Zabezpečení systému Linux

Linux System Security

Jakub Havlíček

Bakalářská práce
2013

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2012/2013

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jakub HAVLÍČEK**
Osobní číslo:	**A10080**
Studijní program:	**B3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Zabezpečení systému Linux**

Zásady pro vypracování:

1. **Proveďte literární rešerši na téma zabezpečení systému Linux a porovnejte ho se zabezpečením systému Windows.**
2. **Popište nejčastější hrozby současnosti především z pohledu operačního systému Linux.**
3. **V teoretické části formulujte postupy, rady, doporučení apod. k zabezpečení systému Linux proti hrozbám popsaným v předchozím bodě.**
4. **V praktické části tyto rady a postupy realizujte na vybraných distribucích operačního systému Linux včetně podrobného popisu.**
5. **Uveďte nejdůležitější doporučení zabezpečení jednotlivých distribucí.**

Rozsah bakalářské práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.**
2. **VÍTEK, Miloš a Marcela VÍTKOVÁ. Sociální vědy a inženýrství. Vyd. 1. Hradec Králové: Gaudeamus, 2004, 164 s. ISBN 80-704-1474-X.**
3. **TOXEN, Bob. Bezpečnost v Linuxu: Prevence a odvrácení napadení systému. Vydání první. Brno: Computer Press, 2003. ISBN 80-7226-716-7.**
4. **HONTANÓN, J. Ramón a Ludvík ROUBÍČEK. Linux: Praktická bezpečnost. Vydání první. Brno: Grada Publishing a.s., 2003. ISBN 80-247-0652-0.**
5. **KRČMÁŘ Petr. Linux: Tipy a triky pro bezpečnost. Praha: Grada Publishing a.s., 2004. ISBN 80-247-0812-4.**

Vedoucí bakalářské práce: **Ing. Jiří Vojtěšek, Ph.D.**
Ústav řízení procesů

Datum zadání bakalářské práce: **25. února 2013**

Termín odevzdání bakalářské práce: **30. května 2013**

Ve Zlíně dne 25. února 2013

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Bakalářská práce je zaměřena na problematiku zabezpečení operačního systému Linux. V teoretické části této práce se seznámíte s úvodem do operačního systému Linux, výhodami oproti konkurenčnímu systému Windows a dále pak s jednotlivými prvky zabezpečení. V praktické části jsou realizovány rady a postupy, jak operační systém Linux zabezpečit. V neposlední řadě jsou zde uvedena určitá doporučení pro bezpečnost tohoto operačního systému.

Klíčová slova: Linux, bezpečnost, operační systém [OS], software, hardware, Windows, uživatel

ABSTRACT

This Bachelor thesis is focused on the issues of security of OS Linux. In the theoretical part of this thesis you will be familiar with an introduction to the Linux OS, advantages and disadvantages over the competitive OS Windows and then with individual elements of the security. In the practical part are implemented some hints and procedures how to secure OS Linux. In the end, there are some recommendations for the safety of the OS Linux.

Keywords: Linux, security, operating system [OS], software, hardware, Windows, user

Rád bych poděkoval vedoucímu své bakalářské práce Ing. Jiřímu Vojtěškovi Ph.D. za jeho odborné vedení a podnětné rady. Dále děkuji své rodině za podporu.

Prohlašuji, že

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

Prohlašuji,

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

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Počítačová bezpečnost je v dnešní době čím dál více řešeným tématem. Počítače se dnes používají k různým věcem. Hlavní věcí je ta, že jsou v něm uložena data, informace a ty mají ve většině případů hodnotu daleko větší než samotný počítač. Právě proto se mnoho lidí snaží dostat k informacím cizím, ať už za účelem zbohatnutí, špionáže nebo z dalších důvodů. Pokud je počítač připojen k veřejné síti – internetu, riziko je o to větší. Každý by si měl chránit svá data, aby se nedostali do nepovolaných rukou.

Dnešní počítače fungují ve většině případů na komerčním operačním systému Windows od firmy Microsoft. Tato práce bude ale zaměřena na jeho nejbližší konkurenci a tou je operační systém Linux. Linux je možné stáhnout, nainstalovat a pracovat na něm zadarmo. Používá se jak na desktopech, tak na serverech. Říká se, že z hlediska bezpečnosti je na tom lépe právě méně používaný Linux. Linux je totiž uložen v podvědomí běžných uživatelů pod pojmy – složitý, náročný na ovládání, instalace a práce přes příkazový řádek. Ano, dříve se Linux možná takhle prezentoval, ovšem dnes je tomu jinak. Z hlediska uživatelské přívětivosti se Linux posunul obrovským krokem kupředu, blíže Windows. Teď už záleží jenom na uživatelích, který z operačních systémů, budou používat.

Bakalářská práce porovnává výhody/nevýhody Linuxu proti Windows. Dále jsou popisovány rady a typy na zabezpečení operačního systému Linux proti nebezpečí, které mu může hrozit. Praktická část se zabývá realizováním některých doporučení, které by měl uživatel dodržet při používání operačního systému Linux.

Ať už používáte jakýkoli operační systém, mějte na paměti, že pokud si nedáte pozor a nebudete dodržovat určitá pravidla bezpečnosti, tak můžete přijít o víc, než jen počítač.

I. TEORETICKÁ ČÁST

1 CO JE TO LINUX?

1.1 Charakteristika

Linux je stejně jako Microsoft Windows nebo Mac OS operační systém (OS). Linux je označení pro Unixový OS. Je to jádro operačního systému, které společně s programovým vybavením, aplikacemi, utilitami a grafickým rozhraním tvoří OS. Název Linuxu je odvozený ze jména Linuse Torvaldse, který tento systém začal tvořit. Spolu s dalšími programátory z celého světa se Linux rozvíjel a dostal se až do dnešní podoby. Linux je šířen pomocí takzvaných Linuxových distribucí. Některé z nich budou v další části této práci zmíněny. Linux se od jiných operačních systémů liší hlavně v tom, že je poskytován s licencí, která uživatele neomezuje. Naopak, za dodržení právních podmínek je dovoleno kopírovat a poskytovat Linux a jeho software dalším osobám. To u jiných operačních systémů provádět nelze, protože by byl porušen zákon. Hlavním pozitivem Linuxu, je takzvaný Open Source (otevřený kód). Ten umožňuje uživatelům získávat zdrojové kódy programů, popřípadě i jádra systému, a dále je upravovat a rozvíjet. Pro ochranu před zneužitím zdrojových kódů se používají různé licence. [15]

Jádro Linuxu je chráněno a šířeno pod licencí GPLv2 (General Public License), což do češtiny přeloženo znamená – všeobecná veřejná licence. Tato licence byla napsaná Richardem Stallmanem. Dalo by se říci, že se jedná o licenci, která uživatelům počítačového programu poskytuje právo svobodného softwaru. Jedná se o licenci, která vyžaduje, aby další díla, která vzniknou z děl chráněných pod touto licencí, byla dostupná pod stejnou licencí. [12]

Distribuce Linuxu jsou také chráněny různými licencemi (LGPL, MPL, BSD licence). Jádro Linuxu podporuje multitasking (běh více programů „současně“). Linux je také víceuživatelský OS, to znamená, že je na něm schopno pracovat více uživatelů zároveň. Proto jsou v Linuxu zavedeny uživatelské účty, které jsou chráněny autentizačním mechanismem (jména + heslo). K tomu jsou též zavedena přístupová oprávnění, která umožňují omezit přístup jednotlivých uživatelů k souborovému systému (soubory a adresáře). Linux, ke svému běhu nepotřebuje žádné extrémní hardwarové nároky. Je schopný fungovat v příkazové řádce, ale aby se stal více uživatelsky přístupnější, tak začal používat různá grafická prostředí (GNOME, KDE atd.). To má za následek i vyšší hardwarovou náročnost. Ovšem ne všechen hardware je kompatibilní s Linuxem. Logem

a maskotem Linuxu se stal přátelský tučňák Tux, který je zobrazen na obrázku č. 1. Vychází z obrázku Larryho Ewinga z roku 1996. [13]

Obrázek 1 – Tučňák Tux

1.2 Historie

V roce 1991 začal vývoj jádra, které nakonec dostalo jméno Linux. Původně ho začal psát student Linus Torvalds, který studoval informatiku na helsinské univerzitě. Torvalds vycházel z Minixu, což byl zjednodušený klon Unixu napsaný Andrewem Tanenbaumem pro účely výuky návrhu operačních systémů. Tanenbaum ovšem nikomu nedal svolení k úpravě svého systému, a tak Torvalds napsal vlastní náhradu Minixu. První verze Linuxového jádra (0.01) byla vydána na Internetu 17. Září 1991. O tento rozpracovaný systém byl velký zájem. Programátoři začali Linusovi posílat další podněty, opravy a zdrojové kódy. A tak další verze následovala už v říjnu téhož roku. Od té doby se na tomto projektu podílely tisíce vývojářů z celého světa. Linuxový systém zanedlouho předběhl Minix co do funkčnosti. Torvalds a další vývojáři uzpůsobili jádro tak, aby lépe spolupracovalo s komponentami z projektu GNU a s dalšími uživatelskými programy, aby tak vzniknul plně funkční, svobodný OS. Linus Torvalds dodnes pokračuje přímo ve vývoji jádra, zatímco ostatní subsystémy jako třeba GNU komponenty jsou vyvíjeny samostatně. Vývoj kompletních systémů, které zahrnují základní systém spolu s grafickými prostředími jako KDE a GNOME a množstvím aplikačního softwaru, dnes obstarává mnoho distribucí. Linuxové distribuce dnes vyvíjejí a spravují neziskové organizace, komerční společnosti ale i jednotlivci. [15]

1.3 Distribuce

GNU/Linux není jeden OS. Dalo by se říct, že je to označení pro řadu relativně nezávislých projektů, jejichž sestavením vznikne konkrétní OS. Operačním systémům založeným na GNU/Linuxu se říká distribuce. V dnešní době existuje mnoho distribucí operačních systémů založení na jádře Linuxu. Samozřejmě existují různá kritéria pro výběr distribuce. Která se Vám bude hodit nejvíce? Některé jsou určení pro běžné uživatele, jiné zase pro pokročilé uživatele, některé jsou univerzální a jiné mají velmi specifické použití, atd. Jelikož v dnešní době je distribucí Linuxu celá řádka, výběr pro začínajícího uživatele bývá většinou kritický, protože když si vybere špatně, tak jeho volba ho může velmi snadno odradit od celého Linuxu.

1.3.1 Live CD

Jedná se o nabootovatelný disk, ze kterého je možné bez nutnosti instalace spustit kompletní OS Linux. Live CD nevyužívá pevného disku počítače. To znamená, že nic neukládá a po vyjmutí tohoto CD z mechaniky a restartování počítače se Vám načte původní OS. Live CD ukládá svá potřebná data do dočasné paměti, např. RAM. To má ovšem za následek zpomalení výkonu počítače. Live CD je velmi dobrou volbou, pokud si potřebujete vyzkoušet nový OS a nechcete ho prozatím instalovat přímo na Váš pevný disk. [14]

1.3.2 Ukázky Linuxových distribucí

Tato část práce se bude zabývat několika Linuxovými distribucemi. Některé z nich se hodí spíše pro začátečníky, některé pro pokročilé uživatele. Dále je možné distribuce rozdělit na uživatelské a distribuce určené pro server.

Ubuntu

V současné době je Ubuntu hojně využívanou distribucí, která se hodí i pro začínající uživatele. Ubuntu vychází z distribuce Debian. Jedná se o nekomerční variantu, která vychází zhruba každého půl roku a dokonce je i možné si ji nechat poslat poštou. Ubuntu má k dispozici velké množství softwaru. Díky spoustě uživatelů, kteří Ubuntu používají, se vytvořila velmi ochotná komunita. Distribuce Ubuntu má přibaleno i spoustu návodů na to, jak co udělat. Instalační médium je zároveň i Live CD. Zdarma ke stažení z webu *www.ubuntu.com.*

OpenSUSE

Tuto distribuci spravuje společnost Novell. Jedná se o nekomerční variantu distribuce SuSe. Díky svému komplexnímu ovládacímu centru Yast a řadou grafických konfiguračních nástrojů se tato distribuce stala uživatelsky přívětivou a získala si hodně uživatelů. Samozřejmě i pro tuto distribuci existuje celá řada návodů, článků a diskusních fór, na které je možno se obrátit při jakýchkoli potížích. Oficiální stránky distribuce *www.opensuse.org*

Fedora

Jedná se o distribuci, která je pod taktovkou společnosti RedHat. Jako většina Linuxových distribucí, tak i tato je nekomerční. Fedora obsahuje některé grafické konfigurační nástroje, které ji umožňují pohodlněji používat, ale příkazové řádce se zřejmě vyhnout nedá. Česká dokumentace a diskusní fóra jsou samozřejmostí. Dostupné z webu *fedora.cz*

Debian

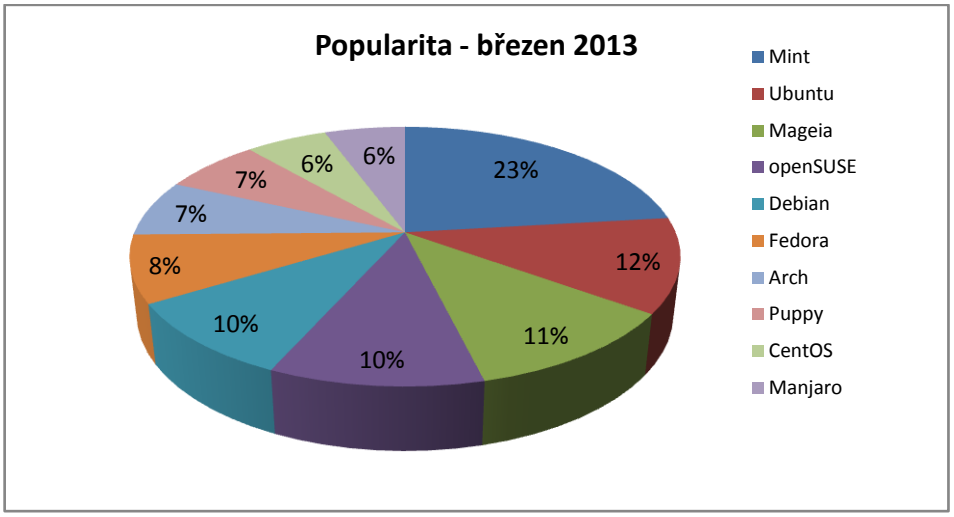
Jedná se o jednu z nejstarších a nejrozsáhlejších distribucí. Mnoho věcí se v Debianu konfiguruje ručně, proto je spíše určena pokročilejším uživatelům. Vychází z něj distribuce Ubuntu, která je více uživatelsky přívětivá. Nejčastěji se Debian používá pro serverové řešení. Ke stažení z internetových stránek *www.debian.org*

Mint

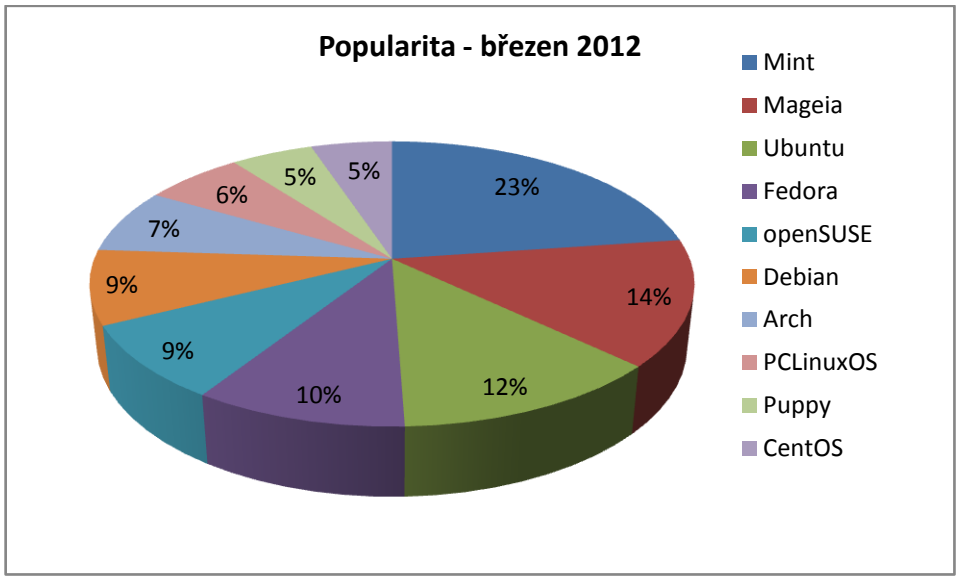
Podle serveru *http://distrowatch.com* se v současnosti jedná o nejoblíbenější Linuxovou distribuci (porovnání lze vidět v další podkapitole), která vychází z Ubuntu. Mint se oproti Ubuntu liší hlavně v grafickém uspořádání plochy a uživatelským rozhraním a kolekcí systémových nástrojů pro snadnější správu systému a uživatelských práv. Je to elegantní a pohodlná distribuce Linuxu, která je výkonná a snadno ovladatelná. Zdarma ke stažení z webu *www.linuxmint.com*

1.3.3 Nejoblíbenější distribuce

Jak je vidět z grafů, za poslední rok se pořadí oblíbenosti OS nějak extrémně nemění. Jednoznačně nejoblíbenějším systémem minulého roku je Mint. Na dalších místech se postupně umisťuje Ubuntu, Mageia, Fedora, OpenSUSE a Debian. Tyto informace jsou uveřejněny na serveru *http://distrowatch.com*, kde každý může zhodnotit danou distribuci. [20]



Obrázek 2 – Graf oblíbenosti distribucí 2013



Obrázek 3 – Graf oblíbenosti distribucí 2012

	2012		2013			2012		2013	
1.	Mint	23%	Mint	23%	**6.**	Debian	9%	Fedora	8%
2.	Mageia	14%	Ubuntu	12%	**7.**	Arch	7%	Arch	7%
3.	Ubuntu	12%	Mageia	11%	**8.**	PCLinuxOS	6%	Puppy	7%
4.	Fedora	10%	openSUSE	10%	**9.**	Puppy	5%	CentOS	6%
5.	openSUSE	9%	Debian	10%	**10.**	CentOS	5%	Manjaro	6%

Tabulka 1 – Srovnání popularity distribucí 2012/213

2 LINUX VS WINDOWS

Než se zaměříme přímo na bezpečnost Linuxu, tak zhodnotíme dva operační systémy, které mezi sebou vedou tichou válku už hodně dlouho. Jedná se o systém od firmy Microsoft Windows a o Linux. Všude po internetu se vedou rozsáhlé diskuse o tom, který z těchto systémů je lepší a proč. Uveďme si tedy pár smysluplných informací, které o této problematice existují, a pokusme si je osvětlit. Nejrozšířenějším operačním systémem mezi uživateli je Windows. Linux mu z tohoto hlediska konkurovat nemůže. Rozdíly v těchto operačních systémech jsou opravdu velké a pro uživatele je těžké si vybrat, který z nich používat.

Linux nebo Windows? Windows nebo Linux? U takového rozhodování se už určitě pozastavila velká řádka uživatelů, kteří nevěděli, pro jaký systém se rozhodnout. Člověk si musí položit pár základních otázek, jejichž odpovědi ho dovedou k tomu pravému operačnímu systému právě pro něj. První a zřejmě nedůležitější otázkou je ta, co budu s operačním systémem dělat a na co ho budu používat. Pokud ho budu chtít používat takzvaně „na doma“, budu na něm chtít používat základní programy, spouštět hry a prohlížet internet, tak si uživatel nejspíše vybere Windows. A to z toho důvodu, jelikož je nejrozšířenější, je snadno ovladatelný a pracuje v pěkném a jednoduchém grafickém prostředí, je podporovaný převážnou většinou hardwaru a je na něj k sehnání nepřeberné množství různých programů a aplikací. Další a to velmi důležitá otázka je ta, kolik jsme schopni do takového operačního systému investovat peněz. Jak už bylo zmíněno, většina Linuxových distribucí je zdarma, což se dá považovat za hlavní výhodu oproti Windows, jehož pořizovací náklady se pohybují v rámci tisíců korun. Další hodně diskutovanou otázkou je právě bezpečnost systému. Když teď srovnám jenom to, kolik počítačových virů může „chytit“ Windows a Linux, tak je to celkem nepoměr. Na OS Windows existují tisíce různých virů, oproti tomu viry na Linux by se daly spočítat na prstech jedné ruky, možná na dvou. Samozřejmě otázka bezpečnosti záleží hlavně na uživateli – administrátorovi. Existují i další otázky, podle kterých si uživatel vybere svůj OS, ale to už je výhradně na něm. Pro snadné zobrazení výhod a nevýhod u systémů Windows a Linux, byla vytvořena tabulka, která je zobrazena v příloze č. I. [17]

2.1 Výhody Linuxu

- Většina distribucí je zdarma (Open-source licence)
- Časté aktualizace, vysoká bezpečnost díky velkému množství testerů
- Velké množství distribucí
- Live CD (spuštění systému bez nutnosti instalace)
- Nízké hardwarové nároky

Velké množství distribucí, ve kterých je Linux dodáván, je určitě výhodou. Dokáže pokrýt individuální potřeby a vkus zákazníků (systém pro netbooky, pro starší PC, s grafickým prostředím, pro účely vzdělávání, pro tvorbu grafiky a multimédií). Výhoda z hlediska bezpečnosti – pro Linux neexistují životaschopné viry, červy a malware. Tyto problémy se na Linuxu nevyskytovaly a doufejme, že se neobjeví ani v budoucnu. Další výhodou Linuxu oproti Windows je bezúdržbovost. V Linuxu není třeba „čistit a uklízet“ jako ve Windows. Je možné tvrdit, že Linux po nainstalováni funguje takřka do nekonečna. Dalo by se říci, že nemusíte defragmentovat disk (pokud máte dobře zvolený souborový systém a na pevném disku zhruba přes 20% volného místa). Nové instalace a bezpečnostní aktualizace Vás neobtěžují restartem počítače. Výhoda v otázce licence. U Linuxu můžete provádět bezplatně neomezený počet instalací a distribuci volně využívat, legálně a bezplatně distribuci stahovat z internetu přímo od výrobce. Další výhodou v Linuxu je vybavenost. S distribucí se dodává i software jako kancelářský balík, nástroje pro práci s grafikou atd. U Windows se za legální verze takového softwaru platí tisíce korun. Nízké hardwarové nároky pro spuštění Linuxu určitě potěší u uživatele, kteří mají počítač třeba i deset let starý. Pro Ubuntu je doporučovaná konfigurace alespoň 700MHz procesor, 400MB operační paměti a 1GB diskového prostoru. [18]

2.2 Nevýhody Linuxu

- Nižší kompatibilita hardwaru než u Windows
- U některých distribucí složité ovládání
- Menší výběr softwaru než u Windows

Tím, že se Linux nesnaží napodobovat Windows, tak pro většinu uživatelů je přechod z Windows na Linux složitější. Jak již bylo zmíněno, spousta modelů hardware nemá zajištěnou podporu pro Linux. Sice existují ovladače právě pro Linux, někdy to ale

trvá týdny, měsíce než je výrobce vydá. Stále toho mnoho pod Linuxem nejde korektně zprovoznit. Dalším problémem u Linuxu je (oproti Windows) nedostatek softwaru vyvíjeného právě pro něj. Tyto nedostatky se týkají zejména graficky náročných 3D her (Na Linux existuje jen několik málo nativních 3D her – Glest, OpenArena). Pro uživatele desktopů je toto zásadní problém. V souvislosti s nedostatkem profesionálních aplikací je často uváděn AutoCAD. Pro většinu uživatelů se zdá Linux složitějším v těchto aspektech – Linux nabízí velké možnosti výběru a konfigurace – Systém udělá přesně to, co zadáte – Systém není navržen tak, aby administrátor náhodně zkoušel různé postupy s nadějí, že se problém nějak vyřeší (místo zkoušení by se měla číst nápověda, chybové výstupy a přemýšlet) – V návodech se obvykle uvádí univerzální příkazy do terminálu, protože grafické nadstavby mohou být u každé distribuce jiné (Práce v příkazové řádce ne každému vyhovuje). [19]

2.3 Výhody Windows

- Nejpoužívanější OS
- Kompatibilní s většinou hardwaru
- Velký výběr softwaru a jeho vysoká propracovanost
- Velmi pokročilé funkce systému

Výhody operačního systému Windows jsou zcela zřejmé. Jeho rozšiřitelnost zaručila firmě Microsoft to, co Linux zatím postrádá. Návyk většiny uživatelů. Ať už se podíváte kamkoliv (z hlediska počítačů), tak ve většině případů narazíte na Windows. Tohle usnadňuje výběr většině uživatelů operačního systému. Uživatelé prostě obdrží Windows už třeba při koupi svého PC. To většinu uživatelů vedu k závěru, že znají jenom Windows. [17]

2.4 Nevýhody Windows

- Vyšší nároky na hardware
- Vysoká pořizovací cena (i softwaru)
- Velké množství virů, červů atd. (snížení bezpečnosti systému)

Bude zde citován výrok Scotta Grannemana „*To mess up a Linux box, you need to work at it; to mess up your Windows box, you just need to work on it*.“ To volně přeloženo do češtiny znamená „*Abyste rozbili Linux, musíte na tom zapracovat; k rozbití Windows*

Vám postačí s ním pracovat.“ Windows má potíže se stabilitou. Může to být způsobeno již architekturou Windows (uzavřeností, registry, správou knihoven atd.). Vzhledem k absenci centralizované správy softwaru se Windows při instalaci a odinstalaci softwaru zanáší, hromadí se problémy, zanáší se registry. To všechno vede k pozdější reinstalaci systému. Někteří uživatelé mohou vidět problém Windows v bezpečnosti. Zkušený uživatel si dokáže svůj systém, ať už je to Linux nebo Windows, správně zabezpečit. Ovšem s viry, spyware, malware a podobnými nepříjemnými záležitostmi se uživatel Windows setkává skoro každý den. Je tedy potřeba klást důraz a to i větší námahu na zabezpečení Windows oproti Linuxu. [17]

3 BEZPEČNOST LINUXU

Bezpečnost Vašeho operačního systému, v tomto případě Linuxu, mohou ohrozit zejména dva základní faktory. Mezi první určitě patří příroda a fyzikální jevy. Nejhorší na nich je to, že někdy se nedají předvídat a proto je třeba být připraven na různé situace, které mohou nastat. Druhým faktorem je určitě ten lidský. Na světě existuje spousta lidí, kteří prahnout po tom, dostat se do Vaše počítače, zjistit spousty informací, ukrást spoustu dat nebo Váš počítač použít pro jiné účely. Dělají to buď pro svou vlastní zábavu a pocit, kterým si něco dokazují, nebo jednoduše pro peníze. Spoustu uživatelů si myslím, že si nainstalují systém a tím to končí, hlavně u systému Linux, o kterém se často tvrdí, že je bezpečný. Z jisté stránky je to pravda, rozhodně je bezpečnější než Windows. Ovšem i po tom, co Linux nainstalujete, nemáte vyhráno. Pro úplné zabezpečení svého systému, je třeba toho udělat ještě spoustu. V této práci, bude zmíněno pár věcí, rad a tipů, které Vám mohou pomoci svůj OS Linux zabezpečit.

3.1 Social engineering

Jedná se o jednu z mnoha metod průniku do systému, která plně využívá lidského faktoru. Běžný uživatel se stává pro útočníka snadnou obětí a to zejména z neznalosti základních pravidel bezpečnosti. Při jejich porušení uživatel útočníkovi velmi usnadní přístup do systému. Útočníci jsou si vědomi možnosti selhání lidského faktoru. Je pro ně mnohem jednodušší se na heslo zeptat, než jej složitě analyzovat a dešifrovat. Uveďme si názorný příklad.

Aby se útočníkovi podařilo z uživatele informace dostat, musí splnit několik málo podmínek:

- Musí mít komunikační kanál směrem do firmy (e-mail, telefon atd.)
- Potřebuje základní informace o firmě, o jejich vnitřním uspořádání, znát pár jmen je také výhodou.
- Připravit si pár vět a trošku zapracovat na psychologii (jistý hlas atd.)

Malá ukázka telefonního hovoru ve větší firmě:

Uživatel: „Dobrý den, firma ABC, u telefonu Novák“

Útočník: „Dobrý den pane Novák, tady je IT oddělení, inženýr Šebesta, máme tu malý problém s Vaším účtem, nějak nám z něj zmizela data“

Uživatel: „Cože? Já jsem zase určitě něco pokazil! To je strašné, mám tam faktury za poslední tři roky! Co mám dělat?“

Útočník: „Nebojte se, pokusíme se tento problém vyřešit, jaké je přesně Vaše uživatelské jméno?“

Uživatel: „Novak.T“

Útočník: „Aha, už to vidím a Vaše heslo?“

Uživatel´: „K čemu potřebujete heslo?“

Útočník: „No… jinak se k tomu nedostanu a nemůžu to opravit.“

Uživatel: „Aha, heslo je ‚stromeček‘.“

Útočník: „Moment… ano, všechno už je opraveno, faktury máte zpátky.“

Uživatel: „Uf, to jsem rád, děkuji mnohokrát, nashledanou.“

U sociálního inženýrství se nemusí jednat jenom o nepřímou komunikaci, ale také je potřeba dát si pozor na klasické věty typu – „Tak jsem tady, jdu Vám opravit tu kopírku“. Proti sociálnímu inženýrství je třeba se bránit. Nejlépe pomůže především osvěta uživatelů, kterým je potřeba to názorně vysvětlit na příkladu. A taky fakt, že heslo nesmějí nikomu dávat! [5]

3.2 Fyzické zajištění serveru

Velmi důležitou věcí, kterou je třeba brát v potaz, je ta, že pokud se každý útočník dostane přímo ke zdroji, v tomhle případě máme na mysli server, data, tak mu tím zcela usnadníme přístup do naší sítě, k našim datům. Pokud se tak stane, tak nám pomůže už jenom šifrovaný souborový systém. Abychom tomu předešli, je potřeba si vyhradit speciální místnost, ve které budeme udržovat náš server, data v bezpečí. Přístup do této místnosti by měl být povolen jenom několika málo pověřeným osobám a tato místnost by měla být dobře zajištěna. Dalšími kritickými místy, kterými usnadníme útočníkovi průchod do našeho systému, mohou být metalické rozvody vedené budovami, switche, které nebudou dostatečně chráněné proti nedovolené manipulaci s nimi. Samozřejmě náš server nemusí zničit jenom člověk. Může se jednat i o běžné fyzikální vlivy, které to jsou a jak se proti nim bránit je uvedeno a vysvětleno níže. Otázka fyzického zajištění serveru je dobře popsána v knize od Petra Krčmáře – Linux tipy a triky pro bezpečnost. [5]

Elektřina – je klíčová pro chod výpočetní techniky. Jelikož jsou na ní počítače tak závislé, jsou zároveň citlivé na její výkyvy. Výpadek napětí dokáže vyřadit z provozu i celou síť. Proto je velmi důležité pořídit na kritická místa v síti UPS (zdroj záložního napájení), který zabezpečí chod i během výpadku napětí. Správný UPS zdroj udrží systém v plném provozu tak dlouho, aby uložil rozdělanou práci, odpojil disky a vypnul se. UPS jsou jedinou ochranou před nevyhnutelnými výchylkami v provozu elektrické sítě.

Teplota a vlhkost vzduchu – často podceňovaní nepřátelé elektroniky. Servery, počítače samy o sobě vyrábí velké množství tepelné energie a proto je potřeba místnosti, kde jsou uložené dostatečně klimatizovat. Klimatizace dokáže vyřešit i problém s vlhkostí, která by mohla vést ke zkratování obvodů.

Oheň – nepřítel, který zničí skoro vše. Je potřeba se proti němu bránit, ať už dodržováním běžných protipožárních pravidel (používání nehořlavých materiálů, zákaz práce s otevřeným ohněm) nebo kvalitním, ideálně automatizovaným protipožárním systémem. Ideální rozmístění a výběr hasicích přístrojů (práškové).

Voda – dokáže napáchat velké škody, pokud přijde do styku s elektřinou. Proto je velmi důležité, bránit se před záplavami, prasklými vodovodními rozvody atd. Toto riziko lze dostatečně omezit vhodným umístěním strategických bodů, ve kterých se bude uchovávat důležitá techniku.

3.3 Práva souborů a adresářů

Linux je víceuživatelský systém, a proto je nutné zajistit, co kteří uživatelé nesmí a někteří naopak smí se systémem dělat. Každý soubor i adresář v Linuxu má přidělená práva, která upravují práci se souborem. Tradiční Unixová oprávnění jsou rozdělena do tří trojic. Každý soubor a adresář má oprávnění pro:

- Vlastníka (user)
- Skupinu (group)
- Ostatní uživatele (others)

Každé oprávnění se skládá ze tří práv:

- r – čtení (read)
- w – zápis (write)
- x – spuštění souboru nebo vstupu do adresáře (execute)

Z toho vyplývá, že se přístupová práva určují podle nejkonkrétnější trojice, tj. pokud k souboru přistupuje vlastník, pak se na něj aplikují pouze práva z první trojice (vlastníka). Pokud k souboru přistupuje ten, který není vlastník, ale patří do stejné skupiny jako soubor, tak se na něj uplatňuje trojice oprávnění pro skupinu. A pokud k souboru nebo adresáři přistupuje uživatel, který není ani jeho vlastník a ani nepatří do stejné skupiny, tak se na něj vztahuje poslední trojice a to oprávnění pro ostatní uživatele.

Ukázka – výpis práv k systémovému souboru *fdisk*: `ls -l /sbin/fdisk`

```
-rwxr-x--- 1 root   spravci 73432 dub 15 2013 /sbin/fdisk
```

Z tohoto výpisu vyplývá, že jeho majitel *root* může soubor číst, spouštět i do něj zapisovat. Uživatelé ve skupině *spravci* jej mohou pouze číst a spouštět a ostatní uživatelé na soubor nemají žádná práva.

Význam oprávnění pro soubory a adresáře se trochu liší. Tyto odlišnosti jsou znázorněny v tabulce.

	Soubor	**Adresář**
Read	čtení obsahu souboru	výpis obsahu adresáře
Write	zápis do souboru	zápis do adresáře (vytváření, mazání, přejmenování
eXecute	spouštění (program, skript)	vstup do adresáře

Tabulka 2 – Oprávnění pro soubory a adresáře

Změna oprávnění

Změnu oprávnění je schopný provést buďto majitel souboru nebo správce počítače (*root*). Oprávnění lze zadávat dvěma způsoby. Oktalově nebo symbolicky. Pro změnu práv slouží příkaz `chmod`.

V oktalovém zápisu je každá trojice (vlastník, skupina, ostatní) reprezentována jedním číslem, jehož hodnota je dána bitovým vyjádřením práv *rwx*. (součet existujících oprávnění). 4 -2 -1 představují hodnoty pro jednotlivá oprávnění.

- Čtení – read: r; 4
- Zápis – write: w; 2

- Spuštění – exekute: x; 1
- Ukázka – `chmod 750 soubor.txt`
  Nastaví práva na *soubor.txt* (pro vlastníka čtení, zápis, spouštění, pro skupinu čtení, spouštění, pro ostatní nic)

V symbolickém zápisu musíme nejprve zdůraznit, komu jsou práva přidělována, jestli vlastníkovi, skupině nebo ostatním. (**u:** Vlastník-user, **g:** Skupina-group, **o:** Ostatní-others) Poté se zapisuje operace s oprávněními (**+:** přidej, **-:** odeber, **=:** nastav). Nakonec se do zápisu píše, jaká práva se budou nastavovat (**r:** čtení-read, **w:** zápis-write, **x:** spuštění, execute).

- Ukázka – `chmodug=rwx soubor.txt`

Nastavení práv na *soubor.txt* pro čtení, zápis, spouštění pro majitele a skupinu.

3.4 Uživatelé, skupiny, hesla

U Unixových víceuživatelských systémů je potřeba od sebe jednotlivé uživatele oddělit a chránit jejich běžící procesy a data. Řadoví uživatelé mají proto velmi omezené možnosti a mohou pracovat jen s běžnými programy či zapisovat pouze do svého domovského adresáře. Systémové části by však určitě měly zůstat řadovým uživatelům přístupny maximálně ke čtení, aby do nich nemohl nijak zasahovat. Právě proto je v každém systému definován alespoň jeden uživatel, která má všechna privilegia – *root*, superuživatel, správce neboli administrátor. Tento privilegovaný uživatel má v podstatě v systému neomezené možnosti.

3.4.1 Uživatelé

Uživatelské účty jsou jasně definovány v databázi textového souboru */etc/passwd*. Na každém řádku tohoto souboru je uveden jeden účet. V řádku jsou od sebe jednotlivé položky odděleny dvojtečkou. Struktura záznamu je pevně dána takto:

```
prihlasovaci.jmeno:heslo(je-li uvedeno):UID:GID:Plné
Jméno:/domaci/adresar:/implicitni_shell

havlicekj:x:1001:1001:Jakub Havlicek:/home/havlicekj:/bin/bash
```

Každý řádek v tomto souboru obsahuje informace o jednom uživateli, které jsou oddělené dvojtečkou v následujícím pořadí:

Přihlašovací jméno

Přihlašovací jméno může obsahovat malá písmena ASCII tabulky a některé speciální znaky (většinou je povolena pomlčka a tečka). Velká písmena se nedoporučují používat, jelikož mohou způsobit problémy při doručování elektronické pošty, ve které při adrese záleží na velikosti písmen.

Heslo

Heslo se v dnešní době už neukládá do souboru */etc/passwd*, dnes je na této pozici většinou písmeno x, jelikož heslo je uschováno v souboru */etc/shadow* (kvůli ochraně proti útoku). Je to z toho důvodu, že soubor */etc/passwd* má nastavena taková oprávnění, že se do něj mohou podívat i běžní uživatelé, takže i případný útočník. Například pomocí slovníkového útoku by heslo mohl rozluštit. Proto se hesla začaly ukládat do souboru */etc/shadow*, ke kterému má přístupná práva pouze administrátor.

- Ukázka hesla ze souboru */etc/shadow*:

```
root:PV/67t9IGetjU:0:0:root:/root:/bin/bash
```

- Ukázka oprávnění na soubor */etc/shadow*

```
-rw-r----- 1 root shadow 623 dub 15 12:35 /etc/shadow
```

- Ukázka oprávnění na soubor */etc/passwd*

```
-rw-r--r-- 1 root root 1613 dub 18 11:23 /etc/passwd
```

UID

UID je identifikátor, který je pro každý systém jedinečný. Tím je zapříčiněno to, že u souborů je místo jména vlastníka uloženo jeho UID. Až pomocí */etc/passwd* se zjišťuje, kdo je skutečným vlastníkem souboru.

GID

Je identifikační číslo skupiny, podobně jako u UID, identifikuje primární skupinu, do níž uživatel patří.

Plné jméno

Obvykle jméno a příjmení uživatele. Občas se za čárky uvádí ještě kancelář a telefony. Plné jméno je využíváno některými programy (např. klient elektronické pošty, který plné jméno používá implicitně pro jméno odesílatele). Uživatel si může své plné

jméno měnit příkazem `chfn`. V dnešní době tato položka slouží spíše jen pro lepší orientaci administrátora.

Domácí adresář

Slouží pro uložení konfiguračních souborů a uživatelských dat. Konfigurační soubory typicky začínají tečkou a jsou skryté. Většinou jsou domácí adresáře umístěny v */home/prihlasovaci.jmeno*, ale není to pravidlo. Do domácího adresáře je obvykle při založení uživatele nakopírován obsah adresáře */etc/skel*, který obsahuje několik implicitních uživatelských konfiguračních souborů. (např. *~/.bashrc* pro inicializaci shellu BASH při přihlášení)

Implicitní shell

Je interpret příkazů, který je spouštěn při přihlášení uživatele, což je typicky */bin/bash*. Uživatel si může změnit implicitní shell za použití příkazu `chsh`. Může ale vybírat jenom z těch, které jsou uvedeny v souboru */etc/shells*. [6]

3.4.2 Skupiny

Uživatelské skupiny slouží k diferenciaci uživatelských pravomocí. To znamená rozdělování uživatelů právě do skupin, na kterých jsou nastavena různá oprávnění. Vezměme si například, že některým uživatelům chceme zakázat hraní her. Přiřadíme je tedy do skupiny Game, na které budou nastaveny příslušná oprávnění a všichni uživatelé v této skupině budou sdílet tato oprávnění. Každý uživatel musí být alespoň v jedné skupině. Ovšem může patřit i do více skupin. Tímto způsobem je možné kombinovat práva podle potřeb uživatele. Skupiny, jejich nastavení a členové jsou vedeny v souboru */etc/group* a hesla jsou na tom podobně jako u uživatelů, takže jsou umístěna v jiném souboru */etc/gshadow*. Řádek v souboru */etc/group* může vypadat takto:

```
game:x:101:kuba,pavel,zdenek
```

Informace oddělené dvojtečkou v následujícím pořadí:

- Identifikační jméno skupiny
- Heslo skupiny (většinou se nepoužívá)
- GID**:** identifikační číslo primární skupiny uživatele. Uživatel musí být členem vždy alespoň jedné skupiny
- Seznam členů

3.4.3 Hesla

V dnešní době se jedná o nejrozšířenější a nejpoužívanější způsob ověřování identity. Často je to jediný způsob, jak zjistit, že je uživatel tím, za koho se opravdu vydává. Je zarážející, jak se takto důležité věci nevěnuje dostatek pozornosti. Pokud by se útočník dostal přes nedostatečně silné heslo do systému, ve kterém bude mít třeba jen minimální práva, tak i to může být velmi nebezpečné. Proto je důležité, aby uživatelé věděli, jak správně s hesly zacházet.

Hesla jsou v Linuxu šifrována jednosměrně. Nelze tedy z utajené podoby hesla získat originál. Při pokusu o přihlášení se heslo zašifruje a porovná s uloženou podobou hesla správného. Pokud souhlasí, je uživatel identifikován a má právo vstoupit do systému.

Nejefektivnější metodou pro získání hesla se stal slovníkový útok. Ten využívá slovníku, který je již předem vytvořený, k tomu, aby byla slova z něj postupně šifrována a porovnávána s hesly uloženými v systému. Hesla jsou uložena v souboru */etc/shadow*, k němuž má přístup pouze administrátor. To znamená pro útočníka jediné. Musí získat soubor s hesly.

Následuje výčet základních pravidel pro tvorbu a práci s hesly:

1. Mít účet bez hesla se rovná otevřené cestě do našeho systému. (Eliminovat takovéto účty – guest, host atd.)
2. Heslo, které se rovná uživatelskému jménu, se skoro rovná žádnému heslu. (Slovníková metoda počítá i s touto variantou a tyto hesla jsou zkoušena mezi prvními)
3. Triviální hesla typu 123456, aaa, qwert a podobně jsou také k ničemu. Jsou lehce odhadnutelná.
4. Slova, které obsahuje slovník, ať česká nebo cizojazyčná, jsou také velmi nevhodná. (Slovníková metoda)
5. Jednoduše zjistitelné informace – rodné číslo, telefonní číslo, datum narození, jména z rodiny – nevhodné!
6. Je vhodné složit heslo z malých i velkých písmen a doplnit jej o speciální znaky (@#%/-)
7. Jakkoliv dobré heslo, které je někde napsané nebo jste ho někomu řekli, také není bezpečným heslem.

Heslo by mělo mít pro danou osobu alespoň nějaký smysl, aby se nedalo zapomenout, mělo by být co nejméně běžné a mělo by obsahovat neobvyklé znaky. Je zde i možnost použít generátory hesel. Pro OS Linux existuje spousta utilit právě pro generování takových hesel. Mezi nejznámější asi patří: `pwgen`, `apg`, `gpw`, `makepasswd`, `otp`. [5], [8]

3.5 Disková pole – zálohování

3.5.1 Disková pole

U mechanických zařízení, v našem případě to budou pevné disky, dochází k opotřebování. To má za následek zkolabování celého počítače, serveru a tak kritické ohrožení chodu celé sítě. Tato ztráta je pro uživatele velmi bolestivá, protože zde neztratí pouze finanční hodnotu disku, ale především hodnotu informací, které byly na disku uloženy, popřípadě finanční hodnotu, která je spojena s řádným chodem takového zařízení. Často si firma nemůže dovolit ani krátký výpadek, protože by tak přišla o obrovské peníze. A tak jediným řešením této situace jsou disková pole. Ovšem mějme na paměti, že každý pevný disk se jednou opotřebuje, a proto se doporučuje minimálně jednou za pět let zainvestovat a vyměnit staré disky za nové.

Disková pole se skládají ze dvou a více jednotlivých disků, na kterých jsou data ukládána podle různých logických uspořádání tak, aby výpadek jednoho disku nezpůsobil havárii celého pole. Tento systém se nazývá RAID (Redundant Array of Independent Disks) a má různá označení.

RAID 0

Toto pole ale neslouží ke zvýšení bezpečnosti, nýbrž ke zvýšení výkonu. Spojí se kapacita dvou disků a zápis je prováděn prokládaně. Jednotlivé datové bloky o konstantní velikosti jsou ukládány za sebe na oba disky střídavě (stripping). Tím se výrazně zkrátí doba zápisu i doba čtení. Poškození u jednoho z disků vede ke kolapsu celého pole a veškerá data jsou ztracena. Pro servery je naprosto nevhodný.

RAID 1

Zástupce takzvaného zrcadlení dat (mirroring), při kterém se na všech discích zrcadlí stejná data. Při výpadku jednoho disku se pole neohrozí, jelikož na druhém disku jsou uchovávána stejná data. Kapacita neroste, ovšem rapidně se zvýší spolehlivost.

RAID 2

Rozšíření pole RAID 0, ovšem přidává do jeho funkce ECC (Error Check-king and Correction). Je to systém korekcí, který dokáže zamezit některým druhům výpadku. Je však podmíněn hardwarovou podporou ze strany disků, která se příliš nerozšířila, proto se tato disková pole dnes téměř nevyskytují.

RAID 3

Rozšíření pole RAID 0, ke kterému je přidán ještě jeden disk navíc, a na tento disk jsou ukládány paritní informace. Jednoduše řečeno, paritní informace je rozdíl dat uložených, který je počítán pro každý bit zvlášť. Při výpadku jednoho disku, lze ztracená data obnovit dopočítáním paritních informací. Ovšem výkon při dopočítávání výrazně klesá. Nevýhodou tohoto pole je závislost na paritním disku.

RAID 4

Rozšíření RAID 3, které přináší práci s jinou velikostí dat. Pro zápis jsou používány větší bloky. Zvyšuje to výkon při čtení, zápory z pole RAID 3 ovšem zůstávají.

RAID 5

Velmi oblíbený typ pole, které odstraňuje řadu nevýhod RAID 3 a 4. Funguje také na principu ukládání paritních informací, ovšem už ne na samostatný disk, nýbrž informace jsou rozděleny mezi jednotlivé disky. Tím se urychlí zápis.

RAID 6

Jedná se o rozšíření RAID 5 o druhý disk, na který se ukládají paritní informace. Ty jsou ukládány na všechny disky zároveň. To umožní správný chod pole i při výpadku dvou disků. Rychlost čtení zůstává, ovšem rychlost zápisu se sníží, protože je potřeba zapisovat dvakrát větší množství dat. RAID 6 je hodně spolehlivý typ pole.

Pro větší bezpečnost disků se vytvořila hybridní pole, která vždy kombinují RAID 0 s jiným typem.

RAID 10

Jedná se o kombinaci RAID 0 a RAID 1. K provozu je potřeba alespoň čtyř disků a dva z nich jsou spojena v poli 0 a na další dva se zrcadlí (RAID 1). Tímto způsobem dosáhneme výhod obou dvou typů polí. Jedinou nevýhodou zde je to, že potřebujeme dvojnásobnou kapacitu, než jakou nakonec získáme.

RAID 30 a RAID 50

Kombinace RAID 0 s RAID 3 nebo 5. Nejsou zde potřeba zrcadlové disky, protože se paritní informace ukládají na všechny použité disky. Výhodou oproti RAID 10 je vyšší dosažená kapacita, která zbude pro uložení uživatelských dat.

„Do diskových polí se kvůli výkonu doporučuje používat (nejlépe úplně) stejné disky, ideálně z jedné série. Disky jsou pak stejně rychlé a nemusejí na sebe vzájemně čekat. Toto doporučení je však z hlediska bezpečnosti zcela chybné! Je pravděpodobné, že disky z jedné série mohou mít stejnou vadu, případně celkovou životnost. Mohou se proto odporoučet během extrémně krátkého období.“ [5]

3.5.2 Zálohování

I když se budeme o náš systém hodně starat a budeme používat spousty bezpečnostních prvků (UPS, disková pole atd.), abychom předešli jeho ztrátě, je nutné mít na paměti, že vždycky nás může něco překvapit. A proto je důležité starat se o svá data i takovým způsobem jako je právě zálohování. Pro mnohé z firem mají právě data finanční hodnotu mnohokrát převyšující hodnotu majetkovou.

Zálohovat lze na libovolné médium, které spolehlivě udrží data – disky, pásky, ZIP diskety, CD, DVD, USB disky, paměťové karty a další média. Správné médium bychom měli volit podle potřebné kapacity, možností firmy, ceny a podle toho, jak často budeme zálohovat. Pro zálohování platí několik bezpečnostních pravidel.

1. Udržovat zálohy na jiném místě než originální data. Je to kvůli možnému poškození a zničení jak dat, tak i záloh. Doporučuje se udržovat zálohy nejlépe v jiné budově.
2. Nenechat si zálohy odcizit. Útočník by toho pak mohl lehce využít, případně získané informace prodat. Doporučuje se používat trezor.
3. Vytvořit a dodržovat zálohovací plán, protože zastaralé zálohy jsou nám k ničemu.
4. Po zápisu dat vždy zkontrolovat zálohu. Vadné médium může napáchat velké škody.
5. Správná přeprava a skladování médií.

V ideálním případě se zálohuje úplně všechno. Tím se vyřeší spoustu problémů a času při obnově dat (instalace, obnovení, aktualizace atd.). Pokud nemůžeme zálohovat úplně všechno, tak bychom se měli soustředit na ty nejdůležitější věci. To jsou data, která

se nedají jiným způsobem dohledat a obnovit. Domovské adresáře uživatelů (/*home*), systémová nastavení (*/etc, /bin, /usr/bin*), logy (*/var/log*).

Existují dva typy záloh. Úplná a doplňková. Úplná zálohuje vše a doplňková záloha obsahuje pouze změněná data od posledního zálohování. U doplňkové zálohy ušetříme velkou část kapacity média. Zálohy se dají různě kombinovat. Vše záleží na tom, jaký bude zvolen zálohovací plán. Např.: Jednou za týden úplná záloha a poté každý další den doplňková záloha. Zálohovaná data by se měla uchovávat delší dobu. Pro vytváření záloh lze použít archivační programy (tar) nebo i programy určené přímo k zálohování (`backup, dump/restore`). Zálohy lze komprimovat, to nám ušetří další kapacitu média. [5]

3.6 Firewall

V této kapitole budou popsány některé Linuxové nástroje a programy, které slouží pro tvorbu firewallu. Pamatujte, že i pro firewall je třeba dodržovat některá bezpečnostní pravidla a doporučení. Například pokud provozujete server, tak by bylo dobré vyčlenit si pro firewall vlastní počítač. Ten bude chránit celou síť a neměl by dovnitř propustit to, co není výslovně povoleno. Ovšem je potřeba chránit i samotný firewall. Společně s firewallem by počítač neměl poskytovat další služby.

3.6.1 Iptables

Linux má ve svém jádře přímo zabudovaný filtr, který se jmenuje *iptables*. Jedná se o nejpoužívanější variantu firewallu pro Linux. *Iptables* poskytuje filtrování paketů, překlady síťových adres (NAT) a překlady adres portů (PAT). Paketový filtr zkoumá hlavičky příchozích TCP/IP paketů a podle předem nadefinovaných filtrů rozhoduje, co se s pakety bude dít dále. Linux rozdělí pakety do tří různých kategorií, řetězců podle toho, kudy putují:

- INPUT – jsou to pakety přicházející pro danou stanici (pakety pro určitou službu, která na dané stanici běží)
- OUTPUT – řetězec, který obsahuje pakety, které se snaží odejít z dané stanice
- FORWARD – tudy procházejí pakety, které směřují jinam a pochází také odjinud. Většinou se jedná o routery.

- Existují ještě dva další řetězce – PREROUTING a POSTROUTING – ale nepoužívají se pro filtrování paketů. Administrátor si může definovat i své vlastní řetězce a k nim přiřazovat další pravidla.

Pakety prochází všemi pravidly, která jsou na něj postupně aplikována. Pokud některé pravidlo definitivně rozhodne, tak se paket přesune na konec řetězce a je provedena zvolená akce. Pokud nerozhodne žádné pravidlo, tak platí poslední pravidlo a tomu se říká *policy*. To definitivně rozhodne o osudu paketu. S řetězci a pravidly se dá samozřejmě pracovat a lze je vytvářet. Pomocí různých parametrů příkazu `iptables` lze nastavit kvalitní firewall pro Váš počítač. Pár základních příkazů pomocí *iptables* je zobrazeno níže.

```
Iptables-A FORWARD -s 192.168.2.0/24 -j DENY
```

Jedná se o základní pravidlo, které říká, ať zahodí všechnu průchozí komunikaci ze zadané sítě.

- `-A` – slouží pro vytvoření nového pravidla.
- `-s` - udává zdrojovou adresu paketu.
- `-j` – určuje, co je provedeno při splnění pravidla

Pomocí *iptables* lze celkem jednoduše zamezit příjímání, přeposílání nebo odesílání paketů, které nechceme a tak z části zajistit ochranu našeho systému. Musíme ale brát v potaz ten fakt, že každý paket, který přijde, je testován každým pravidlem. Pokud nadefinujeme příliš mnoho pravidel, mohlo by dojít k velkému nárůstu zátěže. Proto je potřeba volit pravidla rozumně.

3.6.2 IPCop

Jedná se o Linuxovou distribuci, která je primárně určena pro tvorbu firewallu a je zdarma. IPCop se používá hlavně v malých firmách nebo domácích sítích. Má velmi přívětivé uživatelské rozhraní, které se snadno používá. Pro jeho fungování je zapotřebí pouze samostatný počítač s dvěma síťovými kartami. Jedna bude určena pro spojení s vnitřní sítí a druhá pro spojení s vnější (Internetem). Dá se bezplatně stáhnout z internetových stránek *www.ipcop.org*. [11]

3.6.3 Shorewall

Dalším zástupcem, který je schopný vytvořit kvalitní firewall pro Linux je Shorewall. Shorewall je sada skriptů usnadňující nastavení Linuxového firewallu, který je obsažen v jádře. Vše se dělá přes konfigurační soubory, které si lze nastavit přesně podle svých potřeb. Shorewall se dá použít na specializování firewallu, multifunkční odchozí brána, router a serveru. Vše potřebné lze nalézt ke stažení na webu *shorewall.net.* [11]

3.7 Antivir

Všeobecně je velmi rozšířené tvrzení, že Linux nepotřebuje antivirový program, jelikož na Linux neexistují žádné viry. Z části je toto tvrzení pravdivé. Na Linux se do této doby opravdu neobjevil žádný vir, který by byl životaschopný. Viry mají svoji specifickou vlastnost a to šířitelnost. V Linuxu se viry šířit nedokážou, alespoň ne dostatečně dlouho, aniž by si toho nikdo nevšiml. Otázkou tedy zůstává, proč existují společnosti, které se zabývají vývojem právě antivirových programů určených pro Linux? Dělají to převážně kvůli systému Windows. Většina serverových řešení je totiž postavena na Linuxu, ať už třeba z důvodu dobré odolnosti proti virům nebo z dalších, ovšem tyto servery mohou poskytovat spoustu služeb právě uživatelům systému Windows, například správa pošty, ukládání a stahování dat. Přitom musí zajistit, aby se k nim skrz tyto služby nedostaly viry. Je třeba si položit i další otázku, bude Linux takhle bezpečný i v budoucnu? Já osobně si myslím, že ne. Pokud se Linux začne více rozšiřovat mezi uživatele, tak vzroste procento virů, červů a počet napadení tohoto systému. [9], [10]

Důvody proč není zapotřebí antivirus:

1. Instalace softwaru ze zdrojů – Většina aplikací v Linuxových distribucích se instaluje z ověřených zdrojů. To znamená, že se nemusí stát to, že si něco omylem stáhnete a nainstalujete vir.
2. Oddělení účtu administrátora – Systém uživatelů a oprávnění je v Linuxu nastaven tak, že některé úkony lze dělat jenom s omezenými oprávněními. To znamená, že vir, který byste případně mohli chytit, nebude mít dostatek oprávnění k tomu, aby se dostal k systémovým složkám nebo souborům.

3. Malé rozšíření Linuxu – Jelikož není Linux tak rozšířeným systémem jako Windows, vývojářům virů se proto ani nevyplatí vytvářet viry, které by zasáhly pouze malé procento uživatelů.
4. Open Source – Může se zdát, že prohlížení otevřeného kódu může být spíše nevýhodou Linuxu, není tomu tak. Otevřený kód může být prohlížen stovkami programátorů, kteří v něm budou schopni objevit a opravit poničený kód virem.

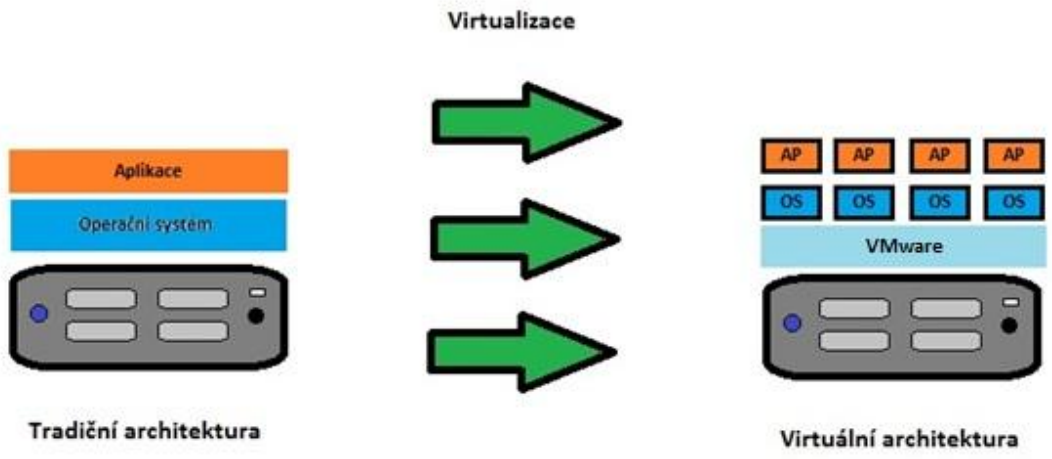
II. PRAKTICKÁ ČÁST

4 INSTALACE

4.1 Instalace

V dnešní době je instalace všech Linuxových distribucí s grafickým prostředím velmi jednoduchá a zvládne ji snad opravdu každý. Proto zde bude uvedeno jen několik málo informací, které jsou pro instalaci důležité. Jako první je potřeba si stáhnout soubor ISO obrazu, které je ke stažení z oficiálních stránek OS, například Linux Mint *http://www.linuxmint.com/*. Velikost ISO souboru záleží na distribuci, může se jednat o stovky MB až po několik GB. Soubor je poté potřeba vypálit na DVD nebo otevřít pomocí virtuální mechaniky. Pokud ale nechcete instalovat systém přímo do PC, existuje zde možnost virtualizace.

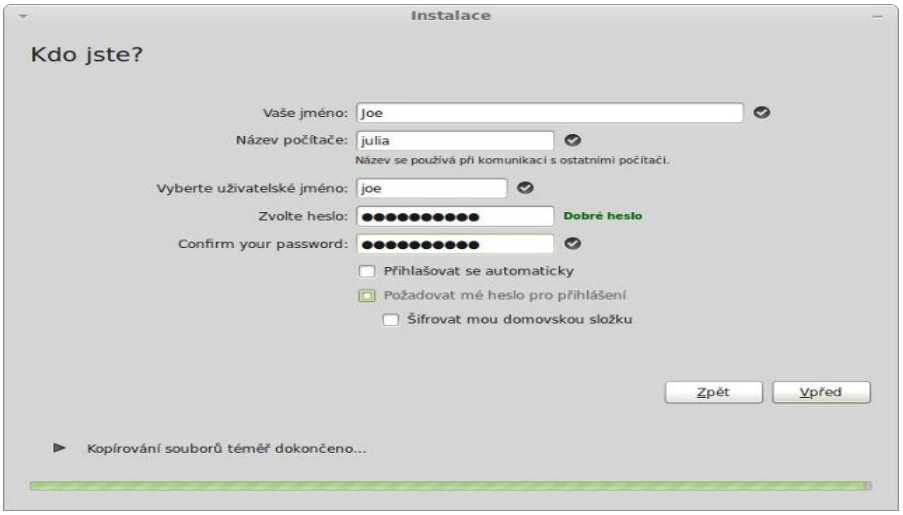
Virtualizace = abstrakce výpočetních zdrojů, rozdělení výpočetních zdrojů jednoho fyzického systému. Jinými slovy lze říci, že pomocí vizualizace jsme schopni jeden zdroj (pod pojmem zdroj si můžeme představit celý server, případně jeho části – procesor, paměť, síťová karta, datové úložiště) využít pro více než jeden OS (viz. Obrázek č. 4). Na jednom fyzickém serveru lze provozovat více serverů virtuálních při současném zlepšení IT infrastruktury (efektivita, dostupnost, flexibilita, správa).



Obrázek 4 - Virtualizace

Já osobně jsem využil na pomoc a práci virtualizační program VMware Player. Pomocí live DVD je možné spustit plně funkční OS bez nutnosti instalace. Je možné ho vyzkoušet a až poté se rozhodnout, jestli instalovat nebo ne.

Pokud máme staženo, vypáleno nebo nainstalovaný vizualizační program, vložíme DVD do mechaniky, restartujeme počítač a poté se spustí instalátor systému. Za pomocí několika nastavovacích obrazovek Vás instalátor provede instalací. Na ukázku jsem vybral obrazovku, kde se nastavuje uživatelské jméno, heslo, název počítače atd., jak je vidět na obrázku č. 5. Můžete si všimnout, že je zde automaticky kontrolována síla hesla. Doporučoval bych, aby heslo od prvního vytvořeného účtu bylo dostatečně silné, jelikož se bude jednat o uživatele, který bude moci spouštět příkazy pod uživatelem *root*. Je dobré dodržovat určitá pravidla pro tvorbu hesel, která jsou již výše zmíněna v této práci.



Obrázek 5 - Instalace Linux Mint – vyplnění přihlašovacích údajů [21]

Instalace systému zabere asi 10 až 15 minut, ale závisí to na HW daného PC. Jakmile se instalace dokončí, tak lze spustit OS. Před spuštěním se objeví uvítací obrazovka, která vyzývá k vyplnění uživatelského jména a hesla. Po úspěšném zadání všech údajů se přihlásíte do systému a můžete daný OS začít používat.

4.2 Použité OS

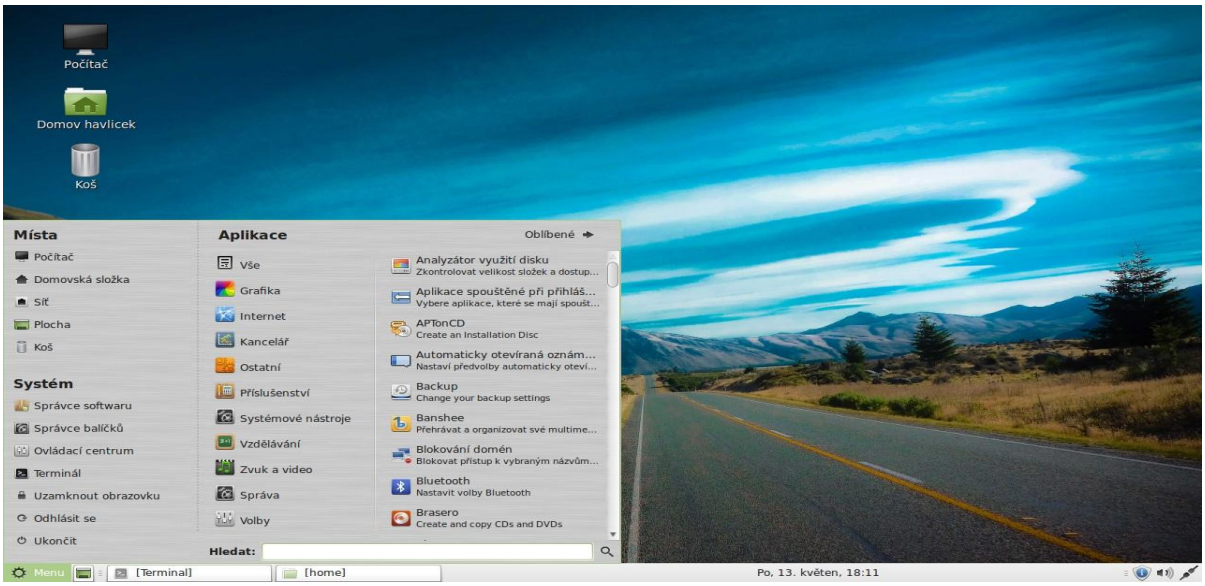
V praktické části této práce jsem pracoval na těchto OS:

Linux Mint 14.1: Jak již bylo řečeno, jedná se o nejoblíbenější distribuci za poslední rok. Jeho první verze vyšla 27.8.2006 a do dnešní doby se vydalo 14 verzí, přitom 15-tá by měla vyjít na konci května roku 2013. Pracuje ve velmi pěkném a jednoduchém grafickém prostředí Cinnamon. Minimální HW požadavky pro tento OS: CPU – 600MHz, 512MB RAM, 5 GB volného místa na pevném disku. Doporučené požadavky jsou zhruba 1x větší.

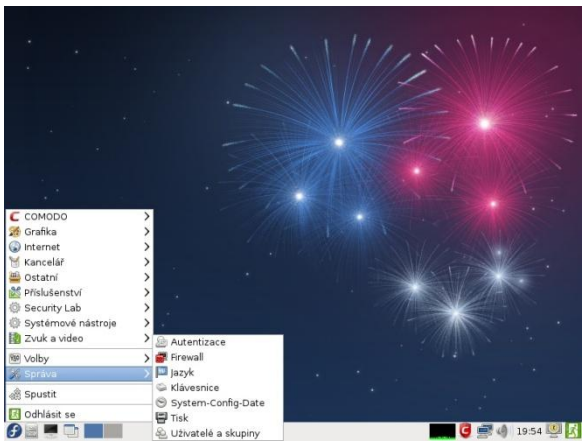
openSUSE 12.2: Také se jedná o velmi rozšířenou a oblíbenou distribuci, která je vhodná pro všechny typy uživatelů. Nejaktuálnější verzí je verze 12.3 a v budoucnu se můžeme těšit na verzi 13.1. Jako pracovní prostředí používá KDE 4. Minimální HW požadavky jsou: CPU 500MHz, 512 MB RAM, 3 GB volného místa na pevném disku.

Fedora 17 – Live Security: Je to distribuce, kterou používají spíše pokročilejší uživatelé. Ve verzi Live Security, která pracuje v pracovním prostředí LXDE, se nachází spousta nástrojů, kterými je možné sledovat, testovat nebo zachraňovat systém. Minimální HW požadavky na tento OS: CPU 400MHz, 1 GB RAM, 10 GB volného místa na pevném disku.

Ukázky grafických prostředí:



Obrázek 6 - – Linux Mint - Cinnamon



Obrázek 8 – Fedora - LXDE

Obrázek 7 – openSUSE – KDE4

5 REALIZACE RAD A DOPORUČENÍ

V následujících kapitolách se práce bude zabývat realizováním rad a tipů, které byly popsány v teoretické části této práce. Pro většinu akcí, které se v praktické části budou provádět, jsou potřeba oprávnění uživatele *root*. Tento superuživatel si může v systému dělat naprosto cokoli, z toho vyplývá, že mít jeho oprávnění je velice nebezpečné. Napsáním špatného příkazu se může celý systém velmi jednoduše zhroutit. Výchozím nastavením novějších distribucí Linuxu (Ubuntu, Mint) je, že účet *root* je uzamčen. Systém je nastaven tak, aby správu počítače mohl provádět prvně vytvořený uživatel při instalaci. Tato správa poté probíhá pomocí příkazu `sudo`. Ostatní uživatelé tento příkaz používat nemohou, pokud jim to není povoleno. Pro příkazy vyžadující oprávnění uživatele *root*, je tedy nutné používat příkaz `sudo`. Pokud si `sudo` žádá heslo, tak je to vaše uživatelské heslo, žádné *root* heslo není potřeba.

5.1 Uživatelé, skupiny, hesla

5.1.1 Tvorba uživatelů

Uživatelé, respektive uživatelské účty lze na vybraných OS vytvářet dvěma způsoby. Jedná se o způsob tvorby uživatele z příkazové řádky a pomocí systémových nástrojů v grafickém prostředí. Tvorba z příkazové řádky je u všech distribucí stejná, tvorba pomocí nástrojů se nepatrně liší, většinou pouze grafickým zobrazením. V dnešní době jsou systémové nástroje v Linuxu velmi přívětivé a jednoduché na ovládání, takže tvorba uživatelů se stává maličkostí. Jak již bylo zmíněno, informace o uživatelích a jejich účtech jsou zapsány v souboru */etc/passwd*.

Příkazový řádek – nový uživatelský účet lze vytvořit příkazem/programem `useradd` anebo také `adduser`. Rozdíl v těchto dvou příkazech je takový, že `adduser` se na všechny potřebné údaje zeptá, není tudíž potřeba znát všechny parametry jako u `useradd`. Začínajícím uživatelům Linuxu bych doporučil spíše `adduser`.

`useradd`

Tento příkaz upravuje a mění soubor */etc/passwd*. Bude zde zmíněno jen několik parametrů, ostatní lze dohledat po zadání příkazu `useradd` nebo `man useradd`.

```
useradd [parametry] prihlasovaci_jmeno
```

```
useradd –c "Jakub Havlicek" –m –s /bin/bash –g users –G
omezeni,mail –u 1010 Kubin
```

Parametry: `-c` komentář, plné jméno uživatele

`-m` vytvoří domovský adresář (/home/novy_uzivatel)

`-s` definuje přihlašovací shell

`-g` defaultní skupina uživatele

`-G` seznam skupin, v nichž je uživatel zařazen

`-u` nastaví dané UID uživateli.

Tento příkaz vytvoří uživatele s přihlašovacím jménem *Kubin*. Plné jméno uživatele bude *Jakub Havlicek*. Vytvoří se mu domovský adresář, bude používat *bashshell*. *UID* uživatele bude nastaveno na *1010*. Jeho primární skupinou bude skupina *users* a dále bude zařazen ve skupinách *omezeni* a *mail*. Lze si všimnout, že nikde není zadáváno heslo pro uživatele – na uživatelský účet se nebude dát přihlásit. Je proto nutné heslo nastavit. Na to nám slouží příkaz `passwd`. Pomocí parametrů lze nastavovat například životnost hesla atd.

```
passwd [parametry]Kubin
Nové heslo:[zadání hesla] (Kvůli bezpečnosti se nevypisuje na obrazovku)
Opakujte nové heslo:[zadání hesla]
```

Další nastavení uživatelského účtu a hesla lze provést přes příkaz `chage`.

```
chade -E 2013-05-17 -I 6 -m 7 -W 4 Kubin
```

Parametry: `-E` nastaví konec platnosti účtu

`-I` životnost účtu (dny) po expiraci hesla

`-m` nastaví min. platnost hesla (dny)

`-W` varování před vypršením hesla (dny)

`adduser`

Zadáním příkazu `adduser [jmeno_uzivatele]`, se vytvoří uživatel se svým ID a skupinou a domovským adresářem. Bude požádáno o heslo pro uživatele a následné potvrzení hesla. Poté lze vyplnit doplňující informace jako plné jméno, telefonní číslo a

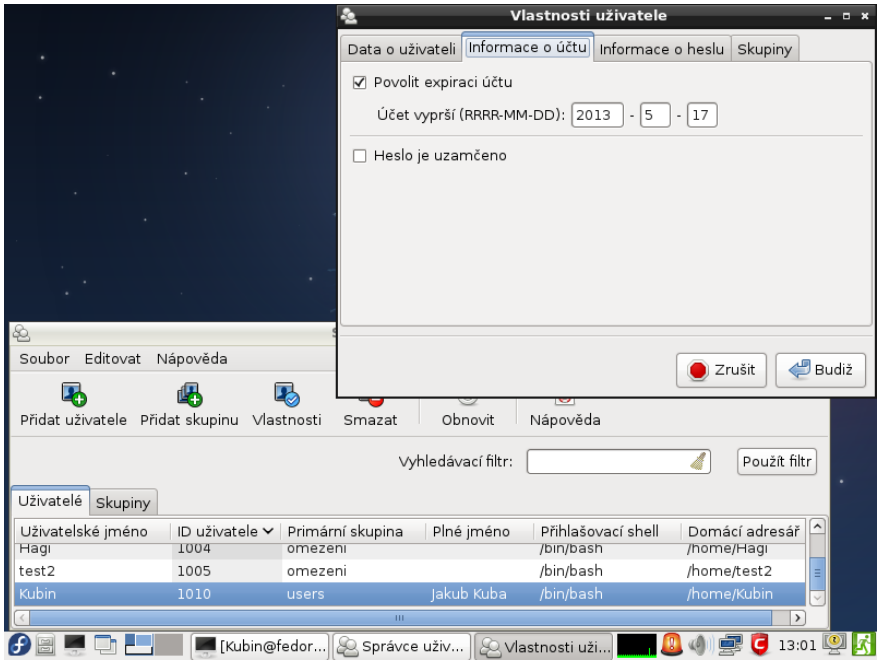
další. Nakonec je potřeba potvrdit a uživatel je vytvořen. Zde je vyobrazena ukázka tohoto příkazu, tučně je zobrazeno pouze to, co musí uživatel zadat ručně, zbytek za něj vytvoří program `adduser`.

```
havlicek-virtual-machinehavlicek # adduserdavid
Addinguser `david' ...
Addingnewgroup `david' (1004) ...
Addingnew user `david' (1004) withgroup `david' ...
Creatinghomedirectory `/home/david' ...
Copyingfilesfrom `/etc/skel' ...
Enter new UNIX password: skryté heslo
Retypenew UNIX password: skryté heslo
passwd: passwordupdatedsuccessfully
Changingthe user informationfordavid
Enter thenewvalue, orpress ENTER forthe default
    Full Name []: David Snajdr
    RoomNumber []: 535
    WorkPhone []: 721514215
    HomePhone []: 125645879
    Other []: Spolubydlici
Istheinformationcorrect? [Y/n] Y
```

Grafické nástroje - tvorba a nastavování uživatelských účtů pomocí systémových nástrojů je jednoduchá a přehledná. U většiny distribucí to funguje na podobném principu i podobném grafickém vyobrazení, jak je vidět z následujících obrázků.

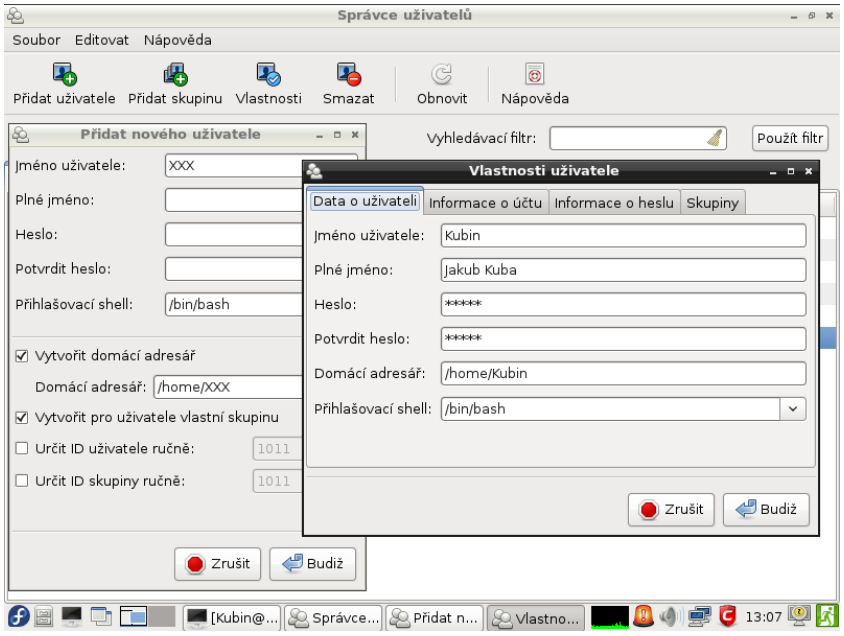
Fedora

Jak je vidět na obrázku č. 9, tak všechny příkazy se v příkazovém řádku provedly a jdou zobrazovat a upravovat ve správci uživatelů a skupin.



Obrázek 9 - Fedora – Správce uživatelů

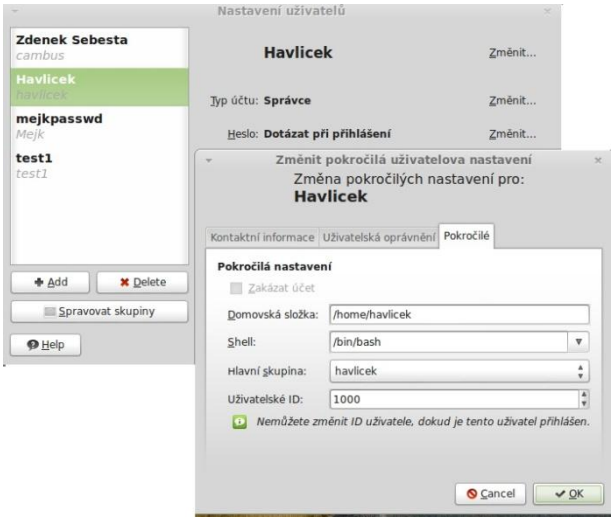
Vytvoření a nastavování uživatelského účtu pomocí správce uživatelů je jednoduché. Stačí kliknout na ikonu Přidat uživatele, poté vyplnit potřebné informace jako přihlašovací jméno a heslo. Další nastavení a informace účtu, hesla lze provádět po vybrání účtu a kliknutí na tlačítko Vlastnosti. Vše je vyobrazeno na obrázku č. 10.



Obrázek 10 - Fedora – Tvorba, úprava uživatelského účtu

Linux Mint

Také zde je vidět jednoduchost ovládání. Uživatele je možné zde přidávat, odebírat, měnit pokročilá nastavení.



Obrázek 11 - Linux Mint – Tvorba, úprava uživatelského účtu

openSUSE

Jak je vidět na obrázku č. 12, tvorba uživatelských účtů pomocí ovládacího centra YaST2 je také velmi jednoduchá a přehledná.

Obrázek 12 - openSUSE – Tvorba, úprava uživatelského účtu

5.1.2 Tvorba skupin

Tvorba skupin je velmi podobná tvorbě uživatelů, jak u příkazového řádku, tak i pomocí systémových nástrojů. Všechny parametry jsou k nalezení pomocí příkazu `man groupadd`.

Příkazový řádek

Příkazem, který upravujeme soubor */etc/group* a vytváříme tak i novou skupinu je `groupadd`.

```
groupadd [parametry] skupina
```

```
groupadd –g 1020 Skupina
```

Vytvoření skupiny s názvem Skupina a GID 1020

Parametry: `-g` GID ID pro skupinu, nesmí být záporná hodnota

Pomocí příkazu `gpasswd` lze u skupin vytvářet, měnit, mazat hesla a přiřazovat uživatele do skupin. Příklad přidání uživatele *Kubin* do skupiny *Skupina*.

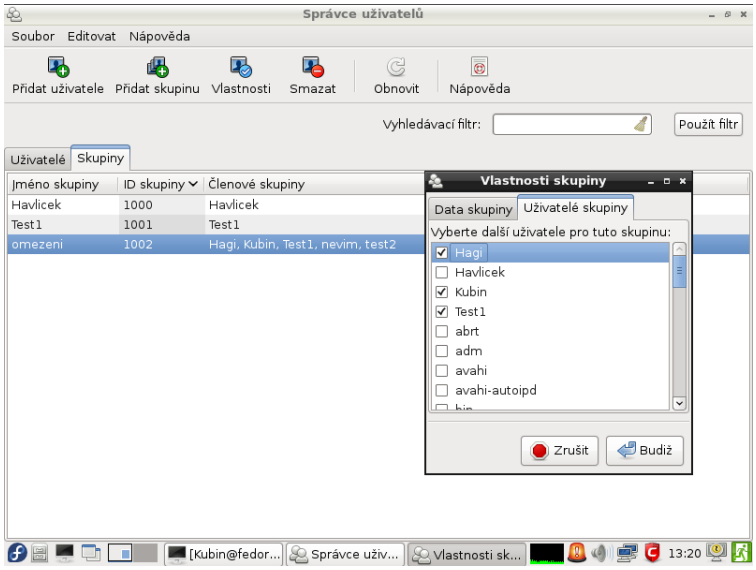
```
gpasswd –a Kubin Skupina
```

Další příkaz, který by mohl být užitečný je `newgrp [skupina]`. Ten aktivního uživatele přehlásí do nově zadané skupiny.

Grafické nástroje

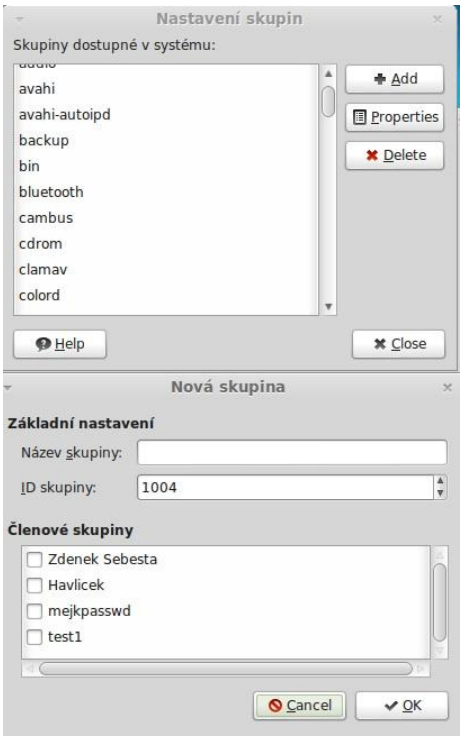
Fedora

Vytváření skupin pomocí správce uživatelů je znázorněno na obrázku č. 13. Po kliknutí na tlačítko *Přidat skupinu* si zadáte název skupiny a její případné ID. Po vytvoření lze přidávat uživatele do skupiny přes *Vlastnosti*. Podobně je tomu tak i u jiných distribucí, jak je vidět na obrázcích č. 14 a 15.

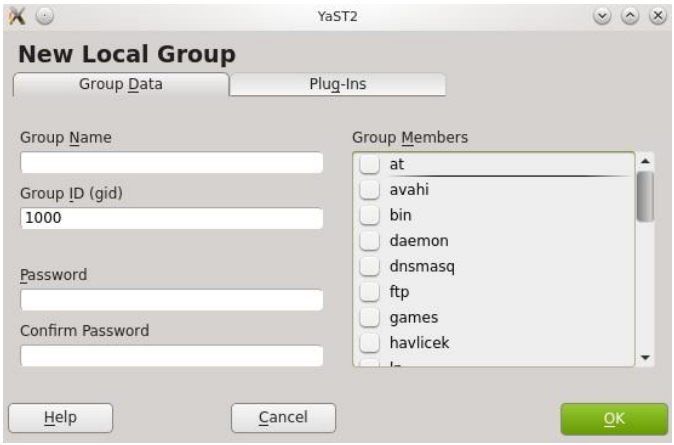


Obrázek 13 - Fedora – Tvorba, vlastnosti skupin

Linux Mint **openSUSE**



Obrázek 14 – Linux Mint – Tvorba skupin



Obrázek 15 – openSUSE – Tvorba skupin

5.1.3 Tvorba hesla

Jak již bylo zmíněno v teoretické části, na práci s hesly je třeba dávat pozor. Přílišná jednoduchost hesla by se nemusela vyplatit. Jak tedy takovým situacím zabránit? Uživatel by měl volit heslo dostatečně silné. Existují různé programy a systémové nástroje, které Vám v tom mohou pomoci.

V OS Fedora existuje nástroj Konfigurace autentizace, která nám v tomto případě pomůže nastavit minimální požadavky na heslo, jak je vidět na obrázku č. 16. Při nesplnění minimálních požadavků Vás systém upozorní na slabost hesla.

Obrázek 16 – Fedora – Konfigurace autentizace

Na tvorbu náhodného hesla z příkazové řádky existují různé programy. Mezi těmi nejznámějšími lze zmínit `pwgen` a `apg`. Tyto dva programy byly zkoušeny v příkazovém řádku pod Linuxem Mint. `Apg` byl již nainstalovaný. Po zadání příkazu `apg` do příkazové řádky se program dotáže na řetězec 16-ti náhodných znaků. Na základě těchto 16-ti vložených znaků vytvoří hesla. Samozřejmě lze i nastavovat parametry, jako jsou třeba délka hesla nebo počet generovaných hesel. (`apg -n 2 -m 20`)

```
havlicek-virtual-machine havlicek # apg
Please enter some random data (only first 16 are
significant)(eg. your old password):>
darc4Swuind (darc-FOUR-Swu-ind)
ikivDebDud3 (i-kiv-Deb-Dud-THREE)
```

```
tonthacPhec7 (tonth-ac-Phec-SEVEN)
Beolm4WreafA (Be-olm-FOUR-Wreaf-A)
jag6QuoangO (jag-SIX-Quoang-O)
KruvugAg7 (Kruv-ug-Ag-SEVEN)
havlicek-virtual-machine havlicek # apg -n 2 -m 20
bufritfaddyoobRigphi
shievDoivhildOcogjoi
```

Pwgen nainstalovaný nebyl, bylo ho potřeba doinstalovat. Zadáním příkazu `sudo apt-get install pwgen` se potřebný balíček stáhnul a nainstaloval. `Pwgen` stejně jako `agp` generuje náhodné heslo, ale už po uživateli nechce řetězec náhodných znaků. Hesla generována pomocí `pwgen` by měla být vyslovitelná, ale bezvýznamná.

```
havlicek-virtual-machine havlicek # pwgen
Aigaex8b aiThoo8y iu6Pieng Eichoo0A NaPhah2a Jaebah1a
havlicek-virtual-machine havlicek # pwgen -n 5 10
uC6ei eGh3O De0bu ieL7e Yot7s ri7oC Boo5e Lee4n Six7s
raeY0
```

5.2 Zálohování

Zálohování je zřejmě nejdůležitější částí bezpečnosti, jak chránit svá data uložená v PC. V případě ztráty dat může být kvalitní záloha tou jedinou možností, jak svá data získat zpět. Záloha by se samozřejmě měla ukládat na jiná média než ta, která jsou obsažena v počítači.

5.2.1 Příkazový řádek

Tar, gzip

Tar je standardní archivační prostředek a slouží k archivaci a uložení určených souborů do jednoho souboru archivu. Pro použití se provádí příkaz `tar`, který lze doplnit o další řadu parametrů. Jsou zde vyjmenovány jen ty nejzákladnější, ostatní lze nalézt v rozsáhlé nápovědě `man tar`. Program `gzip` je asi nejčastěji používaný program pro kompresi. Výsledný soubor má příponu .gz a dá se kombinovat s tar.

Následující příkaz archivuje domovský adresář uživatele *havlicek* do souboru *havlicek.tar*.

```
tar -cvf havlicek.tar /home/havlicek
```

Další parametry:
`-c` vytvoří archiv
`-v` vypisování informací v průběhu archivace
`-f` jméno souboru archivu
`-A` připojení dalšího archivu
`-t` vypisuje obsah archivu
`-x` rozbalení souborů z archivu
`-z` komprimace metodou zip (menší velikost)

`tar -cvzf havlicek.tar.gz /home/havlicek` –archivace pomocí `tar` a komprimací metodou `gzip`

`tar -xvzf havlicek.tar.gz` – obnovení souboru komprimovaného `gzip`

`gzip soubor.txt` – výsledný soubor = *soubor.txt.gz* (původní soubor byl ale smazán!)
`gzip -d soubor.txt.gz` – obnovení souboru – *soubor.txt*
`gunzip soubor.txt.gz` – obnovení souboru – *soubor.txt*

Rsync

Jedná se o program, který se spouští z příkazového řádku a dokáže synchronizovat soubory a složky. Dá se velmi jednoduše a efektivně využít i pro zálohování. Je zde vypsáno pár základních příkazů, pro práci s tímto programem. Syntaxe pro tento program je jednoduchá: `rsync [parametry] [zdroj] [cíl]`

```
rsync -av /home/havlicek/Dokumenty /home/tmp/
```

Tento příkaz zkopíruje složku Dokumenty do složky tmp. Na tomto příkladu jde vidět podobnost s příkazem `cp`, který slouží pro kopírování. Jenže `rsync` má ještě další funkce. Pokud by se obsah složky *Dokumenty* změnil a my ho chtěli zálohovat na stejné místo, tak stačí příkaz zopakovat a `rsync` bude zálohovat pouze nové, změněné soubory. Je to velmi výhodná metoda.

Použité parametry:
`-a` archivuje (zachová oprávnění, vlastnické informace, zkopíruje symbolické odkazy, soubory zařízení atd.)
`-v` vypisování informací

Další ukázka archivuje adresář *Dokumenty*, ovšem bez všech textových souborů. To se zařídí parametrem `--exclude`.

```
rsync -av --exclude="*.txt" /home/havlicek/Dokumenty
/home/tmp/
```

Pokud bude potřeba zálohovat opět adresář *Dokumenty* do stejné cílové složky (*/home/tmp*), ale něco z něj bude vymazáno, tak za použití stejného příkazu jako minule smazaný soubor pořád zůstane v záloze. Kvůli téhle situaci existuje parametr `--delete`, který zajistí, že se z cílové složky odsraní ty soubory, které již ve zdrojové složce neexistují.

```
rsync -av --delete /home/havlicek/Dokumenty /home/tmp/
```

5.2.2 Grafické nástroje

Pro jednoduché zálohování v sobě Linux Mint obsahuje *Zálohovací nástroj*. Pomocí tohoto nástroje je velmi rychlé a jednoduché zálohovat to, co je potřeba, ať už se jedná o složky, soubory nebo seznam softwaru. Na obrázku č. 17 lze vidět programové prostředí zálohovacího nástroje, které je velmi jednoduché na ovládání. Stačí si vybrat zdroj, cíl, výstup zálohování (tar, zip, bzip2) nebo třeba i možnost zachovat přístupová práva. Obnova dat probíhá velmi podobně. Stačí pouze vybrat zálohovaný soubor a místo, kam ho rozbalit.

Obrázek 17 – Linux Mint – Zálohovací nástroj

5.3 Aktualizace

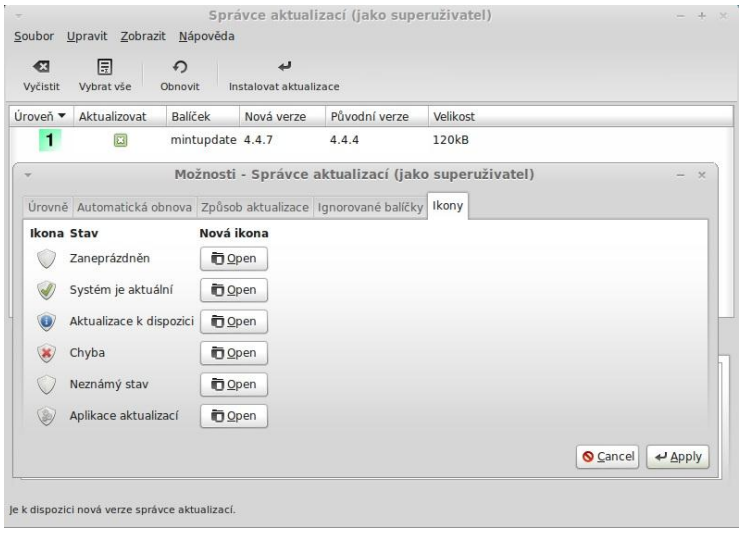
Aktualizace je také jedním z důležitých prvků bezpečnosti OS. Ani Linux není z hlediska bezpečnosti dokonalý, a pokud se někde objeví chyba, nejlepší je tu chybu co nejrychleji odstranit. Může se tak stát u některého vydaného balíčku, programu. Proto je potřeba pravidelně aktualizovat jak systém, tak software.

Linux Mint

Linux Mint lze aktualizovat dvěma způsoby. Jako první lze aktualizaci provést z příkazové řádky. Za použití pouze dvou příkazů, lze aktualizovat všechny zastaralé balíčky.

```
Sudo apt-get update; sudo apt-get upgrade
```

Další způsob je přes grafický nástroj, který je defaultně nainstalován, Správce aktualizací. Ten si stáhne informace o balících a najde možné aktualizace, které vypíše, a bude si možno vybrat, kterou aktualizace nainstalujete. V možnostech této aplikace lze nastavit například, jak často se mají aktualizace provádět, já bych doporučil alespoň jednou denně. Informace o stavu aktualizací může uživatel vidět na dolní liště pracovní plochy. Výpis, co která ikona znamená a grafické prostředí tohoto nástroje lze vidět na obrázku č. 18.



Obrázek 18 – Linux Mint – Správce aktualizací

Fedora

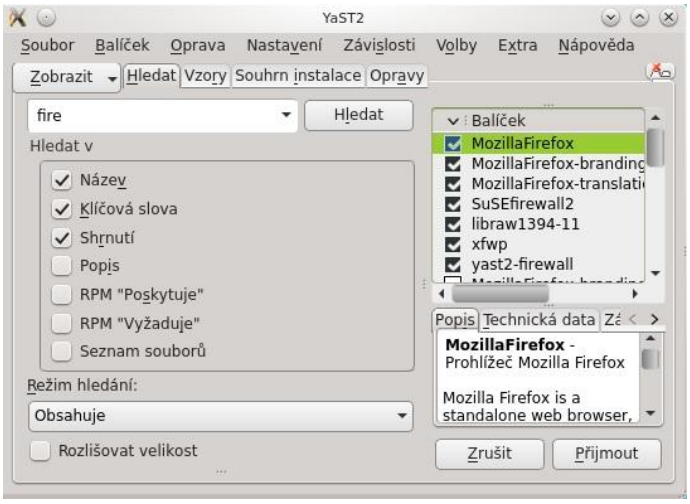
Pro OS Fedora se provádí aktualizace podobně. Pracuje se zde se správcem balíčku `yum`. Příkazy pro aktualizaci Fedory.

```
yum update

yum upgrade
```

opeSUSE

U openSUSE se dá provést aktualizace systému, balíčků z příkazové řádky pomocí příkazu `zyper up` nebo pomocí grafického nástroje Update (Software repositories).



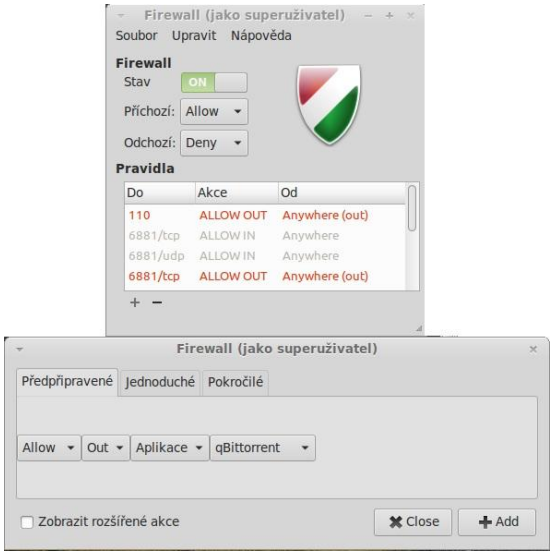
Obrázek 19 – openSUSE – Aktualizační/instalační nástroj

5.4 Firewall

Z hlediska bezpečnosti je velmi důležité, aby byl na operačním systému nainstalován a zprovozněn firewall. Chrání počítač proti nepovolanému přístupu ze sítě. Správně nastavený firewall může být kámen úrazu pro útočníky.

Linux Mint

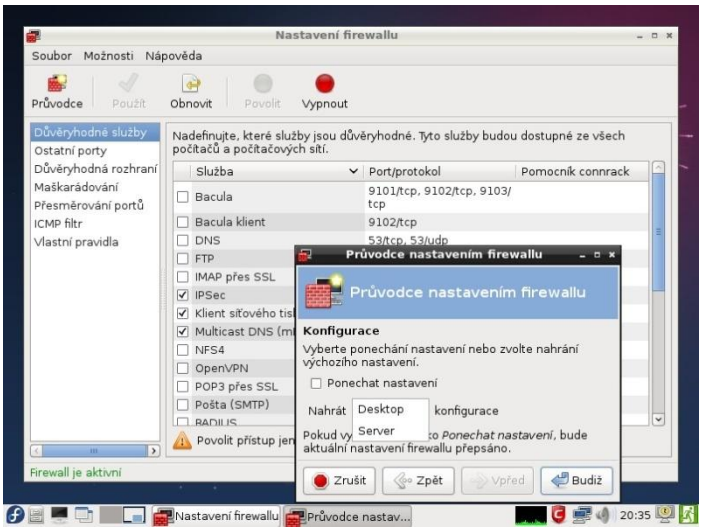
Má v sobě již nainstalovaný firewall, ovšem ten je defaultně vypnutý. Doporučoval bych ho zapnout. Samozřejmě jako superuživatel, například z příkazového řádku pomocí příkazu `gufw`. Grafický nástroj pro firewall v Linuxu Mint je zobrazen na obrázku č. 20. Je možné si vytvářet svá pravidla, pomocí kterých si nastaví firewall podle své potřeby. Nastavování Vám může připomenout již zmíněný *iptables*. Je zde možné vybrat si z předpřipravených pravidel, zadávání jednoduchých nebo i pokročilých pravidel. Ke stažení jsou i další programy k tvorbě firewallu, například *Firestarter*.



Obrázek 20 – Linux Mint – Konfigurace firewallu

Fedora

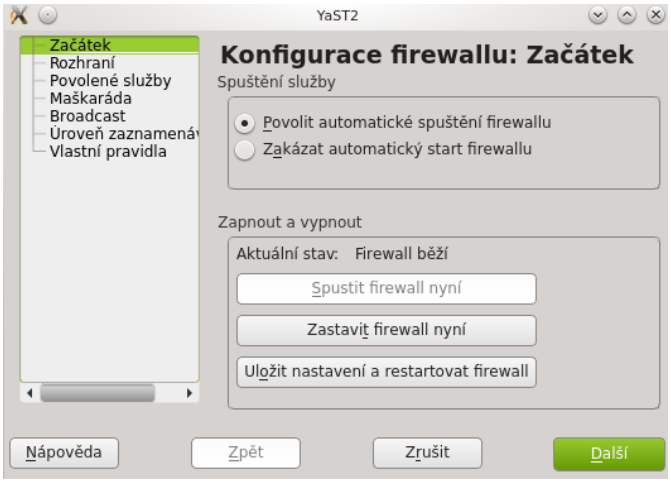
Fedora poskytuje možnost nastavování firewallu pomocí již defaultně nainstalovaného a aktivního konfiguračního nástroje firewallu. Tento nástroj nám udává několik možností, jak firewall nastavit. Jednou a tou nejjednodušší z nich bude nastavení podle průvodce. Ten se v několika málo krocích zeptá na to, zdali je PC připojen k síti, jestli PC používáte jako desktop nebo server, jestli jste začátečník nebo pokročilý. Pokud bude uvedeno například začátečník/desktop, tak bude znemožněn přístup do rozsáhlejší konfigurace firewallu (jde to změnit). Hlavní oblast pro nastavování firewallu je v levé části panelu. Můžete zde přidávat a nastavovat pravidla pro důvěryhodné služby a rozhraní, ICMP filtr atd.



Obrázek 21 – Fedora – Průvodce nastavením firewallu

openSUSE

I v openSUSE je defaultně nainstalován nástroj pro konfiguraci firewallu. Lze ho nalézt v řídícím centru YaST v záložce Bezpečnost a uživatelé pod položkou Firewall. Nastavování firewallu je podobné jako u ostatních distribucí, které zde již byly probrány. Dají se nastavovat rozhraní, povolené služby, porty atd.



Obrázek 22 – openSUSE – Konfigurace firewallu

5.5 Antivir

Jak již bylo zmíněno, antivir v Linuxu teoreticky není potřeba, pokud například neprovozujete e-mail server a další služby, které jsou poskytovány pro Windows. Ovšem může se stát, že se sem tam objeví nějaký červ nebo přijde nějaký spam. A tak pro pocit absolutního klidu a bezpečí existují antivirové programy pro Linux.

Linux Mint: Avast! Free Antivirus

Mezi dvě základní funkce co AFA provozuje, patří:

- Blokuje viry a spyware
- Umožní podporu od technicky zdatnějšího přítele

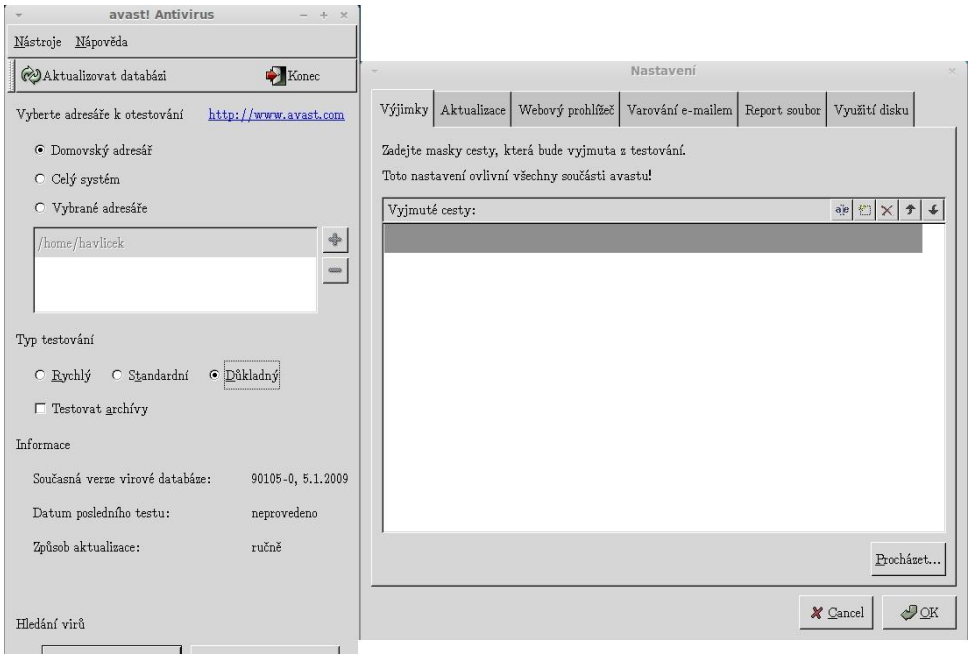
Existuje i rozšířená verze AFA – Avast Internet Security, která má více funkcí, ale ten už je potřeba si zaplatit.

Instalace probíhá z terminálu zadáním těchto příkazů:

```
wgethttp://files.avast.com/files/linux/avast4workstation_1.3.
0-2_i386.deb
```

```
sudo dpkg -i avast4workstation_1.3.0-2_i386.deb
```

Po instalaci a spuštění AFA, budete požádáni o registraci a na Váš e-mail bude zaslán licenční klíč na 1 rok používání zdarma. Při spuštění naskočí obyčejný panel, na kterém jde zvolit některé funkce. Výběr toho, co chceme nechat otestovat a jakým typem testování. Je zde i možnost nastavování (výjimky, aktualizace, varování e-mailem atd.). Antivirus obsahuje i vlastní databázi virů, kterou si je možné prohlédnout.



Obrázek 23 – Linux Mint - AFA

Fedora: Comodo Antivirus

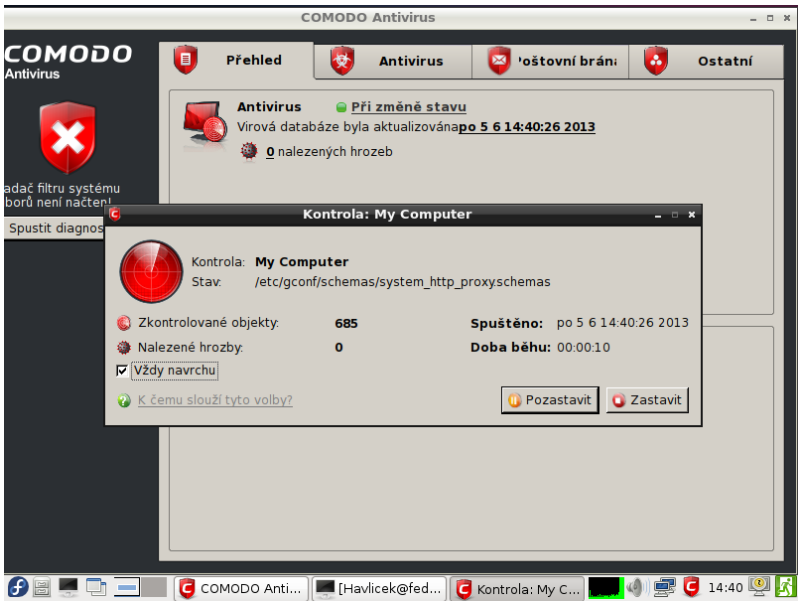
Mezi jeho kladné vlastnosti patří:

- Proaktivní ochrana zachytí všechny známé hrozby
- Automatické aktualizace aktuální protivirové ochrany (několikrát denně)
- E-mailové brány na zachytávání spamu
- Nainstaluj a zapomeň – žádné falešné poplachy, jen kvalitní antivirová ochrana
- Jednoduchý na ovládání a používání

CAV pro Linux je zdarma ke stažení na stránkách výrobce – *www.comodo.com*. Stáhne se do vašeho počítače jako balíček *rpm*. Proto je potřeba ho také tak nainstalovat. Nutná jsou oprávnění uživatele *root*. Tímto příkazem se spustí instalace.

```
Sudorpm –i CAV_LINUX-1.1.268025-1.i686.rpm
```

Pro dokončení instalace je potřeba spustit ještě jeden soubor a to `/opt/COMODO/post_setup.sh`. Na obrázku č. 24 je vidět pracovní prostředí CAV a právě spuštěná kontrola počítače.



Obrázek 24 – Fedora - CAV

openSUSE

U openSUSE se jedná o stejný případ jako u dvou předchozích systémů. Pokud byste chtěli mít na svém PC antivirový program pro pocit bezpečí, tak jej lze stáhnout, nainstalovat a poté používat stejně jako u předešlých OS.

6 DOPORUČENÍ PRO ZABEZPEČENÍ

V následující kapitole budou shrnuta doporučení pro zabezpečení OS Linux. Tato doporučení jsou reakcí na možné bezpečnostní trhliny a nedostatky v systému. Uživatel by si toho měl být vědom a také podle toho přizpůsobit svůj operační systém.

6.1 Sociální inženýrství

Jak již bylo řečeno, jedná se o velmi nebezpečnou metodu, která zajistí útočníkovi snadný přístup do systému. Využívá chyby lidského faktoru, proto je velmi těžké se proti ní bránit. Prakticky jediným možným řešením je proškolování uživatelů o politikách bezpečnosti.

6.2 Silné heslo

Při tvorbě nových uživatelských účtů, by si každý uživatel měl zvolit své (nebo by mu mělo být přiděleno) dostatečně silné heslo. Toto heslo by mělo splňovat určitá bezpečností pravidla, které již byla zmíněna v teoretické části této práce, ale ty nejdůležitější zde budou ještě zopakovány. Délka hesla alespoň 8 znaků, složitost hesla (malá, velká písmena, speciální znaky, číslice), popřípadě občasná změna hesla.

6.3 Nepracovat jako *root*

V dnešních OS Linux již bývá uživatel *root* standardně vypnutý (Ubuntu, Linux Mint). To znamená, že nový uživatel systému nemá taková oprávnění jako právě superuživatel. S těmito oprávněními lze ovšem pracovat pomocí příkazu `sudo`. Každý uživatel by ho měl využívat pouze tehdy, kdy je to nezbytně nutné, protože by byl někdo schopný získat oprávnění superuživatele, mohl by v systému dělat vše, co se mu zachce a to z hlediska bezpečnosti není dobrý nápad a mohlo by se to vymstít.

6.4 Zálohovat

Dalším velmi důležitým doporučením, jak zabezpečit svůj OS, respektive data, co jsou v něm, je zálohování. Jak bylo popsáno, zálohovat lze různými způsoby, takže si stačí vybrat jenom ten, který se vám nejvíc líbí a směle do toho. Doporučil bych zálohovat pokaždé, když se v OS něco důležitého změní, nainstaluje nebo vytvoří. Zálohování provádějte na kvalitní média, snažte se předejít ztrátám záloh a zálohy si ponechávejte

dostatečně dlouhou dobu. Proti ztrátě dat se lze také chránit pomocí diskových polí RAID. Ty bych rozhodně doporučoval použít, pokud provozujete server.

6.5 Aktualizace OS

Linux je sice bezpečnější OS než Windows, ale stále je potřeba k němu instalovat a aktualizovat software, různé záplaty a aktualizace programů, balíčků. Proto provádějte aktualizace OS v pravidelných intervalech.

6.6 Firewall

Firewall může váš systém ochránit před hrozbami, které na něj budou působit z vnější sítě. Pokud jej nemáte zapnutý, tak to určitě udělejte. A pokud ho zapnutý máte, tak na něm proveďte alespoň základní nastavení, která budou schopna ochránit systém před vnějšími hrozbami.

6.7 Antivir

Pokud nevěříte aktualizacím ani firewallu, tak bych vám doporučil nainstalování některého z antivirových programů určených pro Linux. Většina z nich je pro Linux dostačujících, takže si stačí pouze vybrat. Pokud ho již budete mít nainstalovaný, tak by bylo dobré jednou za čas spustit celkovou analýzu systému, která systém prohledá, případně vyčistí.

ZÁVĚR

V teoretické této části této práce se porovnával operační systém Linux s operačním systémem Windows. Z hlediska zabezpečení lze říci, že OS Linux je bezpečnější a to hned z několika důvodů. Jako první lze uvést fakt, že Linux není oproti Windows tak rozšířeným operačním systémem. Tudíž útočníkům se na něj jednoduše nevyplatí útočit různými viry, červy a podobně. Instalace na programů/balíčků probíhají z ověřených zdrojů. Dalším důvodem je to, že Linux je tzv. open source. To znamená, že jakýkoliv programátor může nahlédnout do kódu, jádra a pokud by se objevil škodlivý kód, tak se na jeho opravě může podílet sousta programátorů.

V průběhu práce bylo uvedeno několik rad a doporučení proti současným hrozbám, které mohou postihnout právě OS Linux. Mezi hrozbami bych vyzdvihnul obzvláště sociální inženýrství. Jedná se o metodu průniku do systému, která je založena na chybě lidského faktoru. Prakticky nezkušený uživatel uvolní útočníkovi cestu do systému. Další hrozbou, která může postihnout váš počítač a s tím i váš OS je selhání pevných disků a tím i ztráta dat. S tím souvisí pojem zálohování. Jedná se o velmi důležitou funkci, kterou by měl provádět pravidelně každý uživatel operačního systému, aby nepřišel o svá data.

V praktické části této práce jsem se pokusil uvést pár rad, postupů a doporučení pro vybrané distribuce OS Linux (Linux Mint 14., Fedora 17., openSUSE 12.2.). Mezi hlavní doporučení patří určitě volba dostatečně silného hesla. Pokud nebude mít uživatel žádné nebo slabé heslo do systému, velmi tak usnadní útočníkovi cestu. Pro volbu hesla lze využít určitá pravidla nebo i programy, které vytvoří heslo dostatečně silné.

V dnešní době, operační systém Linux není stále tak rozšířený a proto je stále bezpečnější než konkurenční OS Windows. Ovšem pokud se Linux trochu více prosadí mezi uživateli, tak je dost možné, že to ohrozí i jeho bezpečnost.

ZÁVĚR V ANGLIČTINĚ

In the theoretical part of this work there were compared Linux OS with the Windows OS. From a security perspective we can say that Linux is more secure and that´s because of this reasons. As the first one I would to mention the fact that Linux is not as widespread as Windows OS. Attackers are simply not worth it to attack at it with a variety of viruses, worms etc. Installing the programs / packages is from verified sources. Another reason is that Linux is the open source. This means that any programmer can look into the code, kernel, and if bad code would appeared then to its repair may contribute by lots of programmers.

In the course of my work I have listed a few tips and recommendations against current threats that can affect the Linux OS. Among the threats I would especially point out the social engineering. This is the method to attack a system, which is based on human error. Practically inexperienced user reveals attacker way into the system. Another threat that may affect your computer and thus your OS is the failure of hard disks and the loss of data. It is related with term backup. This is a very important function that should be performed regularly by every user who is using operating system to avoid loss of their data.

In the practical part of this thesis I have tried to give some advices, procedures and recommendations for selected distributions of Linux OS (Linux Mint 14th, 17th Fedora, openSUSE 12.2). The main recommendations include choosing a sufficiently strong password. If the user does not have a password or if he has weak password, way into the system will be so much easier for the attacker. Certain rules or programs could be used to create a password that should be strong enough.

Nowadays, OS Linux isn´t as widespread as competing OS Windows, that is why, Linux is still safer. However, if Linux catch on more among users, its safety could be threatened.

SEZNAM POUŽITÉ LITERATURY

[1] LUDVÍK, Miroslav a Bohumír ŠTĚDROŇ. Teorie bezpečnosti počítačových sítí. Kralice na Hané: Computer Media, 2008. ISBN 978-80-86686-35-6.

[2] VÍTEK, Miloš a Marcela VÍTKOVÁ. Sociální vědy a inženýrství. Vyd. 1. Hradec Králové: Gaudeamus, 2004, 164 s. ISBN 80-704-1474-X.

[3] TOXEN, Bob. Bezpečnost v Linuxu: Prevence a odvrácení napadení systému. Vydání první. Brno: ComputerPress, 2003. ISBN 80-7226-716-7.

[4] HONTANÓN, J. Ramón a Ludvík ROUBÍČEK. Linux: Praktická bezpečnost. Vydání první. Brno: GradaPublishing a.s., 2003. ISBN 80-247-0652-0.

[5] KRČMÁŘ Petr. Linux: Tipy a triky pro bezpečnost. Praha: GradaPublishing a.s., 2004. ISBN 80-247-0812-4.

[6] Sedláme Linux. KYSELA, Martin. Živě [online]. 18.7.2003. 2003 [cit. 2013-04-03]. Dostupné z: http://www.zive.cz/clanky/sedlame-linux-5-dil-uzivatele-a-skupiny/sc-3-a-112712/default.aspx

[7] O Linuxu: Co je Linux. REDAKCE MAGAZÍNU LINUXEXPRES. Linuxexpres [online]. 17.8.2006. 2006 [cit. 2013-04-03]. Dostupné z: http://www.linuxexpres.cz/o-linuxu

[8] Linuxsoft: Linuxová bezpečnost z pohledu uživatele. . Linuxsoft [online]. 27.4.2004. 2004 [cit. 2013-04-03]. Dostupné z: http://www.linuxsoft.cz/article.php?id_article=115

[9] Root: Bude váš Linux potřebovat antivirus?. BEDNÁŘ, Vojtěch. Root [online]. 14.11.2005. 2005 [cit. 2013-04-04]. Dostupné z: http://www.root.cz/clanky/bude-vas-linux-potrebovat-antivirus/

[10] Wiki.ubuntu. RYŠÁN, Mirek. Wiki.ubuntu [online]. 30.9.2012. 2012 [cit. 2013-04-04]. Dostupné z: http://wiki.ubuntu.cz/antivirus

[11] Thegeekstuff: Top 5 best Linux firewalls. NATARAJAN, Remesh. Thegeekstuff [online]. 15.2.2010. 2010 [cit. 2013-04-05]. Dostupné z: http://www.thegeekstuff.com/2010/02/top-5-best-linux-firewalls/

[12] GNU General Public License. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): WikimediaFoundation, 2001-, 2.4.2013 [cit. 2013-04-05]. Dostupné z: http://cs.wikipedia.org/wiki/GNU_General_Public_License#Verze_2

[13] Linuxexpres: Co je Linux?. REDAKCE MAGAZÍNU LINUXEXPRES. Linuxexpres [online]. 17.8.2006. 2006 [cit. 2013-04-05]. Dostupné z: http://www.linuxexpres.cz/co-je-linux

[14] Live CD. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): WikimediaFoundation, 2001-, 9.3.2013 [cit. 2013-04-05]. Dostupné z: http://cs.wikipedia.org/wiki/Live_CD#Linux

[15] Linux. In: Wikipedia: the free encyclopedia [online]. San Francisco (CA): WikimediaFoundation, 2001-, 4.4.2013 [cit. 2013-04-05]. Dostupné z: http://cs.wikipedia.org/wiki/Linux

[16] Poznejlinux: Nejpoužívanější Linuxové distribuce. DOČEKAL, Michal. Poznejlinux [online]. 2010, 10.9.2010 [cit. 2013-04-05]. Dostupné z: http://www.poznejlinux.cz/svet/distribuce/start

[17] Svethardware: Bezpečnost: Linux vs Windows. ČERNÝ, Jiří. Svethardware [online]. 10.2.2009. 2009 [cit. 2013-04-05]. Dostupné z: http://www.svethardware.cz/bezpecnost-windows-vs-linux/25687

[18] Linux z blízka: Největší výhody Linuxu. In: Zive: Linux z blízka [online]. 2010 [cit. 2013-04-05]. Dostupné z: http://linuxzblizka.blog.zive.cz/2010/01/nejvetsi-vyhody-linuxu/

[19] Linux z blízka: Největší nevýhody Linuxu. In: Zive: Linux z blízka [online]. 2010 [cit. 2013-04-05]. Dostupné z: http://linuxzblizka.blog.zive.cz/2010/01/nejvetsi-nevyhody-linuxu/

[20] Distrowatch: DistroWatchPage Hit Ranking [online]. 2001, 4.4.2013 [cit. 2013-04-05]. Dostupné z: http://distrowatch.com/dwres.php?resource=popularity

[21] Linux Mint: Documentation. Linux Mint [online]. 2006 [cit. 2013-05-15]. Dostupné z: http://www.linuxmint.com/documentation.php

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

GPLv2	General Public License verze 2
LGPL	Lesser General Public License
MPL	Mozzila Public License
BSD	Berkeley Software Distribution
UID	User Identifier
GID	Group Identifier
RAID	Redundant Array of Independent Disks
UPS	Uninterruptible Power Supply
CD	Compact Disk
DVD	Digital Video Disc
USB	Universal Serial Bus
ZIP	Souborový formát pro kompresi
TCP/IP	Transmission Control Protocol/Internet Protocol
ECC	Error Check-king and Correction
MB	Megabajt
GB	Gigabajt
RAM	Random Access Memory
CPU	Central Processing Unit
ICMP	Internet Control Message Protocol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA I: POROVNÁNÍ LINUX VS WINDOWS

	Linux	Windows
Cena	Většina Linuxových variant (distribucí) je k dispozici zdarma nebo za mnohem nižší cenu než u Windows	OS od firmy Microsoft Windows se pohybují cenově mezi 1499 - 6500 Kč.
Snadnost ovládání	Linux je stále pro uživatele obtížněji ovladatelný než Windows. (ale každým rokem se zlepšuje)	Snažší, jednoduché používání systému pro nové uživatele.
Spolehlivost	Většina Linuxových distribucí a verzí je notoricky spolehlivých. Mohou běžet měsíce i roky bez nutnosti restartu.	Přestože M. Windows učinil oproti minulým verzím systému jistá vylepšení, stále nemůže konkurovat spolehlivosti Linuxu.
Software	Linux má velké množství dostupných SW programů, utilit a her. Nicméně Windows má mnohem větší výběr Sw.	Vzhledem k velkému množství uživatelů M. Windows, má mnohem větší dostupnost SW programů, utilit a her.
Software Náklady	Mnohé z dostupných SW programů, her jsou na Linuxu freeware nebo open source. (Gimp, OpenOffice, Wine)	Většina SW programů, utilit a her se musí platit.
Hardware	V dnešní době je HW podpora Linuxu dobrá, ovšem někteří výrobci stále nenabízejí ovladače nebo podporu HW pro Linux	Vzhledem k velkému množství uživatelů má M. Windows mnohem větší podporu HW zařízení a ovladačů

Zabezpečení	Linux je velmi bezpeční OS. V porovnání s Windows je mnohem bezpečnější.	Přestože Microsoft učinil velké zlepšení v průběhu let z hlediska bezpečnosti, stále je nejzranitelnější vůči virům a jiným útokům
Open Source	Mnoho z Linuxových variant (distribucí), programů je open source. Umožňují uživatelům přizpůsobit si kód.	Microsoft Windows ani většina programů není open source.
Podpora	Linux má velké množství dostupných on-line dokumentací, knih. (Možná je obtížnější je najít - oproti Windows)	Microsoft obsahuje vlastní nápovědu a má velké množství on-line dokumentací, knih, na každou verzi OS.

Tabulka 3 – Porovnání Linux vs Windows