky jinde, než systém, vůči kterému se autentizuje, byly vyvinuty autentizační protokoly, které slouží k zajištění přenosu dat mezi uživatelem k autentizačnímu serveru. [3, 10]

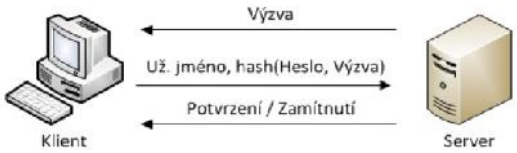
Mezi ty nejstarší autentizační protokoly patří **PAP**, kdy autentizaci iniciuje vždy uživatel na začátku spojení a protokol přenáší uživatelské jméno a heslo v otevřeném tvaru a jeho napadení tak není komplikované. [10]



Obrázek 2: Autentizační protokol PAP

Zdroj: [10]

Mezi další starší protokoly patří protokol **CHAP**. Autentizaci iniciuje vždy server a může probíhat opakovaně, nejen na začátku, ale i v průběhu spojení. Heslo není posíláno v otevřeném tvaru. [10]



Obrázek 3: Autentizační protokol CHAP

Zdroj: [10]

V současnosti se používá protokol EAP – Extensible Authentication Protocol. EAP představuje pouze obecný rámec pro autentizaci u modelu klient-server. Vlastní proces autentizace ale neřeší. Samotný proces autentizace (ověřovací metody) je definovaný až v jeho jednotlivých variantách, kterých je více jak 40. Mezi ty nejznámější patří EAP-MD5, EAP-TLS, EAP-FAST, EAP-PEAP, EAP-PKM. Díky tomu je možné vytvářet nové autentizační mechanismy na stejném autentizačním rámci EAP. Při použití EAP nejsou autentizační informace zahrnuty do informací, ale spíše k informacím. To umožňuje vzdáleným systémům vyjednat nutnou autentizaci ještě předtím, než přijmou nebo předají jakékoli informace. [10]

Často se lze setkat s pojmem AAA protokoly (Authenication, Authorization, Accounting). Jedné se o komplexní protokoly, které zajišťují autentizaci, autorizaci a účtování a používá se spíše u větších počítačových sítí. Účtování znamená sledování využívání síťových zdrojů, jako množství přenesených dat nebo doba strávená v systému. Do této skupiny patří například RADIUS, Kerberos nebo Diameter. [10]

4.1.3 Útoky na autentizační protokoly

Útoků na autentizací protokoly existuje celá řada, ale mezi ty základní lze zařadit útok opakováním, útok ze středu, útok na hesla a útok na integritu zpráv.

Princip útoku opakováním spočívá v odposlechu části komunikace mezi autentizačními stranami a použití těchto informací. Může se jednat o odposlech komunikace obsahující heslo. V případě útoku ze středu je útočník mezi komunikujícími stranami a celou komunikaci kontroluje. Pro uživatele se tak útočník jeví jako autentizací server a autentizací server považuje útočníka za uživatele. Při útoku na hesla se snaží útočník různými možnosti zjistit uživatelovo heslo, například hrubou silou nebo slovníkovým útokem. Útok na integritu zpráv spoléhá s nedokonalým návrhem autentizačního protokolu, kdy chování protokolu nemusí být pro určité situace definována, čehož může útočník využít. [3]

4.2 Šifrování

Šifrování je součást vědy, která se nazývá kryptologie. Kryptologie se skládá z kryptografie (šifrování), která se zabývá šifrovacími algoritmy a kryptoanalýzou, která se tyto šifrovací algoritmy snaží prolomit. [3]

Principem šifrování je převod otevřeného textu (v čitelné podobě) do šifrovaného textu, který je nečitelný. Šifrování se používá pro zajištění důvěrnosti dat, tedy aby si data nemohl přečíst někdo nepovolaný. I při zcizení dat to automaticky neznamená jejich prozrazení. Šifrování se používá pro ochranu dat na počítači, ke kterému mohou získat přístup i jiné osoby, buďto přímo z počítače nebo ze sítě či internetu, ale i při přenosu dat. [3]

4.2.1 Symetrické a asymetrické šifrování

Rozlišují se základní dva typy šifrování – symetrické a asymetrické. U symetrického šifrování používají obě strany komunikace stejný klíč a to jak k zašifrování, tak i dešifrování textu. Nevýhodou je neúměrný nárůst počtu klíčů při růstu komunikujících stran a s tím také rostou náklady na správu. Při komunikaci tří je potřeba tří klíčů, při čtyřech je to šest klíčů atd. Při komunikaci *n* stran, je počet potřebných klíčů dán rovnicí n(n-1)/2. [3, 12]

Proto byly vyvinuty asymetrické algoritmy, které využívají dvojici klíčů – soukromý a veřejný klíč. Každý z komunikujících stran má tedy tuto dvojici klíčů, kdy soukromý klíč uchovávají v tajnosti a veřejný klíč poskytnou všem, se kterými chtějí komunikovat. Pokud odesílatel chce poslat zprávu, zašifruje ji veřejným klíčem příjemce, který ji rozšifruje použitím svého soukromého klíče. Zpráva tak není šifrována a dešifrována pouze jedním klíčem. Princip asymetrického šifrování se používá i u digitálního podpisu. [3, 12]

U asymetrického šifrování je snazší správa klíčů, protože každý se musí postarat o bezpečné uložení svého soukromého klíče. Celkový počet klíčů se rovná dvojnásobku počtu komunikujících stran. [3, 12]

Symetrické šifrování je však rychlejší a i délka klíče je menší jak u asymetrického šifrování. Symetrické šifrování si vystačí se 128 bitovým klíčem, asymetrické šifrování potřebuje pro zajištění stejné bezpečnosti 1024 bitů. [3, 12]

V praxi se lze setkat s kombinací symetrického a asymetrického šifrování. V tom případě se vygeneruje před šifrováním textu náhodné číslo, relační symetrický klíč, kterým se zašifruje hlavní text. Samotný relační klíč se zašifruje pomocí asymetrického algoritmu a zašifrovaný symetrický klíč je poslán spolu se zašifrovaným textem. Příjemce pak nejprve dešifruje symetrický klíč svým asymetrickým klíčem a tímto dešifrovaným klíčem pak dešifruje celý text. Tak se podaří odstranit nevýhodu symetrického šifrování (velké množství klíčů) i asymetrického šifrování (příliš velká časová náročnost šifrování u rozsáhlých textů). [3, 12]

4.2.2 Útoky na šifrovací algoritmy

Luštěním šifrovací algoritmů se zabývá část kryptologie, kryptoanalýza. Cílem je získání samotného klíče. Není cílem získat šifrovací algoritmus, protože ten není předmět utajení a v současnosti jsou nejčastěji používané šifrovací algoritmy i veřejně známé. [3]

Jednou z metod zjišťování klíčů je útok hrubou silou. Útočník používá výkonný systém a snaží se o dešifrování textu postupným zkoušením všech možností, kombinace znaků nebo může procházet všechna známá slova, tzv. slovníkový útok. [3]

Další možností je, že má útočník k dispozici několik šifrovaných textů, které byly šifrovány stejným algoritmem a stejným klíčem a snaží se je převést do otevřeného textu. Podobnou možností je, když se útočníkovi podaří získat jak zašifrované zprávy, tak i stejné zprávy v otevřeném textu. Útočník se v tomto případě snaží získat klíč. [3]

Lze použít i frekvenční analýzu, která využívá toho, že jednotlivá písmena abecedy se vyskytují ve slovech s určitou frekvencí, které se využívá při rozluštění textu. Při luštění se ne vždy musí použít informačních technologií, je možné získat klíč i od samotného vlastníka pomocí různých přesvědčovacích metod (úplatek, sociotechnika, výhružky, mučení). [3]

4.2.3 Šifrování v MS Windows

Jednou ze základních možností pro šifrování v MS Windows je EFS – Encrypting File Systém. Tato technologie je součástí systému Windows verze 2000 a novější. [13]

EFS zajišťuje šifrování na úrovni dat, takže pokud se útočníkovi podaří se fyzicky dostat k datům, není schopný je bez klíče přečíst. Pomocí této technologie lze samostatně šifrovat zvolené soubory a složky. EFS pracuje na kombinování symetrického a asymetrického šifrování. Samotná dat (soubory) jsou šifrována symetricky, kvůli vyšší rychlosti. Pro šifrování generuje vždy operační systém nový šifrovací klíč FEK – File Encryption Key, který je v zašifrované podobě (asymetrickým šifrováním) uložen spolu se souborem. Tento klíč uživatel nezná a ani jej znát nepotřebuje. FEK se šifruje veřejným klíčem uživatele a dešifruje se privátním klíčem. Jako veřejný klíč slouží certifikát. Jedná se o soubor, který obsahuje tento veřejný klíč, plus další doplňující informace. Tyto certifikáty jsou veřejné a v systému dostupné. Každý uživatel může tento certifikát získat po prvním zašifrování libovolného souboru. [5, 13, 16]

4.3 Ochrana proti škodlivému softwaru

Souhrnný název pro programy, jejichž účelem je škodit, se nazývají škodlivý software, nebo také anglicky malware. Do této skupiny patří počítačové viry, červi, trojské koně, spyware nebo Spam a další. A čím tedy tyto programy škodí? To se liší podle jednotlivých druhů těchto programů. Ty nejmírnější pouze zobrazují nevyžádaný text, na horší naopak dokážou smazat celý harddisk nebo provádějí změny na počítači, kterých si uživatel nemusí hned ani všimnout. [3, 18]

Nejznámějším druhem malware je virus. Většinou se jedná o spustitelný program nebo soubor, který ke svému šíření potřebuje hostitele. Počítačový virus se tedy šíří tak, že se nakopíruje do jiného počítačového programu nebo do systémových oblastí disků. [3, 18]

Červ oproti viru nepotřebuje ke svému šíření hostitele a je schopný šířit se sám, například tím, že se odešle jako příloha u e-mailu. Červ se tedy šíří pomocí sítě a ne kopírováním

se do jiných souborů. Může ke svému šíření využívat hostitelský soubor, ale ten se nemění. [3, 18]

Další typ škodlivého programu je trojský kůň, který kromě činnosti, ke které je určen, vykonává bez vědomí uživatele i další činnost, jako například zjišťuje heslo, maže soubory nebo zjišťuje, které stránky na internetu uživatel otvírá. Trojský kůň se oproti viru a červu dále nereprodukuje. [3, 18]

Určitým druhem trojského koně je i spyware a adware. Adware je program, který zobrazuje nevyžádanou reklamu. Spyware naopak shromažďuje informace o uživateli, jako používané hesla, nejnavštěvovanější stránky na internetu, a může tyto informace odesílat přes internet. [3, 18]

Prostředkem k ochraně proti virům, červům, trojským koňům, spamům a mnohdy i spywaru slouží antivirové programy. Dokážou viry nalézt, ale většinou i nakažený soubor vyléčit. Všechny antiviry pracují na základě různých vyhledávacích metod. [3, 18]

Mezi tu nejběžnější metodu patří vyhledávání na základě charakteristických řetězců. Tato metoda je založená na předpokladu, že většina virů obsahuje určitou specifickou posloupnost znaků, signaturu, pomocí které lze virus jednoznačně identifikovat. Pokud antivirus nalezne danou posloupnost znaků v určitém souboru, označí jej jako napadený. [3, 18]

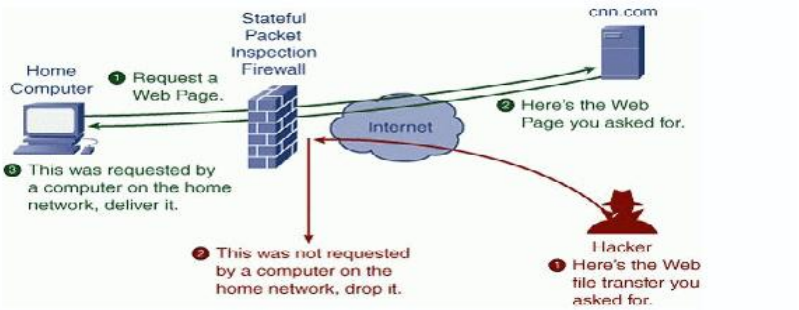
Další metodou je srovnávací metoda, nebo také metoda integrity. Při prvním spuštění antivirového programu si vytvoří informace o systému a při dalším spuštění srovnává aktuální stav s původním a podle změn detekuje virus. Tato metoda tedy pouze detekuje změnu systému, ale není schopná určit konkrétní virus. [3, 18]

Heuristická metoda prohledává a analyzuje texty programových souborů a vyhledává instrukce charakteristické pro viry. Touto metodou je tedy možné detekovat i viry, které jsou doposud neznámé a nebyly pro ně doposud vytvořeny signatury. Mezi další používané metody patří například metoda návnady, která odhaluje rezidentní souborové viry nebo rezidentní hlídač, který po spuštění počítače kontroluje vybrané typy souborů a e-maily a detekuje viry ještě dřív, než se spustí. [3, 18]

Nestačí si však antivirový program nainstalovat a spustit, je potřeba provádět pravidelnou antivirovou kontrolu a provádět pravidelnou aktualizaci databázi virů. Bohužel viry jsou vždy o krok před antivirovými programy, takže nemůžou zabezpečit stoprocentní ochranu. [3, 18]

4.4 Firewall

Firewall slouží jako softwarová nebo hardwarová ochrana před útoky na počítač nebo celou počítačovou síť z vnější sítě (internetu). Firewall je „ozbrojená stráž“ u přístupového bodu s vnější sítí. Umisťuje se mezi dvě sítě, většinou mezi vnitřní síť a internet. [3, 20]

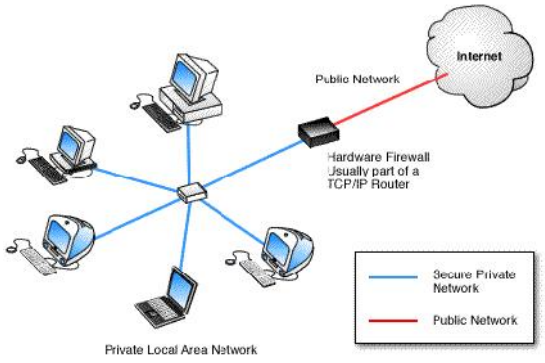


Obrázek 4: Firewall

Zdroj: [20]

Firewall zajišťuje ochranu před útoky hackerů nebo proti škodlivému malwaru a blokuje odchozí spojení, které by mohl malware vytvářet. Firewall se řídí příchozími a odchozími pravidly, které si firewall postupně vytváří. Tyto pravidla ale může nastavovat i samotný uživatel. Lze tedy říci, že se jedná o systém sloužící k řízení síťového provozu. [3, 20, 21]

U většiny počítačů je firewall již součástí operačního systémů, lze si jej však stáhnout jako samostatný software, někdy bývá i součástí antivirových programů. V rámci sítě bývá umístěn na serveru spolu s dalšími aplikacemi. Nerozlišuje se však pouze softwarový firewall, ale také hardwarový. Hardwarový firewall je většinou součástí síťového multifunkčního zařízení (router), které zajišťuje bezdrátovou komunikaci. Jedná se o softwarový firewall, který běží na vyhrazeném hardware. Výhodou softwarového firewallu však je, že většinou nabízí větší množství funkcí a zpravidla i nižší cenu. [3, 20, 21]



Obrázek 5: Hardwarový firewall

Zdroj: [20]

Obě varianty firewallů fungují na třech základních technologií používané u firewallů, které jsou - jednoduchý IP filtr, stavový IP filtr a proxy. [3]

Jednoduchý IP filtr blokuje internetový provoz. Zakazuje/povoluje provoz na jednotlivých portech (speciální číslo k rozlišení aplikace v rámci počítače) podle určité sady pravidel. Provoz, který není definovaný jako zakázaný, je povolený. Neumožňuje však analyzovat procházející dat. Vylepšením je stavový IP filtr, který je schopný sledovat navázané relace a propouští pouze ty pakety, které jsou součástí již povolené relace. Filtr tedy sleduje komunikaci vyšší vrstvy a povoluje průchod všech paketů směřující ven z vlastní sítě, ale opačným směrem pustí pouze pakety, které jsou zevnitř vyprovokované relací. Nejpokročilejší technologií je aplikační proxy. Jedná se o program pro jeden určitý protokol. Filtruje pakety podle toho, která aplikace s nimi pracuje, a na kterém portu. Podle toho pak programy mají, nebo nemají, přístup k jednotlivým portům. [3]

V rámci sítě je vhodné mít nejen jeden firewall na serveru (routeru) pro celou síť, ale mít i firewall na každém počítači. Zvyšuje to tak celkovou bezpečnost a je možné takto firewall nastavit podle požadavků uživatele a počítač je chráněný i mimo tuto síť. [3]

4.5 Zabezpečení používaných protokolů

Při přenosu dat se používají komunikační protokoly, existuje tak protokol pro příjem/odesílání elektronické pošty, protokol pro přenos souborů a další. A právě tyto protokoly je také potřeba zabezpečit, přesto se však lze setkat i s nezabezpečenou verzí těchto protokolů. [3]

4.5.1 Vzdálená správa - Telnet a SSH

Oba protokoly a zároveň i programy se používají pro zajištění připojení a práci na vzdáleném počítači přes internet. Jedná se o protokol typu klient-server. Pomocí tohoto protokolu se navazuje spojení s jiným počítačem na internetu. U protokolu Telnet je komunikace mezi serverem a klientem nezabezpečená, není šifrovaná a to i přes to, že se při komunikaci přenášejí přihlašovací údaje nebo příkazy, které je možné odposlouchávat nebo modifikovat. Telnet je možné použít i pro jiné účely, jako např. přístup k e-mailu nebo databázím. [3]

SSH – Secure Shell je protokol, který je zabezpečenou náhradou za Telnet. Při přenosu dat dochází k jejich šifrování přes nedůvěryhodnou síť (internet), která může být

odposlouchávána. Tento protokol umožňuje i tunelové spojení a používá například u Virtuální privátní sítě, která bude ještě vysvětlena. [3]

4.5.2 Přenos souborů – FTP a SecureFTP

Tyto dva protokoly se používají pro přenos souborů. Také se jedná o protokol typu klient-server. Komunikace mezi klientem a serverem a samotný přenos dat probíhá odděleným kanálem (na různých portech). Na jednom kanálu naváže klient spojení se serverem, prokáže se přihlašovacím jménem a heslem. Pokud si klient požádá o zaslání nějakého souboru, otevře server jiný datový port, přes který probíhá samotný datový přenos. Nevýhodou tohoto protokolu je jeho nezabezpečenost, jak soubory, tak i příkazy jsou přenášeny bez šifrování. A právě zabezpečenou formou FTP je SecureFTP, který využívá bezpečného tunelu pomocí SSH. [3]

4.5.3 Web – HTTP a HTTPS

Protokol HTTP slouží k přenosu HTML souborů (webových stránek). Slouží také jako přístup k e-mailu přes internet. Opět se jedná o nezabezpečený protokol, který neumožňuje šifrování ani zabezpečení integrity dat. Vzhledem k tomu, že se v současnosti hodně využívají například aplikace internetového bankovnictví, je potřeba přenos dat protokolem HTTP zabezpečit. A právě k tomu se používá speciální vrstva, protokol TLS, nebo starší SSL a takto zabezpečený web se označuje HTTPS. Protokol TLS se používá i například pro zabezpečení elektronické pošty. [3]

4.5.4 Elektronická pošta

Možností jak zabezpečit vlastní elektronickou poštu je několik. Jeden se způsobů je nespoléhat se na bezpečnostní protokoly a samotnou zprávu před jejím odesláním si vlastnoručně zašifrovat pomocí šifrovacího programu. Je vhodné také šifrovat připojení mezi uživatelem a poskytovatelem e-mailové schránky, ale i všechny uložené e-maily a e-maily v archivu. Pro zabezpečení odesílaných e-mailů lze použít šifrovací program. Obě strany komunikace samozřejmě ale musejí používat stejný a musí si dohodnout šifrovací klíč. Jednou z nejrozšířenějších aplikací je například OpenPGP. [3]

4.6 Zabezpečení dat u bezdrátové sítě

U bezdrátové sítě je zabezpečení komunikace mnohem složitější, protože signál se šíří do všech stran a provoz může kdokoliv odposlouchávat nebo se zapojit do sítě. Je důležité, aby

si dvě zařízení při komunikaci „rozuměla“ a byla schopná se domluvit a také aby byla zajištěna integrita a důvěrnost dat. Základem zabezpečení sítě je pomocí autentizace a šifrování, které jsou součástí bezpečnostních protokolů a standardů.

4.6.1 WEP

Wired Equivalent Privacy. Jedná se o nejstarší bezpečnostní protokol a od jeho užívání se upouští, u domácích sítí je však stále používán. Tento protokol byl prolomen již v roce 2001 a v současnosti je používán především protokol WPA2. [1]

Princip spočívá v zašifrování odesílané zprávy a rozšifrování na straně přijímače tím stejným klíčem. Funguje tedy na principu symetrického šifrování. WEP ověřuje fyzickou adresu síťové karty (tzv. MAC adresu) a ne uživatele samotného. Mezi hlavní nevýhodu WEP tak patří neměnnost klíče. Klíč se nemění automaticky po určité době a musí jej změnit sám uživatel a klíč není možné automaticky obměňovat během komunikace. [1]

4.6.2 IEEE 802.11i

Vzhledem k tomu, že WEP se ukázal jako nedostatečný pro bezpečnost dat u bezdrátové sítě, byla proto vyvinuta další norma – 802.11i. Jejím základem byl protokol WPA (WIFI Protected Access), který řeší základní slabiny WEP, prakticky nulovou autentizaci a používání statického klíče.

Autentizace se zlepšila zavedením obecného rámce řízení přístupu podle 802.1x, EAP nebo přednastaveného sdíleného klíče (PSK). Šifrování bylo nahrazeno novým protokolem TKIP (Temporal Key Integrity Protocol), kdy probíhá průběžná a automatickou výměnu klíčů pro šifrování. Délka klíče pro šifrování se také zvětšila na 128 bitů (původní klíč pro WEP byl 40 bitový). Dále tento standard používá i MAC filtr, který umožňuje přístup do sítě pouze určitým uživatelům podle fyzické adresy jejich WIFI zařízení, která je pro každé zařízení jedinečná. Tato funkce byla používána již před zavedením tohoto standardu. [1, 7]

WPA však bylo původně navrženo tak, aby bylo možné jej implementovat i na hardware, který byl původně navržen pro WEP, proto byly při jeho sestavování přijaty určité kompromisy. Pro zabezpečení domácnosti nebo malé firmy je WPA dostačující, ale u aplikací, kdy je potřeba zajistit maximální bezpečnost je nedostačující a v těchto případech se používá WPA2, který je rozšířením původní WPA a zajišťuje tak účinnější algoritmus pro šifrování a mechanismy zabezpečení jsou již na vysoké úrovni. Místo protokolu TKIP se používá silnější šifrování pomocí EAS (Advanced Encryption Standard), který je považován za dostatečný šifrovací mechanismus i pro vládní účely. [1, 7]

Srovnání jednotlivých bezpečnostních řešení pro bezdrátové sítě proti různým druhům útoku na sítě jsou uvedeny v následujících dvou tabulkách. [1, 7]

Tabulka 1: Srovnání WEP, WPA a WPA2

Metoda	Ověření identity	Síla šifry	Použití pro domácí a malé sítě	Použití pro podnikové sítě
WEP	Žádné	Slabší	Dobré, avšak relativně slabé	nedostatečné
WPA (PSK)	Slabší (předem sdílený klíč)	Dobrá	Velmi dobré	Slabé
WPA2 (PSK)	Slabší (předem sdílený klíč)	Výborná	Velmi dobré	Slabé
WPA (plná)	Dobré	Dobrá	Velmi dobré	Dobré
WPA2 (plná)	Dobré	výborná	výborné	Velmi dobré

Zdroj: [7]

Tabulka 2: Odolnost proti útokům na počítačové sítě

	WEP	**WPA**	**WPA2**
Autentizace	Otevřená	EAP nebo PEAP (Protected EAP)	EAP nebp PEAP
Šifrování	Statický WEP	TKIP	EAS
Útok	**Odolnost**		
Na integritu, důvěrnost dat	Dobrá	Lepší	Nejlepší
Falešná autentizace	Horší	nejlepší	Nejlepší
Na slabý klíč	Horší	Nejlepší	Nejlepší
Falšované pakety	Minimální	Nejlepší	Nejlepší
Falešný přístupový bod	Minimální	Lepší	Lepší
Úroveň šifrování	Pro domácí síť	Pro podnikovou síť	Pro podniky i vládu

Zdroj: [7]

4.7 Virtuální privátní síť

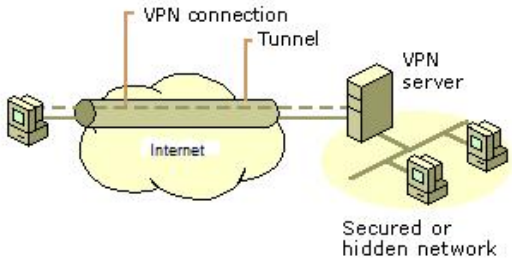
Jednou z možností, jak zajistit zabezpečené propojení mezi dvěma body je provozování virtuální privátní sítě (VPN). VPN jsou určeny spíše pro firemní, než domácí prostředí, umožňuje firmě propojit několik jejich LAN sítí. Jejich účelem je vyšší bezpečnost a snižování nákladů. Ve firmách jsou VPN náhradou za drahé telekomunikační okruhy - privátní linky. Vytvořením VPN také pro firmu odpadají problémy s přímým propojením jednotlivých poboček nebo prodejců. Pro vytvoření VPN je potřeba, aby byla firemní síť připojena k internetu, protože funguje nad veřejným internetem. Proto se také nazývá virtuální. [26, 27]

VPN může být také použita uvnitř vlastní sítě, pro zajištění dalšího zabezpečení přístupu k důležitým informacím. Firma může obzvlášť citlivá data z určitého oddělení oddělit od zbylých dat na síti a vzájemně je propojit právě virtuální privátní sítí. [26, 28]

Odborně řečeno se jedná o vytvoření šifrovaného síťového spojení, mezi jejichž dvěma koncovými body se využívá bezpečný komunikační tunel, vedený přes internet. [26]

Podle účelu, který VPN plní, lze rozlišit její tři základní typy:

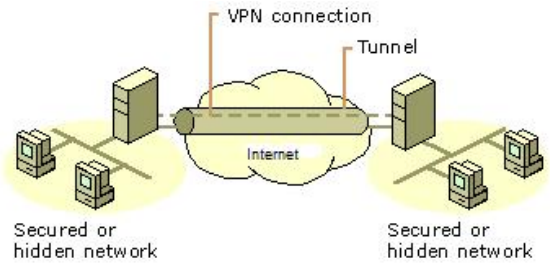
- **VPN pro vzdálený přístup** umožňuje propojení jednotlivých uživatelů s centrálním pracovištěm přes internet. Slouží tedy k připojení zaměstnanců, kteří se můžou nacházet kdekoliv, s firemní sítí. [26, 28]



Obrázek 6: Znázornění vzdáleného přístupu

Zdroj:Upraveno podle [28]

- **VPN pro spojení pracovišť** umožňuje rozšíření sítě LAN i na jiné budovy a pracoviště. Tento typ VPN bývá trvale aktivně propojený a všichni zaměstnanci mají přístup ke stejným službám jak pracovníci v ústředí. Tento typ bývá také označován jako intranetová VPN nebo VPN mezi sítěmi LAN. [26, 28]



Obrázek 7: VPN pro spojení pracovišť

Zdroj: Upraveno podle[28]

- **Extranetová VPN** je rozšířením intranetové VPN, akorát nepropojuje jednotlivé budovy nebo pobočky, ale poskytuje bezpečné spojení s obchodními partnery, dodavateli nebo zákazníky. [26]

A jak tedy virtuální privátní sítě fungují? Pro zabezpečení přenosu dat se používá bezpečnostní protokol (IPsec/IKE, PPTP, SSL, OpenVPN). Spojení s VPN iniciuje klient pomocí speciálních protokolů tunelových propojení virtuální sítě, server potom ověří klienta, zda má příslušná oprávnění a umožní mu přístup. Toto spojení mezi dvěma body v serveru je prováděno přes internet. Veškerá data, která jsou přenášena, jsou kvůli zabezpečení šifrována, takže i v případě jejich zcizení je k jejich přečtení potřeba dešifrovací klíč. Jak příjemce, tak i odesílatel používají stejný klíč. Data bývají také zapouzdřena pomocí hlavičky, která obsahuje informace odkud, kam mají data putovat přes internet. [28, 29]

4.8 Zálohování

Zálohování dat není prostředek, jak znesnadnit útočníkům získat data ze sítě, ale i přesto je to jeden z prostředků pro ochranu dat. Cílem útočníka nemusí být pouze data získat, ale jeho cílem může být i data zničit a bez jejich zálohování by tak uživatelé o ně stejně přišli. [22]

Zálohování dat slouží k uložení vybraných dat z jednoho záznamového média na jiné médium a vytvoření tak kopie pro případ, že by byla originální data zničena nebo zcizena. Slouží tedy jako preventivní opatření v případě, že by se něco stalo. Zálohují se tedy data, která jsou nepostradatelná. Důležité je pravidelné provádění zálohování. [22]

V podniku má zálohování dat větší význam než v domácnosti. Firma si uchovává data, která pro ni mají užitnou hodnotu (účetní záznamy, záznamy o zákaznících, dodavatelích a další) a která jsou součástí jejího know-how. Jsou určitá data, která je firma povinna uchovávat i ze zákona a to po dobu až několika let (například záznamy o finančním hospodaření firmy). Firma musí také řešit otázku vhodného úložiště, v případě firmy ji nestačí např. flash disk. Jednou z možností je např. využití služeb datového centra – jedná se o místo, kde firma platí za uskladnění svých dat, bez toho, aniž by musela sama takové centrum budovat. Zároveň má tak zajištěnou vysokou dostupnost dat a rychlou obnovu dat. Pro řízení zálohování a obnovu dat ve firmě existuje manažerská disciplína BCM – Business Continuity Management. Tato disciplína se zabývá potenciálními dopady havárie na činnosti firmy, jak co nejlépe na možné situace reagovat, zajistit vyšší odolnost a zajistit tak pokračování a obnovu činnosti firmy. BCM je tedy metodou pro zefektivnění zálohovacích procesů ve firmách. [23, 25]

5 POKYNY K VYTVOŘENÍ ZABEZPEČENÉ DOMÁCÍ POČÍTAČOVÉ SÍTĚ

Vytvoření domácí počítačové sítě již není nijak složitým procesem a je schopný to zvládnout i člověk bez hlubších znalostí počítačů. Vytvoření domácí počítačové sítě již ani není pro domácnost takovou finanční zátěží. Při tvorbě počítačové sítě je důležité se věnovat výběru správného hardwaru a softwaru a jejich nastavení, aby se zajistila bezproblémová a zabezpečená síť. V této kapitole jsou popsány zásady jak zabezpečit nově vytvářenou zabezpečenou síť a jak se v rámci takové sítě chovat pro zajištění její bezpečnosti. Předpokladem při popisu zabezpečení na počítačích je používání operačního systému MS Windows 7.

5.1 Výběr potřebného hardwaru

V případě, že má domácnost zařízení (stolní počítače, notebooky, tiskárny atd.), která chce zapojit do počítačové sítě, potřebuje k jejímu vytvoření tento hardware:

- Router;
- Kabeláž.

Hlavním problémem je výběr vhodného routeru. Jedná se o síťové zařízení, které spojuje dvě sítě, tedy internet s domácí sítí a zabezpečuje komunikaci mezi nimi. Jedná se o bránu mezi internetem a domácností. V současnosti může router plnit různé funkce a podle toho se také odvíjí jeho cena. Při výběru je potřeba, aby odpovídal požadavkům na danou počítačovou síť. Mezi možné vlastnosti na které se při výběru routeru zaměřit jsou:

- Zabezpečení přenosu dat – pomocí WEP, WPA nebo WPA2. Nejlépe by měl router podporovat WPA2.
- Provozní pásma – router by měl využívat pásmo 2,4 GHz i 5 GHz. Použít provoz v pásmu 5 GHz je vhodné v hustě obydlené oblasti, kde je pásmo 2,4 GHz více využívané. Vzhledem k tomu, že většina zařízení v domácnosti v současnosti v pásmu 5 GHz nepracuje, jedná se o vhodnou alternativu do budoucnosti.
- Počet USB portů – USB port je vhodný pro připojení zařízení, jako např. tiskárny;
- Počet LAN konektorů, které slouží k připojení dalších zařízení do sítě (např. stolní počítač nebo NAS server).

- Kompatabilita s IEEE 802.11n, nebo ještě lépe 802.11ac.
- Maximální rychlost. I když udávaná maximální rychlost routeru je teoretická hodnota při dosažení ideálních podmínek a v případě využití obou provozních pásem (pokud v obou pásmech pracuje). Reálná rychlost je mnohonásobně nižší a závisí na konkrétních zařízeních, prostředí a tarifu poskytovatele.

5.2 Zásady zabezpečení sítě

- Pokud je to možné, připojit co největší množství zařízení pomocí kabelu. Je to z důvodu větší bezpečnosti sítě, žádná bezdrátová komunikace nikdy nebude stejně bezpečná jako ta „kabelová“.
- Při vedení kabelu dbát na to, aby k nim nebyl volný přístup cizích osob (například, aby kabel nevedl přes veřejně přístupnou chodbu v bytovém domě).

Nastavení routeru:

- Prvotní nastavení routeru provádět vždy pomocí pevného ethernetového připojení a ne pomocí Wifi.
- Nikdy nenechávat defaultní nastavení od výrobce, jednalo by se o bezpečnostní chybu a je proto potřeba věnovat čas tomuto nastavení;
- U bezdrátové komunikace v rámci LAN používat vždy šifrování.
- Při prvotním nastavení je potřeba si změnit heslo pro administraci routeru.
- Na routeru má byt zapnutý firewall, DoS protection a jiné ochranné prvky.
- Při volbě SSID (jména sítě) zvolit takové jméno, které neukazuje na provozovatele sítě. Tento název sítě je také možné skrýt, tedy že se nezobrazuje v seznamu dostupných sítí. Pro připojení do takovéto sítě je potřeba zadat přesný název sítě. Nejedná se tedy o zrovna vhodnou ochranu, útočníka skrytí názvu sítě zrovna neodradí.
- Použít filtrování MAC adres.

Filtrování MAC adres nebo skytí SSID potenciálního útočníka doopravdy nezastaví, jediným účinným opatřením proti útoku na bezdrátovou síť je WPA a nebo WPA2.

5.3 Zásady počítačové bezpečnosti

- Provádět aktualizace firmware všech wifi zařízení.

- Provádět aktualizace driverů a firmware všech klientských adaptérů (ve stolních počítačích, noteboocích).
- Provádět aktualizace operačního systému.
- Pro zabezpečení důležitých dat používat šifrování.
- Důležitá data zálohovat a to na jiné zařízení, než je uložen originál.
- Na každém počítači musí být zapnutý antivirový program a pravidelně by se měla provádět kontrola počítače.
- Na každém počítači musí být zapnutý firewall, a to i přes to, že je zapnutý i na routeru. Při nastavování seznamu povolených programů je vhodnější nejprve všechny zakázat a povolit pouze ty, které je potřeba.
- Provádět po určité době změnu hesel.
- Na každém počítači by mělo být pouze nezbytně nutný počet uživatelských účtů a každý účet by měl být zabezpečen heslem.
- Volená hesla by neměla být triviální a nemělo by se jednat o slovo prolomitelné slovníkovým útokem. Možnosti, jak by mohlo heslo vypadat, jsou:
    - použít alespoň jedno velké písmeno;
    - Použít alespoň jednu číslici nebo speciální znak;
    - Zvolit dostatečnou délku hesla (např. 12 znaků);
    - Heslo po určité době měnit.
- Uživatel by měl volit takové heslo a měnit jej v takových intervalech, aby pro něj bylo zapamatovatelné. Příliš složité heslo a častá doba jeho změny může vést k tomu, že si jej uživatel bude zapisovat a bude jej mít umístěné u počítače, což ve výsledku vede ke snížení bezpečnosti.

5.4 Zásady bezpečného chování

- Umožnit připojení k síti co nejmenšímu počtu lidí.
- Neumožnit přístup ke svému uživatelskému účtu cizím osobám.
- Platná hesla si nezapisovat a neumisťovat v blízkosti počítače.
- Neotvírat přílohy e-mailů, jejichž obsah není znám.

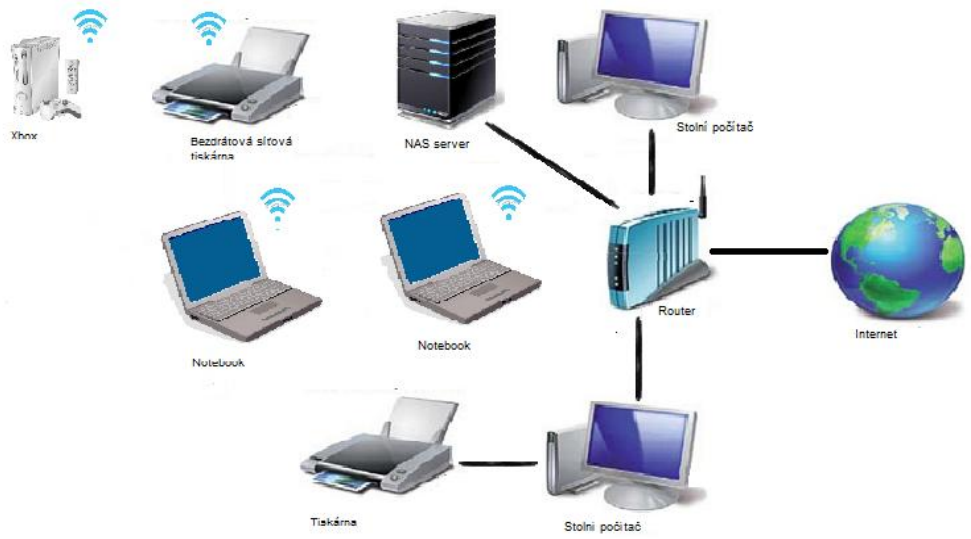
- Nikdy nereagovat na emaily, ve kterých je požadováno sdělení soukromých údajů třetí osobě.
- Nenavštěvovat podezřelé internetové stránky a ani neotvírat odkazy na neznámé stránky.
- Nestahovat nelegální sdílený obsah.
- Omezit sdílení souborů přes internet.
- Nevěřit vyskakujícím oknům na internetu, která žádají o stažení software.
- Nikdy nevypínat antivirový program a nejlépe používat i antispywarový software.
- Mít neustále zapnutý firewall.
- Přes internet neposílat citlivá data.

6 NÁVRH DOMÁCÍ POČÍTAČOVÉ SÍTĚ

Pro návrh malé počítačové sítě byla zvolena modelovou domácnost žijící ve třípokojovém bytě. Rodina má čtyři členy, rodiče a dvě děti. Otec rodiny je podnikatel a v bytě využívá jeden notebook. Dále se v domácnosti nachází ještě další notebook, který využívá dcera s matkou, a jeden stolní počítač, který vlastní syn. Navíc v přízemí domu je kancelář firmy s dalším počítačem. Na všech počítačích je nainstalovaný MS Windows 7. Dále chtějí do sítě zapojit dvě tiskárny, herní konzolu Xbox, NAS server a příležitostně mobilní telefony či tablet.

Domácnost má tak k vytvoření sítě k dispozici dva stolní počítače, dva notebooky, dvě multifunkční tiskárny, konzoli Xbox 360E a vlastní mobilní telefony a tablety. Pro vytvoření kompletní sítě tak ještě potřebují router, který slouží pro připojení domácí sítě k internetu, kabeláž a NAS server, který by měl sloužit pro sdílení a zálohování dat. NAS server však k vytvoření sítě není nezbytně nutný, jedná se o nástavbový prvek celé sítě. Logické schéma sítě je zobrazeno na obrázku 8.

Domácí síť bude připojena k internetu pomocí DSL. Jedná se tak o permanentní připojení (opak je vytáčené připojení přes telefonní linku v minulosti) s uzlem páteřní sítě přes pronajatou linku. Druhou možností připojení k internetu by bylo frame-relay připojení, tedy o rádiové spojení vzduchem. Jedná se o dva nejpoužívanější způsoby připojení k internetu. Vzhledem k zajištění bezpečnosti je však DSL připojení lepší volba.



Obrázek 8: Logické schéma sítě

Zdroj: vlastní

Pro vytvoření počítačové sítě tedy domácnost potřebuje nakoupit router, který spojuje domácí a vnější síť (internet) a zabezpečuje komunikaci mezi nimi. Jedná se tedy o bránu mezi internetem a domácností. Vlastnosti, které mohou routery mít a vlastnosti, na něž by se mělo při výběru přihlédnout, byly popsány v předcházející kapitole. Pro výběr routeru byly použity tři routery, které byly hodnoceny při testu routerů v osmém čísle časopisu Computer v roce 2014. Aktuální cena těchto routerů byla zjištěna na internetových stránkách www.alza.cz.

Tabulka 3: Srovnání routerů

Název routeru	**Netgear R6300-100PES**	**Edimax BR-6478AC**	**Linksys EA 6700-CE**
Cena routeru v Kč	3 719	2 699	5 129
Zabezpečení přenosu dat	WPA, WPA2	WPA, WPA2	WPA, WPA2
Provozní pásmo	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz	2,4 GHz, 5 GHz
Počet USB portů	1	0	2
Počet LAN konektorů	4	4	4
Maximální rychlost Mb/s	1 750	1 200	1 750
Podpora standardu 802.11ac	ano	ano	ano

Zdroj: Vlastní na základě [36]

Tyto routery mají podobné vlastnosti a liší se pouze v ceně, počtu USB portů a maximální rychlosti. Tyto tři vlastnosti byly použity jako rozhodovací kritéria. Rozhodovací problém byl řešen pomocí programu CDP (Criterium Decision Plus). Jedná se o speciální program, který je určený pro zpracování rozhodovacího problému od formulace až po analýzu.

Tabulka 4: Kritéria rozhodování

Kritérium	**Minimalizační/ Maximalizační**	**Stupnice hodnocení vyjádřená důležitostí**	**Intenzita důležitosti**
K1 – Cena	Minimalizační	Nejvýznamnější	7
K2 – Počet USB portů	Maximalizační	Nejméně významné	3
K3 – Maximální rychlost	Maximalizační	Méně významné	5

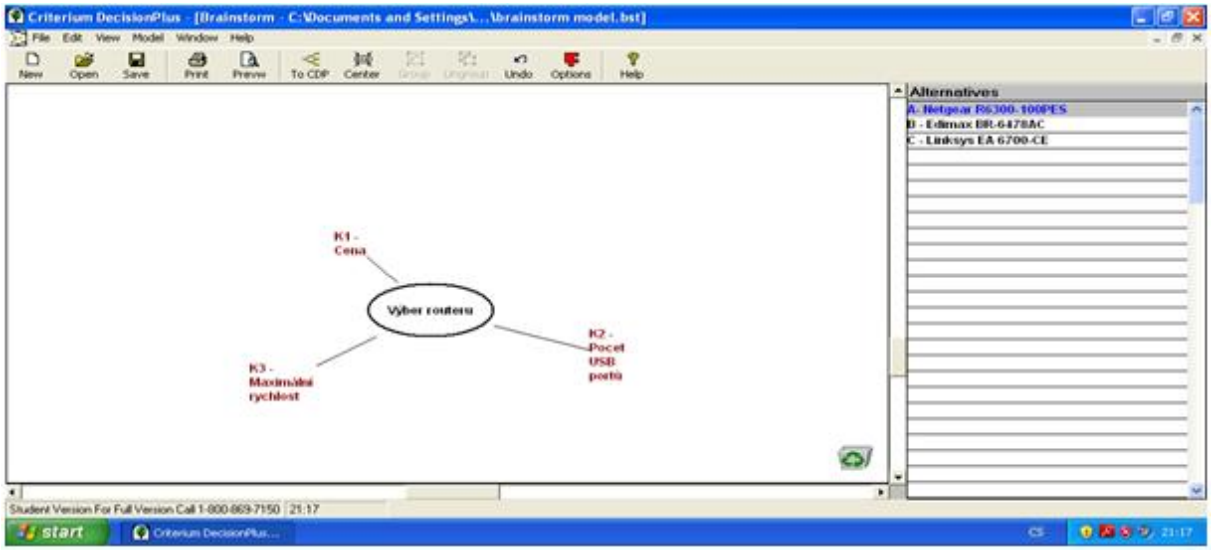
Zdroj: vlastní

Tabulka 5: Rozhodovací tabulka

Kritérium	Varianta		
	A - Netgear R6300-100PES	B - Edimax BR-6478AC	C - Linksys EA 6700-CE
K_1	3 719	2 699	5 129
K_2	1	0	2
K_3	1 750	1 200	1 750

Zdroj: vlastní

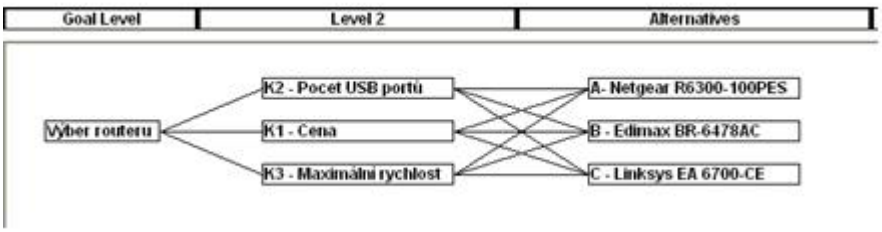
Nejprve byl vytvořen brainstormingový model, který obsahuje všechna kritéria, varianty rozhodování a cíl, kterého se má dosáhnout. Tento model je zobrazen na následujícím obrázku.



Obrázek 9: Brainstormingový model

Zdroj: vlastní

Rozhodovací problém byl řešen pomocí metody AHP (analytickou hierarchická metoda), která využívá dekompozici rozhodovacího systému na víceúrovňovou hierarchickou strukturu, kterou lze vidět na dalším obrázku.

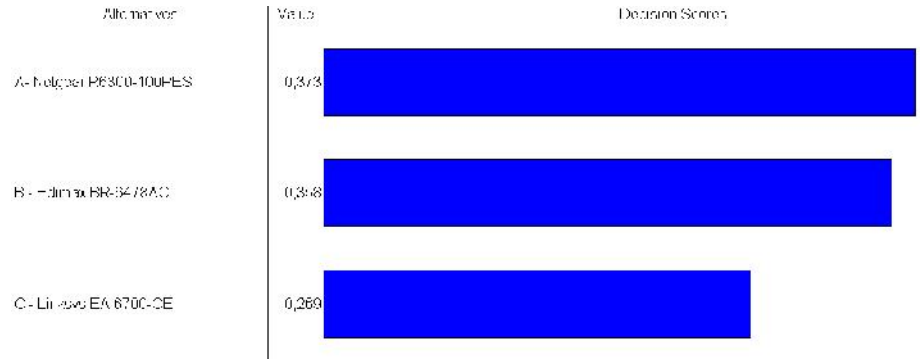


Obrázek 10: Hierarchický model

Zdroj: vlastní

Analytickou hierarchická metoda funguje na principu Saatyho matice, kdy se porovnávají preferenční vztahy důležitosti dvojic kritérií uvedených v tabulce 4. Sestavenou Saatyho matici si lze zkontrolovat pomocí indexu konzistence CI, jehož hodnota by měla být nižší jak 0,1. Hodnota indexu konzistence u tohoto rozhodovacího problému byla 0,021. Lze tedy říct, že Saatyho matice byla sestavena smysluplně.

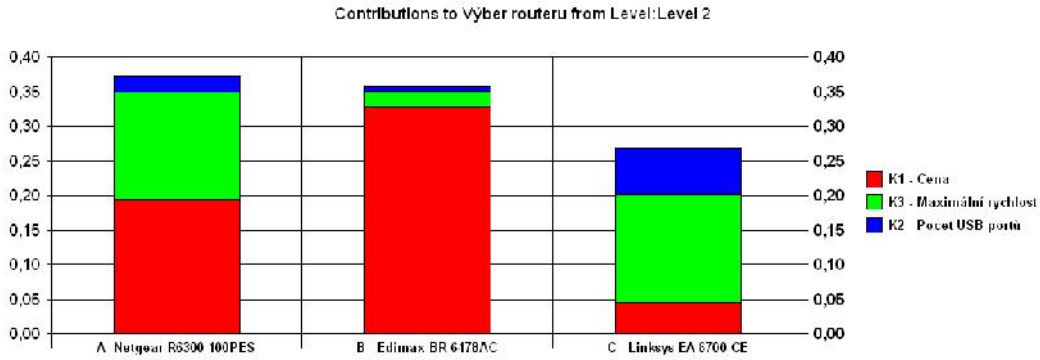
Celkové porovnání všech tří variant lze vidět na dalším obrázku. Jako optimální varianta jeví varianta A – router Netgear R6300-100PES s celkovým skóre 0,373. Lze vidět, že varianta A a B byly velmi vyrovnané.



Obrázek 11: Porovnání variant

Zdroj: vlastní

Pro lepší názornost výsledku rozhodovacího problému je na následujícím obrázku vidět, jak se jednotlivá kritéria podílela na výsledku jednotlivých variantách. Lze tak vidět, že vyrovnané hodnocení varianty A a B bylo způsobeno především nízkou cenou varianty B.



Obrázek 12: Porovnání variant dle jednotlivých kritérií

Zdroj: vlastní

Pro tuto domácí počítačovou síť tak byl vybrán router Netgear R6300-100PES za 3 719 Kč. Pro propojení dvou stolních počítačů (v přízemí a bytě) s routerem bude použit

ethernetový kabel přímý. Cena za 20 metrů tohoto kabelu se pohybuje do 150 Kč a pro vytvoření počítačové sítě jsou potřeba dva kusy. Na počítač v přízemí bude napojena jedna multifunkční tiskárna přes USB kabel.

K routeru bude ještě kabeláží připojen NAS server, ostatní zařízení budou s routerem připojeny bezdrátově. V dnešní době je tak možno připojit jednotlivé notebooky, tiskárny, herní konzole jako je Xbox, mobilní telefony, tablety a další zařízení.

Jako jedno ze zařízení celé počítačové sítě byl zvolen i NAS server. Jedná se o síťové zařízení pro ukládání a sdílení dat v síti. Není potom nutné jednotlivé počítače vzájemně propojovat a všechna sdílená data jsou ukládána na tomto serveru. NAS obsahuje jeden nebo více pevných disků, které tak budou sloužit jako centrální úložiště pro celou rodinu. Mezi hlavní výhody NAS serveru patří:

- Data jsou dostupná pro všechna zařízení v síti.
- Vhodný prostředek i pro zálohování dat. Pokud má NAS server sloužit pro sdílení dat a zálohování, je vhodné pořídit si dvoudiskový NAS server.
- Umožňují vytváření uživatelů nebo skupiny uživatelů a přidělování jim práva ke čtení nebo zápisu dat.
- Možnost připojení přes VPN.
- Možnost šifrování dat, rychlost a další.

Pořízení NAS serveru je však finančně náročnější záležitost. Například ve čtvrtém čísle časopisu Computer v roce 2015 byly testovány dvoudiskové NAS servery a na prvním místě se umístil NAS server Asustor AS-5002T v ceně 8 999 Kč. K této ceně je nutno si ještě připočíst cenu za dva pevné disky o kapacitě až 8 TB, které nejsou součástí. [37]

Co se týká softwarového vybavení, tak domácnost potřebuje samotný MS Windows, který je již součástí všech počítačů a antivirový program. V dubnovém čísle dTestu byly porovnávány antivirové programy a vítězové se staly antivirové programy ESET Smart Security 8 a Symantec Norton Security 2015. Cena roční licence na jedno PC u programu ESET je 1510 Kč a u Nortonu 1280 Kč. Vzhledem k tomu, že má rodina čtyři počítače v celé síti, vyplatí se jí koupit rodinné balíčky. Firma ESET nabízí na svých oficiálních internetových stránkách www.eset.com rodinný balíček pro tři zařízení za cenu 1511 Kč. K tomu by potřebovali ještě jednu samostatnou licenci za 1510 Kč a celkem by antivirový program ESET Smart Security vyšel na 3021 Kč. Dle oficiálních internetových stránek www.cz.norton.com stojí Norton Security pro 5 zařízení na 1 rok 1 200 Kč. Proto byl kvůli

cenové výhodnost zvolen antivirový program Norton Security. Celkové náklady na vytvoření a zabezpečení počítačové sítě jsou uvedeny v následující tabulce. [38]

Tabulka 6: Náklady na domácí počítačovou síť

Hardware	**Náklady (Kč)**
Netgear R6300-100PES	3 719,00
Kabeláž	300,00
Software	**Náklady (Kč)**
Antivirový program Norton Security	1 200,00
CELKEM	**5 219,00**

Zdroj: vlastní na základě [36, 38]

Do celkových nákladů na počítačovou síť nebyly započítány náklady na MS Windows, které jsou již součástí počítačů a náklady na NAS server, protože pro vytvoření počítačové sítě není nutností, ale byl v této kapitole zmíněn jako možný návrh jak síť rozšířit. Jeho pořízení pak závisí na finanční situaci domácnost.

Poslední věc, kterou by měla rodina při budování sítě zvážit, je připojení tiskárny. Jak už bylo napsáno, tiskárna v přízemí bude napojena přes USB přímo na počítač a bude pouze z tohoto počítače využívána. V bytě však bude jedna tiskárna využívána všemi členy rodiny. Jedná se o multifunkční Wi-fi tiskárnu a je možné ji zapojit do sítě třemi způsoby:

- připojení pomocí Wi-fi (větší možnost odposlouchávání);
- připojení tiskárny na jeden počítač přes USB a její sdílení s ostatními počítači. Tato metoda má ale nevýhodu v tom, že pro tisk je potřeba, aby byl zapnutý počítač, ke kterému je připojena;
- připojení přímo k routeru (jak přes USB nebo přes síťový kabel s koncovkou RJ45, pokud jí tiskárna disponuje), což je v případě této rodiny nejvhodnější varianta.

6.1 Ochrana sítě před útoky

V páté kapitole byly uvedeny zásady, které je nutné dodržovat pro zajištění bezpečnosti počítačové sítě. V této části kapitoly je popsáno, jak s jednotlivými prvky obrany dat pracovat, správně je nastavit a používat.

6.1.1 Router

Jeden z prvků zabezpečení je samotný router. Většina routerů je schopno pracovat bez zvláštního nastavení hned od výrobce, ale jednalo by se o bezpečnostní chybu a je potřeba věnovat chvilku času pro jeho zabezpečení.

Prvním krokem je zjistit IP adresu routeru, kterou lze najít v manuálu, nebo pomocí příkazu **ipconfig**, kde je IP adresa routeru je skryta pod adresou brány. Tuto adresu potom stačí zadat do internetového prohlížeče a otevře se nastavení routeru. V případě, že by router neměl zapnutý DHCP server, je potřeba nejprve na počítači manuálně nastavit IP adresu počítače ve stejném rozsahu jako je IP adresa routeru. Poté je postup k nastavení routeru stejný, jako v případě zapnutého DHCP serveru. V rámci nastavení doporučuji zapnout službu DHCP serveru na routeru a na počítačích mít nastaveno automatické získávání IP adresy.

Mezi ty základní prvky zabezpečení, na které je potřeba myslet při nastavení routeru, patří:

- změnit heslo pro administraci routeru;
- vyplnit SSID;
- zapnout firewall, DoS protection, vypnout „Web Access from WAN“;
- filtrovat MAC adresy;
- šifrování sítě.

Filtrováním MAC adresy lze umožnit přístup k síti pouze konkrétním počítačům. MAC adresa je specifické číslo síťové karty. Pokud by se tedy zadaly MAC adresy pouze čtyř počítačů v domácnosti, nikomu jinému by router nedovolil se připojit k Wi-fi. Při použití tohoto řešení je však nutno jakýkoliv jiný počítač, který chceme přidat k připojení, doplnit v nastavení.

Nejdůležitější a nejspolehlivější metodou je použití šifrování. Router podporuje šifrování WPA i WPA2. Nejlepší je tedy použít WPA2. Při šifrování se v síti nastaví heslo a celá síť se zašifruje a bez znalosti tohoto hesla není možné se k síti připojit. Při stanovování hesla je potřeba dbát na pravidla pro silné heslo a je také potřeba jej občas měnit. Stejně tak je potřeba měnit i administrátorské heslo. Po prvotním nastavení routeru je vhodné jej restartovat.

Obrázek 13: Nastavení zabezpečení na routeru Netgear R6300-100PES

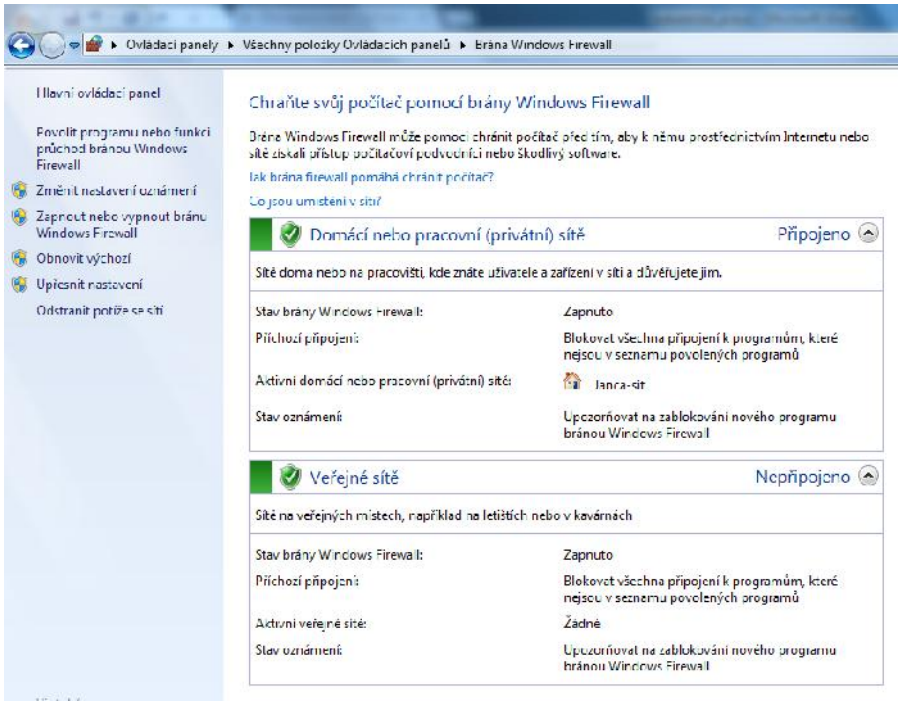
Zdroj: vlastní

6.1.2 Firewall

Firewall by tedy měl být zapnutý jak na jednotlivých počítačích, tak i na routeru, který plní úlohu přístupového bodu. Firewall slouží jako bezpečnostní brána a odděluje provoz mezi dvěma sítěmi (domácí a internetem) tím, že oběma směry propouští pakety podle předem definovaných pravidel.

Přístup k nastavení firewallu na počítači s Windows 7 je přes tlačítko **Start – Ovládací panely**, kde se nastaví zobrazení malých ikon a vybere se volba Brána Windows Firewall. Jako první se zobrazí stránka s přehledem o nastavení firewallu pro jednotlivé síťové profily. Při připojení k síti si lze vybrat z těchto dvou profilů:

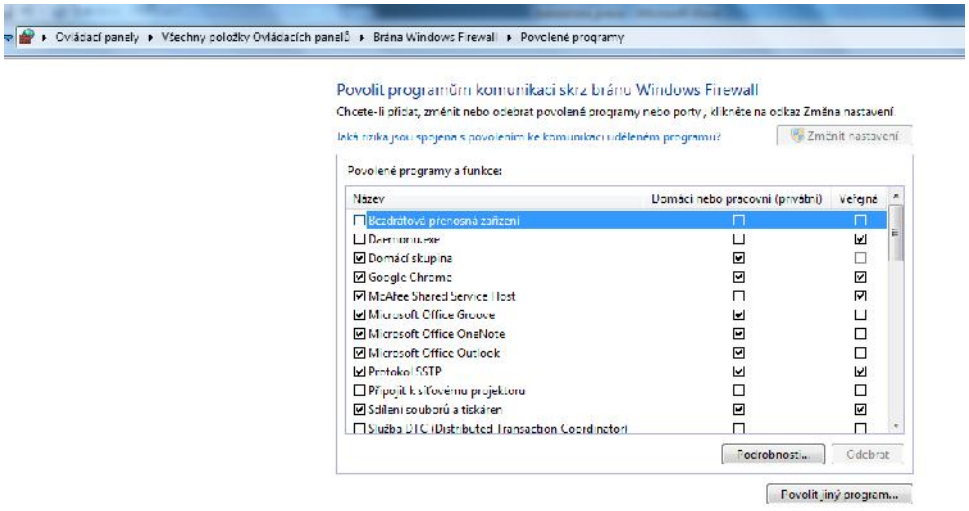
- **Domácí nebo pracovní (privátní) síť** – skládá se z důvěryhodných počítačů a je oddělena od jiných sítí (např. Internet). Jedná se tedy i o popisovanou síť.
- **Veřejná síť** – jedná se o nedůvěryhodnou síť, kde nejsou známy všechny počítače a proto je i nastavení firewallu přísnější než u první možnosti.



Obrázek 14: Nastavení firewallu

Zdroj: vlastní

Firewall musí být zapnut pro oba síťové profily, jak je možno vidět na obrázku 14. Pro běžnou činnost na počítači je potřeba si nastavit seznam povolených programů a to kliknutím na odkaz **Povolit programu nebo funkci průchod bránou Windows Firewall**. Otevře se tak okno a pak stačí kliknout na **Změnit nastavení** a zaškrtáváním políček tak lze měnit nastavení. Program, který se v seznamu nenachází, lze doplnit kliknutím na **Povolit jiný program**. O blokaci nebo povolení přístupu jednotlivých programů lze rozhodnout už při jejich instalaci, kdy se firewall zeptá, zda má komunikaci povolit.



Obrázek 15: Nastavení povolení programů

Zdroj: vlastní

I na samotném routeru Netgear R6300-100PES je firewall. Jeho nastavení může být provedeno zároveň při první konfiguraci samotného routeru. Po přihlášení se k nastavení routeru přes internetový prohlížeč, jak bylo popsáno v kapitole 6.1.1 Router, je možné upravovat nastavení kliknutím v levé části okna na záložku **Advanced** vybrat **Security**.

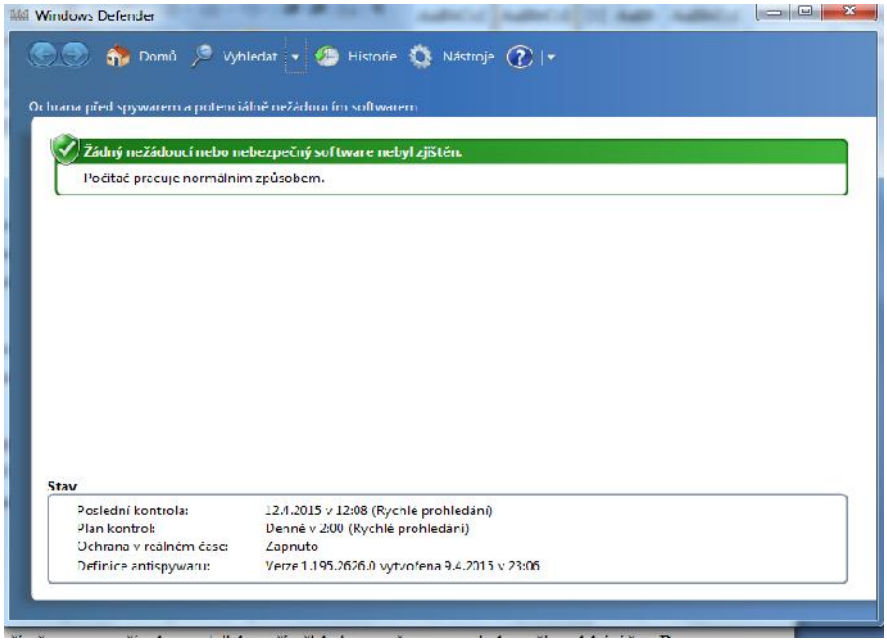
6.1.3 Ochrana proti škodlivému softwaru

Základním prostředkem pro ochranu před malware je antivirový program. Pro účely této domácí počítačové sítě byl vybrán Norton Security. Existuje i možnost si některé antivirové programy dokonce stáhnout i zdarma, jako například Avast Free Antivirus nebo Avira Free Antivirus. Tyto antiviry však poskytují pouze základní ochranu oproti těm placeným.

Většina antivirových programů je po nainstalování již nakonfigurovaná. Ale je důležité prověřit, zda je nastavena automatická aktualizace virové databáze, která je základem pro funkčnost antivirového programu a čas od času provádět kontrolu počítače.

Součástí antivirových programů jsou i další ochrany proti škodlivému softwaru, jako je antiadware nebo antispyware. Co mnoho uživatelů ani neví, ale součástí Windows je i Windows Defender, který poskytuje ochranu před spywaru. Lze jej spustit přes **Start-Ovládací panely**, přepnout na zobrazení ikon a zvolit **Windows Defender**.

Jak lze vidět na obrázku, program informuje o aktuálním stavu, kdy byla provedena poslední kontrola spywaru a jaký je plán provádění kontrol. Kliknutím na **Vyhledat** lze také spustit kontrolu počítače.



Obrázek 16: Windows Defender

Zdroj: vlastní

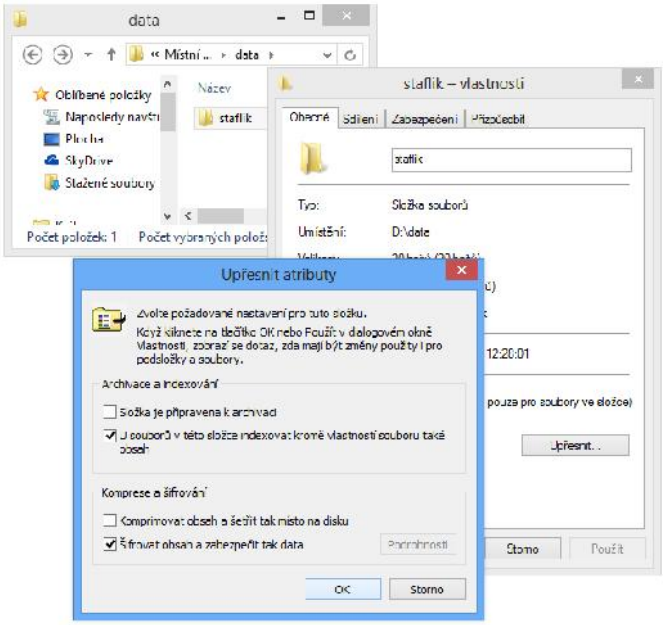
6.1.4 Správa uživatelských účtů

Další prvkem zabezpečení je správa uživatelských účtů. Otec se synem mají každý vlastní počítač, proto stačí, aby na jejich počítači byl vytvořen pouze jeden uživatelský účet. Dcera s matkou se dělí o jeden společný počítač, proto je vhodné, aby na tomto počítači byly účty dva. Je potřebné, aby všechny účty byly opatřeny heslem. Při každém spuštění počítače je poté potřeba toto heslo zadat, aby byl uživateli umožněn přístup k datům na počítači (jedná se o autentizaci znalostí). Heslo lze velmi jednoduše nastavit přes tlačítko **Start – Ovládací panely – Uživatelské účty a zabezpečení rodiny – Uživatelské účty – Vytvořit heslo pro vlastní účet**. I při tvorbě uživatelského hesla je nutné dbát na pravidla pro silné heslo (tipy jak vytvořit silné heslo jsou součásti okna Vytvořit heslo).

6.1.5 Šifrování

I přes to, že mají všichni členové rodiny své účty chráněné heslem, může se podařit útočníkovi jej prolomit. Proto je vhodné, aby uživatelé své důležité soubory ještě šifrovali. K tomuto účelu není potřeba, aby rodina kupovala další software, v rámci MS Windows k tomuto účelu lze využít EFS.

Pokud si budou šifrovat soubory pouze na svém počítači, budou pravděpodobně chtít, aby byli jediní, kteří k takovému souboru budou mít přístup. V tom případě se jedná o nejjednodušší variantu a postup je velmi jednoduchý. Na danou složku nebo soubor se klikne pravým tlačítkem myši, zvolí se **Vlastnosti** a potom **Upřesnit**. Poté se zaškrtne políčko **Šifrovat obsah a zabezpečit tak data** a **OK**. Dále se akorát zvolí, zda zašifrovat jenom složky, nebo i podsložky a podsoubory a všechno je hotovo. Pokud se vybere druhá možnost, automaticky se vždy zašifruje vše, co je do dané složky nakopírováno nebo je v ní vytvořeno.



Obrázek 17: Šifrování složky pomocí EFS

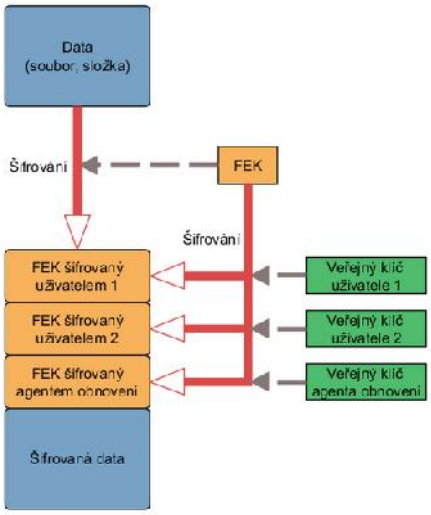
Zdroj: [14]

Pokud se k takto zašifrované složce snaží dostat jiný uživatel, operační systém mu to nepovolí.

Pokud však budou členové rodiny ukládat data na NAS server a budou chtít, aby k takovýmto datům měli přístup i ostatní členové rodiny, je postup trochu komplikovanější. Každý z členů rodiny si získá svůj certifikát tím, že zašifruje nějaký soubor. Potom je potřeba, aby si členové rodiny tyto certifikáty navzájem vyměnili (nejvhodnější variantou je přes Flash disk). Samotný export certifikátu lze provést stisknutím kláves **Win+R**, napsat certmgr.msc. Tím se zobrazí konzole pro správu certifikátů. Po nalezení certifikátu pro EFS se na něj klikne pravým tlačítkem myši a zvolí se **Všechny úkoly** a **exportovat**. Takto vyexportované certifikáty uživatelé distribuují všem, kteří jim chtějí zpřístupnit jimi zašifrované data.

Uživatel, který pak danou složku či soubor šifruje, musí importovat všechny certifikáty a při kliknutí pravým tlačítkem myši na soubor zvolí **Vlastnosti**, pak **Upřesnit**, **Podrobnosti** a **Přidat** vybere certifikáty všech uživatelů, jimž chce soubor zpřístupnit.

Přidáním jednotlivých certifikátů uživatelů dochází k tomu, že FEK je pak šifrovaný pomocí všech certifikátů, ne pouze pomocí certifikátu jednoho uživatele. Celý proces šifrování je zobrazen na následujícím obrázku. Tímto jednoduchým způsobem si můžou všichni členové rodiny zajistit, že k datům na společném NAS serveru bude mít přístup jen ten, koho opravdu chtějí.



Obrázek 18: Šifrování dat pro více uživatelů

Zdroj: [14]

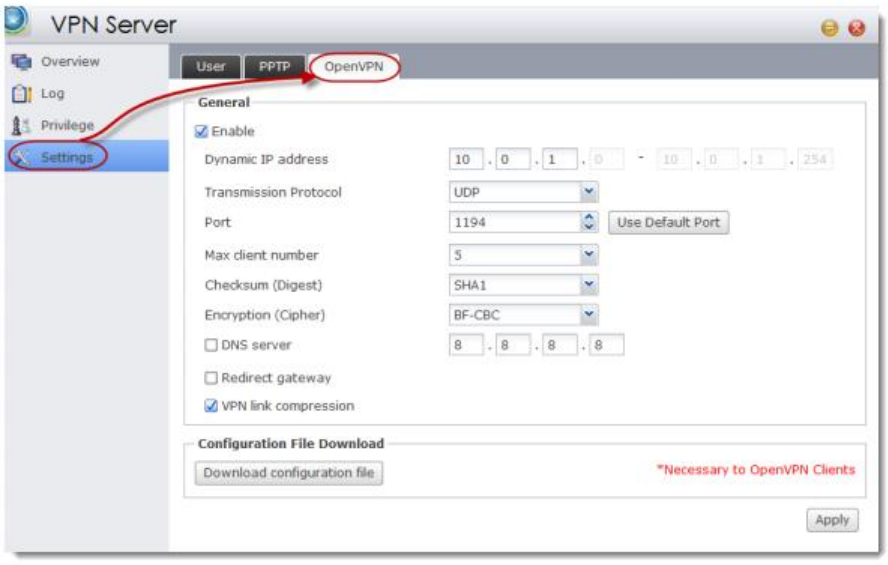
6.1.6 Virtuální privátní síť

Pokud bude mít otec na NAS serveru uložena i svá firemní data, může se někdy stát, že k nim bude potřebovat přistupovat i z jiného místa, než jen v rámci domácí sítě. Jednoduchým řešením je nastavení NAS serveru jako VPN server a nechat ostatní členy rodiny se k němu připojit.

Již zmíněný NAS server Asustor AS-5002T podporuje VPN server a stačí si jej pouze nainstalovat a přidat uživatele. Tento NAS server umožňuje vytvoření VPN pomocí PPTP nebo OpenVPN. V roce 2012 došlo k prolomení protokolu PPTP, proto je lepší použít OpenVPN.

Nejprve je potřeba v **App Central** zvolit VPN server a nainstalovat jej. V záložce **Overview** se klikne pod nápis **OpenVPN** k povolení této služby. Nový uživatel se pak přidá kliknutím na **Privilege** vlevo v horní části – **User-Add**, vybere se uživatel a vše se uloží. Dále se zaškrtne políčko **OpenVPN** a **Apply** a je tak vytvořen uživatel pro připojení k NAS serveru.

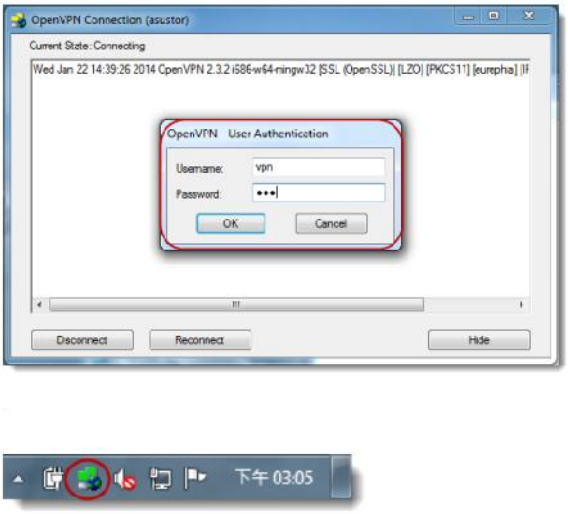
V rámci pokročilého nastavení přes **Settings-OpenVPN** lze upravit nastavení pro dynaminkou IP adresu, typ protokolu, maximální počet připojených uživatelů, typ šifrování a další.



Obrázek 19: Pokročilé nastavení VPN

Zdroj: [39]

Potom je potřeba vytvořit připojení k VPN serveru na uživatelském počítači. K tomu je potřeba stáhnout si OpenVPN klienta z internetových stránek společnosti Asustor. Z Asustor NAS se musí stáhnout konfigurační soubor pro OpenVPN klienta **asustor.ovpn** a otevřít ho v poznámkovém bloku. Tam se změní IP adresa na IP adresu serveru a změny se uloží. Tento soubor je potřeba zkopírovat do složky **C:\Program Files\OpenVPNconfig**. Připojení k NAS serveru se spustí pomocí **OpenVPN GUI**, kliknutím na spodní lištu obrazovky, jak je zobrazeno na následujícím obrázku. Pak stačí akorát zadat jméno a heslo Asustor NAS VPN serveru a kliknout na Ok. Připojení k VPN serveru je signalizováno telenou ikonkou.



Obrázek 20: Připojení k NAS serveru přes VPN

Zdroj: [39]

Vytvoření VPN tak umožní otci nebo ostatním členům rodiny bezpečnou práci s daty na NAS serveru i mimo domácnost, například na služebních cestách nebo ze školy.

6.1.7 Zálohování dat

Při zálohování dat v domácnosti se zálohují data, která sám uživatel považuje za důležitá, nejrůznější soubory, elektronická pošta, filmy, hudba a mnohdy se jedná i o zbytečná data, jako instalační soubory programů, které je možné si stáhnout na internetu. Jako zálohovací média se nejčastěji používají flash disky, přenosné HDD nebo CD a DVD. Zálohovat data na domácím počítači v rámci Windows lze jednoduše ručně nebo automaticky přes panel **Zálohování a obnovení**. Stačí klinout na tlačítko **Start - Ovládací panely**, pak na položku **Systém a zabezpečení** a na položku **Zálohování a obnovení**. Pokud se jedná o první zálohování, je potřeba nejprve nastavit zálohování kliknutím na tlačítko Nastavit zálohování. Lze tak nastavit, zda má počítač provádět zálohy pravidelně automaticky sám, nebo je bude provádět ručně uživatel.

ZÁVĚR

Cílem této práce bylo seznámit čtenáře s možnými způsoby obrany dat v počítačových sítích. Nejprve byly popsány základní prvky, které tvoří počítačovou síť, jak softwarové, tak i hardwarové a jaké existují možnosti zabezpečení počítačové sítě, včetně možných útoků.

Hlavní část práce tvořil návrh počítačové sítě. Nejprve byly popsány zásady, které jsou důležité pro vytvoření bezpečné domácí počítačové sítě. Tyto zásady mohou tvořit základ směrnic pro domácnost, jak si vytvořit zabezpečenou domácí počítačovou síť.

V další části potom byl popsán samotný návrh počítačové sítě. Vzhledem k tomu, že domácnost měla všechna zařízení, která chtěla propojit do jedné sítě, pro její vytvoření tak rodině chyběl router a kabeláž. Výběr vhodného routeru byl proveden vícekriteriálním hodnocením pomocí analyticko-hierarchické metody (AHP) ve speciálním programu CDP.

Jediný softwarový prostředek, který rodina k zabezpečení sítě potřebuje nakoupit, je antivirový program. Těch existuje celá řada, každý rok je zveřejňováno několik hodnocení antivirových programů. V práci byly uvedeny dva, které zvítězily v dubnovém testu antivirových programů v dTestu – ESET Smart Securiy a Norton Security.

Jako možné vylepšení celé počítačové sítě byl součástí návrhu i NAS server, tedy síťové datové úložiště. Jedná se o zařízení, které je vhodné jako centrální úložiště dat, pro jejich zálohování a sdílení i několika uživateli na více zařízeních současně. Přístup k nim je možný i vzdáleně. Jeho pořízení je však již relativně finančně náročné a záleží tak na rodině, zda by si ho pořídila.

V poslední části pak byl popsán praktický návod, jak postupovat při zabezpečení počítačové sítě – nastavení routeru, šifrování souborů, antivirová kontrola nebo nastavení firewallu. Veškeré tyto postupy byly vysvětleny v rámci operačního systému MS Windows.

Vzhledem k množství dat, které si v současnosti většina lidí ukládá na počítačích, je potřeba právě bezpečnosti počítačové sítě věnovat dostatečnou pozornost. Tyto sítě jsou často neustále připojeny k internetu a stávají se tak zranitelné proti vnějším útokům. Pokud tedy uživatelé chtějí ochránit svá data, je potřeba se věnovat také jejich zabezpečení.

Navíc zabezpečení počítačové sítě není nijak náročná záležitost a zvládnou to i lidé bez hlubších znalostí počítačů. Náklady na vytvoření i zabezpečení malé domácí počítačové sítě se staly přijatelné pro většinu běžných uživatelů a proto k jejímu vytvoření přistupuje stále více domácností.

POUŽITÁ LITERATURA

[1] HORÁK, Jaroslav; KERŠLÁGER, Milan. *Počítačové sítě pro začínající správce*. Vyd. 1. Brno: Computer Press, 2006. 211 s. ISBN 80-251-0892-9.

[2] JEGER, Dag; PECINOVSKÝ, Josef. *Postavte si vlastní počítačovou sít: podrobný průvodce začínajícího uživatele*. Vyd. 1. Praha: Grada Publishing, 2000. 160 s. ISBN 80-7169-700-1.

[3] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. Vyd. 1. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1.

[4] HORÁK, Jaroslav. *Malá počítačová síť doma a ve firmě*. Vyd. 1. Praha: Grada Publishing, 2003. 184 s. ISBN 80-247-0582-6.

[5] HORÁK, Jaroslav. *Bezpečnost malých počítačových sítí*. Vyd. 1. Praha: Grada Publishing, 2003. 200 s. ISBN 80-247-0663-6.

[6] ODVÁRKA, Petr. *Technologie pro zlepšení bezpečnosti datových sítí – standard 802.1x* [online]. Aktualizace 2004-09-02 [cit. 28. Prosince 2014]. Dostupné na: <http://www.svetsiti.cz/clanek.asp?cid=Technologie-pro-zlepseni-bezpecnosti-datovych-siti-standard-8021x-1-922004>

[7] PUŽMANOVÁ, Rita. *WLAN konečně bezpečné* [online]. Aktualizace 2004-08-07 [cit. 28. Prosince 2014]. Dostupné na: <http://www.lupa.cz/clanky/wlan-konecne-bezpecne/>.

[8] JECH, Vladimír. *Moderní metody zabezpečení uživatelských počítačů* [online]. Aktualizace 2011 [cit. 10. ledna 2015]. Dostupné na: <http://www.systemonline.cz/it-security/moderni-metody-zabezpeceni-uzivatelskych-pocitacu-1-dil.htm>.

[9] KNOPOVÁ, Martina. *Bezpečnost dat v informačních systémech* [online]. Aktualizace 2011 [cit. 11. února 2015]. Dostupné na: <http://ikaros.cz/bezpecnost-dat-v-informacnich-systemech>.

[10] VANĚK, Tomáš. *Autentizační protokoly v telekomunikačních a datových sítích* [online]. [cit. 12. února 2015]. Dostupné na: <http://data.cedupoint.cz/oppa_e-learning/2_KME/044.pdf>.

[11] BURDA, Karel. *Řízení přístupu v počítačových sítích*. Elektrorevue [online]. 2012 [cit. 13. února 2015]. ISSN 1213-1539. Dostupné na: <http://www.svetsiti.cz/clanek.asp?cid=Technologie-pro-zlepseni-bezpecnosti-datovych-siti-standard-8021x-1-922004>.

[12] DOHNAL, Pavel. *Bezpečnost a ochrana dat v počítačových sítích malých organizací*. Praha, 2007. Diplomová práce. Vysoká škola ekonomická v Praze. Fakulta managementu v Jindřichově Hradci. Vedoucí práce Ing. Pavel Pokorný.

[13] BEDNAŘÍK, Jan. *Šifrování souborů ve windows pomocí EFS* [online]. Aktualizace 2013-14-07 [cit. 16. února 2015]. Dostupné na: <http://pcworld.cz/software/jak-na-sifrovani-dat-a-ochranu-systemu-2-dil-46280>.

[14] BEDNAŘÍK, Jan. *Šifrování a dešifrování dat* [online]. Aktualizace 2013-15-07 [cit. 16. února 2015]. Dostupné na: <http://pcworld.cz/software/bezpecnost-predevsim-aneb-jak-na-sifrovani-dat-a-ochranu-systemu-3-dil-46296>.

[15] BEDNAŘÍK, Jan. *Šifrování pro více uživatelů na více počítačích* [online]. Aktualizace 2013-17-07 [cit. 16. února 2015]. Dostupné na: <http://pcworld.cz/software/bezpecnost-predevsim-aneb-jak-na-sifrovani-dat-a-ochranu-systemu-5-dil-46302>.

[16] BEDNAŘÍK, Jan. *Jak celé EFS funguje?* [online]. Aktualizace 2013-22-07 [cit. 16. února 2015]. Dostupné na: <http://pcworld.cz/software/jak-na-sifrovani-dat-a-ochranu-systemu-10-dil-46335>.

[17] BEDNAŘÍK, Jan. *Šifrování pro více uživatelů* [online]. Aktualizace 2013-23-07 [cit. 16. února 2015]. Dostupné na: <http://pcworld.cz/software/jak-na-sifrovani-dat-a-ochranu-systemu-11-dil-46336>.

[18] SIPVZ. *Počítačové viry, zásady počítačové bezpečnosti* [online]. 2005 [cit. 21. února 2015]. Dostupné na: < http://sipvz.amoskadan.cz/pdf/Viry.pdf>.

[19] MICROSOFT. *How to boost you malware defense and protect your PC* [online]. [cit. 21. února 2015]. Dostupné na: <http://www.microsoft.com/security/pc-security/protect-pc.aspx>.

[20] PCPoradenství. *Ze zabezpečení počítače: co je firewall?* [online]. [cit. 21. února 2015]. Dostupné na: <http://www.pcporadenstvi.cz/ze-zabezpeceni-pocitace-co-je-firewall>.

[21] PŘIBYL, Tomáš. *Firewall: software nebo hardware?* [online]. [cit. 21. února 2015]. Dostupné na: <http://www.ictsecurity.cz/odborne-clanky/firewall-software-nebo-hardware.html>.

[22] JUNEK, Pavel. *Zálohování a archivace dat v podnikovém prostředí – 1. díl, základní seznámení* [online]. Aktualizace 2013-07-08 [cit. 21. února 2015]. Dostupné na:

<http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-1-dil-zakladni-seznameni/>.

[23] JUNEK, Pavel. *Zálohování a archivace dat v podnikovém prostředí – 2. díl, Dvojí pohled: domácnost vs. firmy* [online]. Aktualizace 2013-14-08 [cit. 22. února 2015]. Dostupné na: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-1-dil-zakladni-seznameni/>.

[24] WINDOWS. Zálohování souborů [online]. [cit. 22. února 2015]. Dostupné na: <http://windows.microsoft.com/cs-cz/windows/back-up-files#1TC=windows-7>.

[25] JUNEK, Pavel. *Zálohování a archivace dat v podnikovém prostředí – 6. díl, Business Continuity Management* [online]. Aktualizace 2013-11-09 [cit. 22. února 2015]. Dostupné na: <http://www.zalohovani.net/zalohovani-a-archivace-dat-v-podnikovem-prostredi-6-dil-cast-13-business-continuity-management-bcm/>.

[26] THOMAS, M. Thomas. *Zabezpečení počítačových sítí bez předchozích znalostí*. Vyd. 1. Brno: CP Books, 2005. 338 s. ISBN 80-251-0417-6.

[27] PUŽMANOVÁ, Rita. *Bezpečnost bezdrátové komunikace. Jak zabezpečit Wi-fi, Bluetooth, GPRS či 3G*. Vyd. 1. Brno: CP Books, 2005. 179 s. ISBN 80-251-0791-4.

[28] MICROSOFT. *Připojení VPN v intranetu* [online]. [cit. 23. února 2015]. Dostupné na: <https://technet.microsoft.com/cs-cz/library/cc784305(v=ws.10).aspx>.

[29] MICROSOFT. *Připojení VPN v intranetu* [online]. [cit. 24. února 2015]. Dostupné na: <https://technet.microsoft.com/cs-cz/library/cc731954(v=ws.10).aspx>.

[30] KOSTRHOUN, Aleš. *Stavíme si malou síť ve Windows XP a 2000*. Vyd. 1. Brno: Computer Press, 2003. 214 s. ISBN 80-251-0024-3.

[31] GEIER, Eric; KREUZIGER, Pavel. *8 nezbytných funkcí routeru pro domácnost i business – 1. díl* [online]. Aktualizace 2013-03-06 [cit. 27. února 2015]. Dostupné na: <http://pcworld.cz/hardware/8-nezbytnych-funkci-routeru-pro-domacnost-i-business-1-dil-46108>.

[32] GEIER, Eric; KREUZIGER, Pavel. *8 nezbytných funkcí routeru pro domácnost i business – 2. díl* [online]. Aktualizace 2013-07-06 [cit. 27. února 2015]. Dostupné na: <http://pcworld.cz/hardware/8-nezbytnych-funkci-routeru-pro-domacnost-i-business-2-dil-46109>.

[33] HORÁK, Jaroslav. *Vytváříme domácí bezdrátovou síť*. Vyd. 1. Brno: Computer Press, 2011. 293 s. ISBN 978-80-251-2977-7.

[34] ČANDÍK, Marek. *Informační bezpečnosti* [online]. [cit. 10. března 2015]. Dostupné na: <http://www.cybersecurity.cz/data/candik2.pdf>.

[35] DVRČEK, Daniel. *Není nad zámek*…[online]. [cit. 10. března 2015]. Dostupné na: <http://www.fit.vutbr.cz/~cvrcek/system/fyzicka.pdf>.

[36] DORŇÁK, Radek. *Vzduchem ještě rychleji*. Computer: žijte s námi digitálním světem, srpen 2014, č. 8, str. 18 – 29.

[37] KUČERA, Petr. KOS, Dušan. *Stírání rozdílů*. Computer: žijte s námi digitálním světem, duben 2015, č. 4, str. 36 – 43

[38] dTest.cz. *Ochrana počítače*. dTest, duben 2015, str. 42 – 48.

[39] Asustor College. *NAS 323, NAS jako VPN server* [online]. [cit. 25. dubna 2015]. Dostupné na: <http://download.asustor.com/college/cs/NAS_323_Using_Your_NAS_as_a_VPN_Server.pdf>.

SEZNAM PŘÍLOH

Příloha A SWOT analýza autentizacích metod

Příloha A

Strenghts (silné stránky)	Weaknesses (slabé stránky)
• nevyžaduje instalaci speciální HW nebo SW komponenty při přihlašování uživatele • uživatel se může přihlásit odkudkoliv a nepotřebuje k tomu žádná speciální autentizační zařízení • ochranu hesel zesilují kryptografické systémy (zajišťují větší bezpečnost klíče) • jednoduchost používání a spravování • levná • pohodlný mechanismus pro zrealizování •snadno zapamatovatelná • rychlá	• uživatelé si své heslo musí pamatovat v okamžiku, kdy se přihlašují do více systémů • kladeny značné nároky na paměť uživatele • závislé na uživateli (nejslabší složkou systému je lidský faktor) • používání mnoha hesel • slabá forma ochrany • uhádnutí nebo prolomení ochrany •odchycení hesla na softwarové úrovni
Opportunities (příležitosti)	**Threats (hrozby)**
•automatické generování hesel • bezpečnostní příručka • vhodná kombinace číslice a písmena – pokud to aplikace dovoluje • používání delších hesel (hesla o více znacích) • širší kombinace možných bitů (vhodný 64bitový klíč) • kombinace s jinou autentizační metodou • zabezpečovací technologie šifrování	• většina uživatelů používá pro přístup do systémů stejná hesla • velká šance na prolomení hesla • nevhodné pro zabezpečení lokální počítačové sítě (více cílů) • konstantní identifikace/ověřování informací • registrace hesel zdarma=použití hesel pro marketingové účely nikoliv bezpečnostní (výsledkem je šíření hesel) • sociální inženýrství • krádež identity

Obrázek 21: SWOT analýza autentizace znalostí

Zdroj:[9]

Strenghts (silné stránky)	Weaknesses (slabé stránky)
• rychlá zjistitelnost ztráty tokenu • úspěšná autentizace je podmíněna použitím tokenu • autentizační informaci nelze sdílet tak jednoduše jako heslo • jednoduchost používání a spravování • nelze snadno zkopírovat • většinou obsahuje šifrovací klíč chráněný pinem •žádné HW nebo SW úpravy na straně klienta • jednorázový kód (při zasílání ověřovacích SMS-např. mobilní telefon) •chrání uložené kryptografické údaje	• fyzická ztráta, zničení • mechanické poškození • falešná odmítnutí • počítačové viry • vyžaduje tajné informace • potřeba speciální čtečky • bez tokenu není autentizace možná, uživatel jej musí mít stále při sobě • porucha nemusí být vždy jednoduše zjistitelná uživatelem •potřeba token fyzicky vlastnit
Opportunities (příležitosti)	**Threats (hrozby)**
•obtížné kopírování • bezpečné uložení tajné informace-klíč uložený v kalkulátoru • při opakovaném chybném zadání PINu se zablokují • některé při pokusu o násilné vniknutí do přístroje dokonce zničí uchovávanou informaci	• v případě poruchy nebo ztráty je uživatel odkázán na servisní středisko a nemůže autentizace využívat • softwarové chyby • PKI obsahuje velmi dlouhé řetězce znaků a na rozdíl od hesel nejdou tak snadno zapamatovat • zneužití různých chyb v aplikacích • nová rizika

Obrázek 22: SWOT analýza autentizace vlastnictvím

Zdroj:[9]

Strenghts (silné stránky)	Weaknesses (slabé stránky)
• ověření identity osoby -je vysoké • velmi vysoká spolehlivost • používána v bezpečnostních aplikacích (kriminalistika, armáda) • využívání vícefaktorové autentizace (kombinování alespoň s jednou z výše uvedených metod) • měřitelnost – charakteristika by měla být opakovaně měřitelná • nízká míra oklamání systému podvodnými technikami • nemohou být ukradeny ani ztraceny	• především behaviorální charakteristiky často podléhají změnám (hlas, podpis) • stoprocentní ověření osoby není možné • stále ve fázi vývoje, především co se týče přesnosti a rychlosti • nemožnost registrace všech osob (osoby s chybějícími orgány) • zavádění dodatečných informací (které zvyšují náklady a složitost systému a snižují bezpečnost • nutnost neustálé údržby přístrojů
Opportunities (příležitosti)	**Threats (hrozby)**
• prosazuje se ve veřejném sektoru (bankovnictví, kontrola pasů) • uživatel si nemusí pamatovat žádné informace • biometriky nejsou tajné (jako např. heslo) • musí být vždy aktuální a snímány v průběhu autentizace	• možnost okopírování • nedostatečná legislativní úprava • odpor některých uživatelů k biometrikám, nechtějí se podrobit měření, ani ukládání dat do systému • biometrická data nejsou tajná a bezpečnost systému nemůže být založena na jejich utajení • mohou výrazně narušit soukromí uživatele • etické faktory a legislativní omezení • obsahují mnoho citlivých informací • ztráta anonymity

Obrázek 23: SWOT analýza autentizace vlastností

Zdroj:[9